Assessing countermeasures against spyware

Terje Mjømen

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2005

The MSc programme in Information Security
is run in cooperation with the Royal Institute
of Technology (KTH) in Stockholm.

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Assessing countermeasures against spyware

Terje Mjømen
NISlab, Gjøvik University College
terje@mjomen.com

Abstract. *Spyware are increasingly growing to become a serious security problem in today's networked society and several web sites state their worries about this development. The varied nature of spyware causes confusion about the security issues this software represents. The use of spyware is very well capable of committing identity theft by stealing personal information that the web users work at, or is being transmitted through the Internet. As a result of this threat, commercial and free tools have emerged, and we present a method that uses specific metrics to assess and evaluate the effectiveness and usability of various countermeasures, making it possible to assess new countermeasures as they are developed.*

Key words: Information security, security metrics, spyware, identity theft, assessment.

Sammendrag

Andelen av personlig informasjon som er i omløp og er tilgjengelig for uvedkommende er antatt å være omfattende, og spyware er bare en av mange mulige metoder for å gjennomføre et identitetstyveri. Utbredelsen av slike programmer ser ut til å stige uforminsket også i fremtiden, så det er nødvendig å oppnå en forståelse av problemet og omfanget i den hensikt å i det hele tatt kunne begrense konsekvensene. Med å utvikle metrikker som spesifikt tar for seg måling av mottiltak til spyware kan en få en generell metode som fastsetter dyktigheten til flere ulike typer av forsvar mot spyware, ikke bare "spyware removal tools". Det at en har en generell målemetode som dekker flere måleaspekter gjør at en kan sammenligne helt ulike måter å forsvare et system mot spyware på. Det er ikke til forfatterens forståelse at en slik sammenligning av ulike mottiltak er blitt gjennomført tidligere.

Table of contents

List of tables

List of figures

Preface

The MSc thesis is the final project of the Masters course in Information Security at Gjøvik University College (Høyskolen i Gjøvik), Norway, and is due 1 st of July 2005.

For me the master course is a 2 year extension on top of my Bachelor in Engineering degree, a 3 year higher engineering education combining technical and theoretical knowledge with practical skills within computer system management. The final thesis at the Bachelor course was within information security field, and therefore it seemed quite natural to extend my insight into this field.

Spyware was, and still are an increasing problem, almost terrorizing the web users every day. The propagation of such software has resulted in speculations of the Internet's future, whether it may survive the extra traffic, the distrust to sites and applications, and the fear of identity theft and economical consequences of purchasing anything online. The importance of this topic was a motive power for completing the thesis, and I soon experienced the rapid changes within this field.

I've noticed that several companies reported that they sued or brought an action against researchers that claim that their software is spyware. I have chosen to present a definition of spyware, and some characteristics of spyware, and use the definition accompanied with other resources that confirm that the software is in fact spyware. As mentioned later there are a lot of different definitions of spyware, or a lack of a general definition of such, and therefore this may be in confrontation with various companies' own definitions of spyware.

Terje Mjømen, 2005.

1 Introduction

A disturbing trend has been the increasing number of cases of identity theft, in which criminals gain access to identifying information about a person for the intent to pass oneself off as that person. Financial gain is one of the most common motives when an identity theft is performed [59]. For example, credit cards may be used under an assumed name, or other's credit card information may be used for buying properties. Spyware may very likely be a tool for performing such crimes [33]. More often, spyware are used as information gathering tools for profiling the market, optimizing an advertising campaign, and some spyware are even designed to disable competitive spyware on a victim's computer to gain more market possession [49]. The distribution and value of spyware has grown into a huge billion dollar market [62]. Spyware do in high degree affect the confidentiality of private information stored or processed on a computer. A user's privacy will not be kept safely and an adversary may take advantage of the collected information.

A survey conducted by the norwegian Statistisk Sentralbyrå [34] in 2003 regarding the use of Information and Communication Technology within private households (households that had computers connected to Internet during this period) revealed that 4% had experienced a misuse of private information of some kind, and 2% experienced "dishonest use of credit cards" within the last 12 months. Federal Trade Commission estimates in a survey [1], conducted in 2003, that 4.6% of the inhabitants in USA were victims of identity theft in some form within the last year, thereof 3% reported misuse of Internet accounts. Numbers calculated by Earthlink (a major American Internet Service Provider) estimates that there is an average of 26 instances of spyware per scanned PC [35]. The numbers listed above confirm that spyware has become a very real and severe threat in today's society. An article [24] tells us that users are avoiding purchasing online because of the threats it implies.

An update to Federal Trade Commission's survey, released by Better Business Bureau [36] in 2005, shows that around 5% of identity theft origins from spyware and 11.6% in total through computer crime, though the numbers are based on "victims that know the identity and method used by the criminal". We may question the value of such numbers, while it is quite easy to discover that one's wallet is missing, it is not that easy to detect the previous activity on one's computer, certainly not if one is not familiar and aware of the online threats.

Many tools have been presented as spyware countermeasures. Not all of them perform satisfactory. A general method that assesses the countermeasures would ease the comparisons of the countermeasures, making it fast and reliable for each time a comparison is needed, which we intend to design in this thesis.

Spyware is defined as software that gets installed on a user's computer without the user's consent or awareness, and transmits personal information or non-personal information to a recipient, without concern to the intentions of the collection process [5,8]. Further, "unawareness" is meant that a user would not install the software under normal circumstances and fully enlightened software intentions.

The intentions may be hidden in the EULAs[1], the privacy statement or even not told at all. Some software even collects more information than it is stated [7]. It seems to be no general agreement on what constitutes spyware; like spyware is a sub-set of adware, or the opposite, and is spyware a sub-set of virus? Several authors do mix

[1] End-User License Agreement

these terms, with the confusion that entails. Definitions and studies of how the distribution of spyware is performed, mostly peer-to-peer file sharing software [5], and how they infect computers are given by several other authors [3], [5] and [7].

The rapid changing of attack methods and techniques, distribution methods and how they collect and transmit information makes it difficult to keep up to date within this field. Scientific reports and documents may not be valid or have scientific interest in the long run, or may not be complete, since the nature of malware varies and evolves at such high speed.

1.1 Topic

This project works around leakage of personal information on the Internet that may be used to commit identity theft and assessment of countermeasures to this leakage. The focus of this thesis is on spyware, countermeasures to spyware, and methods of assessing the various countermeasures. Users that uncritically use Internet may soon experience that spyware are directed at them in the purpose of deriving personal information.

1.2 Research problem

Spyware have the potential to collect and retrieve personal information that is being stored at a hard drive. Spyware may even collect such information live, and transmit the information to a receiving server on the outside of the user's perimeter. The transmitting maybe hidden or obfuscated in such a way that the users are unaware of the processes that are ongoing in the background, and the users most often do not know the extent or the threat of these processes, which may vary from innocent user statistics, marketing/profiling to the more severe identity theft. The Internet has become a vital part of today's society, and these illegitimate processes are just not acceptable in order to preserve Internet's integrity and users' trust.

1.3 Motivation and justification

Identity theft may potentially cause huge problems for the victims, mainly economical problems. We assume that most spyware do not collect information in purpose of committing identity theft, but the possibilities of such are still present. Many studies on spyware have been carried out so far, but most of them focus on distribution and how the traffic generated from spyware affects the bandwidth in networks. There are also many tests of spyware removal tools, done by commercial web sites or alike, and almost none of these have been approved or reviewed by serious researchers within this field. A general method that assesses spyware countermeasures may ease the comparison of countermeasures of the same kind and countermeasures of different kind.

1.4 Research questions

The following research questions are defined:

1. How can effectiveness of countermeasures be assessed?

2. How effective are the countermeasures?

This project focuses on assessing the effectiveness of countermeasures, and defines a method that is adjusted to measure such effectiveness.

1.5 Choice of methods

Creswell [6] claims that a quantitative approach is suitable for developing knowledge, employing strategies of inquiry such as experiments and surveys, and collecting data on predetermined instruments that yield statistical data.

A quantitative approach is systematic and well defined. It seeks to develop relevant true statements which explain causal relationships. The information will be formatted into numeric values. We derive our results from a relatively small amount of spyware components, through experiments. This fits the definition of a quantitative approach described in [6].

At this point, we do not know what kind of results or numbers a spyware experiment will reveal, or how we may best perform experiments on spyware programs. Creswell points out that qualitative research takes place in the natural setting. As we have to distinguish between the various categories of spyware components and their impact on a computer, we have to derive numerical representations of these severities. This conversion implies that we have to choose a qualitative approach when assessing the spyware countermeasures. Creswell states further; “qualitative research is exploratory and is useful when the researcher does not know the important variables to examine.”

A literature study of others attempt to assess effectiveness of similar countermeasures will be performed. Literature study will also assist the spyware category definition and defining the spyware category values. One must define methods that cover the different categories of efforts, and evaluate reliability and validity of possible experiments.

- A well defined method may cover all important aspects of the task.
- If the reliability and validity of the method is acceptable, using the method on experiments will give results that represent the truevalues.

The assessment will be completed by performing experiments, using the defined methods on various countermeasures to achieve a score.

- The methods will give us a numeric value of the effectiveness of different countermeasures.
- A metric where the validity and reliability is acceptable will produce results that represent the true value of the effectiveness.

A mixed research approach [6] combines qualitative methods and quantitative methods of collecting data.

2 Background

2.1 Classifying Spyware

Spyware appear in many different kinds [8][2]. The phenomenon is as new as computer programming, and there is no precise definition of spyware.

Currently it seems to be no general agreement of what constitutes spyware [64]. For instance, some authors include trojans in the spyware definition, and others do not. Erbschloe [14] distinguishes trojans, spyware, adware and stealware, but notifies that the terms spyware, stealware, and adware are sometimes used to describe the same or similar types of malicious code. Erbschloe emphasises the accessibility to system files and remote controlling of the victim's computer to be distinctive characteristics of trojans or similar backdoor programs. [14] calims that adware are used by larger web sites to collect information about the sites the Internet users visit and what they do at those web sites, and usually post a privacy policy to convince the user that their privacy are protected. Some websites may request information from visitors in exchange of custom or personal pages or specialized sales approaches, where this information are being transmitted by the use of cookies. Further, [14] describes spyware as "any computer technology that gathers information about a person or organization *without their knowledge* or consent." Erbschloe clearly points out that a program that collects and transmits information about users without first notifying them is defined as spyware. A paper [64] from a workshop on spyware confirms the statements of [14] and defines spyware as software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge. [64] also discussed whether or not software should do harm if it ought to be labelled as spyware.

Stealware are defined as various types of affiliate marketing programs, i.e. rerouting users' traffic to specified servers. Other authors, like [8], define several of the categories defined by Erbschloe as a subset of spyware (e.g. adware is a subset of spyware).

The non-profit web site Consumer Webwatch [37] defines spyware into 5 different categories, while [8] defines spyware into 7 categories. The classification mentioned in [8] is also used in [3] but the terminology origins from SpyBot S&D [15], a free spyware removal tool. Their decision to embed "malware" into the spyware category may be questionable, though they comment the fact that spyware is one form of malware. The earlier mentioned company Earthlink separates adware, adware cookies and system monitors, where system monitors constitute applications that may spy on somebody by capturing virtually everything he or she does on the computer. The web site Toptenreviews.com [38] names the detection capabilities of tested spyware removal tools, and several of these categories overlap with other's definitions of what constitutes spyware. For instance, they define detection of spyware as one capability while they later on define the capability to detect keyloggers, browser hijackers and

[2] Note: [8] refers to Earthlink's data and implies that the numbers indicate that there are (at that date) 12.1 million *different* spyware types around the Internet, which is not true; the numbers show that there were 12.1 million *instances* of spyware found by Webroot's and Earthlink's Spy Audit programs, where one kind of spyware is likely to appear several times.

tracking cookies. When these terms are put alongside the spyware term, the terms are not within the definition of spyware.

Table 1 presents an overview of different authors' attempts to categorize spyware.

Table 1. Spyware categories

Author	Ranking	Category
Boldt et al. [8]	Impact	Cookies and web bugs Adware Tracks Browser hijackers Spybots System monitors Malware
Consumer Webwatch [37]	Behavior	Adware networks Stalking-horses Trojan-horses Backdoor santas High risk programs
TopTenReviews.com [38]	Not defined	Adware Spyware Keyloggers Trojans ActiveX configuration Scumware Dialers Malware Data mining Parasites Toolbars Drive-by downloads Tracking cookies Spyware registry keys Browser Hijackers/BHO's
Earthlink	Not defined	System monitors Trojan horses Adware Adware cookies
Other		Tricklers Pop-ups/Pop-under

Here we briefly present definitions of basic concepts used in [8]:
Cookies: Cookies are a text file stoen on clients' computers on behalf of the servers. The cookie represents a state of communication or previous communications on a web site. Cookies are a passive form of spyware and can only be retrieved by the web site that initially stored them.
Adware: Adware displays advertisements tuned to the user's current activity. We notice that [8] defines adware as a subset of spyware.
Tracks: Tracks collect information recorded by an operating system or application about actions that the user has performed.
Browser hijackers: Browser hijackers configure the users' Internet browser settings, may bevisible or hidden.
Spybots: Spybots monitor the user's behavior, collect logs of activity and transmit them to third parties.
System monitors: System monitors monitor various actions on computer systems, e.g. key logging.

Malware: Malware are a set of instructions that run on a computer and make the system do something that an attacker wants it to do.

Malware are more common referred to a term that covers most of the unwanted software or code on a coputer [23], including trojans, virus, and spyware.

Consumer Webwatch [37] has defined their categories as follows:
Adware networks: Embedded as advertisement in software, logging user behavior for marketing purposes.
Stalking-horses: Programs that enable the adware networks to function on desktops. All collect some sort of information.
Trojan-horses: Usually come with the ad-serving networks' basic software and at least one stalking horse.
Backdoor-santas: Programs that incorporate similar approaches but have no links to adware networks. Nonetheless they collect information from users.
High risk programs: Programs that pose security risks, execute elaborate stealth routines on PCs with no disclosure whatsoever or are just difficult for even experts to remove.

The vague definitions by [37] do not conform to the general view of what constitutes spyware. Backdoor-santas, Trojan-horses, and Stalking-horses would be more likely to include into a malware category. The definitions may be written in the understanding that spyware are programs that may give an intruder capabilities to access and control another's computer.

The definitions used by TopTenReviews are not all spyware categories; Trojans and scumware are most often referred to as malware, but not spyware. Data mining are a method of collecting information or patterns across e.g. databases for profiling a person. The categorization done by Earthlink is somewhat the same as [8], but includes Trojans as spyware and refers to spying software as belonging to system monitors, leaving out browser hijackers.

[68] defines spyware as programs that monitor the computer's usage and sends the information back to a receiving server. It may also display advertisements that are dependent on the usage of the computer. Further, the spyware do not enlighten the user about the information gathering and transmission of the information. At last, spyware have no uninstaller. [68] does not include programs that are designed to diagnose or resolve technical difficulties, software that report to an Internet web site about information stored on a user's computer, such as cookies, hmtl-code or java scripts, and does not include operating systems.

A study group [21] worked out a report about malware in 2000. First, they explain how to install malware; java attack applets (embedded in web pages), ActiveX controls (allow a fragment of code to control applications or OS), attack scripts and exploitation of security weaknesses in applications (Buffer overflow –Smashing the stack[3] and memory leaks, poor data validation and conflicting libraries). The term "spyware" is not mentioned at all, which indicates that this work is not complete.

As [4] points out, spyware are program components that gather information without users' awareness. Several known vendors have built a spyware acceptance within the EULA, and therefore such programs that gather e.g. browser history would be classified as adware. On the other hand, these EULAs are written in a very confusing or deceptive manner, and in many cases the end-user will be unaware of the unwanted

[3] Aleph One; Smashing the stack for fun and profit, originally published at www.phrack.org 1996

background processes. One may therefore question the "user awareness" in these situations, and either defines such programs as spyware or legal software. Even though the information gathering is stated in the EULA, there are several instances of information gathering that exceed the statement in the EULA [8].

[25] includes the intention of profiling and marketing purposes of spyware, and the information collected by spyware may be resold to other agencies. [25] does not extract adware as its own term, and defines web-bugs as a "1x1-pixel" on a web site that has capabilities to track users. Erbschloe claims in [14] that cookies are sometimes called web bugs; this seems not to be the case. Java-scripts are formally standardized as ECMA scripts, and are the cause of pop-ups (which it is claimed to avoid by removing the "new window"-command in the code).

Spyware writers may use certain method to install the spyware used as known in the spyware Trickler, a variant of Gator [39]. The Trickler spyware install first a small piece of code before it installs itself by downloading small pieces of the client over a period of time and gathers itself into a complete client. Other methods of installing spyware, or more correctly ensuring it to reside on victim's computer are to ensure that different spyware components are present at any time. The components are likely to reside at different locations on a computer, and each component checks if the other components are present. If they are not, then it replicates itself to replace the missing component and to ensure the spyware existence.

Spyware attacks are also defined as part of a more general classification of attacks against computer systems. A suggestion of such classification scheme is given in [2], where the classification is dependent on the location, cause and impact. It is assumed that spyware attacks spread out and belong to several categories as defined in [2] because of their varied nature of attack methods.

[17] treats malware as a whole, and defines malware, or non-viral malware as stealth programs that capture passwords or other sensitive data. [20] claims that malicious code infiltrates a host by exploiting known software flaws, hidden functionality in regular programs, and social engineering. The social engineering part is based on making the users install the harmful software by confusing them in form of bad EULAs or ambiguous statements when prompted for installing ActiveX components.

Spyware may also be classified regarding how it integrates itself into a computer. Spyware may integrate into the Operating System or other applications [22] and take advantage of Autostart Integration Points and get executed whenever the computer reboots or starts up. Spyware may even appear as a stand alone application and use the auto-start procedures, leaving a reference in the "run"-location in Windows Registry. Spyware may also appear as executions or plug-ins to existing applications that are automatically started (e.g. winlogon.exe). The operation mode of spyware may also include changing computer settings, like Internet Explorer security zones, certificates and windows host-file.

Malware is usually classified according to its propagation method and goal [12]. Viruses, worms, Trojan horses, backdoor programs and spyware have all different propagation patterns and/or intents.

2.2 Information being transmitted

Edelman [4] carries out an experiment, in which he takes a closer look at 2 pieces of spyware; WhenU and Gator. He claims that WhenU transmits information about users' web browsing patterns, location, IP-address and information of how and when

WhenU got installed. Edelman claims further that newer versions of Gator transmit information hidden in other legitimate traffic, or by use of encryption, but anyway the connections between the victims' client and external servers were present. Gribble et al. [3] investigate the distribution of spyware in a university network environment. This exploration claims that the spyware program Cydoor does not encrypt information that is being transmitted between a client and a server, but uses some form of obfuscation to make it more difficult for the user to be aware of these background processes. This claim is based upon what it is possible to retrieve from the http-headers of the packets. The experiment in [3] focuses on the distribution of spyware and does not prioritize the traffic analysis, and assumptions are made about the operation modes of spyware. The experiments performed in [3] stand in opposition to what [4] claims regarding to what traffic WhenU generates.

Jacobsson et al. [5] could only prove 2 pieces of spyware to be present in the same file sharing applications that [8] investigated. Table 2 presents an overview of the traffic certain spyware programs generate.

Table 2. Spyware traffic

Author	Spyware	Information	Transmitting
Edelman	WhenU	IP-address, location, browser-history, how it got installed	Clear text
Edelman	Gator	Browser-history, location, IP-address, uniqueID*	Newer version uses obfuscation or encryption
Gribble et al.	Cydoor	Possibly personal information	Possibly hidden or encrypted
Gribble et al.	SaveNow**	Keywords	Parameters
Jacobsson et al.	StopAtHomeSelect	Browser –history	Not stated
Jacobsson et al.	SaveNow	Internet history scores, user information	Not stated

* Unique ID assigned from Gator, ** SaveNow transmits information to WhenU-servers [40].

[8] conduct their experiments on a "clean" computer, and test the spyware that is bundled with 5 file sharing applications, namely the free versions of Bearshare, iMesh, Kazaa, Limewire and Morpheus, all downloaded 30.june 2004.

The experiments referred to above present the most likely and assumed methods of transmitting information; through the http protocol. What about the information that does not get transmitted through the port 80, but uses other protocols or side/covert channels? Is it possible to estimate the contents of such traffic? The experiments conducted in [3], [4] and [8] investigate only a few pieces of spyware which one cannot make any generalizations of. Further work on this topic is preferred and needed, which [5] comments in the summary.

Traffic that uses covert channels when transmitting information is not easily detectable. A covert channel is described as "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy." [66]. Information can be concealed and transmitted by using certain fields in IP header and TCP header [67]. The traffic may also be hidden in other ways,

like routing it to external servers or proxies for traffic monitoring. This means that even though no personal information is being sent in the data field of packets, information can be transmitted in other ways.

Earthlink claims that user information is gathered and stored on user's computer for later retrieval [35]. The information is stored in an encrypted log file, and may even be transmitted through email to other locations.

2.3 Categories of spyware

As mentioned above, it seems to be no general agreement on what constitutes spyware, or whether adware is a sub-set of spyware and whether a virus is a worm. Still, it is essential [41] to define spyware and malware in order to ensure that we are discussing the same threat, and are able to provide a specific and detailed diagnostic of a problem or a threat. The need for a more specific definition of malware is also commented in [17], while [20] claims that there is a lack of methods for evaluating malware detectors.

A definition of spyware will never be totally complete due to new versions of spyware with new attributes that will not fit into one precise category. There are many hybrid-versions of spyware, which may fit into several categories. But still it is important to avoid making up new names and categories for each new hybrid. New names and definitions may cause more harm than good. For instance, a virus may not be universally defined, but it is universally known, and in many cases that is good enough.

The classification should be developed in such a way that hybrid versions do not bypass so many definitions, and if a piece of spyware fits into several categories it should be listed within each one of them. In this way, any author may not need to come up with new names or other definitions of existing ones.

Boldt et al. [8] describe a model (Table 3), which specifies in what ways "*spyware might decrease the utility of belonging to a large virtual network*". The model shows that spyware intrude a user's privacy and affects systems and networks. Due to the incomplete classification of privacy breaches, the model is not appropriate to be used in a more thorough analysis of effect of spyware on privacy.

Table 3. Spyware effects

	User	**Computer**	**Network**
Moderate	Commercially salable data	Consumption of capacity	Consumption of bandwidth
Severe	Personal data	Inferior code dissemination	Malware distribution
Disastrous	Critical data	Takeover	Breakdown

By summarizing the above we present the main spyware categories in Table 4. As mentioned before spyware are programs that transmit user information, like Browsing history (URLs), IP-addresses, system information, Operating System and CPU information to a server outside the user's perimeter. The spyware is transmitting information *without a user's consent or awareness*, though the collecting process may be stated in a loose or misleading privacy statement. The term "aware" is not easily defined; the EULAs and ActiveX components may be deceptive and confusing.

Further, a spyware program may vary from "harmless" tracking cookies to more severe information gathering programs as trackware and keyloggers.

Table 4. Main categories of spyware

Category	Description
Adware	Showing advertisement through so-called pop-ups on a user's computer may transmit browser history and user habits. Intends to increase marketing revenue by profiling users and customizing/specializing advertisement to each user [5]. Adware is sometimes considered to be violating the privacy while gathering the personal information from the computer [5]. There are different degrees of potential security threats it represents. For example, an auto-updater will potentially cause vital damage on a computer or leakage of personal information if the adserver is hacked and loaded harmful code into.
Tracking cookie	A Tracking cookie is a small text-file stored at a client's computer to track user browsing and/or gathering/sharing information across multiple web sites. Each user/cookie is assigned a unique user ID.
BHO	A Browser Helper Object is an extension to the web browser, and starts every time one starts the browser. A malicious extension / plug-in may monitor messages and actions, detect events and change the browser's default home page. It is difficult for a firewall to detect such traffic since it is an extension to the browser. The firewall cannot distinguish traffic that origins from the same component [5]. Transponder [48] is a well known piece of spyware of this kind.
Hijacker	A Hijacker may install itself in a stealth manner (through exploits), and changes settings without informing or asking for permission. It also changes the browser settings to point to another site, potentially capturing information and addresses on the way [5]. But mostly they are just annoying. A Hijacker can restore itself after a user has customized the browser settings, or make itself "impossible" to edit. There may be references to themselves in the Startup or in the Registry.
LSP[4]	The malicious software may integrate itself with the Layered Service Provider, which makes it able to spy on habits and data of the user. The LSP resides within the TCP/IP layer, which means it can access all TCP/IP traffic. Special precautions must be taken when removing these kinds of software. If it is simply removed, the network possibilities may be lost.
Trackware	Trackware employs an Internet connection in the background and transmit information like behavior, e-mail addresses, IP-addresses and system information without consent. Trackware is sometimes referred to as spybots.
Keylogger	A keylogger works as a background process and records all keystrokes on the computer. In terms of spyware, a keylogger is mainly used to obtain passwords and other highly sensitive information, like credit card information. The Keylogger may store the recorded information locally or transmit it to a receiving server.

[4] More on LSP:
http://research.pestpatrol.com/HowTo/How_To_Restore_Your_Internet_Connection.asp

Spyware may infect a computer in many ways, depending on their nature. The main spyware installation methods are given in Table 5.

Table 5. Spyware installation methods

Method	Description
Bundle	Spyware is sometimes embedded in other software (like dynamic link libraries), and the application may not operate without the spyware, or they may be in separate executive files. Spyware are common to come along with file sharing applications, and are sometimes not disclosed at all. Bundling is sometimes referred to as piggybacking [23].
Exploit	An exploit is a way of breaking into a system using buffer overflow, directoryclimbing, defaults and DoS[5] etc. It basically takes advantage of poorly written applications and overrides the security measures [23].
Drive-by downloads	A visit to web sites or viewing html e-mail messages may cause an automatic download and installation of a program to the computer, all without the user's consent or awareness. ActiveX is an applet-like application that gives the user an opportunity to interact with distribution of application from web sites. Spyware writers make thesecomplex, or find ways to install spyware even if the user chooses not to install this questionable software. If the security settings are set to low, the spyware may get auto-installed without notifying the user.
Scripts	Java scripts may get installed through a browser, and are primary components of dynamic Hypertext Markup Language (DHTML) and a core feature of every web browser in use today. VBScripts are the visual basic counterpart of JavaScripts.
One spyware installs another	The spyware installs itself by first injecting a small piece of code on a computer, and then it completes the isntallation by downloading small pieces of the client over days and gathers itself into a client. The download distribution makes the spyware hard to detect.

Spyware may affect the user in several ways. Some categories are commented in [7, 28, 29] and summarized in [8]:

- **Consumption of system capacity.** Affecting system performance when loading and executing spyware.
- **Consumption of bandwidth.** Generated traffic from spyware and adware (ads and pop-ups) affects the bandwidth, especially in networks where the traffic is accumulated into few nodes.
- **Security issues.** One cannot be sure of the traffic that is being transmitted, and some spyware may include weaknesses and expose the system to further attacks.
- **Privacy issues.** Personal information is being gathered and transmitted to third parties.

[5] DoS: Denial of Service

There are several ways to categorize spyware attacks. We prefer treating the privacy issues of spyware, and thus we divide the attacks into 4 distinctive characteristics; how the spyware are distributed or installed, how the spyware behaves, how it affects the security and privacy.

Drive-by downloads are defined as downloads that are transparent to users while surfing web sites. Downloading of ActiveX components qualifies as transparent download if the policy in the browser is set to low or configured to accept ActiveX components without prompting the users.

Scripts may be used as tools for installing spyware when users visit web pages. A notification may appear when 3rd party software tries to infect the computer. If no notifications appear, the installation would be classified as a Drive-by download.

A user may interact with the distribution of spyware. For instance, the user may choose not to install any suspicious software, which bundles spyware. Further, there are pieces of spyware that override the denials of spyware installations or install spyware without any interaction from the user. A passive mode is defined as when a user is not blamable for the infections, like vulnerabilities in software. A process may be terminable and still it comes back the next time the computer is rebooted. An embedded piece of spyware may integrate itself with e.g. the Internet Explorer browser, and one cannot disable spyware without disabling the browser. Some pieces of spyware have entries to the "add/remove programs" in the "Control Panel" or they come with their own uninstaller. Either way this is represented as "uninstaller" in Table 6.

Table 6. Classification of spyware by distribution method

<table>
<tr><th colspan="4">Dirstribution</th></tr>
<tr><th>Mode</th><th>Distribution</th><th colspan="2">Installation</th><th>Removing</th></tr>
<tr><td rowspan="3">Active</td><td>Bundle</td><td rowspan="2">Interaction</td><td>Permission</td><td>Uninstaller</td></tr>
<tr><td>Scripts</td><td>Override permission</td><td>Terminable</td></tr>
<tr><td>Drive-by downloads</td><td colspan="2">No interaction</td><td>Embedded</td></tr>
<tr><td rowspan="2">Passive</td><td>Exploits</td><td colspan="2" rowspan="2">Hidden plug-ins</td><td rowspan="2">Reinstalls itself</td></tr>
<tr><td>One spyware installs another</td></tr>
</table>

Table 7. Classification of spyware by behavior

Behavior		
Component	**Terminable**	**Behavior**
Process	Terminate	Redirection
		Web browser configuration
	Auto restart	Modifying content
Non-process		Toolbar/BHO
	Auto restore	Modifying host-file
		Logging
	Embedded	Pop-up/pop-under

Table 7 shows a classification of spyware behaviour. A process may be terminable, or it may restart every time it is stopped, or it may start every time the computer is booted as a result of an automatic restoration of registry keys. The spyware may appear as visible or hidden and it may appear both on web or non-web interfaces, and be embedded into existing applications like Internet Explorer. Pop-ups may be pushed independent on the user's activity. Pop-under is quite the same as a pop-up, but instead of intercepting the user's web surfing it hides behind the already open window. In doing so the user will not be intercepted in his or her web surfing. Logging is referred to as the process of collecting e.g. browser history and/or transfering the log to an external server.

Table 8 presents a classification of spyware by security issues. Malware that modify security settings or blocking security or privacy software, like killing anti-virus applications are not defined as spyware, and therefore are left out from this classification. Malware that open a port for later connections are more suited being defined as Trojans or backdoors rather than spyware. But spyware may include such functionality and therefore represents a security threat of that kind. Spyware may also modify e.g. Internet Explorer policy to allow cookies to be transmitted or more severe; harmful or privacy invasive applications.

Table 8. Classification of spyware by security issues

Security		
Awareness	**Action**	**Entity**
Permission	Modify	OS security SW security
No permission	*Block*	*Software*
Hidden	Transfer	Encrypted/obfuscated
		Clear

The privacy statement may be presented in a EULA or in a privacy policy, or the information gathering is not stated at all. Different pieces of spyware may transmit different kinds of information such as IP-addresses, browser history, ZIP code or other information (Table 9). Online activity is separated from browser history for representing the keylogger threat.

Table 9. Classification of spyware by privacy issues

Privacy		
Method	**Stated privacy**	**Information**
LSP	EULA	Locations (city, state, ZIP code)
Tracking cookie		
Trackware	Privacy policy	Browser history
Adware		
Keylogger	None	Online activity
BHO / Hijacker		Other personal identifiable information

2.4 Countermeasures

The author tempts to achieve an overview of countermeasures or barriers to spyware, where he in the first place has to work out an overview and categorization of spyware that make the countermeasures to be assessed.

One of the main issues for countering spyware is the detection of the malware. [12] describes a method to detect malicious patterns within program codes. The paper

focuses on methods to recognize obfuscation viruses, and the methods are not embedded in commercial products to be tested. When assessing patterns one avoids the problems during matching of an unknown code string to a database of spyware signatures. [17] claims that Anti-virus software cannot actually perform an analysis or matching on a new piece of malware (malware detection capabilities are integrated in some Anti-virus software).

The article [60] says that a signature based intrusion system will not protect a system against spyware. Spyware changes frequently, and pattern recognition is preferable. A program described in [13] is such an attempt to detect covert traffic.

Signature based detectors are further commented in the article [42]. It claims that "*the most popular detection and removal tools 'fail miserably' at addressing the growing spyware/malware scourge.*" The test revealed that the best performing anti-spyware scanner failed to detect about 25 % of the "critical" files and registry entries. The classic detection approach is effective when the code does not change significantly over time [12], which unfortunately one must say that spyware and malware do.

[3] points out in chapter 6 that the techniques developed for intrusion detection systems may be functional in detecting spyware attacks based on signatures derived for passively detecting spyware traffic.

The study group in [21] proposes 4 methods of defence against malware;

1. Analyse the code –and reject identified malware.
2. Rewrite before execution –insert extra code to perform dynamic checks.
3. Monitor the code while executing –and stop it before it does harm.
4. Audit code during execution –take action if some harm is done.

It seems that several of these countermeasures, like the ones mentioned above, would result in a cumulative high processing burden on any OS. The study group displays an overview of existing methods to defend oneself against malware in 2000, and refers to OS-based reference monitors and scanning for known malicious code. Address translation, timer interrupts, system calls for invoking a trusted software base are used in combination to enforce limited forms of availability, fault containment, and authorization properties in the OS-based reference monitors. Spyware target the common user that in average has an average CPU capacity in their computer, therof should the countemeasures not affect the total CPU load in a great amount. The study group shares the general agreement of the limitations of malware scanners, which only identifies known malware.

So called "anti spyware software" or "spyware removal tools" have become a business for a lot of enterprises. The web site www.download.com requires the distributors of software to explicitly inform users whether the software contains spyware or not, whether there are components that transmit information and what information is being transmitted.

There are possibilities that users' computers get infected with spyware when surfing suspicious web sites. To avoid this it may be worthwhile to anonymize the user, which is examined closer in [11]. There are products available, like Anonymizer 2004[6] and FindNot.com[7] that claim to anonymize the user on the Internet.

[6] http://www.anonymizer.com
[7] http://www.findnot.com/?1_surfing_anonymous

[12] and [16] enlighten that malware may use obfuscation to install itself on a computer by changing the sequence of the instructions; e.g. inserting "NOP"[8]-instructions in different places within the code which will change the signature for that specific code or program. [12] and [16] also point out that signature-matching is not the optimal way to prevent malware to get installed. Malware detectors, like Anti-virus software match the code sequence to a database of known signatures, which does not contain all variety of threats. Such detectors only identify known malware, and therefore they are not accurate enough. [12] proposes a heuristic method for looking for abnormal structures in certain program locations; e.g. the program starts with a "jump"-instruction.

Intrusion Detection Systems (IDS) may be used to detect illegitimate network traffic by identifying certain patterns [27]. Jha et al. introduce in [18] a statistical anomaly detection algorithm based on Markov Chains. Jha et al. point out that one of the disadvantages to anomaly detection is the false alarm rate, where signature based systems, like Snort have a lower rate of false alarms. IDSs may be installed as Host based (HIDS), Network based (NIDS), and they operate in real-time or non-real-time.

The detection of spyware relies on identifying harmful code sequences in executables or alike. [19] analyses the possibility to identify buffer overrun vulnerabilities by statically analyzing C source code. However, this method is not implemented in any commercial products as we know of.

Blocking of suspicious sites or blocking ActiveX install attempts from listed sites is one way of protecting systems. SpywareGuide.com [43] has developed a register file that blocks such attempts, though only operational with Internet Explorer. An ActiveX control contains a unique identifier for the Class Identifier (CLSID) [44]. The data value of the Compatibility Flags DWORDS is sometimes referred to as a "kill bit". If the CLSID for the ActiveX control is listed in a certain path in the registry, the ActiveX control will be blocked from operating on the computer, and thus the computer is protected against spyware programs that propagate through ActiveX controls.

In the flora of spyware, there are several kinds of countermeasures. We assume that one countermeasure is not enough to protect a system against spyware. Erbschloe [19] says that there is a variety of malicious code types, and in order to defend against attacks, organizations need to deploy multiple defensive methods to protect computers and networking devices [14].

It turns out that several methods and tools may affect the operation of various spyware programs. Some of the possible countermeasures against spyware are listed in Table 10.

[8] Note: NOP instruction: No-OPeration

Table 10. Proposed countermeasures against spyware

Countermeasure	Action	Approach
Disable Java	Block spyware installation	Preventive
Disable ActiveX	Block spyware installation	Preventive
IDS	Detect spyware	Proactive
Spyware removal tools	Detect & remove spyware	Proactive
Anti-virus software	Automatic scan downloads, detect & remove spyware	Preventive/proactive
Patch weaknesses in software / OS	Block spyware installation	Preventive
Block cookies	Avoid spyware	Preventive
Block known web sites	Avoid spyware	Preventive
Awareness	Avoid & detect spyware	Preventive/proactive
Personal firewall	Block connections	Preventive
Privacy policy settings	Block spyware installation	Preventive
Legislation	Reduce amount of spyware	Preventive

The Platform for Privacy Preferences (P3P) is developed by the World Wide Web Consortium (www.w3.org) and is more or less a standard that serves as an automated way for controlling our own personal information. The P3P is a set of standardized questions, and web sites present answers to these questions and are automatically loaded into the browser (check http headers for a P3P Compact Policy) for comparing the web site statements with a browser policy, like cookie handling in newer versions of Internet Explorer. A human readable version of the policy should also be present in a "Privacy Report" obtainable through the browser.

Howes [65] is skeptical about such P3P programs, i.e. the principle of "opt-out". That means that the web sites may collect and distribute personal identifiable information until the user tells the company otherwise. Further, Howes says that by using the slide bar in IE 6.0 "no normal user could reliably predict what cookies will be accepted or blocked at the various slider levels."

2.5 Personal information

We have carried out a simple experiment to determine what information spyware programs transmit back to external servers. It turned out that most of the traffic was encrypted or obfuscated.

Different "index.dat" files are located in the Windows OS, which are keeping track of cookies, and browser history, like typed URLs and such. The "open source" spyware [63] confirms that spyware looks for these specific paths and transmits information back to its origin, though the "KSpyware" is not tested by the author. By monitoring access to these files, and comparing this activity to network activity one may be able to define which processes transmit information that is stored in these files.

Spyware may hide their transmission of information and not have a static open connection to a server. Keyloggers may transmit information right away, or collect a greater portion if information before it is sent to an external server [57]. By monitoring active processes that are parallel to user activity, one may be able to identify the presence of such processes.

After installing the bundled spyware, the network traffic increased and connections to external servers appeared. When capturing packets on the network for 10 minutes, the

average bytes pr second before the infection was 115, and 220 after the infection. This may indicate usage of covert channels and embedding into legitimate processes or the difference could be simply a coincidence. This small test was not copmrehensiv enough to make any conclusions. While testing the amount of packets on the network, no other activities were performed, no web surfing and no applications other than monitors and OS were running.

When installing the spyware from Grokster there were connections to TopMoxie Inc. servers (64.62.182.4), several different ISPs, and connections to Joltid.net (80.160.91.3).

The traffic on the network seemed to be of mostly obfuscated or encrypted data. The Trickler (Gain/Gator/Claria) transmitted for instance the following:

- POST/gs_tricklerHTTP/1.1..Host: ts.gator.com..Content-type:application/x-www-form-urlencoded..Content-length:153..User-Agent: Gator/5.0..Cache-Control:no-cache..Accept:*/*..X-UA:CxSocket....TRICKLER4=START%05915DC827%2d06D1%2d4887%2dB525%2d66E020C58EB%05422217c5%0500006BA7%05422346C2%05BIC%5fGrokster%054%2e2%2e0%2e3%05%05SAR%5fOK%05NOPI%05&...

- HEAD /dc/download/g181511.exe HTTP/1.1..User-Agent: g181511..Host: content.delfinproject.com..Content-Length: 0..Cache-Control: no-cache...

Other data that was transmitted between the test computer and external servers were:

- GET /external/builds/pages/remv1150c.lsp HTTP/1.1..Accept:*/*..User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)..Host: www.topmoxie.com..Connection: Keep-Alive..Cache-Control: no-cache...

- POST /.pkt HTTP/1.1..Content-Type:application/x-www-form-urlencoded..Host: 80.160.91.3:35..Content-Length: 26..Cache-Control: no-cache.

- GET /external/builds/downloads2/merc1151.dat HTTP/1.1..Accept: */*..User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)..Host: www.topmoxie.com..Connection: Keep-Alive..Cache-Control: no-cache...

Some spyware triggers on specific keywords in the title field at the sites the user is visiting [58], like eBay, Bank, or Amazon. The rules and keywords may be stored in a local file. Since spyware may only trigger on specific keywords, one may not detect the spyware operations while being idle or visiting predefined web sites that do not match the keywords.

Edelman [58] explains the method of keyword triggering and refers to a configuration file in eXact Advertising software.

The SurfSideKick logged newly visited URLs into a log file, containing data in clear text and obfuscated/encrypted. An extraction of the log file looked like this;

- (http://ads.flashtrack.net/js/jsnew2.php?grp=600&
  ver=27&guid=C6F624E8-2D61-4BD5-B457-
  AE4A41BC5823&ft_id=37705&c=0&k=
  http://www.ebay.com/) Dict(C:\Documents and
  Settings\Terje Mjømen\Programdata\Sskcwrd.dll)
  invalid!
  (http://search.ebay.com/spyware
  Keyword(search.ebay.com, 1, 2)
  (https://scgi.ebay.com/ws/eBayISAPI.dll

The author was browsing eBay while the SurfSideKick was operating, and the eBay-entries were stored in clear text and easily readable. Clearly there is a connection between SurfSideKick and the IE browser.

As mentioned, some spyware programs have their own uninstaller or entry in the add/remove programs in control panel. Not all of these uninstallers do what one expects of an uninstaller. After removing the 3rd party entries listed in the ”add/remove programs” in Windows Control Panel Ad-Aware still detected several entries that originate from the claimed removed software; for instance the p2p networking.exe process was still running, so did cmesys.exe, btv.exe, wsxsvc.exe, vmss.exe, and gmt.exe. Registry entries like HKCR\CLSID\{...} and HKCR\{...} from Claria, FlashEnhancer, and SurfSideKick were present. Autorun entries related to CMESys, SurfSideKick, BTV, and WebRebates were also present in the registry. MySearchBar, which does not consist of any .exe files and has its own process was untouched by the add/remove operation.

We confirmed the “duplicate-mechanism” some of the spyware operates with. When we closed the “WebRebates0” process, it automatically restarted. The same thing happened with “WebCPR0”.

The spyware performed operations while the test computer was idle, and queried the “index.dat” file located in the “Temporary Internet Files” catalogue. The FilMon from Sysinternals.com reported these among other these operations;

- P2P Networking.exe

QUERY INFORMATION C:\Documents and
Settings\Terje Mjømen\Lokale innstillinger\Temporary
Internet Files\Content.IE5\index.dat

- GMT.exe

QUERY SECURITY
C:\Programfiler\Fellesfiler\GMT\ex56114l6z\gb\31058
BUFFER OVERFLOW
QUERY INFORMATION C:\Documents and
Settings\Terje Mjømen\Lokale innstillinger\Temporary
Internet Files\Content.IE5\index.dat

- CMESys.exe

QUERY INFORMATION C:\Documents and
Settings\Terje Mjømen\Lokale innstillinger\Temporary
Internet Files\Content.IE5\index.dat

The installed spyware made changes to the registry while being idle as well. Processes like P2p networking.exe, GMT.exe, WebRebates0.exe, CMEsys.exe, WebCPR.exe, wsxsvc.exe, iexplore.exe, and explorer.exe made continuously changes or queries to the registry.

Some of the most interesting operations were the operations made by WebRebates0.exe and WebCPR0.exe:

WebRebates0.exe
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WebRebates0
""C:\Programfiler\Web_Rebates\WebRebates0.exe""
CloseKey
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WebRebates0
""C:\Programfiler\Web_Rebates\WebRebates0.exe""
CloseKey
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

WebCpr0.exe
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WebCpr0 ""C:\Programfiler\Web_Cpr\WebCpr0.exe""
CloseKey
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

We notice that WebRebates0.exe and WebCPR0.exe set values in the \run-entry several times, overwriting existing ones if they already exist, or re-write the entries if they are missing making it useless to delete these run-entries because they will reappear in short time. The iexplore.exe and explorer.exe made queries to entries that pointed to toolbars in the registry (MyBar).

The installed keylogger had its own process. It was active as long as the author was logged on, and it was not visible without monitoring active processes. The information collected by the keylogger was stored locally, and sent via email to a receipent, conforming to the statements made in [35] and [64]. A keylogger does not need to be a separate process; it could very likely be embedded into the other spyware processes. The potential threat of a keylogger is extremely high. It has the capability of collecing and transmitting all entered usernames and passwords to external servers, credit card information and other non-sensitive information.

3 Previous work

1. Assessing effectiveness of countermeasures against spyware

TopTenReviews.com [38] compares different spyware-removal tools, evaluated by detection and removal capabilities, features and costs. The removal capability is defined through counting the amount of pieces of spyware detected on a system. This means that the removal-tool not necessarily detects all spyware that have infected the system.

Cookies can be assessed by analyzing the traffic that the cookies are generating and whether they transfer personal information in clear text. An option to this could be to evaluate to what extent sessionID can be spoofed. If cookies store personal information in clear text, even on the client computer, it would be a security issue. The author tested some file sharing applications and searched for cookie files and the folder "cookie". The result was quite interesting; the author got in hold of thousands of other users' cookies that were, presumably, unintentionally shared with the whole world.

A method to analyze malware is presented in [17] where a project is carried out in a laboratory setting that simulates Internet. By decompilation / reverse engineering and editing some of the code (the signature) they analyze the impact, and test the detection capabilities of various anti-virus software. As an introduction they comment that there exists no single, standard index or scale to easily quantify the intent and threat potential of such malware. The Ashburn-Sulcoski Index [17] defines three levels (low, medium, and high) for each contributor to malware threat potential (impact, capability and intent).

[20] presents a technique based on program obfuscation for generating tests for malware detectors. Their work focuses on viruses and obfuscation, but should be applicable to other types of malware. They examine the input space of a potential malware, and extract the signature. Further, the software is classified as malicious or benign.

Spyware programs create files and registry entries when infecting a computer. Howes identifies in [45] some critical detections when comparing anti-spyware tools, including

- Executable files (.exe / .com)
- Dynamic link libraries (.dll)
- BHO-related registry entries
- Toolbar-related registry entries
- Browser setting-related registry entries
- Browser extension-related registry entries
- Auto-start registry entries

The list of critical detections is generated by analyzing the entries made by the spyware applications accompanied with Grokster, which did not contain CoolWebSearch, assumably the most complex and dangerous spyware application there is. Howes points out that these "critical" detections do not cover all the entries from spyware, but constitute the most important files and registry entries.

In order to compare various countermeasures, we have to obtain some values for each method or utility. We have to do some measurements of performances. [26] defines a

measurement as the "process of linking abstract concepts to empirical indicants", using empirical and theoretical considerations, and "metrics" are a means to realize that in practice. The process of measuring performance is described by Frost [9], and further designing of metrics is explained in [10], but none of these are suitable for use in assessing the effectiveness of spyware countermeasures.

Metrics for assessing the effectiveness of spyware countermeasures

Metrics are tools designed to facilitate decision making through a specified process of collection, analysis, and reporting of performance data [10]. The general idea is to develop a certain way of assessing performance, for comparisons of e.g. products and designs which may be used or retested by others at a later stage. The metrics should be repeatable (a second assessment by the same evaluator produces the same results) and they should be reproducible (a second assessment by a different set of operators produces the same results).

The NIST sp800-55 [10] defines the design of security metrics as follows;

> *"IT security metrics must yield quantifiable information for comparison purposes, apply formulas for analysis, and track changes using the same points of reference. Percentages or averages are most common, and absolute numbers are sometimes useful, depending on the activity that is being measured."*

The most important feature is the numerical representation of some performance, making it possible to compare performance in a structured manner. Further, the metrics must provide relevant and correct performance trends over time, and measure each aspect of an organization's (or user's computer) security. NIST states:

> *"IT security metrics can be created to measure each aspect of the organization's security. For example, the results of risk assessments, penetration testing, security testing and evaluation, and other security-related activities can be quantified and used as data sources for metrics."*

NIST define the metrics to cover most of the aspects of an organization's security, 5 levels in total; "Policy developed", "Procedures developed", "Procedures and controls implemented", "Procedures and controls tested", and "Procedures and controls integrated". Such comprehensive coverage does not comply with our intentions with the metrics, which are mostly based on technical capabilities and user-friendliness, and aimed for basic web user's utilities and methods for preserving privacy.

The number of metrics developed per stakeholder should be between 5-10 [10], and weighting scales may be used to differentiate between the importance of selected metrics, which ensures that the results reflect the security priorities.

Table 11 presents a template of security metrics defined in [10].

Table 11. Template of metric -NIST

Critical Element	A vital part of security, defined as a question.
Subordinate Question	Define a more detailed question of "Critical Element" that one needs to achieve measurements for.
Metric	Define the metric by describing the quantitative measurements(s) provided by the metric. "Percentage", "number", frequency," average", or other similar terms.
Purpose	Describe the overall functionality obtained by collecting the metric.
Implementation Evidence	List proofs of the security controls' existence that validates implementation.
Frequency	Propose time periods for collection of data that are used for measuring changes over time.
Formula	Describes the calculation to be performed that results in a numeric expression of a metric.
Data source	List the location of the data to be used in calculating the metric.
Indicators	Information of the meaning of the metric and its performance trend.

The template from NIST does not include reliability or validity assessment. [26] defines reliability as how reproducible the measurements are, which indicates that a good reliability equals low influence from random errors, quoted;

> *"...the extent to which an experiment, test, or any measuring procedure yields the same results on repeated trials".*

A good validity is defined as the absence of systematic errors in the measurements [26]. The measurements may be reproducible and still be invalid if there are static influences that we have not calculated. While reliability refers to empirical indicators, validity refers to the relationship between the theoretically designed methods of measuring and the indicators, which means that one should minimize random *and* nonrandom measurement errors.

For evaluating information security [30] defines Information Security as a value that *"...represents an IS-related quality of some object of concern."* Further, an assessment is used as a decision support, such as risk management. In the paper, the term Information Security is used as a representation of a metric, measure, score, rating, rank, or assessment result (this is not an exhaustive list) to avoid disagreement or discussions on terminology. Some of the conclusions given in [30] are:

- "No single IS (metric) will successfully quantify the assurance present in a system."
- "Software and systems engineering are very much related to this problem. For example, the quality of software delivered the architectures and designs chosen, the tools used to build systems, and the requirements specified are related to the assurance to be quantified."
- "Penetration testing is in use today as a valid IS."

- "In the past, attempts to quantify and obtain a partial ordering of the security attributes of systems have not been successful to a large degree (e.g. the TCSEC[9] and the CC[10])."
- "Processes, procedures, tools, and people all interact to produce assurance in systems ISs that incorporate these aspects will remain critical to successful IT system operations."

The statements from [30] indicate that there must be several metrics to assess several problems of security into quantitative expressions.

Payne [31] differentiates measurements and metrics by defining measurement as "single-point-in-time" views, while metrics are derived over time, comparing two or more measurements. Another difference is the objective data counted in measurements, while metrics are either objective or subjective interpretations of data. Payne defines a guide of 7 key steps to establish a security metrics program, including defining goals and objectives, metrics, benchmarking, reporting, action plan, and program refinement.

For the IT security metric development process, NIST [10] defines 2 major activities;

- "Identification and definition of the current IT security program; and"
- "Development and selection of specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls."

Somewhat similar as [31], NIST describes 7 activities for establishing a security metric program. The identification and definition part consists of: stakeholder interest identification, goals and objectives definition, IT security policies, guidance, and procedures review, system security program implementation review. The metrics development and selection consist of: level of implementation, program results, and business/mission impact.

[32] includes product evaluation criteria identification, information assurance (IA) strength quantification, risk assessment/analysis methodology development into the concept of "security metrics". [32] lists examples of proposed criteria for IA metrics;

- "**Scope**. The portion of the IS problem domain the IA metric describes should be clearly characterized."
- "**Sound foundation**. The metric should be based on a well-defined model of the portion of the information system problem domain it describes."
- "**Process**. The metric assessment process should be well defined. The process definition should include qualifications of evaluators, identification of required information, instructions on how specific factors are to be measured or assessed, algorithms for combining factor values into final values, and explanations of sources of uncertainty."
- "**Repeatable**, i.e. a second assessment by the same evaluators produces the same result."
- "**Reproducible**, i.e. a second assessment by a different set of evaluators produces the same results."
- "**Relevance**. The IA metrics should be useful to decision-makers. (...)"

[9] Note: Trusted Computer System Evaluation Criteria. The Department of Defense published a Trusted Computer System Evaluation Criteria (TCSEC) in 1983, and republished as a DoD standard in 1985. The level of trust is arranged into a scale that extends from minimal to high level of trust. http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-021.html

[10] Note: Common Criteria. Common Criteria became an ISO standard in 1999, and sets requirements for security features. http://csrc.nist.gov/cc/

- "**Effectiveness.** It should be possible to evaluate the IA metric quickly enough, and with low enough costs, for it to be useful to the decision-makers who will use it."

One may design metrics to cover different categories of security. [32] describes 3 security categories as:

- Organizational security metrics: Measuring organizational programs and processes.
- Operational metrics: Measuring the organization's operational readiness and effectiveness in providing information assurance.
- Technical metrics: Measuring the capabilities of technical object or system.

The technical metrics may further be designed for strength assessment or weakness assessment. The organizational metrics may be sub-divided into into IA Program Development Metrics, Support Metrics, Operational Metrics, and Effectiveness Metrics. The Operational Metrics may be divided into Operational Readiness metrics, Operational Practice metrics, and effectiveness metrics.

Comparing different tools and utilities as countermeasures against spyware, and ranking them against each other imply that technical metrics need to be designed and carried out.

Some of the criteria are mentioned by other authors, like repeatability and reproducibility of the measurements. For ensuring repeatability and reproducibility the assessment process needs to be described, and for persuading decision makers to use the metrics, it must not be too costly to apply them. Further, [32] mentions that the metrics "*must evolve*", adapt the changes in technology and regulations, and be tuned as a result of gained experience.

2. Effectiveness of the countermeasures against spyware

TopTenReviews.com evaluated SpySweeper Eliminator to be the best spyware-removal tool (per 12.12.2004). This tool simply removed more pieces of spyware than its competitors. The values of these tests are somewhat questionable or at least limited since the test procedure or settings are not publicly stated and are therefore not re-examinable. The spyware removal tools are also signature based, which means they can only detect spyware that are known and already defined. There are several instances where the spyware removal tools have embedded spyware within themselves and the differences between the removal tools are very likely to depend on how each tool-author defines or classifies spyware.

Howes has done a well defined test on anti-spyware tools [45], which is more detailed and well documented than TopTenReview's attempt. The test environment is well described, and the anti-spyware feature comparison is listed, divided into scan methods, scan configuration, protection, diagnostic and updates. The results from Howes' test shows that the spyware removal tools do not give the necessary protection alone. According to [42], the best spyware removal tools will leave at least 25 % of critical entries go unnoticed. A combination of two or more spyware removal tools is preferred. In an interview [46] Howes says that only 12 of 110 tested malware removal programs functioned in a satisfactory way. As mentioned, this test refers only to spyware removal tools and not to other countermeasures like e.g. disabling ActiveX.

Brandt in [47] tested 6 spyware removal tools, comparing the free version Spybot Search&Destroy to 5 commercial versions of such tools. The free version seemed to outperform the commercial products. The test environment is described, but the

details about the results are not presented. The analyzing tool (InCtrl5) used in the experiment is a commercial product. The article states that the registry processes and files associated with spyware were monitored, and Brandt considers only spyware removal tools which are only one of several possible countermeasures to be evaluated.

4 Evaluating countermeasures

In this chapter we design metrics that are to be used when assessing the various countermeasures.

Metrics for evaluating spyware countermeasures

The metrics we used in this project are characterized by:

- Type of object: what we want to measure
  - Technical
- Purpose: why we need to measure it
  - Comparison
- Intended audience: who we are measuring for
  - Decision makers
  - Common web users

The metrics were designed as qualitative metrics, where we converted a measurement into a number, sometimes into a fixed scale. The ideal design would be a metric where we achieved a true numeric value of some measurement (a quantitative measurement that is) which a may be achievable in some of the metrics but not all. We chose to design all the metrics in such a way that the outputs are in the same format (a number between 0 and 100, or between 0 and 500). NIST [10] points out that setting performance targets for efficiency, effectiveness, and impact metrics is more complex than for implementation metrics because "these aspects of security operation do not assume a specific level of performance." For determining security levels, one needs to apply qualitative and subjective reasoning, and one should be able to adjust these levels when sufficient experience is gained.

The following metric (Table 12) is based on a template defined in [10]. The template is used by NIST to define the sample metric as in Appendix I. In this project we changed the template as follows;

- "Critical element" and "Subordinate question" have been replaced by "Metric ID" and "Name"; since these metric will be used in a very limited area of operation we only need to differentiate between them.
- Rows for "Validity" and "Reliability" have been added. As defined in [26] validity and reliability are important properties when it comes to the use of metrics, which estimate how well the results correspond to the actual and true values.
- "Frequency" has been left out; one should not retest the countermeasures every time a new tool or method are introduced, or reexamine the countermeasures too often.
- The "Data source" is also removed; this because the information collection process is defined in the implementation evidence at each metric.

Table 12. Template of a metric

Metric ID	A unique identifier for the metric.
Name	Name of the metric.
Description	Description of the metric. "Percentage", "number", "frequency", and "average".
Metric	Description of what we are trying to measure with this metric.
Formula	Describes the calculation that will convert the metric into a numerical expression.
Purpose	What the goal and overall functionality are obtained by using this metric.
Implementation Evidence	How the measurements are gathered. List proof of the security controls' existence that validates implementation.
Indicators	Information about what the metric values indicate in terms of security.
Validity	An evaluation of the possibility that we are not actually measuring what we defined as the purpose of the metric.
Reliability	An evaluation of the chance of random errors with this metric.

[10] divides the types of metrics into implementation, efficiency and effectiveness, and impact. These are the metrics that can realistically be obtained and give reasonable performance results. On the basis of those types, we have defined the following metrics to assess the effectiveness of the various spyware countermeasures against spyware;

- A-1 User-friendliness
- A-2 Method of detection
- A-3 Cost
- A-4 Category of spyware it is intended to work with
- A-5 Spyware detection
- A-6 Spyware removal
- A-7 Spyware blocking
- A-8 False positives

The metrics will be of qualitative values and will be run through fixed scales or formulas to produce a numerical representation of the performances for comparison of various countermeasures against spyware. The ideal metric will produce a quantifiable value, which may be obtainable for some of the designed metrics. The metrics are further designed to produce results in the same format, namely a number between 0 and 100, except for A-5, A-6, and A-7 which will have a potential score between 0 and 500. The features of detecting, removing, and blocking are vital for any spyware countermeasure. For instance, the cost of the countermeasure is not as important as the capabilities of the countermeasures.

Theoretically, it is possible to detect a spyware program before its installation and then block it from infecting the system, and a countermeasure may block a spyware operation, like when a firewall denies a connection, and still be able to remove the spyware.

When referring to detection, removal, or blockage of spyware the following definitions are used:

Detect. Recognize spyware.

- Either by identifying it by name and alerting its presence or by listing the spyware component in a log file without identifying it as spyware.

Remove. Delete installed spyware.

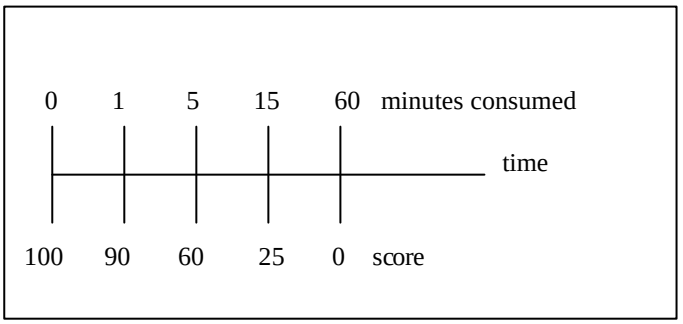
- Permanently remove the component from the computer, either as a process, registry entry or a file. A component is permanently removed if the component does not reappear after some time or a reboot.

Block. Prevent installation of spyware, or prevent operation of spyware.

- A spyware installation process may be blocked, or the spyware operation process may be blocked. In either way the spyware program does not transmit information back to external servers.

A-1 User-friendliness

Table 13. A-1 Metric: User-friendliness

Metric ID	A-1
Name	User-friendliness.
Description	This metric assesses the effort in configuring or running the countermeasures.
Metric	A numerical representation of the time it takes to configure the countermeasures.
Formula	Plot the result into the scale illustrated in "implementation evidence" and read off the corresponding value.
Purpose	The purpose of this metric is to distinguish countermeasures by how well they guide the user to ensure the correct usage.
Implementation Evidence	The average time consumed during configuration is translated into a scaled numeric representation. By configuring we exclude the time spent in purely installing the tools. The number of persons involved in this test should exceed 30. If the countermeasure does not require any configuration, it scores '100', while utility that requires close to 15 minutes scores '25'. 
Indicators	The time it takes to configure the utilities indicates whether it is user-friendly or not. Novice users may not choose the more demanding utilities.
Validity	The scale may not be perfectly realistic or tuned. The values should be redefined when sufficient experience in this field is achieved. Time spent in configuring processes is not the only component of user-friendliness; how well the information is presented, and the guiding to ensure correct installation and correct use of software are also important.
Reliability	The time required for configuring will depend on the users' experience with similar or previous versions of the utility or method. It is preferable to get a significant number of test-results that eliminates any random errors.

It is preferable to use methods that do not consume much effort or time to configure or execute. Since there are, presumably, users that are not aware of the threats they are exposed to, ease of use would be vital in preserving the privacy. An inexperienced user may not know how to configure a Host Intrusion Detection System, potentially configuring it in a wrong way, or simply give up.

The main feature of this metric is the calculation of time consumption when applying the countermeasure. The methods or utilities may vary in nature and operation mode, which thereby will differ in configuring requirements, so we have to calculate the time spent into a fixed scale. “Plug & Play” tools will mostly result in no configuring time.

The value starts at 100 when 0 minutes are consumed in configuring the countermeasure, and decreases with the time consumed. At first, the values decrease quite fast before they flatten out and end up in a score of 0 when the configuring time exceeds 60 minutes.

When defining configuring time, one does not include the time consumed by the hardware in copying files or installing the software. The human-machine interaction is counted for in this metric.

A-2 Method of detection

Table 14. A-2 Metric: Method of detection

Metric ID	A-2
Name	Method of detection.
Description	This metric assesses the countermeasures based upon their abilities to continuously scan for spyware.
Metric	A numerical representation of the ability to continuously detect spyware.
Formula	Continuous detection (real-time) gives a score of 100, and non-continuous detection 30.
Purpose	The purpose of this metric is to distinguish countermeasures by their abilities to prevent the installation of spyware.
Implementation Evidence	The methods or utilities may be continuously preventing/detecting the system against spyware or checking the system once in a while leaving the system vulnerable for some time. A utility that scans the systems periodically is considered as being non-real time. Real-time Control Score 100 30
Indicators	Utilities or methods that prevent spyware from getting installed at the first place continuously protect the system, while methods that are initiated by the user do not.
Validity	The scale may not be perfectly realistic or tuned. The values should be redefined when sufficient experience in this field is achieved.
Reliability	There should be no problem to define a method or utility as being continuous or control based.

The countermeasures may not block the installation process, which means the spyware may operate and transmit information for some time before it gets detected.

Some countermeasures scan a computer for non-legitimate processes, files, or registry keys while others scan the downloaded stream. The difference between those two approaches is the time the spyware potentially may harm the user; scanning the downloaded streams will prevent spyware from getting installed in the first place and therefore from doing any harm. A utility that periodically scans the system for spyware will leave the system vulnerable for some time, namely the time between the scans.

If there are hybrid versions (real-time and control features that is), the highest score is assigned.

The idea of normalizing the metrics is to achieve comparable results and that the numerical representations from the different metrics have the same value (a score of e.g. 90 in metric A-1 equals a score of 90 in metric A-2). A score of 30 will indicate that the countermeasure does not operate in real-time, and 30 are chosen to comply with the idea of normalization. A score of 0 within this metric would have made it as bad as 0 at metric A-4, which would indicate that the countermeasure did not work around any spyware categories.

A-3 Cost

Table 15. A-3 Metric: Cost

Metric ID	A-3
Name	Cost
Description	This metric assesses the countermeasures based upon their investment costs.
Metric	A numeric representation of the cost of each utility/method.
Formula	The corresponding value of the cost represents the score.
Purpose	The purpose of this metric is to distinguish countermeasures by their investment costs.
Implementation Evidence	The more the users must pay for the utility the more they avoid them. Many products (spyware removal tools and anti-virus software) cost around $30 to $60.
Indicators	The cost of utilities affects the user's willingness to invest or install the countermeasures.
Validity	Expensive products are not automatically better than cheaper ones, and free utilities are in general preferred by the average user. The formula/table for converting cost into a range of numeric number may not be perfect and should be revised when sufficient expertise is obtained.
Reliability	The price of one product may vary from store to store; an average of at least 10 distributors should be obtained.

Score	$
100	0
70	20
50	30
40	40
25	50
15	60
5	80
0	>80

The cost and expense of countermeasure will influence the user's decision-making when choosing a defence against spyware. One will prefer a utility that is free, and even do the same job, or even better [47], over one that costs a great amount. Assumably, there is a great difference between a utility that is free and one that cost $1 due to the registration and payment process. There may be free versions of some tools, but these are most often "light" versions of more feature-rich commercial "pro" versions. By including a metric based on costs into the experiments, the experiment and results will accommodate the average user that evaluates the different countermeasure by their cost, and users that are not dependent on achieving a 100 % secure system.

A-4 Category of spyware it is intended to work with.

Table 16. A-4 Metric: Category of spyware

<table>
<tr><td>Metric ID</td><td>A-4</td></tr>
<tr><td>Name</td><td>Category of spyware.</td></tr>
<tr><td>Description</td><td>This metric assesses the countermeasures based upon their designed ability to detect spyware esthat constitutes severe threats.</td></tr>
<tr><td>Metric</td><td>A numerical representation of the supported categories and their threat.</td></tr>
<tr><td>Formula</td><td>$score = \left(\sum_{i=1} i \right)$, where i is the ID-number of each supported category.</td></tr>
<tr><td>Purpose</td><td>The purpose of this metric is to distinguish countermeasures by their ability to detect categories of spyware.</td></tr>
<tr><td>Implementation Evidence</td><td>The method or utility should apply to some of the categories of spyware listed below. Each category got a value, and the utility's score is based on summarizing the scores of all the categories that it defends against.

By analysing the feature specificatio n from the vendor and/or analysing the activity, we can tell something about what category it is intended to work with.

<table>
<tr><th>ID i</th><th>Spyware</th><th>Score</th></tr>
<tr><td>1</td><td>Web-bug</td><td>1</td></tr>
<tr><td>2</td><td>Cookie</td><td>3</td></tr>
<tr><td>3</td><td>Pop-up</td><td>4</td></tr>
<tr><td>4</td><td>Hijacker</td><td>12</td></tr>
<tr><td>5</td><td>Tracker</td><td>20</td></tr>
<tr><td>6</td><td>LSP</td><td>24</td></tr>
<tr><td>7</td><td>Keylogger</td><td>36</td></tr>
</table>

If a countermeasure operates on every category it will thereby score a 100.</td></tr>
<tr><td>Indicators</td><td>The kind of spyware the methods and utilities detect indicates how complete the utility / method is.</td></tr>
<tr><td>Validity</td><td>The scale may not be perfectly realistic or adjusted. The values should be redefined when sufficient experience in this field is achieved.</td></tr>
<tr><td>Reliability</td><td>Wrong conclusions may be stated if one does not discover all the supported categories, or the statement from the distributor claims a support for something their product does not support. The vendors may operate with other classifications which leave us to investigate the activity and transform it into our classification of spyware.</td></tr>
</table>

The utilities and methods may be designed to detect different forms of spyware components, which differ in potential threats. Cookies are not by far as severe as keyloggers and methods that defend a system against keyloggers should be of more value to a user.

A countermeasure that protects a system against all forms of spyware attacks scores a 100, while only blocking cookies would result in a score of 3. This metric supports the general idea of finding the countermeasure that best protects a system by defining which sort of threat they are able to face.

The values of the categories are set from an ordinal scale [70], based on literature study of what components that threatens a user's privacy. The categories form a total order and there is no fixed distance between the categories.

A-5 Spyware detection

Table 17. A-5 Metric: Spyware detetion

<table>
<tr><td>Metric ID</td><td>A-5</td></tr>
<tr><td>Name</td><td>Spyware detection.</td></tr>
<tr><td>Description</td><td>This metric assesses the countermeasures based upon their ability to detect spyware components.</td></tr>
<tr><td>Metric</td><td>A numerical representation of the ability to detect spyware.</td></tr>
<tr><td>Formula</td><td>The amount of detected spyware:
$$Score = \frac{Amount\,recognized}{Total\ value\ of\ \ spyware\ components} \times 500$$</td></tr>
<tr><td>Purpose</td><td>The purpose of this metric is to distinguish countermeasures by their ability to detect spyware.</td></tr>
<tr><td>Implementation Evidence</td><td>Experiment:
1. Install monitoring tools on a clean computer (the reference system).
2. Take notice of the legitimate traffic and processes on the system.
3. Back-up the system for later use.
4. Install certain spyware and/or browse certain web sites.
5. Reboot system to allow spyware to finish their installation.
6. Investigate the illegitimate processes and changes in the system.
7. Roll-back the system by using the back-up created in pt.3.
8. Apply countermeasure.
9. Install certain spyware and/or browse certain web sites.
10. Investigate the illegitimate processes and changes in the system (file creation, registry entries, settings and alike).

Roll-back the system when testing another countermeasure, proceeding from pt.8.

<table><tr><th>Value</th><th>Category</th><th>Detected #</th><th>Actual #</th></tr><tr><td>55</td><td>Processes</td><td></td><td></td></tr><tr><td>20</td><td>Autoruns in registry</td><td></td><td></td></tr><tr><td>10</td><td>Hijacks (bho,hosts file)</td><td></td><td></td></tr><tr><td>7</td><td>Executive files</td><td></td><td></td></tr><tr><td>5</td><td>Dynamic link library</td><td></td><td></td></tr><tr><td>2</td><td>Entries in registry</td><td></td><td></td></tr><tr><td>1</td><td>Cookies</td><td></td><td></td></tr><tr><td>Total</td><td></td><td></td><td></td></tr></table>
Note that the experiments should be performed in shortest possible time to avoid testing on different spyware components.</td></tr>
<tr><td>Indicators</td><td>The remaining spyware on the system are spyware that the countermeasure did not detect or prevent from installing.</td></tr>
<tr><td>Validity</td><td>The countermeasure may detect a spyware program but cannot prevent it from getting installed. If the utility / method reports this,</td></tr>
</table>

	it should be counted for as detection. Some spyware may be capable of preventing installation of certain countermeasures.
Reliability	The reliability depends on how many spyware programs attempt to get installed on the system; too few will make the results invalid. The different tools/methods may have classified spyware differently, and therefore different results on the same piece of spyware may appear. Some tools may not trigger on one specific spyware program while others do (caused by partnership between the tool's author and spyware author). Some spyware may be very difficult to detect (covert channels and hiding within legitimate traffic) so one needs to compare the system state before and after infection carefully. The performance of similar methods or utilities may vary; it is preferable to test several similar utilities to rule out reliability issues. Another problem is the update-frequency of each tool; many unknown spyware programs may get installed if the signature database is out-dated. The infecting spyware may not be representative for the spyware programs in general. The spyware program may not operate within the time the experiment is performed; e.g. if the spyware only activates itself on certain dates. The utilities that are being used for monitoring purposes may not detect all spyware activities.

We differentiate between the ability to detect and the ability to remove a spyware program. The most severe spyware programs detected, according to the table within the metric A-4, will be prioritized when ranking the countermeasures, if applicable.

Spyware detection is mainly based on signature matching where the software compares incoming traffic or activity to known signatures stored in a database. Blocking of all cookies is not a method of detection since no signatures are matched.

When using external software for monitoring the system we cannot be sure that the monitoring utilities do not contain spyware by themselves. By comparing the system state before the infection and the state after the infection one will detect the differences between the two states.

Detections that are not true (false positives) will not be counted for in the detection metric, but detections of that kind will influence the overall result via the false-positive metric A-8.

The maximum score is 500.

As metric A-4, the values of the categories are in this metric (and metric A-6, A-7, and A-8) is set from an ordinal scale [70], based on literature study of what components that threatens a user's privacy. The categories form a total order and there is no fixed distance between the categories.

A-6 Spyware removal

Table 18. A-6 Metric: Spyware removal

<table>
<tr><td>Metric ID</td><td>A-6</td></tr>
<tr><td>Name</td><td>Spyware removal.</td></tr>
<tr><td>Description</td><td>This metric assesses the countermeasures based upon their ability to remove spyware components.</td></tr>
<tr><td>Metric</td><td>A numerical representation of the ability to remove spyware.</td></tr>
<tr><td>Formula</td><td>The amount of removed spyware.

$$Score = \frac{Amount\ removed}{Total\ value\ of\ \ spyware\ components} \times 500$$</td></tr>
<tr><td>Purpose</td><td>The purpose of this metric is to distinguish countermeasures by their ability to remove spyware.</td></tr>
<tr><td>Implementation Evidence</td><td>Experiment:

1. Install monitoring tools on a clean computer (the reference system).
2. Take notice of the legitimate traffic and processes on the system.
3. Install certain spyware and/or browse certain web sites.
4. Reboot the system to allow spyware to finish its installation.
5. Analyze modifications to the registry, file system and processes to determine the amount of spyware that are installed.
6. Back-up the system.
7. Apply countermeasure.
8. Investigate the amount of spyware that has been removed.
9. Reboot computer, run countermeasure again.
10. Document the installed spyware.

Roll-back the system when testing another countermeasure, continuing from pt.7.

<table>
<tr><th>Value</th><th>Category</th><th>Detected #</th><th>Actual #</th></tr>
<tr><td>55</td><td>Processes</td><td></td><td></td></tr>
<tr><td>20</td><td>Autoruns in registry</td><td></td><td></td></tr>
<tr><td>10</td><td>Hijacks (bho,hosts file)</td><td></td><td></td></tr>
<tr><td>7</td><td>Executive files</td><td></td><td></td></tr>
<tr><td>5</td><td>Dynamic link library</td><td></td><td></td></tr>
<tr><td>2</td><td>Entries in registry</td><td></td><td></td></tr>
<tr><td>1</td><td>Cookies</td><td></td><td></td></tr>
<tr><td>Total</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Indicators</td><td>The amount of removed spyware components compared to the amount that got installed (taking the different categories into consideration) indicates how well the countermeasure operates.</td></tr>
<tr><td>Validity</td><td>Hybrid version of spyware should be listed in all the involving</td></tr>
</table>

	categories; otherwise one may miss a specific spyware feature.
Reliability	The reliability depends on how many spyware programs are installed on the system; too few will make the results invalid. The different tools/methods may have classified spyware differently, and therefore different results on the same piece of spyware may appear. Some tools may not trigger on one specific spyware program while others do (caused by partnership between the tool's author and spyware author). The performance of similar methods or utilities may vary; it is preferable to test several similar utilities to rule out reliability issues. The infecting spyware may not be representative for the spyware programs in general. The spyware program may not operate within the time the experiment is performed; e.g. if the spyware only activates itself on certain dates. The utilities that are being used for monitoring purposes may not detect all spyware activities.

This metric assesses the various countermeasures' ability to remove spyware, and therefore methods/utilities that prevent spyware from getting installed rather than remove them afterwards will not comply with the term "removing" spyware. For countermeasures that are based on this approach we should consider to count the amount of spyware they prevent from getting installed in the Spyware blocking metric (A-7)

The ability to remove spyware is one of the core features of any spyware removal tool, and is an action based on *detecting* spyware.

The maximum score is a500, the same as for the metric A-5.

A-7 Spyware blocking

Table 19. A-7 Metric: Spyware blocking

<table>
<tr><td>Metric ID</td><td>A-7</td></tr>
<tr><td>Name</td><td>Spyware blocking.</td></tr>
<tr><td>Description</td><td>This metric assessesthe countermeasures based upon their ability to block spyware components.</td></tr>
<tr><td>Metric</td><td>A numerical representation of the ability to block spyware.</td></tr>
<tr><td>Formula</td><td>The amount of blocked spyware.

$$Score = \frac{Amount\,blocked}{Total\ value\ of\ \ spyware\ components} \times 500$$</td></tr>
<tr><td>Purpose</td><td>The purpose of this metric is to distinguish countermeasures by their ability to block spyware.</td></tr>
<tr><td>Implementation Evidence</td><td>Experiment:
1. Install monitoring tools on a clean computer (the reference system).
2. Take notice of the legitimate traffic and processes on the system.
3. Back-up the system.
4. Install certain spyware and/or browse certain web sites.
5. Document the installed spyware.
6. Roll-back using the back-up created in pt.3.
7. Apply countermeasure.
8. Install the same spyware and sites browsed as in pt.4.
9. Document the installed spyware.

Roll-back the system when testing another countermeasure, proceeding from pt.7.
<table>
<tr><th>Value</th><th>Category</th><th>Detected #</th><th>Actual #</th></tr>
<tr><td>55</td><td>Processes</td><td></td><td></td></tr>
<tr><td>20</td><td>Autoruns in registry</td><td></td><td></td></tr>
<tr><td>10</td><td>Hijacks (bho,hosts file)</td><td></td><td></td></tr>
<tr><td>7</td><td>Executive files</td><td></td><td></td></tr>
<tr><td>5</td><td>Dynamic link library</td><td></td><td></td></tr>
<tr><td>2</td><td>Entries in registry</td><td></td><td></td></tr>
<tr><td>1</td><td>Cookies</td><td></td><td></td></tr>
<tr><td>Total</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Indicators</td><td>The difference in amount before and after the implementation of countermeasure indicates how well it blocks spyware from accessing the system.</td></tr>
<tr><td>Validity</td><td>The various method or utilities may have classified spyware differently, which affects the score. Achieving a general idea of each method’s spyware classification is preferable.</td></tr>
<tr><td>Reliability</td><td>The performance of similar methods or utilities may vary; it’s preferable to test several similar utilities to rule out reliability issues. The utilities that are being used for monitoring purposes may not detect all spyware activities.</td></tr>
</table>

Utilities or methods that block spyware (e.g. cookies) may be blocking legitimate traffic. Blocking of cookies is not based upon recognizing any harmful code or activity. Simply all cookies are blocked regardless of intention. Blocking of all cookies is by many not an acceptable solution, so blocking of 3d party cookies may be more appropriate. Compared to the ability to remove and detect spyware, this ability only operates in real-time, and prevents the spyware program from infecting a computer in the first place. For blocking specific spyware programs, there is a process of signature matching to detect if a piece of code may be harmful or not, and the amount of spyware that is being prevented from reaching the system should be counted. Preventing spyware programs from operating or preventing them from transmitting information should be counted as a successful block, though it may affect the performance of the computer and be a risk if one accidentally disables the countermeasures in a way that the spyware are fully functional in the period the countermeasure is disabled. The maximum score possible within this metric is 500.

A-8 False positives

Table 20. A-8 Metric: False positives

<table>
<tr><td>Metric ID</td><td>A-8</td></tr>
<tr><td>Name</td><td>False positives.</td></tr>
<tr><td>Description</td><td>This metric assesses the countermeasures based upon their ability to detect actual spyware.</td></tr>
<tr><td>Metric</td><td>A numerical representation of the ability to report only true spyware.</td></tr>
<tr><td>Formula</td><td>$Score = 100 - \left(\sum_{i=1}^{7} (value \times amount) \right)$, if the score goes below zero, it should be set to 0.</td></tr>
<tr><td>Purpose</td><td>The purpose of this metric is to distinguish countermeasures by their ability to give correct and precise messages.</td></tr>
<tr><td>Implementation Evidence</td><td>Experiment:

<table>
<tr><th>ID i</th><th>False positives</th><th>Value</th><th>Amount</th></tr>
<tr><td>1</td><td>Processes</td><td>10</td><td></td></tr>
<tr><td>2</td><td>Autoruns</td><td>25</td><td></td></tr>
<tr><td>3</td><td>Hijacks</td><td>5</td><td></td></tr>
<tr><td>4</td><td>Executive files</td><td>25</td><td></td></tr>
<tr><td>5</td><td>Dynamic link library</td><td>20</td><td></td></tr>
<tr><td>6</td><td>Entries in registry</td><td>14</td><td></td></tr>
<tr><td>7</td><td>Cookies</td><td>1</td><td></td></tr>
</table>

Ruling out legitimate processes and activities that the countermeasures trigger on.

1. Rollback to an infected computer setting.
2. Apply countermeasure.
3. Investigate the amount of detected spyware that are true spyware.</td></tr>
<tr><td>Indicators</td><td>The amount of legitimate activity that the countermeasure labels as illegitimate.</td></tr>
<tr><td>Validity</td><td>The various countermeasures may operate with different categories and classifications of spyware, and will thereof present different results.</td></tr>
<tr><td>Reliability</td><td>The infecting spyware may not be representative for the spywares in general.</td></tr>
</table>

False positives may cause a user to delete legitimate programs or processes, potentially leaving the computer more vulnerable than before. Killing legitimate processes may not be as serious as deleting autorun entries or executable files since processes will mostly be reinitialized on a reboot. A process may be an application that protects the system in real-time, and the computer will be more vulnerable if such processes are terminated. Autoruns may initialize protection mechanisms, vital system processes or alike, and therefore it is a relatively severe threat if these legitimate entries and files are deleted. Falsely deemed tracking cookies will on the other hand not seriously affect the system.

The categories do not exclude each other, e.g. spyware components in form of an autorun do also fit into the “entries in registry”. To solve this we trigger only the most

severe category and leave the other potential categories with no incrementation of spyware components.

The maximum score is a 100, equally representing the percentage of falsely labelled components.

Not all countermeasures cover all the spyware categories, but theoretically a utility or method may detect, block, and remove spyware from a system. The total score indicates an overall image of how well the countermeasure protects the system and how well they are suited to the average user, where some countermeasures may score low on some metrics but high on others. It is stated in [42] that one countermeasure is not sufficient when protecting a system. But by calculating the scores in this way we can compare what kind of countermeasures are efficient on specific threats, and may further define what combination of countermeasures in fact protects a system sufficiently.

The metrics will cover three main topics of what affects a user's choice and needs when it comes to protecting the system against unwanted spyware. The three topics are capability, user-friendliness, and performance (Figure 1), which describe certain features of the countermeasures. The spyware countermeasure that scores best in total (capability, user-friendlines, and performance) is the best countermeasure to spyware. A countermeasure that scores high on capability and performance may not suit the average user if it costs too much, or if it requires too much time and effort to configure it. The same can be claimed about the other aspects. A spyware countermeasure should score high on all ascpects of measurements.

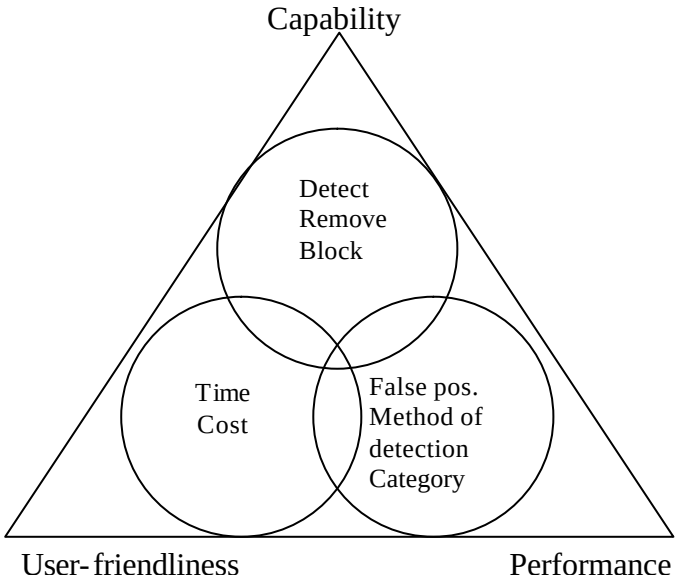


Figure 1. Aspects of measurements

5 The experiment

5.1 Introduction

The values of the metrics defined in the previous chapter have been obtained by means of an experiment. The experiment consisted of installing spyware that were bundled with other applications, and we tested the countermeasures against drive-by downloads. For bundled spyware, the file sharing application Grokster was installed on the computer, and certain web pages were visitied in order to get infected by spyware that propagates through drive-by downloads.

The amount of spyware depends on which pop-ups are shown and what components are downloaded through the Grokster setup. The size of the setup file is only 251 kB, and it establishes a connection between the victim's computer and the Grokster server. The rest of the program and 3rd party software are downloaded from the external server. In this case we have no control of what pieces of spyware are to be installed and we do not know if the same spyware get installed each time we install Grokster. In the drive-by downloads, there are random pushing of pop-ups, pop-ups that may contain different kinds of spyware, and thereby we may have to create a reference configuration to be able to confirm the absence or presence of certain pieces of spyware. Another option is not to perform any action on pop-ups and just let them be.

There may be a problem if the spyware components complete themselves by downloading the rest of the software afterwards, like Grokster does. The spyware servers may update their software, and thereby we may experience different registry entries or files when performing experiments. This may be avoided by completing the experiments in the shortest amount of time possible. Monitoring tools must be implemented to confirm any changes or irregularities.

The experiment consisted of infecting a clean system/computer, monitoring changes made to file system and registry, and monitoring possible spyware operations within 10 minutes after infection. Spyware that do not operate within this 10 minute time period may not be detected and addressed in these experiments.

Reuse of a countermeasure may affect the score. An example is when a participant first tests the time to update the definition file before enabling prevention against tracking cookies. A second countermeasure he or she may test the same utility and take some of the actions within the utility, e.g. blocking ActiveX; this may not affect countermeasures that in general do not require much time in configuration.

The definition of spyware requires that the user is unaware of the information gathering processes that operate in the background. This experiment does not focus on determinig whether or not a 3rd party software comply with the EULA statements. In fact, the EULA in Grokster 2.6 specifies that there are 3rd party software that get installed with the Grokster installation, and display ads through pop-ups of interest as presented by the web sites the user visits. It is further stated in the EULA that no personal information like last names and e-mail addresses are transmitted, that some browser history and amount of time on a site may be transmitted, response to ads (click throughs), system settings (not IP-addresses), installed software, first name, country, city, ZIP-code, non-personal identifiable information on web-pages or forms. It is further stated that an anonymous profile are created for marketing purposes, and information related to this profile may be shared among partners.

Gator makes some questionable demands in their EULA. Of special interest is the following:

> "Any use of a packet sniffer or other device to intercept or access communications between GP and the GAIN AdServer is strictly prohibited."

As a follow up to the questionable EULA, Edelman [52] reflects on the incredible length of the Grokster EULA, 398 page-downs to view the EULA as of October 2004. Furthermore, [52] states that Grokster installs spyware or 3rd party software even if the user clicks on "cancel" when being prompted for installation, but this is likely to be changed.

The 3rd party programs that accompanied Grokster are of many labeled as spyware. Symantec, Lavasoft, processlibrary.com, and WinTasks label these extra programs as spyware.

5.2 Configuration

The basic configurations of each countermeasure, see Appendix D, are described, and handed out to the experiment participant. This to ensure that the participant knows the intention with each countermeasure, and provide a common goal and. Table 21 presents the default configuration and installed software on the test computer.

Table 21. Default configration on test computer

Test Computer	CL56
Hardware	CL56 Centrion 1.7GHz, 512MB, 60GB, DVDR
Drive cfg	C:\%Winnt%\ (60GB)
OS	Windows XP Professional SP1 (WinNT 5.01.2600) Auto update disabled
Installed patches	(none)
Default browser	Internet Explorer 6.0.2800.1106xpsp1.020828-1920
Browser settings	Security Zones Internet Zone: Low Local Intranet: Low Privacy –standard –accept all cookies No Internet filtering
Windows FW	Not enabled
Installed software	Norton Ghost 9.0.0.2583 Total Commander 6.0 Nero Burning Rom 6 WinTasks5 InCtrl5 CommView SmartWhois
Installed protocols/drivers	WinPcap 3.0*

*WinPcap 3.0 is a protocol needed when using Snort in a windows environment for capturing packets on the network. The WinPcap 3.1 Beta did not seem to be compatible with WinSnort 2.3.0RC2

The security zones and privacy policy are set to low, this to be able to assess the effectiveness of each countermeasure and not the countermeasures effectiveness alongside IE protection mechanisms.

5.3 Monitoring tools

The following monitoring tools were used in the experiment:

- File access:
  FileMon (http://www.sysinternals.com)

- Registry:
  RegMon (http://www.sysinternals.com)
  Active Registry Monitor v1.38 (http://www.protect-me.com/arm/?from=prog_arm)

- Network traffic:
  CommView 4.0 (build 281) (http://www.tamos.com)

- Browser Helper Object:
  BHOdemon 2.0.0.21 (http://www.definitivesolutions.com/bhodemon.htm)

- Hijacks
  HijackThis 1.99.0, (http://www.tomcoyote.org/hjt)
  HijackThis examines the registry and hard drive for browser hijackers, but the program lists also legitimate processes that may be harmful for the computer if they are removed. The program creates a list of all the programs/processes that start up when the computer is booted, including host file inspection, LPS inspection, and applications. It does not target specific applications, but targets specific hijacker methods. Usage of HijackThis requires some experience, or at least some expert help to distinguish between legitimate and illegitimate processes.

- Startup manager
  MSConfig (included in Windows XP)

5.4 Countermeasures

The following countermeasures against spyware have been tested in the experiment:

- ZoneAlarm Pro with web filtering 5.5.062.004, http://www.zonelabs.com
  TrueVector security engine 5.5.062.004
  Driver version 5.5.062.004
  ZoneAlarm has abilities to protect a user's privacy by "cookie control", which blocks categories of cookies of user's choice. Furthermore ZoneAlarm can stop ads with "ad blocking", and "mobile code control" blocks active page elements such as Java scripts, vbscripts, and ActiveX. The Web Filtering feature presents an ability to block certain categories of web sites, like "pay to surf sites" and "freeware / software downloads". The firewall logs block attempts of inbound and outbound connections, mapping them to protocol and program, source and destination IP-addresses, and source and destination DNS. Further, ZoneAlarm lists the programs that have accessed or have tried to access the Internet or the local network, and gives the user a choice of allowing the programs to access Internet or to act as a server.

  By blocking installation processes, ZoneAlarm may prevent the installation of some of the named categories, and blocking certain elements on web pages

will prevent some of the spyware installations that use methods that are blocked by ZoneAlarm.

- Outpost Firewall PRO 2.5, http://www.agnitum.com/download/
  Outpost Firewall PRO delivers features such as stateful inspection of data packets, blocking of banner ads and pop-ups, blocking cookies, and active elements blocking of ActiveX, Java, Visual Basic scripts, and Java applets [53].

- Windows Firewall (SP1)
  The firewall embedded in Windows XP is not enabled by default, and the version that comes along Windows XP Service Pack 2 is said to be significantly better than the one in earlier versions [61].

- Internet Explorer –cookie block
  Users of IE have the opportunity to choose whether to accept or block cookies from web sites or cookies from 3rd parties in form of a slide bar which indicates full accept to block all cookies, but the policy may be overridden manually if that is more convenient for the user.

- SpywareBlaster 3.2, http://www.javacoolsoftware.com/spywareblaster.html
  SpywareBlaster is free (donation-ware) for personal use, and block installations of ActiveX-based spyware, adware, and browser hijackers. The tool has also abilities to block cookies in both Internet Explorer and Mozilla/Firefox and potentially dangerous sites can by user's choice be restricted in Internet Explorer. SpywareBlaster 3.2 identifies potentially harmful ActiveX controls and their CLSID which makes it possible to block the malware.

- Spybot Search & Destroy 1.3, http://www.safer-networking.org/en/index.html
  Spybot –Search & Destroy is free and is a well know spyware removal tool, including features for detecting harmful spyware, detecting installed ActiveX components, detecting system startup processes and detecting any installed Winsock LSPs. Spybot is one of the oldest anti-spyware tools. Spybot has been defined as a "trustworthy anti-spyware product" by Eric Howes [51]. The spyware removal tools are not needed to be configured in any specific ways, so the default settings are used, but the definition files must be updated.

- Ad-aware SE Personal
  Ad-aware SE is a free tool that detects and removes spyware from the computer, by scanning active processes and registry entries. Ad-aware does not detect all illegitimate processes as illegitimate, but they are listed.

- WinSnort version 2.3.0RC2, http://www.winsnort.com
  Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. WinSnort is an Intrusion Detection Engine that has been created from the linux-based version Snort. An IDS may be network based or host based. Network based IDS monitor packets on the network wire and match activity patterns to a database of known attack patterns. Host based IDSs monitor what is happening in a specific machine by monitoring logs and boking for changes to the system.

  The IDS tested in this project, WinSnort, requires that the WinPcap 3.0 protocol is installed on the system, this to make the IDS able to capture packets on the network. The latest version, WinPcap3.1, is not compatible with WinSnort. Intrusion Detection Systems that are signature based require that

the signatures are precise and accurate to avoid false positives. WinSnort rules were updated at www.snort.org. Furthermore, rules from www.bleedingsnort.com were also included in this project.

- AVG free version 7.0.300, http://www.grisoft.com/us/us_index.php
  AVG Anti-Virus Free edition is authorized for personal, home computer use only. It schedules updates and virus scans, options of delete, move or heal infected files. Antivirus software like AVG and Norton need to be updated. They operate in real-time as well as non-real-time. The software focuses on detecting viruses and not spyware, and still separate utilities may be needed to be downloaded for removing certain viruses.

- Norton AntiVirus 2005
  Symantec's Norton AntiVirus 2005 removes viruses, worms, and Trojans. It may block certain worms before they reach the system. Symantec claims that the product detects spyware and other non-virus threats [55].

- IE-Spyad by Eric Howes [54]
  IE-Spyad is a free tool operating alongside IE that makes the web sites unable to use ActiveX controls, Java applets, cookies, or scripting in order to invade the user's privacy on a computer. The list of known supspicious sites or domains is associated with known spyware companies.

  A user may configure IE to block suspicious web sites, but these must be manually defined one by one. A link entry into the Restricted Sites category of IE policy will not stop a user from visiting the site, but prevent that site from harming the user's computer, with a potential lack of web site functionality.

- Windows XP update / IE update
  Malware may take advantage of known weaknesses in browsers or operating systems, and vendors race the malware authors to patch these vulnerabilities. By closing any weaknesses in the perimeter, one achieves a more secure system.

- Security policy IE –block ActiveX
  An IE user can choose if he or she wants to accept ActiveX controls, unsigned and signed, and whether web Java scripts are able to run on the computer. The policy is represented by a slide bar, from high to low security, which may be manually overridden by the user.

- SpywareBlaster 3.2 –block ActiveX,
  http://www.javacoolsoftware.com/spywareblaster.html

- SpywareGuard 2.2, http://www.javacoolsoftware.com/spywareguard.html
  SpywareGuard is free (donation-ware) and is currently a "work-in-process". The application protects the system in real-time by scanning downloads (exe and cab files), and stopping browser hijacking attempts in real-time, though only for Internet Explorer.

5.5 Countermeasure features

In Table 22, a survey of features of the countermeasures against spyware listed in the previous section is given. The features are divided into categories of spyware the

countermeasures protect a computer against and the countermeasure's operational mode (real-time vs. control mode).

Table 22. Countermeasure features

Countermeasure	Real-time	Control	Cookie	Pop-up	Web bug	Hijacker	Track-ware	LSP	Key-logger
Personal Firewall (ZoneAlarm)	v	X	v	v	v	v	v	v	v
Personal Firewall (Outpost)	v	X	X	X	X	v	v	v	v
Spyware removal tools (Spybot)	X	v	v	v	X	v	v	v	v
Spyware removal tools (Ad-aware SE)	X	v	v	v	X	v	v	X[11]	v
Intrusion detection (WinSnort)	v	X	X	X	X	v	v	v	v
Anti-virus software (AVG free)	v	v	X	X	X	v	v	v	v
Anti-Virus software (Norton AntiVirus 2005)	v	v	X	X	X	v	v	v	v
Blocking of suspicious web sites (IE-spyad)	v	X	v	v	v	v	v	v	v
Blocking of cookies (Spyware Blaster)	v	X	v	X	X	X	X	X	X
Blocking of cookies (IE)	v	X	v	X	X	X	X	X	X
Patching known weaknesses (WinXP)	v	X	X	X	X	v	v	v	v
Disable ActiveX (IE)	v	X	X	X	X	v	v	v	v
Disable ActiveX (Spyware Blaster)	v	X	X	X	X	v	v	v	v
Kind of FW (SpywareGuard)	v	X	X	X	X	v	v	v	v

The delay between infection and applying countermeasures affects the kind of processes that they detect and remove. For instance, LavaSoft's Ad-Aware does not detect the installation processes that open the computer to a completely new flora of spyware (most likely countermeasures like Ad-Aware will not be run at the exact moment of spyware installation).

[11] Plugins for investigating WinsockLSPs are available for Ad-Aware.

5.6 Spyware download

In the experiment, the spyware accompanied the file sharing application Grokster have been downloaded and installed on the test computer.

When choosing Grokster 2.6 (Table 23) as a "spyware package" we emphasize the intent of this project; since the spyware are present in other software than Grokster or get distributed in other ways, we concentrate on what 3rd party software it installs and how well the countermeasures defend a system against it. The experiment is partially working on bundled spyware and drive-by spyware, of which some are installed when visiting web sites (Table 24).

Table 23. Bundled spyware

Software	Distribution	Assumed Spyware	Source
Grokster 2.6	Bundle	Grokster is known to include many pieces of spyware, though the collection of information is stated in the EULA. These are roaming spyware programs that do infect computers in illegitimate ways.	http://www.download.com

Table 24. Drive-by spyware source

#	Web Site	Activity on web site
1	http://keygen.us	-search "half life 2" and download "*half life 2 crack by FFF*".
2	http://www.lyricsdomain.com	
3	http://www.blazefind.com	-search "*spyware*".
4	http://www.chanceforlove.com	-browse 1 "woman profile".
5	http://www.freephone.cc	-browse bar, including "download", but cancel if applicable.
6	http://www.zoosex.com	-click "*join*".
7	http://iowrestling.com	-click on image

5.7 Experiments

The results depend on the configuration and settings of the countermeasures, and therefore a default configuration must be presented when performing such experiments.

The experiments must be executed within a controllable environment, where the experiment personnel control or administrate any firewalls or alike within the perimeter. Firewalls or alike administrated by ISP's are not assumed to be within this perimeter. The system is not on a NAT-network[12]. The workstation – Traffic Monitor (Figure 2) is placed within the perimeter for collecting information about the network traffic since an abnormal amount of traffic may indicate the presence of spyware.

[12] NAT: Network Address Translation

When installing countermeasures one should make sure of that the version is updated with the latest patches or signatures.

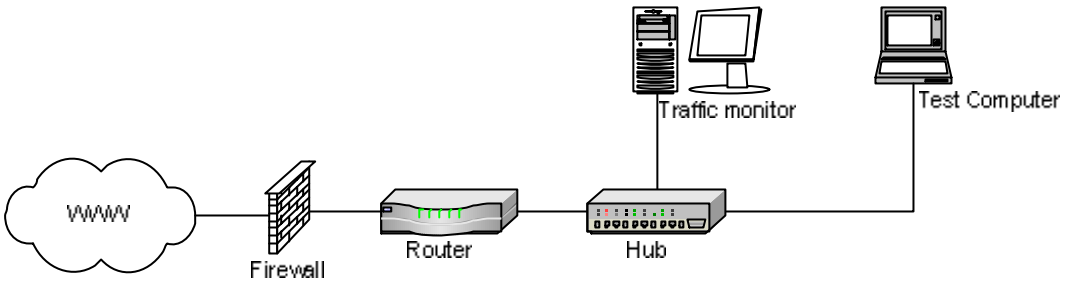


Figure 2. Experimental environment

Experiment A-1 User-friendliness

The average time consumed in configuring the countermeasure indicates the user-friendliness of each countermeasure. Some utilities are plug and play, and therefore do not consume any time in configuring. Methods like changing the default settings for security policies or blocking cookies take some time depending on users' experience and expertise and thereby do not score perfect on the defined scale.

The time consumed for each user in configuring the countermeasure must be measured, and online resources for guidance or potential updates must be available. To avoid extra infection of spyware programs one may not search for resources or help on the Internet from the test computer without ensuring that the registry entries or files are sufficiently documented.

Appendix J shows a proposed design of tables for easing the information collection and calculating the score at each metric.

Experiment A-2 Method of detection

The metric implies no experiments but one need to define the detection feature of each countermeasure, if they are operating in real-time or on scheduled or control basis. It should be no problem defining whether it defends a system in real-time or not. By investigating active processes or just investigating whether the countermeasure triggers on a harmful download we can conclude if it is a real-time defense or not real-time.

Experiment A-3 Cost

The costs of each countermeasure are easily obtainable and no experiments are needed in this metric, though the utility cost may vary from vendor to vendor.

Experiment A-4 Category of spyware

No experiment is needed for determining what categories of spyware the countermeasure is intended to work with. The categories are decided by testing the countermeasures, and reading the feature list and testing whether the statements are true.

Experiment A-5 Spyware detection
An experiment is carried out to investigate the amount of spyware that the countermeasure detects. By following the steps defined in the metric, one ought to compare the system before and after a spyware infection, indicating how good they are in detecting spyware. It may be difficult to point out the illegitimate processes and instances that the countermeasure leaves out, so online resources for recognizing each potential illegitimate process or processes that differ from the reference system must be obtained. In order to identify possible instances of spyware one may use online resources (Table 25).

Table 25. Resources

Type	Resource
Startup	1. http://www.sysinfo.org/startuplist.php
BHO /ActiveX	2. http://www.sysinfo.org/bholist.php 3. http://www.spywaredata.com/spyware/bho.php?status=1 4. http://computercops.biz/CLSID.html
Process	5. http://www.liutilities.com/products/wintaskspro/processlibrary/ 6. http://www.processlibrary.com/
Task list	7. http://www.answersthatwork.com/
Spyware	8. http://www3.ca.com/securityadvisor/pest/browse.aspx 9. http://www.pcpitstop.com/spycheck/Known.asp

Experiment A-6 Spyware removal
The experiment defined in the metric is quite similar to the one defined in A-5, but focuses on comparing the amount of illegitimate processes before and after the removing attempts and the same resources should be available in this case. Note that when comparing these systems, one should not use the test computer to browse any suspicious web sites, preferably not surfing any sites at all. If the test reveals that a removed spyware reappear when the computer is rebooted, this should be counted for as a failed attempt in removing the specific piece of spyware.

Experiment A-7 Spyware blocking
By following the steps defined in metric A-7 one compares the countermeasure's ability to block spyware from reaching the system. Once again, resources must be available, preferably on a separate computer, that do not interact with the test-computer.

Experiment A-8 False positives
The idea is to define the amount of false positives each countermeasure generates. Each false positive may potentially cause serious damage to a computer. By investigating any changes to a system caused by an activity, one can determine if any false positives are generated by the countermeasure.

5.7 Experiment features

- 25 external people were involved in the experiment; they had varied background, from somewhat familiar with the term to daily users of the terms.

- The experiments involving detection, removing, and blocking spyware must be completed in short time to be sure that the same version or the same foundation of the definition files are used. If e.g. Spybot uses an up to date definition file and Ad-aware does not, long term testing with Ad-aware will not represent the actual capabilities that the countermeasures are good for.

- When referring to blocking of sites, one does not entirely block the access to such sites, but disables certain features at these sites, such as scripts, ActiveX controls, cookies and alike.

- The command line when configuring WinSnort should be equivalent to "*c:\snort\bin\snort.exe –dev –l c:\snort\log –c c:\snort\etc\snort.conf*". When using another computer to monitor the network, one may get false positives in form of uPnP[13] messages from the monitoring computer; these may be eliminated by unchecking this rule in the appropriate rule file.

- As for the costs needed in the metrics, Spybot S&D is free, but the developers accept donations, Ad-aware is free of costs, but Ad-aware also exists in a professional version, which is not free.

- An overview of intentions and basic configuration is handed out to every participant immediately before the experiment (Appendix D).

5.8 Critical Detections

In the first place, a general idea of what to trigger on is needed when distinguishing countermeasures by the ability to remove, block, or detect spyware. When a spyware program gets installed, it leaves its signature at several places in the registry and on hard drive, but not all of them are important or critical for its operation.

5.8.1 Detections

By detecting and comparing files, registry entries, and processes this test conforms to [45], a known anti-spyware testing. This means that the defined critical components are based on Howes work [45], but will be updated with our own findings and components. The version of tested spyware may not be equal to the ones that are tested in this project. BHOs, toolbars, browser settings, browser extensions, and auto-start entries are typical values listed in Merijns "HijackThis!" tool [69]. Though, Howes does not say what version of Grokster was tested on, or from what web site it was downloaded.

- executable files (.EXE / .COM)
- dynamic link libraries (.DLL)
- BHO-related Registry entries
- toolbar-related Registry entries
- browser setting-related Registry entries
- browser extension-related Registry entries

[13] uPnP: Universal Plug and Play, a service for automatic detecting of networked services and devices.

- auto-start Registry entries

5.8.2 Critical executable files and dynamic link libraries

The path of executable files and dynamic link libraries are defined as:

C:\programfiles\ or C:\program filer\
C:\%Winnt%\system32\
C:\%Winnt%\

5.8.3 Critical Registry entries

The following critical registry entries are defined:

HKEY_CLASSES_ROOT\
HKEY_CLASSES_ROOT\CLSID
HKEY_CLASSES_ROOT\PROTOCOLS\Handler

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Toolbar
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Toolbar\WebBrowser
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\UrlSearchHooks
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\MenuExt
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Search

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search

5.8.4 Hosts file

The hosts file associates an IP-address with names that are more suitable for reading by humans than numbers. The computer reads this file when it tries to reach web sites, and if no entries match the query the computer contacts the DNS-server for more information. By default there is only one entry in this file; localhost –an address that refers to the computer itself, which means that typing “ping localhost” equals “ping 127.0.0.1”. An example is given below:

---start of file---
127.0.0.1 localhost
---end of file---

Since the computer first opens the hosts file before it calls upon an IDS, it can be used to block unwanted connections to adservers or alike. By typing the domain name to the server, but using our own address (127.0.0.1) instead of the address referring to the ad-server, we have successfully blocked the connection.

6 The effectiveness of countermeasures

6.1 Effectiveness

The effectiveness of how well a countermeasure protects against spyware is calculated by using the defined metrics, making us able to rank the various countermeasures on how well they perform.

6.2 Measurements

The results from the experiments are collected and organized into Table 26. Spyware that are bundled with the file sharing application and the spyware that infected the computer while surfing specific web pages are separated. The details concerning the results are listed in AppendixC.

Table 26. Measurements/results

	Measurements							
	Time (minutes)	Method	Cost	Category	Detection	Removal	Blocking	False positives
					Bundle	Bundle	Bundle	
					Drive-by	Drive-by	Drive-by	
Zone Alarm	3	Rt	$40 (5)	1,2,3,4,5, 6,7	520/2147 0/741	0/2147 0/741	1184/2147 741/741	0
Outpost	2	Rt	$40 (4)	4,5,6,7	520/2147 55/565	0/2147 0/565	1184/2147 476/565	0
Spybot S&D	1	Ctrl	$0	2,4,5,6,7	856/2508 286/646	881/2508 210/646	0/2508 0/646	0
Ad-aware	1	Ctrl	$0	2,4,5,7	931/2508 504/762	739/2508 318/762	0/2508 0/762	1p
WinSnort	39	Rt	$0	4,5,6,7	285/2508 175/730	0/2508 0/730	0/2508 0/730	2p
AVG Free	1	Rt/Ctrl	$0	4,5,6,7	165/2508 0/615	55/2508 0/615	0/2508 0/615	0
Norton AV	1	Rt/Ctrl	$46	4,5,6,7	481/2508 297/875	371/2508 297/875	0/2508 0/875	0
IE-Spyad –block sites	1	Rt	$0	1,2,3,4,5, 6,7	0/2508 0/670	0/2508 0/670	0/2508 670/670	22c
Patching OS	4	Rt	$0	4,5,6,7	0/2508 0/698	0/2508 0/698	0/2508 0/698	0
IE –ActiveX	2	Rt	$0	4,5,6,7	0/2508 0/639	0/2508 0/639	0/2508 635/639	0
IE –block cookies	1	Rt	$0	2	0/2508 0/670	0/2508 0/670	0/2508 9/670	22c
SpywareBlaster –ActiveX	1	Rt	$0	4,5,6,7	0/2508 0/667	0/2508 0/667	0/2508 661/667	0
SpywareBlaster –Block cookies	1	Rt	$0	2	0/2508 0/644	0/2508 0/644	0/2508 5/644	0
SpywareGuard	1	Rt	$0	4,5,6,7	30/2508 10/643	30/2508 10/643	0/2508 0/643	0
XP FW sp1	0	Rt	$0	4,5,6,7	0/2508 0/741	0/2508 0/741	0/2508 0/741	0

Rt: Real-time, Ctrl: Control, c: Cookie, p: Process, category 1 to 7 are defined in the metric A-4.

According to the experiment, freephone.cc, the only site that was expected to be "free of spyware", did not even contain any 3rd party cookies or 1st party cookies. The scores on each countermeasure are presented in Table 27 below.

Table 27. Countermeasure score

	A-1	A-2	A-3	A-4	A-5	A-6	A-7	A-8	Total
ZoneAlarm	60	100	40	100	90	0	335	100	**825**
Outpost	60	100	40	92	105	0	305	100	**802**
Ad-aware	90	30	100	71	220	160	0	90	**761**
Spybot	90	30	100	95	180	175	0	100	**770**
Winsnort	0	100	100	92	70	0	0	80	**497**
AVG	90	100	100	92	25	10	0	100	**517**
Norton AV	90	100	25	92	115	100	0	100	**622**
IE-spyad	100	100	100	100	0	0	105	78	**583**
SpywareBlaster A	90	100	100	92	0	0	105	100	**587**
SpywareBlaster C	90	100	100	3	0	0	0	100	**393**
Patching OS	60	100	100	92	0	0	0	100	**452**
IE ActiveX	60	100	100	92	0	0	100	100	**552**
IE cookies	90	100	100	3	0	0	0	78	**371**
SpywareGuard	90	100	100	92	5	5	0	100	**492**
XP FW sp1	100	100	100	92	0	0	0	100	**492**

6.3 Results

6.3.1 Result A-1, A-2, A-3, and A-4

The first metric calculated the user-friendliness of each countermeasure by the configuration time that is required. The time needed for configuring the most of the countermeasures was within the range of 4 minutes (Figure 3), only WinSnort scored below 60 on this metric. With an average of 39 minutes, and several participants that did not complete the task, WinSnort stands out on these measurements, and scores 0. Some utilities did not even require any configuration time at all. These were operative from the moment they were installed.

The graph A-2 illustrates the method of detection, whether they operate in real-time or just make periodical controls of the system. The spyware removal tools, Spybot S&D and Ad-aware were the countermeasures that did not operate in real-time.

Most of the utilities and methods are free, (graph A-3), but note that some of the utilities are available in "pro" versions which are not free, and some of the free utilities are "donation ware". ZoneAlarm, Outpost and Norton Antivirus do cost from $40 to $50, where Norton Antivirus demands a yearly fee for updating the software and definitions. For the average user, free tools and methods are much more preferable to commercial ones, if they protect the computer sufficiently.

The fourth graph, A-4, in Figure 3, shows the score of which category of spyware the countermeasures support. The graph is naturally dependent on the defined categories that are blocked, such as blocking cookies through configuring the browser policy, which block only cookies. Countermeasures such as using antivirus software may protect against several categories of spyware. ZoneAlarm and IE-Spyad top this graph.

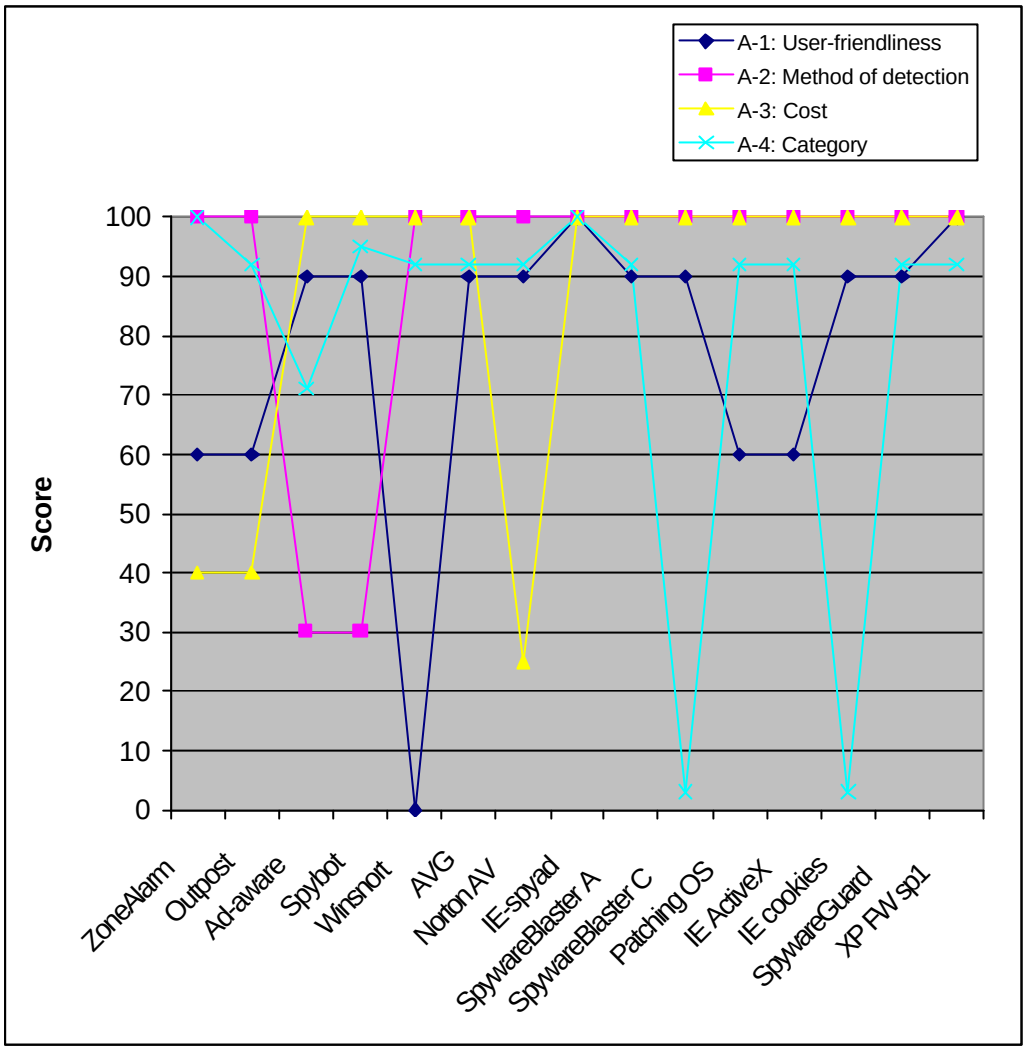


Figure 3. Results A-1, A-2, A-3, and A-4

6.3.2 Results A-5, A-6, and A-7

The results show that the commercial firewalls are ahead of the other countermeasures when it comes to block installation of spyware or blocking their operation. SpywareGuard, which claims to protect a system against spyware and block it from getting installed, scores really low on all 3 metrics in Figure 4. As one may have expected, the spyware removal tools scored best in the removal metric (A-6). The spyware removal tools also scored best in the detection metric (A-5), where the Intrusion Detection System WinSnort was ranked as number 6, outperformed by firewalls such as ZoneAlarm and Outpost, and anti-virus software such as Norton Antivirus.

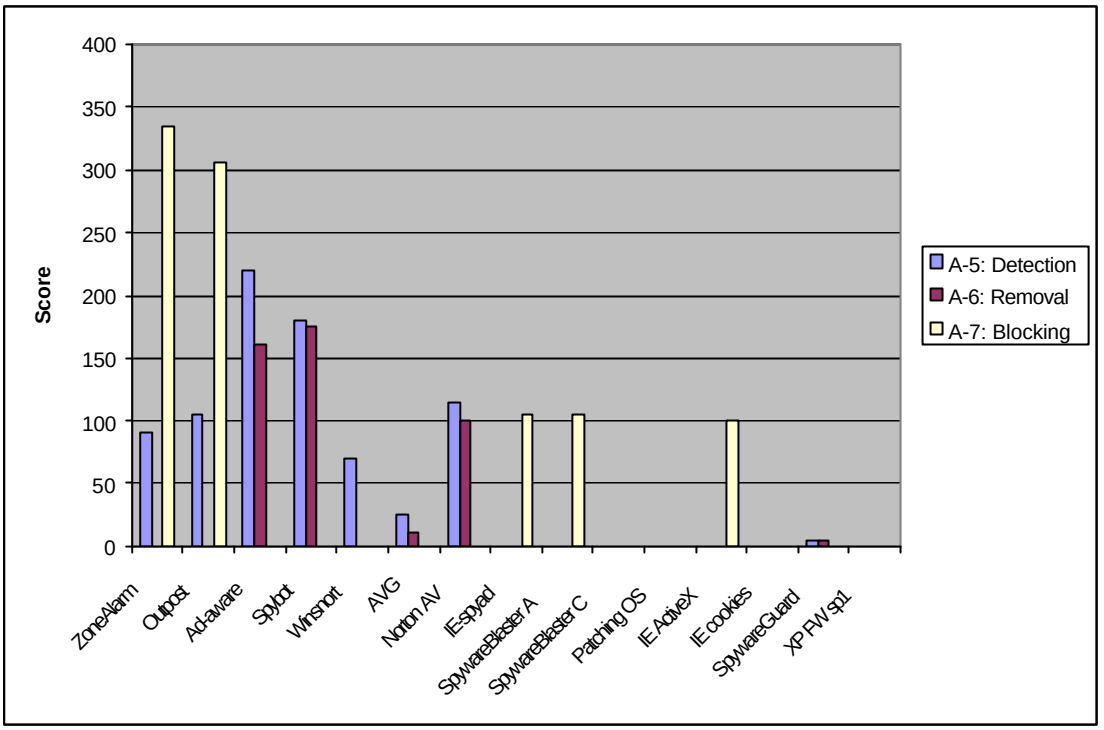


Figure 4. Results A-5, A-6, and A-7

6.3.3 Results A-8

The results from the false positive metric A-8 (Figure 5) show that there are no countermeasures that stand out as critically unreliable when reporting spyware. Configuring browser settings to block cookies results in blocking all cookies that meet the policy, potentially generating a lot of false positives, but the value of one falsely claimed tracking cookie is not severe.

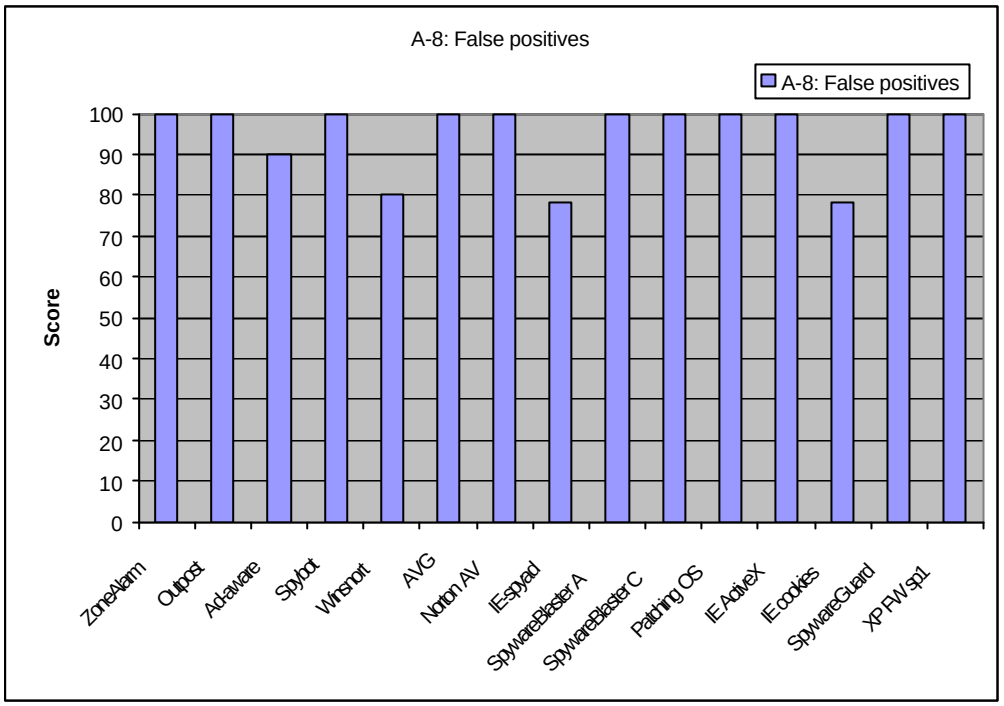


Figure 5. Results A-8

6.3.4 Results summary

Of all the tested countermeasures, ZoneAlarm was the best. Figure 6 shows that the firewalls and spyware removal tools scored above 750, and blocking of cookies doesn't give the desired protection against spyware alone, scoring lower than Windows XP firewall SP1, a countermeasure that did not detect, or removed, or blocked any spyware.

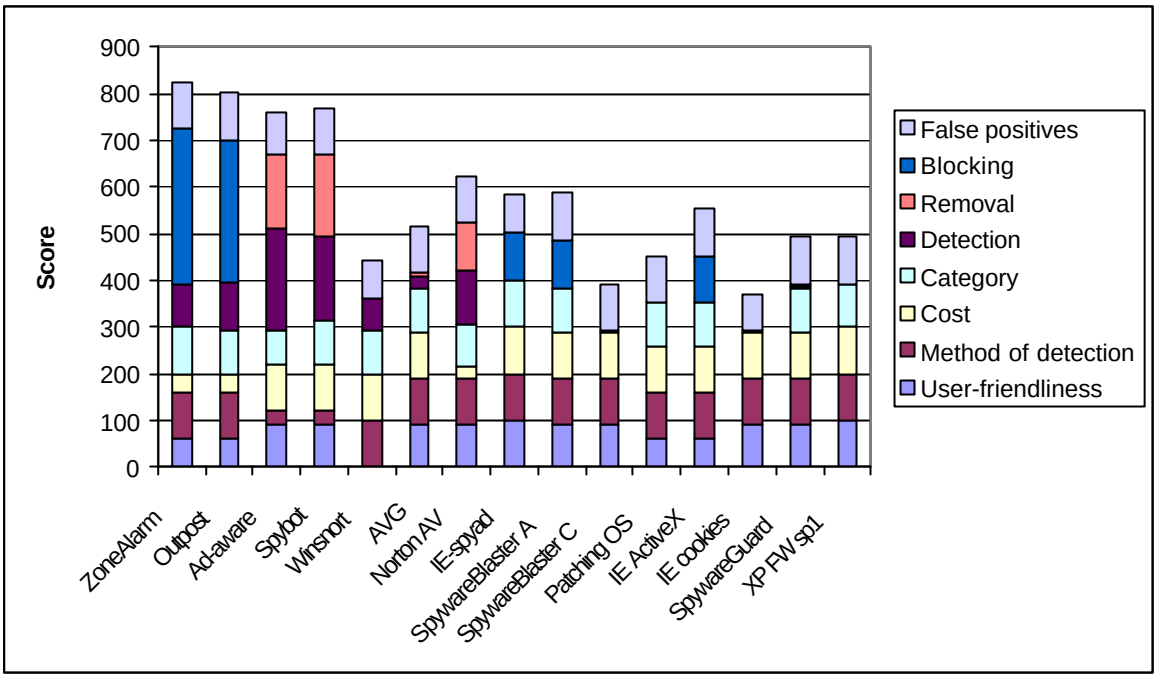


Figure 6. Result summary

The differences in effectiveness of the categories of countermeasures are presented in Figure 7. It shows that the commercial firewalls are just ahead of the spyware removal tools. The test also shows that anti-virus software, ActiveX blocking, and blocking of suspicious sites scores somewhat the same, between 570 and 580.

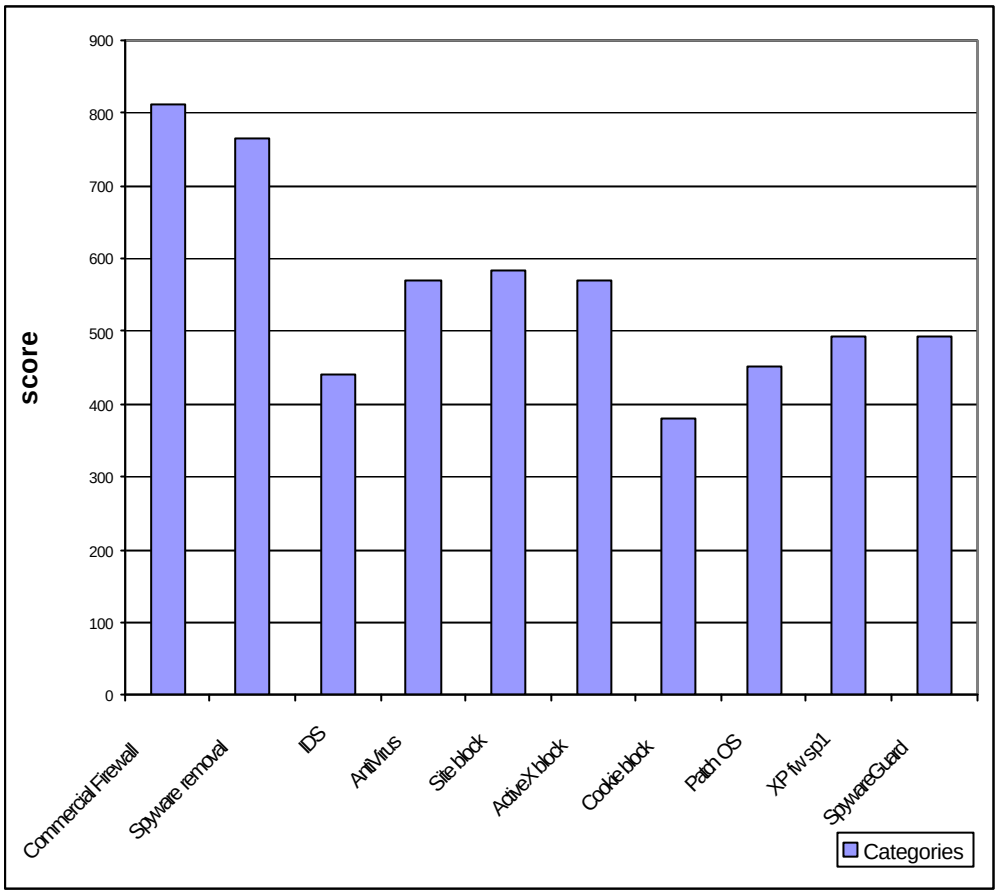


Figure 7. Overall score by category

The firewalls and spyware removal tools got quite well off compared to the other countermeasures, but this image should be compared against the theoretical maximum score (Figure 8), which is 2000, leaving the best countermeasure about 40% of the theoretical maximum score.

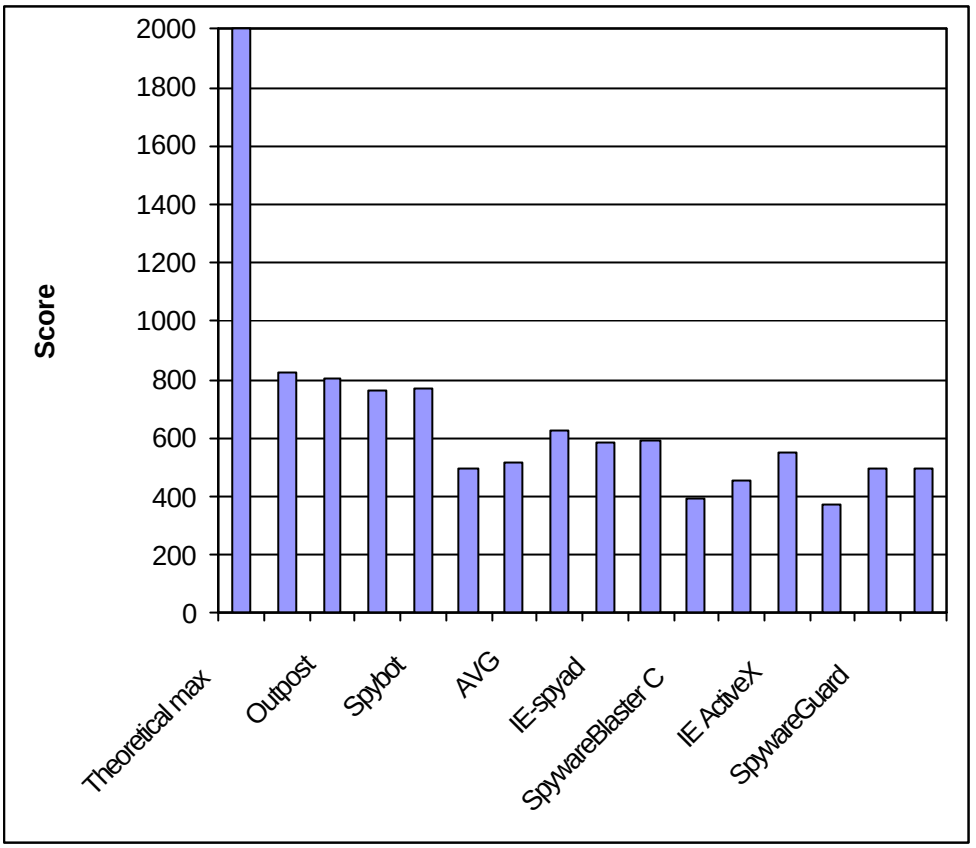


Figure 8. Total score including theoretical max score

The countermeasures have different strength in protecting a computer system, as Figure 9 shows. Several countermeasures score high on blocking spyware installation from drive-by downloads. IE-Spyad, IE ActiveX, SpywareBlaster ActiveX, and ZoneAlarm scored or were close to the maximum value. The commercial firewalls scored best in blocking bundled spyware installations, and not surprisingly the spyware removal tools detected most instances of both bundled and drive-by spyware.

ZoneAlarm with privacy protection blocked all the drive-by downloads, and scored among the best at blocking bundled spyware, but the privacy protection in this firewall doesn't identify any harmful instances. It works just like IE and blocks all of the chosen threats (cookies, ActiveX, scripts etc.). Ad-aware scored best at detecting the spyware that were installed through drive-by downloads. The spyware removal tools were the best in removing the installed spyware, both bundled and drive-by. The IE-Spyad scored high at blocking drive-by downloads and this countermeasure actually identified the suspicious sites. In such a way, any clearly non-harmful web sites may operate as usual. The blocking of web sites doesn't block the access to the sites. Rather it blocks certain functions at it, such as cookies or ActiveX. SpywareBlaster identifies certain ActiveX controls and tracking cookies, which seems to work quite well at blocking drive-by downloads (see Figure 9).

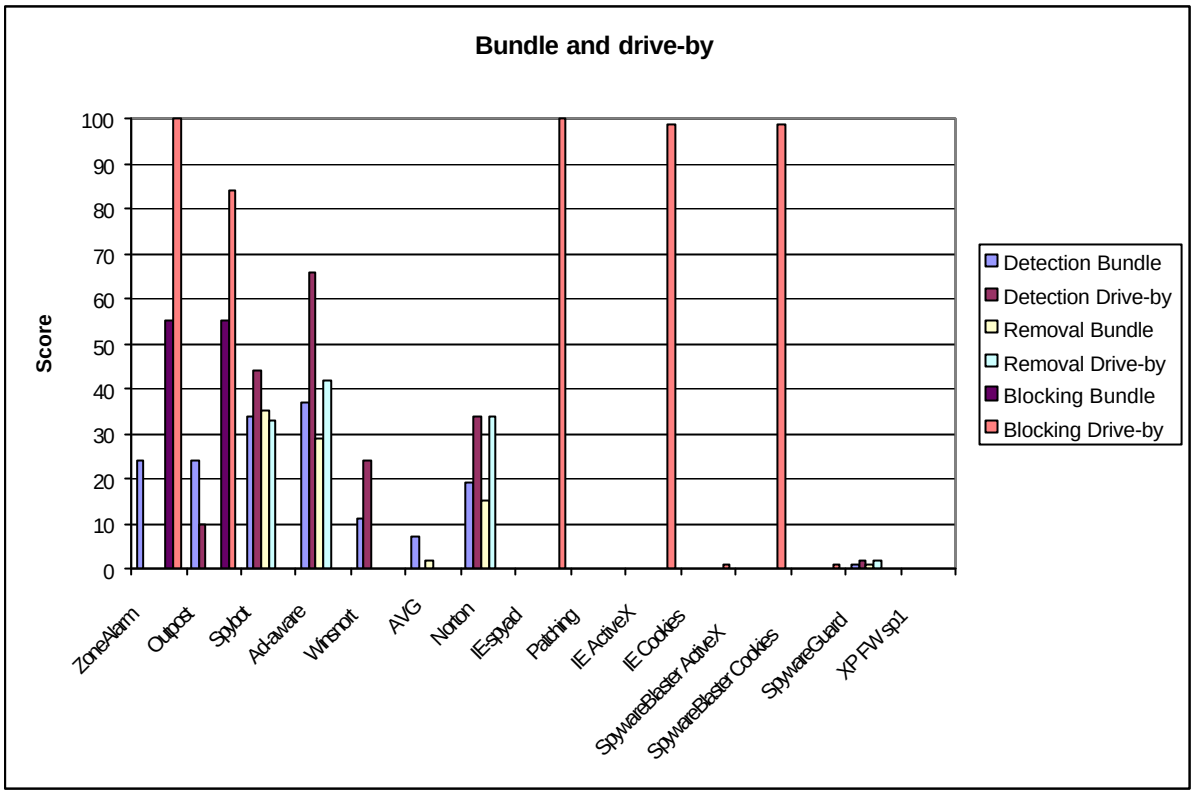


Figure 9. Results -bundle and drive-by

6.4 Further comments regarding experimental results

The installation of 3rd party software is mentioned in the Grokster EULA, but the software is as mentioned in Appendix B defined as spyware/adware. Spyware that do not operate within 10 minutes after installation of Grokster or drive-by downloads are not counted for in this project.

The experiment revealed that there was one basic infection, and in some cases this basic infection was extended with some "extra" spyware components which were identifiable by the monitoring systems implemented. The random infection was more obvious when experimenting on drive-by downloads. In particular one site, keygen.us, was distributing an extended flora of spyware, but these instances were identifiable by a different layout at the web site, and the monitoring tools implemented confirmed the presence and absence of spyware.

The firewalls do not define a process as illegitimate or harmful. They simply enlighten the user that a certain processes are present. However, the firewall presents advices how to handle some of the processes. The use of ZoneAlarm as a spyware countermeasure requires some understanding and knowledge of what processes are legitimate for outbound and inbound connections. False negatives may be more relevant for such countermeasure. The ZoneAlarm has the option to remember previously accepted and rejected processes, making it allowing processes that may be hijacked or accepted by a mistake.

Some of the installation processes operate on the local computer; they do not attempt to reach the network, and therefore are undetectable by the tested firewalls. The toolbar/BHO called MyBar/MyWay was not successfully blocked by the firewalls since the corresponding installation was not connecting to any external servers.

The firewall detected several processes that tried to reach the network, and these were blocked. However, the "child files" of these processes were installed despite the blocking. This may indicate that the attempts to reach the network areconnections for reporting to external servers and not downloading attempts. One process, "i$$.tmp", seemed to be affected by the connection blocking. The "sskupdater.exe" was blocked and the file "ssk.exe" was not reported to be present on the computer.

The SurfSideKick spyware operates partly from randomly named tmp-files, but seems to consist of 3 letters and/or numbers, beginning with "i"; i$$.tmp. The temp files have the ability to write to files and delete them (see Appendix F). The "i$$.tmp" process were detected by the commercial firewalls. SurfSideKick was at the beginning of this project not addressed or targeted by many spyware removal tools, but was included in the latest definition files used by tools like Spybot S&D and Ad-aware in this project.

Grokster seemed to be dependent on allowing "setup.exe" to connect to the network, which means that this process and the spyware components it installed had to be left out from the reference system when assessing the firewalls.

The Outpost firewall blocked 16 processes from operating (which would potentially transmit personal information), and prevented sskupdate.exe and ssk.exe from installing. There were limited downloads from keygen.us in the Outpost experiment, revealing a different version of CoolWebSearch than we have dealt with in earlier experiments. This time it tries to hijack the browser's home page and search page. The attempt was monitored by FileMon, RegMon, and CommView which logged the initial spyware installation attempts. A full version of the installation was monitored at a later stage.

By detecting the iinstall.exe at Lyricsdomain.com and preventing it from connecting to Internet prevents it from installing further software into the system. The iinstall.exe file (mis-pro-09) would have installed WebRebates, Sais, Internet Optimizer, YourSearchBar, istsvc, and PowerScan if it gained access to Internet (Figure 10). ZoneAlarm protects the system as well as Outpost does when it comes to bundled spyware. It seems like the spyware install through ActiveX controls, and by blocking all ActiveX controls these spyware don't get installed on the computer. In the experiment assessing the ZoneAlarm firewall the privacy protection was enabled, and therefore it seems obvious that this countermeasure has a better effect on preventing drive-by downloads compared to the experiment with Outpost firewall. The "iinstall.exe" file needs to connect to Internet for completing its installation, and therefore this may not be representative for all drive-by downloads; it is very likely that drive-by based spyware are installed directly from the software that was downloaded through e.g. ActiveX.

The firewall incorporated with Microsoft Windows XP Professional did not seem to have any effect on the spyware propagation when the spyware is bundled with another software. Note that the test operates on the default settings in the firewall and may therefore not represent the optimal protection that the firewall is capable of.

Ad-aware detected the process of Spybot S&D as an instance of 180solutions (clearly a false positive), but this is expected to be just a mistake by Ad-aware's author Lavasoft and will be fixed in later versions.

While testing IE-spyad (blocking certain functions at web sites), no dysfunctions on any sites were reported. They seemed to load even better when some of the potentially harmful functions were blocked. The effectiveness of this countermeasure depends on the accuracy of the list of suspicious sites. Logically thinking, it is not possible to list 100 % of the suspicious sites, or that all listed sites actually are distributing harmful software. The update frequency of such programs is important for maintaining a high degree of security.

Mis-pro-1 origins from an installation performed by visiting www.lyricsdomain.com and the file "iinstall.exe"; a temporary file that also installs istsvc.exe and ysb.dll. Bpt.exe is related to BroadCastPC.

There were some differences between the countermeasures that are based upon signatures for detecting spyware. For instance, Ad-aware did not target P2P networking as spyware, and Spybot did. Ad-aware detected by definition the P2p networking process, but no registry entries or other files related to this software were triggered on. Ad-aware did not define some of the processes as illegitimate, but they were indeed present in the list of running processes, and therefore have to be defined as a detection to conform with the firewall detections of processes.

The 3 instances of spyware SpywareGuard detected and removed were all Browser Helper Objects, namely MyBar.dll, AdRoar.dll, and XML.dll.

Spybot detected the following executable files that were loaded into memory, but did not define them as illegitimate processes; points manager.exe, asm.exe, wast2.exe, breg.exe, btv.exe, xcpy1.exe, vmss.exe, webCpr1.exe, webCpr0.exe, and webRebates0.exe. It seems that Spybot removes more entries than it reports detected, which may indicate that Spybot reports entries that are representative for each detected spyware.

Norton AV detected the WebCPR0.exe and WebCPR1.exe, but was not able to permanently remove them. They were re-installed on reboot. 2 instances of Mis-pro-08 were installed, one named jNmr3Tj.exe and one named istsvc.exe (though this is not the original istsvc.exe process). The AKlsp.dll is a Winsock LSP hijacker. Removing this may affect the network connection.

After patching the OS, the policies are set to accept all cookies, prompt when unsigned ActiveX-controls are found, disable XP firewall, and disable pop-up blocker. This experiment theoretically evaluated how well patching of weaknesses protects against spyware that uses exploits for its propagation. The updates made are listed below:

> Windows XP Hotfix
> KB867282, KB873333, KB873339, KB885250, KB885835, KB885836, KB886185, KB887472, KB887742, KB888113, KB888302, KB890047, KB890175, KB891781
>
> Microsoft .NET Framework 1.1
> Service Pack 1 (KB867460)

This may indicate that the spyware bundled or spyware downloaded when visiting web sites operates on ActiveX controls and not on weaknesses in the OS.

The tested IDS WinSnort alerted GMT, Points Manager, SSK, WebRebates, P2P, and myWebSearch toolbar activity. Further, WinSnort alerted "web-misc Lotus_Notes .exe script source download attempt" and "Amex.ipsrime.com unknown malware download" several times. The creators of these "bleeding" rules clearly specified that these rules may not be stable. When surfing the specified web sites, WinSnort detected Internet Optimizer, YourSiteBar activity, WebRebates, and another piece of spyware, named "ak-networks spyware" in the Bleeding-rules, and referred to the rundll32.exe process. This process is related to the Winsock LSP aklsp.dll[14]. The accuracy of WinSnort is dependent on the signatures defined in the rules, and which rules are enabled. In this experiment, the standard rules were applied, except the disabling of the "uPnP Scan" at the Scan rule. The external rules from Bleeding were also applied. An IDS is not ment to detect all instances of an attack. It generates an alarm if an attack is present without going into details about the attack.

When testing IE ActiveX the IE was configured not to accept unsigned or signed ActiveX controls, not to run ActiveX controls or plug-in modules, and disable use of scripts on ActiveX controls.

An error occurred when a certain ActiveX component was blocked after the installation of spyware was completed. The version 9.0 of Windows MediaPlayer popped up on the desktop but it failed to play the intended video clip. The presence of the file "msiexec.exe" indicates that there was a background installation of software, and shortly after the version 9.0 of Windows MediaPlayer started. The BroadCastPC is known to download video clips and show them from the desktop (independently from IE browser activity) [56].

The registry was close to be untouched after testing IE ActiveX against drive-by downloads, enabling only the tracking cookies to reach the system. Some of the pages (chanceforlove.com) did not show at all, this due to the design of the web site; the whole site was embedded into a script. This experiment may not be 100% valid, since it is difficult to identify the presence of certain spyware programs. There are some randomness in these drive-by downloads, such as different pop-ups are shown, and to differentiate these one may only assume what spyware programs it tried to install.

The file creations performed by spyware that infected the system through drive-by downloads at lyricsdomain.com are illustrated in Figure 10.

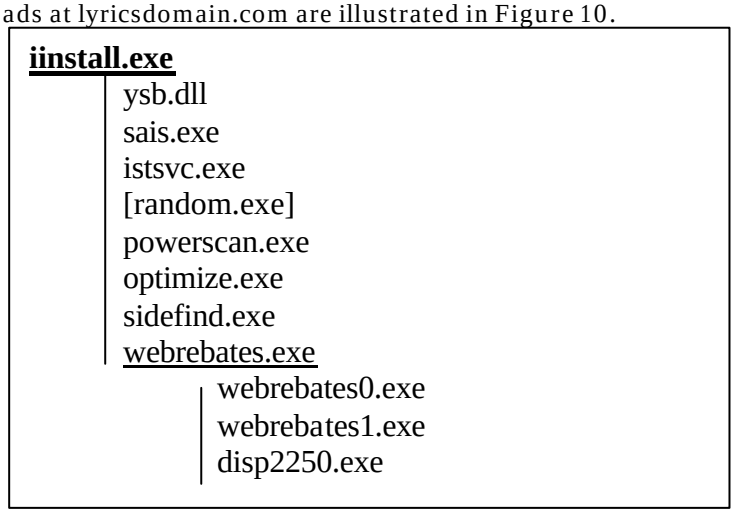


Figure 10. File creation drive-by - downloads

[14] Verified at: http://www.superadblocker.com/R/RUNDLL32.EXE-1030.html

The file creations performed by the spyware bundled with Grokster are illustrated in Figure 11. More details are listed in Appendix F.

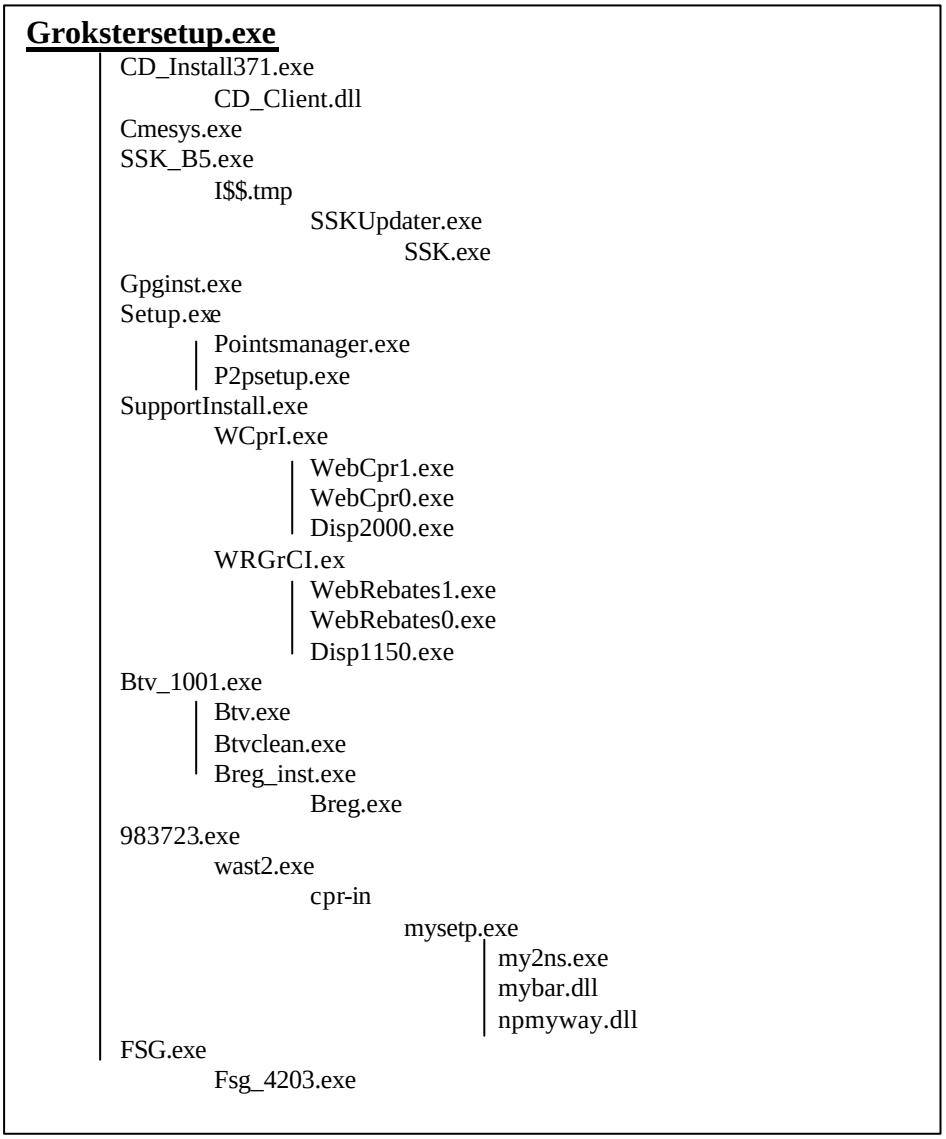


Figure 11. File creation – bundle

If we define all the metrics to score a 100, the countermeasure score would be as presented in Figure 12. In this case the Windows XP firewall scores better than blocking cookies and anti-virus products. The Windows XP firewall is a free utility once we've purchased the Windows XP OS. It does not detect, remove, or block any spyware. Further, there are no specific differences in protection effectiveness between the countermeasures. By designing the metrics this way, the time consumed in configuring the countermeasures, cost, category, and method of detection dominate the total score. Therefore the detection metric, removal metric, and the blocking metric score more than the others, suggestively between 400 and 500 on each metric.

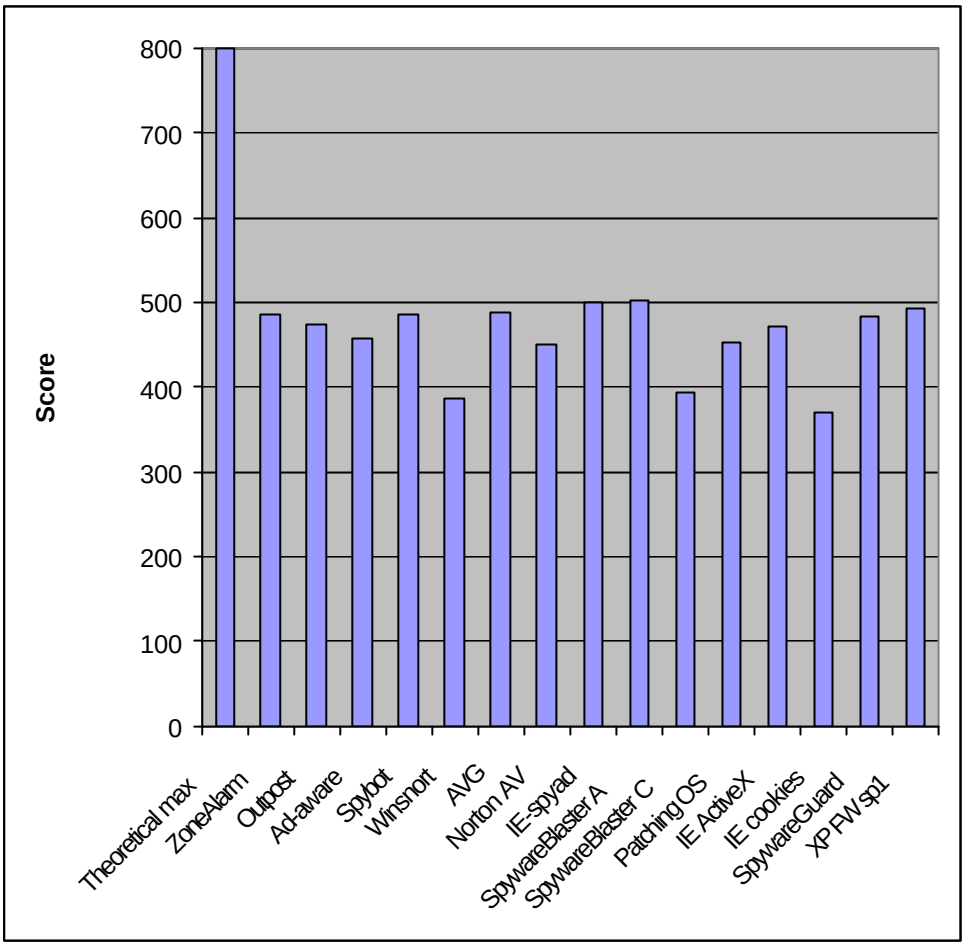


Figure 12. Countermeasure score 100

As mentioned earlier, the countermeasures may not be optimally configured. Outpost firewall was intentionally configured to disable the privacy protection mechanisms that the product presents to a user.

7 Discussion

Howes [50] does not share the view of the spyware classification defined in this thesis; while we categorize spyware to include for example hijackers, cookies and LPSs, [52] argues for defining spyware as software that purely collects information for marketing purposes only, leaving out keyloggers and alike, and belonging to a wider term called "crapware". The results presented at the workshop at FTC [64] disagree with Howes and include the keylogger into the definition of what constitutes spyware.

One may discuss whether the third metric "Cost" should be present in such an assessment. The cost of the countermeasure does not directly affect the security performance of the countermeasure. The average user may first of all prefer free utilities and methods for protecting their privacy and reuse existing tools that they already possess. It is not likely that a user that occasionally uses his or her computer on the Internet will install and configure an Intrusion Detection System, which may be confirmed by the relatively high time consumption while configuring (Figure 3).

Defining true positives is not an easy task. Relying on existing resources and monitoring tools it is not unlikely that mistakes are done.

One may discuss and disagree on the maximum score where one adds the maximum score of all the metrics since blocking spyware installation prevents a detection possibility of the blocked spyware. Theoretically a countermeasure may detect a spyware component, block it from operating, and then remove it from the system.

Other metrics that may be included at a later stage are the amount of known signatures or the frequency of signature updating. A metric of that kind would not apply all of the countermeasures that we have defined, and therefore it was not used in this project. Another metric could be the countermeasures' impact on the system and system resources. A metric that calculates and assesses the extra CPU-load would distinguish "heavy" and "light" countermeasures, quite important on already slow computers.

One should be cautious to use literatures that are several years old. The rapid changes within this topic reduses the validity of such outdated literature.

8 Conclusions

This is the first time, to the author's knowledge, that metrics have been designed to specifically assess countermeasures against spyware, though there have been some tests about the effectiveness of spyware removal tools in particular.

The values of the metrics show that the personal firewalls, except Windows XP firewall, and spyware removal tools were the most effective in protecting against spyware, as one might have expected. The defined metrics are of general purpose, and therefore new countermeasures should be easily included.

The metric assessment is defined, the measurements are repeatable and reproducible, and they are useful for decision makers. The metrics cover the aspects of user-friendliness, capability, and performance of countermeasures. The effectiveness of the metrics is dependent on the monitoring tools used, and the spyware they are tested upon. It should be stressed that there are no random spyware installations to ease the

analyzing process. It is possible to compare various countermeasures at a different time if and only if the spyware reference is not of random being. Thus any comparisons of the effectiveness of countermeasures should be facing newly developed and discovered spyware. Spyware programs that install an enormous amount of files or generate a lot of registry entries should be avoided if possible, this to ease the analysis part of the comparison.

The software firewalls scored well in this experiment, this in contradiction with [64] where it is stated that *"Although firewalls are important for computer security, a panelist explained that they provide limited protection from spyware*". The statements are based on the fact that a firewall only looks at certain attributes of incoming transmissions. The workgroup does not conclude that a firewall is worthless as a countermeasure against spyware, because it has the ability to alert a user when outbound connections are established. Connections that might origin from spyware already installed on the computer may not be reported. The effectiveness of a firewall will be dependent on how the experiments are designed. Our experiment involved spyware that opened connections to external servers, and thereby had the ability to detect and prevent spyware installation.

Countermeasures that blocks suspicious web sites are preferable in a countermeasure combination against spyware. The IE-Spyad blocks spyware that propagate through ActiveX or cookies, but leaves the other components untouched (components that propagates through security weaknesses, bundled spyware or alike). A personal firewall will protect the system in real-time, potentially block installation of spyware or its operation. Spyware removal tools, like Ad-Aware and Spybot S&D, are designed to detect and remove such components. As mentioned one spyware removal tool does not detect all the installed spyware components, at least two programs of this kind are preferable. One may also consider SpywareBlaster, this tool protects against both cookies and ActiveX downloads, though not against bundled spyware.

It should offer a reasonable privacy protection, protecting against both bundle and drive-by downloads, and has abilities to detect the presence of spyware, remove, and block the operation of spyware or the installation of them. The combination operates on known spyware, meaning that legitimate functions and operations are still able to do their work. Note that the ZoneAlarm firewall had its privacy protection enabled and Outpost the privacy protection mechanisms disabled, so that these countermeasures would likely score equal if both privacy protection mechanisms were disabled. The author sees no point in adding the score of these countermeasures, because the countermeasures then would have addressed the same spyware instance several times and the score would not represent the true values. The tested countermeasures in this project may not be representing the best utilities or methods that are available within each countermeasure category. For this, more methods and utilities should be tested.

The time consuming part of a project of this kind is to detect all the true instances of spyware, the registry entries, the file creations, and the processes that they generate. Monitoring tools like FileMon and RegMon from sysinternals.com came handy in this project along to Active Registry Monitor from SmartLine Inc. to compare the registry entries before the infection and afterwards. The monitoring of spyware infection must be performed on each period of experiments, this due to the rapid changes in the "spyware business". A setup file like Grokster's connects to an external server and downloads the file sharing application. The download also distributes spyware, and since we do not have any control of the software that are being downloaded from the external server, we cannot be sure that the exactly the same spyware components are installed every time, at least not when several months have passed since the last analysis. So it is important that the experiments and log collections are done within a short period of time, preferably confirm the status with a monitoring tool like a passive

personal firewall that notifies the user of any network connections (on other countermeasures than the firewall the connections must be accepted, else the experiment would not be valid). If there are sufficient amount of spyware components, new countermeasures may be directly compared to the previous ones.

Bundled spyware that infests a system through software that are located locally on the computer the monitoring tool InCtrl5 would be reasonable to use for monitoring the installation process, logging every file access, file creation, registry entries. This program was somewhat difficult to use on Grokster since it downloaded an external setup file in the temporary catalog. Anyone who wants to retest this method should be sure of that the installed spyware, bundled or drive-by, is the same every time one tests a countermeasure to ease the analyzing part of the project.

Some of the countermeasures' scores are dependent on the time the countermeasures are operative. For example, Ad-aware detects an installation process while scanning the system, but if Ad-aware is run after the installation, it cannot detect the installation process, and therefore there are some uncertainties in the scores of such countermeasure like Ad-aware.

The results given by the metrics are reproducible and repeatable if the same flora of spyware is used for each countermeasure. The effectiveness is dependent on the monitoring tools and the tools used when infecting a system, such as VMWare Workstation from vmware.com.

The metrics are reusable if new countermeasures are to be assessed, and the metrics are reusable if the spyware programs change, though not exceed the defined categories of spyware.

9 Further work

The metric should if possible be calibrated to represent true values for the effectiveness of the countermeasures, meaning the values for e.g. categories of spyware and values for processes, executive files and so on. The collection of metrics may also be extended with the mentioned metrics in chapter 7, if they are designed to be applicable with countermeasures in general.

The metrics could be tested and be either confirmed or disproved by external researchers. In this experiment, no spyware were installed through exploits, indicating that the amount of spyware experimented upon was not too little. Preferably this experiment should be extended with more spyware distributed from several applications like Grokster and more suspicous web sites.

A database of the countermeasure capabilities is desirable, in this way a new countermeasure may be compared to these "stored" results, and one effectively assesses the countermeasure by using the metrics on this specific countermeasure alone.

At the end of this project there was no free version of Grokster 2.6 available for installation. This option had been removed but the user was offered a 5 days free trial of Grokster 2.6 Pro. In this version, no external processes seemed to be installed, the installation itself was much faster than the free version, and no traffic to external servers was reported within 5 minutes of network monitoring, though a pop-up appeared and some packets were sent to Grokster.com when uninstalling the file sharing application. At the same time CNet Download.com alerted a "zero-tolerance"

of bundled adware that had nothing to do with the main program's intention or purpose.

10 References

[1] Synovate (2003), "*Federal Trade Comission – Identity Theft Survey Report*".
[2] Langweg, H and Snekkenes, E (2004), "A Classification of Malicious Software Attacks". *Proceedings of 23rd IEEE International Performance, Computing, and Communications Conference.*
[3] Gribble et al. (2004), "*Measurement and analysis of spyware in a university environment*", Dept. of Computer Science and Engineering, University of Washington, USA.
[4] Edelman, B (2004), "*Methods and Effects of Spyware*", Response to FTC Call for Comments, Harvard University, USA.
[5] Jacobsson et al. (2004), "*Privacy-Invasive software in filesharing tools*", Blekinge Institute of Technology, Sweden.
[6] Creswell, J. (2003) "*Research Design –Qualitative, quantitative and mixed methods approaches*", Sage publications, Inc.2.ed.
[7] Townsend, K. (2003), "*Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Securit*" (technical white paper), PestPatrol,
[8] Boldt et al. (2004), "*Exploring Spyware Effects*", Blekinge Institute of Technology, Sweden.
[9] Frost, B. (2000), "*Measuring Performance*", Measurment International, Revised Edition.
[10]Swanson et al. (2003), "*Security Metrics Guide for Information Technology Systems*", NIST *Special Publication 800-55*, http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf (accessed 25.january.05)
[11] Demuth,T and Ricke,A. (2000), "*Bilateral anonymity and prevention of abusing logged web addresses*." In 2000 Military Communications International Symposium, Los Angeles.
[12] Christodorescu, M and Jha, S (2003),"*Static analysis of executables to detect malicious patterns*", University of Wisconsin, USA.
[13] Borders, K and Prakash, A (2004), "*Web Tap: Detecting covert web traffic*", ACM 1-58113-961-6/04/0010.
[14] Erbschloe, M (2005),"*Trojans, worms, and spyware*", 1.ed., Elsevier Inc.
[15] Spy Bot S&D http://security.kolla.de (accessed 13.january.2005)
[16] Christodorescu, M (2002) "*Detecting malware patterns in executables via model checing*", Presentation notes, University of Wisconsin, USA
[17] Ashburn, M and Sulcoski, M (2004), "*NETSS: A networked environment for testing suspicious software*", Proceedings of the 2004 Systems and Information Engineering Design Symposium.
[18] Jha et al. (2001)"*Marcov chains, classifiers, and Intrusion Detection*", Computer Security Foundations Workshop (CSFW).
[19] Jha et al. (2004) "*Buffer overrun detection using linear programming and static analysis.*" IEEE Symposium on Security and Privacy.
[20] Christodorescu, M and Jha, S (2004) "*Testing Malware Detectors*", International Symposium on Software Testing and Analysis.
[21] McGraw, G and Morriset, G (2000) "*Attacking malicious code*", IEEE Software.
[22] Hallaråker, Ø (2004), "Spyware", Presentation notes, NTNU, Norway.
[23] Ames, W. (2004) "*Understanding spyware: risk and response*", IEEE Computer Society.
[24] Harrison, W. and Bollinger, T. (2004), "*User confidence –and the software developer*", IEEE Computer Security.
[25] Rosen, B. (2003),"*Infrastructural requirements for a privacy preserving Internet*", Yale University, Computer Science Department.
[26] Carmines, E and Zeller, A (1980),"*Reliability and validity assessment*", Sage publications ISBN: 0803913710.

[27] Base, R (2000), "*Intrusion detection*", Macmillian Technical Publishing.
[28] Websense Int. Ltd (2003), "*Emerging Internet threats survey 2003*", commissioned by Websense, http://www.websense.com
[29] McCardle,M (2003), "*How spyware fits into defense in depth*", SANS Institute.
[30] Acsac (2001), "*Workshop on information-security-system rating and ranking (WISSRR)*", workshop sponsored by Applied Computer Security Associatives (ACSA) and the MITRE Corporation, 1st ISSRR, http://www.acsac.org/measurement
[31] Payne, S (2001), "*A guide to security metrics*", SANS Institute 2002.
[32] Vaughn, Jr et al. (2002), "Information assurance measures and metrics – state of practice and proposed taxonomy", Proceedings of the 36th Hawaii International Conference on System Sciences.
[33] Porter,W (2005), "*Identity theft and spyware – the new threat*", XBlock.com http://www.xblock.com/articles/article_show.php?id=19 (accessed 08.feb.2005)
[34] Statistisk Sentralbyrå (2004), "Tre av ti husholdninger har bredbånd", http://www.ssb.no/ikthus/ (accessed 08.february.2005)
[35] Earthlink, Inc (2005), "*Earthlink spy audit*", https://www.earthlink.net/spyaudit/press/ (accessed 08.february.2005).
[36] Better Business bureau (2005) "*New Research Shows That Identity Theft Is More Prevalent Offline with Paper than Online*", http://www.bbb.org/alerts/article.asp?ID=565 (accessed 08.febrary.2005).
[37] Consumer Webwatch (2003) "*Five Major Categories of Spyware*", http://www.consumerwebwatch.org/news/articles/spyware_categories.htm (accessed 15.december.2004).
[38] TopTenReviews (2005), "*Anti-spyware software review*", http://www.anti-spyware-review.toptenreviews.com/ (accessed 08.february.2005).
[39] Cexx.org (2004), "*Foistware / Spyware - Gator, OfferCompanion, Trickler, GAIN*", http://www.cexx.org/gator.htm (accessed 08.february.2005).
[40] SpywareGuide.com (2004), "SaveNow", http://www.spywareguide.com/product_show.php?id=18 (accessed 09.feb.2005).
[41] SCMagazine.com (2004), "*The need to define malware*", http://www.scmagazine.com/features/index.cfm?fuseaction=FeatureDetails&newsUID=0e2c9ecf-e8ef-4d42-8f06-2e7d30bdcbe4&newsType=Features (accessed 09.february.2005).
[42] eWeek.com (2004), "*Study: Tools Let Spyware Slip Through Cracks*", http://www.eweek.com/article2/0,1759,1731474,00.asp (accessed 09.february.2005).
[43] SpywareGuide.com (2004), "Spyware block list file", http://www.spywareguide.com/blockfile.php (accessed 09.february.2005).
[44] Microsoft.com (2004), "*How to Stop an ActiveX Control from Running in Internet Explorer*", http://support.microsoft.com/?id=240797 (accessed 09.february.2005).
[45] Howes, E (2004), "*Anti-spyware testing*", http://spywarewarrior.com/asw-test-guide.htm (accessed 09.february.2005).
[46] Giblin, P (2004), "*Malicious intent*", Modbee.com http://www.modbee.com/business/story/9251564p-10154894c.html (accessed 09.february.2005).
[47] Brandt, A (2004), "*Poor defenders*", PCWorld.com, http://www.pcworld.com/news/article/0,aid,118362,pg,1,00.asp (accessed 09.february.2005).
[48] Trustix (2004), "*Trustix personal firewall spyware*", http://www.personalfirewall.trustix.com/spyware/transponder.html (accessed 12.february.2005).
[49] Edelman, B (2005), "*DirectRevenue Deletes Competitors from Users' Disks* ", http://www.benedelman.org/news/120704-1.html (accessed 141.february.2005).
[50] Howes, E (2004), "*Targeting & inclusion policy*", https://netfiles.uiuc.edu/ehowes/www/target-policy.htm (accessed 15.feb.2005).

[51] Howes, E (2004), *"Rogue/suspect anti-spyware products & web sites"*, http://www.spywarewarrior.com/rogue_anti-spyware.htm (accessed 14.february.2005).
[52] Edelman, B (2004) *"Grokster and Claria Take Licenses to New Lows, and Congress Lets Them Do It"*, http://www.benedelman.org/news/100904-1.html (accessed 14.april.2005).
[53] Agnitum.com (2 005), *"Outpost Personal Firewall Pro Features"*, http://www.agnitum.com/products/outpost/features.html (accessed 17.february.2005).
[54] PCWorld.com (2004),*"IE-Spyad"*, http://www.pcworld.com/downloads/file_description/0,fid,23332,00.asp (accessed 21.february.2005).
[55] Symantec (2005), *"Norton AntiVirus 2005"*, http://www.symantec.com/nav/nav_9xnt/ (accessed 21.february.2005).
[56] Doxdesk (2005), *"Parasite information database"*, http://www.doxdesk.com/parasite/database.html (accessed 16.february.2005).
[57] Allworldsoft.com (2005), *"Remote Keylogger 2.7"*, http://www.allworldsoft.com/software/13-697-remote-keylogger.htm (accessed 19.april.2005).
[58] Edelman, B (2004), *"Exact Advertisers"*, http://www.benedelman.org/spyware/exact-advertisers/ (accessed 19.april.2005).
[59] Cottonwood Police Department, (unknown), *"What is identity theft?"*, http://www.cottonwoodpd.org/detective_tips.htm (accessed 21.april.2005).
[60] NetworkWorldFusion.com (Radcliff, D) (2004), *"How to filter Port 80 traffic"*, http://www.nwfusion.com/research/2004/0126spyport80.html?fsrc=rss-howto (accessed 21.april.2005).
[61]PCWorld.com (Thurrot,P) (2004), *"Windows XP's Big Security Fix"*, http://www.pcworld.com/news/article/0,aid,114593,00.asp (accessed 22.april.2005).
[62] IT Manager's Journal (Lyman, J) (2005), *"Adware market booming to the tune of $billions"*, http://software.itmanagersjournal.com/article.pl?sid=05/04/20/201239&from=rss (accessed 24.april.2005).
[63] Nzeka Labs (2005), *"KSpyware"*, http://cksecurity.free.fr/hacking/KSpyware.htm, (accessed 24.april.2005).
[64] Spyware Workshop (2005), *"Monitoring software on your PC: Spyware, Adware, and other software"*, Federal Trade Commission.
[65] Howes, E (2004), "Privacy policy", https://netfiles.uiuc.edu/ehowes/www/priv-pol.htm (accessed 03.may.2005).
[66] Owens, M (2002), *"A discussion of covert channels and steganography"*, SANS Institute.
[67] Rownland, C (1996), *"Covert channels in the TCP/IP protocol suite"*, First Monday, http://www.firstmonday.org/issues/issue2_5/rowland/ (accessed 03.may.2005).
[68] Utah state legislature (2004), *"Spyware regulation – Spyware control act"*. 13-39-101 to 13-39-201, http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.pdf, State of Utah.
[69] Merijn (2005), *"HijackThis log tutorial "*, http://www.spywareinfo.com/~merijn/htlogtutorial.html, (accessed 03.june.2005).
[70] Salkind, N.J. (2003), *"Exploring research"*, 5th ed. Prentice Hall.

Appendix A – Spyware bundled with Grokster, and drive-by spyware

HKCR = HKEY_CLASSES_ROOT
HKLM = HKEY_LOCAL_MACHINE

Altnet		
Process	**Alt-pro-01** **Alt-pro-02** **Alt-pr0-03**	C:\program files\Altnet\Download Manager\asm.exe C:\program files\Altnet\Points Manager\Points Manager.exe Setup.exe (installation process)
Exe	**Alt-exe-01** **Alt-exe-02**	C:\program files\Altnet\Download Manager\adm4005.exe C:\program files\Altnet\Download Manager\asmend.exe
Dll	**Alt-dll-01** **Alt-dll-02** **Alt-dll-03** **Alt-dll-04** **Alt-dll-05** **Alt-dll-06** **Alt-dll-07** **Alt-dll-08**	C:\program files\Altnet\Download Manager\asmps.dll C:\program files\Altnet\Download Manager\adm4.dll C:\program files\Altnet\Download Manager\admdata.dll C:\program files\Altnet\Download Manager\admdloader.dll C:\program files\Altnet\Download Manager\admfdi.dll C:\program files\Altnet\Download Manager\admprog.dll C:\program files\Altnet\Download Manager\adm25.dll C:\program files\Altnet\Points Manager\sysdetect.dll
Run	**Alt-run-01**	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ AltnetPointsManager
Bho		(TopSearch.dll)
Reg	**Alt-reg-01** **Alt-reg-02** **Alt-reg-03** **Alt-reg-04** **Alt-reg-05** **Alt-reg-06** **Alt-reg-07** **Alt-reg-08** **Alt-reg-09** **Alt-reg-10** **Alt-reg-11** **Alt-reg-12** **Alt-reg-13** **Alt-reg-14** **Alt-reg-15**	HKCR\CLSID\{1D3BCE37-7834-4579-8169-E67681420A98} HKCR\CLSID\{DEF37997-D9C9-4A4B-BF3C-88F99EACEEC2} HKCR\CLSID\{C15B7EA2-A360-43E8-A591-5FAEDC7C4E1D} HKCR\CLSID\{E813099D-5529-47F4-9B37-4AFAFCB00A43} HKCR\CLSID\{9bbcf06c-dcd7-495d-80df-cdd5399d0ff8} HKCR\CLSID\{3646C2BD-3554-49CA-8125-44DEEFB881DE} HKCR\CLSID\{3f4d4f88-0198-4921-b630-957f3eb814e0} HKCR\ADM.ADM HKCR\ADM.ADM.1 HKCR\ADM4.ADM4 HKCR\ADM4.ADM4.1 HKCR\ADM25.ADM25 HKCR\ADM25.ADM25.1 HKCR\signingmodule.signingmodule HKCR\signingmodule.signingmodule.1

BroadCastPC/BTV		
Process	**Bpc-pro-01** **Bpc-pro-02** **Bpc-pro-03** **Bpc-pro-04**	C:\program files\BTV\btv.exe C:\program files\common files\java\breg.exe c:\Program Files\bpc_search\BPCv2.exe btv_1001.exe (installation process)
Exe	**Bpc-exe-01**	C:\program files\BTV\breg_inst.exe

	Bpc-exe-02	C:\program files\BTV\btvclean.exe
Dll		
Run	Bpc-run-01 Bpc-run-02 Bpc-run-03	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "BTV" HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Breg" HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run “BPCv2”
Bho		
Reg		

AdRoar/Wast/Twain-Tech		
Process	AdR-pro-01 AdR-pro-02 AdR-pro-03	C:\windows\wast2.exe C:\windows\arupdate.exe C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\983723.exe (installation process)
Exe		
Dll	AdR-dll-01	C:\WINDOWS\AdRoar.dll
Run	AdR-run-01 AdR-run-02	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\wast “c:\windows\wast2.exe 2” HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\adroarupdate “c:\windows\arupdate.exe”
Bho	AdR-bho-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\Browser Helper Objects\{BDF6CE3D-F5C5-4462-9814-3C8EAC330CA8} - C:\WINDOWS\AdRoar.dll
Reg	AdR-reg-01 AdR-reg-02 AdR-reg-03	HKCR\CLSID\{BDF6CE3D-F5C5-4462-9814-3C8EAC330CA8} HKCR\AdRoar.Band HKCR\AdRoar.Band.1

Cydoor		
Process	Cyd-pro-01	cd_install_371.exe (installation process)
Exe		
Dll	Cyd-dll-01	C:\winnt\system32\cd_clint.dll
Run		
Bho		
Reg		

Gator/Gain/Claria		
Process	Gat-pro-01 Gat-pro-02 Gat-pro-03	C:\program files\common files\CMEII\CMESys.exe C:\program files\common files\GMT\GMT.exe fsg.exe (installation process)
Exe	Gat-exe-01 Gat-exe-02	C:\program files\common files\GMT\GatorStubSetup.exe C:\winnt\FT1_01_0_279_GEPFAH.EXE
Dll		
Run	Gat-run-01 Gat-run-02	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "CMESys" HKLM\SOFTWARE\Microsoft\Windows\currentversio

		n\run\Trickler “fsg_4203”
Bho		
Reg	Gat-reg-01	HKCR\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}

MyWay / MyBar		
Process	Myw-pro-01	mysetp.exe (installation process)
Exe		
Dll	Myw-dll-01 Myw-dll-02	C:\program files\MyWay\myBar\1.bin\MYBAR.DLL C:\program files\MyWay\myBar\1.bin\NPMYWAY.DLL
Run		
Bho	Myw-bho-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{0494D0D1-F8E0-41ad-92A3-14154ECE70AC} -C:\Programfiler\MyWay\myBar\1.bin\MYBAR.DLL
Reg	Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14	HKCR\CLSID\{014DA6C9-189F-421a-88CD-07CFE51CFF10} HKCR\CLSID\{0494D0D1-F8E0-41ad-92A3-14154ECE70AC} HKCR\CLSID\{0494D0D9-F8E0-41ad-92A3-14154ECE70AC} HKCR\CLSID\{014DA6CD-189F-421a-88CD-07CFE51CFF10} HKCR\CLSID\{0494D0D5-F8E0-41ad-92A3-14154ECE70AC} HKCR\CLSID\{0494D0D7-F8E0-41ad-92A3-14154ECE70AC} HKCR\CLSID\{0494D0DB-F8E0-41ad-92A3-14154ECE70AC} HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar "{0494D0D9-F8E0-41ad-92A3-14154ECE70AC}" HKCR\MyWayToolBar.NetscapeShutdown HKCR\MyWayToolBar.NetscapeShutdown.1 HKCR\MyWayToolBar.NetscapeStartup HKCR\MyWayToolBar.NetscapeStartup.1 HKCR\MyWayToolBar.SettingsPlugin HKCR\MyWayToolBar.SettingsPlugin.1

P2p networking		
Process	p2p-pro-01	C:\WINDOWS\System32\P2P Networking\P2P Networking.exe
Exe		
Dll	P2p-dll-01	C:\WINDOWS\System32\P2P Networking\MARSHAL.DLL
Run	P2p-run-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ p2p networking.exe
Bho		
Reg	P2p-reg-01 P2p-reg-02 P2p-reg-03	HKCR\CLSID\{CC7A6223-3759-4075-8CEA-971F5CFC0ED2} HKCR\CLSID\{C91E8926-D4BE-4685-99F4-

	P2p-reg-04 P2p-reg-05 P2p-reg-06	0D996B96BAC0} HKCR\CLSID\{1D6711C8-7154-40BB-8380-3DEA45B69CBF} HKLM\SOFTWARE\microsoft\code store database\distribution units\{1d6711c8-7154-40bb-8380-3dea45b69cbf} HKCR\webp2installer.installer HKCR\webp2installer.installer.1

TopSearch		
Process		
Exe		
Dll	Top-dll-01	C:\program files\grokster\topsearch.dll
Run		
Bho		
Reg		

Web_CPR		
Process	WeC-pro-01 WeC-pro-02	C:\program files\Web_Cpr\WebCpr0.exe C:\program files\Web_Cpr\WebCpr1.exe
Exe	WeC-exe-01	C:\program files\Web_Cpr\disp2000.exe
Dll		
Run	WeC-run-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "WebCpr0"
Bho		
Reg	WeC-reg-01	HKLM\SOFTWARE\microsoft\internet explorer\main\ins“2000”

WebRebates/TopRebates/TopMoxie		
Process	WeR-pro-01 WeR-pro-02	C:\program files\Web_Rebates\WebRebates0.exe C:\program files\Web_Rebates\WebRebates1.exe
Exe	WeR-exe-01	C:\program files\Web_Rebates\disp1150.exe
Dll		
Run	WeR-run-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "WebRebates0"
Bho		
Reg	WeR-reg-01 WeR-reg-02	HKCU\Software\Microsoft\Internet Explorer\MenuExt\Web Rebates HKLM\SOFTWARE\microsoft\internet explorer\main\ins“1150”

FlashenhancerBHO (BroadCastPC variant)		
Process		
Exe	FlE-exe-01 FlE-exe-02	c:\Program Files\XML\xclean.exe c:\Program Files\Common Files\java\xclean.exe
Dll	FlE-dll-01	c:\Program Files\XML\XML.dll
Run	FlE-run-01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Xcpy1.exe

Bho	FlE-bho-01	HKLM\software\microsoft\windows\currentversion\explorer\browser helper objects\{7cd20e91-1f31-41da-8379-479ea31df969}
Reg	FlE-reg-01 FlE-reg-02 FlE-reg-03	HKCR\unawareobj.unawareobj.1 HKCR\unawareobj.unawareobj HKCR\clsid\{7cd20e91-1f31-41da-8379-479ea31df969}

SurfSideKick		
Process	Ssk-pro-01 Ssk-pro-02 Ssk-pro-03	c:\programfiler\surfsidekick 2\ssk.exe C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\SskUpdater.exe ssk_b5.exe (installation process)
Exe		
Dll	Ssk-dll-01 Ssk-dll-02	C:\programfiler\surfsidekick 2\sskbho.dll C:\programfiler\surfsidekick 2\SskCore.dll
Run	Ssk-dll-01	HKLM\software\microsoft\windows\currentversion\run\surfsidekick 2
Bho		
Reg	Ssk-reg-01 Ssk-reg-02	HKCR\CLSID\{ca0e28fa-1afd-4c21-a8dc-70eb5be2f076} HKLM\software\microsoft\internet explorer\urlsearchhooks\ {CA0E28FA-1AFD-4C21-A8DC-70EB5BE2F076}
tmp	Ssk-tmp-01	iXX.tmp (installation process)

Tracking cookies	
Cookie-01	terje mjømen@targetnet[1].txt
Cookie-02	terje mjømen@0[1].txt
Cookie-03	terje mjømen@0[3].txt
Cookie-04	terje mjømen@xxxtoolbar[1].txt
Cookie-05	terje mjømen@advertising[1].txt
Cookie-06	terje mjømen@j.2004cms.com/HTM/413/0
Cookie-07	terje mjømen@jmamma.cjt1.net/HTM/413/0
Cookie-08	terje mjømen@servedby.advertising[1].txt
Cookie-09	terje mjømen@spylog[2].txt
Cookie-10	terje mjømen@stat.onestat.com
Cookie-11	terje mjømen@j.2004cms.com/HTM/474/0
Cookie-12	terje mjømen@imrworldwide.com/cgi-bin
Cookie-13	terje mjømen@jmamma.cjt1.net/HTM/474/0
Cookie-14	terje mjømen@0[2].txt
Cookie-15	terje mjømen@spylog[1].txt
Cookie-16	terje mjømen@ targetnet.com

CoolWebSearch v/SuperSearch popup		
Process		
Exe		
Dll		
Run		
Bho		
Reg	Cws-reg-01 Cws-reg-02 Cws-reg-03	HKCR\CLSID\{4F7681E5-6CAF-478D-9CB8-4CA593BEE7FB} HKCR\XPlugin.XFilter

		HKCR\XPlugin.XFilter.1
Hijacks	Cws-hij-01 Cws-hij-02 Cws-hij-03	HKCU\SOFTWARE\Microsoft\Internet Explorer\Search\SearchAssistant=about:blank HKCU \SOFTWARE\Microsoft\Internet Explorer\Main\Search Bar=about:blank HKCU \SOFTWARE\Microsoft\Internet Explorer\Main\Search Page=http://www.google.com

DyFuCa Internet Optimizer		
Process	CyF-pro-01	C:\Documents and Settings\Terje Mjømen\Internet Optimizer\optimizer.exe
Exe		
Dll	CyF-dll-01	C:\WINDOWS\nem220.dll
Run	CyF-run-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Internet Optimizer
Bho	CyF-bho-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\Browser Helper Objects\{00000010-6f7d-442c-93e3-4a4827c2e4c8}
Reg	CyF-reg-01 CyF-reg-02 CyF-reg-03	HKCR\dyfuca_bh.bhobj.1 HKCR\dyfuca_bh.bhobj HKCR\clsid\{00000010-6f7d-442c-93e3-4a4827c2e4c8}

ISearchTech PowerScan		
Process	IsP-pro-01	C:\Programfiler\Power Scan\powerscan.exe
Exe		
Dll		
Run	IsP-run-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Power Scan
Bho		
Reg	IsP-reg-01	HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\BandRest

ISearchTech SideFind		
Process		
Exe		
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03	C:\Programfiler\sidefind\sfbho.dll C:\Programfiler\sidefind\sfexd001.dll C:\Programfiler\sidefind\sidefind.dll
Run		
Bho	ISF-bho-01	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\Browser Helper Objects\{A3FDD654-A057-4971-9844-4ED8E67DBBB8}
Reg	ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07	HKCR\CLSID\{8CBA1B49-8144-4721-A7B1-64C578C9EED7} HKCR\CLSID\{A3FDD654-A057-4971-9844-4ED8E67DBBB8} HKLM\Software\Microsoft\Internet Explorer\Extensions\{10E42047-DEB9-4535-A118-B3F6EC39B807} HKCR\SideFind.Finder.1 HKCR\SideFind.Finder HKCR\BrowserHelperObject.BAHelper

		HKCR\BrowserHelperObject.BAHelper.1

ISearchTech SearchBar / Slotch		
Process	**IsS-pro-01**	C:\Programfiler\ISTsvc\istsvc.exe
Exe		
Dll		
Run	**IsS-run-01**	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\IST Service
Bho		
Reg		

ISearchTech YSB		
Process		
Exe		
Dll	**IsY-dll-01**	C:\Programfiler\yoursitebar\ysb.dll
Run		
Bho		
Reg	**IsY-reg-01** **IsY-reg-02** **IsY-reg-03** **IsY-reg-04**	HKCR\CLSID\{42F2C9BA-614F-47c0-B3E3-ECFD34EED658} HKCR\YSBactivex.Installer.1 HKCR\YSBactivex.Installer HKLM\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{42F2C9BA-614F-47C0-B3E3-ECFD34EED658}

ISTBar		
Process		
Exe		
Dll		
Run		
Bho		
Reg	**IsB-reg-01** **IsB-reg-02** **IsB-reg-03** **IsB-reg-04**	HKCR\ysb.ysbobj HKCR\ysb.ysbobj.1 HKCR\CLSID\{86227d9c-0efe-4f8a-aa55-30386a3f5686} HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar\{86227D9C-0EFE-4f8a-AA55-30386A3F5686}

ISearch Desktop Search		
Process	**IDS-pro-01** **IDS-pro-02**	c:\windows\isrvs\ffisearch.exe c:\windows\isrvs\desktop.exe
Exe		
Dll		
Run	**IDS-run-01**	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ffis “C:\WINDOWS\isrvs\ffisearch.exe”
Bho		
Reg		

WindUpdates / Blazefind		
Process		
Exe		
Dll		
Run		
Bho		
Reg	**Win-reg-01** **Win-reg-02**	HKCR\CLSID\{15AD4789-CDB4-47E1-A9DA-992EE8E6BAD6} HKLM\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{15ad4789-cdb4-47e1-a9da-992ee8e6bad6}

VX2		
Process		
Exe	**WBI-exe-01**	C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temp\banner.exe
Dll		
Run		
Bho	**WBI-bho-01**	HKLM\software\microsoft\windows\currentversion\explorer\browser helper objects\{00000049-8f91-4d9c-9573-f016e7626484}
Reg	**WBI-reg-01** **WBI-reg-02** **WBI-reg-03** **WBI-reg-04**	HKCR\CLSID\{00000049-8f91-4d9c-9573-f016e7626484} HKCR\ceresdll.ceresdllobj.1 HKCR\ceresdll.ceresdllobj HKCR\SOFTWARE\microsoft\internet explorer\toolbar\webbrowser "{0E5CBF21-D15F-11D0-8301-00AA005B4383}"

180Solutions / n-case		
Process	**180-pro-01** **180-pro-02**	c:\programfiler\180solutions\sais.exe C:\WINDOWS\tsb.exe
Exe		
Dll	**180-dll-01**	C:\Programfiler\180Solutions\saishook.dll
Run	**180-run-01** **180-run-02**	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Sais.exe HKLM\Software\Microsoft\Windows\CurrentVersion\Run\tsb
Bho		
Reg		

DelfinProject/PromulGate		
Process		
Exe		
Dll		
Run		
Bho		
Reg	**Dpr-reg-01** **Dpr-reg-02**	HKCR\CLSID\{A8BD9566-9895-4FA3-918D-A51D4CD15865} HKCR\CLSID\{D0070620-1E72-42E7-A14C-3A255AD31839}

BookedSpace/Bundleware		
Process		
Exe		
Dll	**BoS-dll-01**	C:\WINDOWS\downloaded program files\bm2.dll
Run		
Bho		
Reg	**BoS-reg-01**	HKLM\software\microsoft\code store database\distribution units\{ddffa75a-e81d-4454-89fc-b9fd0631e726}

Misc		
Process	**Mis-pro-01** **Mis-pro-02** **Mis-pro-03** **Mis-pro-04** **Mis-pro-05** **Mis-pro-06** **Mis-pro-07** **Mis-pro-08** **Mis-pro-09** **Mis-pro-10** **Mis-pro-11** **Mis-pro-12** **Mis-pro-13** **Mis-pro-14** **Mis-pro-15**	[upsfctl] C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\gpginst.exe [random?] c:\windows\system32\jzuhwc.exe [winlogon.exe] e.g. C:\WINDOWS\system32\drraw.dll [rundll32.exe] e.g. C:\WINDOWS\system32\dsskperf.dll [farmmext] C:\WINDOWS\farmmext.exe (transponder) [explorer.exe] e.g. c:\programfiler\surfsidekick 2\sskbho.dll C:\WINDOWS\System32\vmss\vmss.exe [Random] C:\WINDOWS\%Random%.exe C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\iinstall.exe [wsxsvc] C:\WINDOWS\System32\wsxsvc\wsxsvc.exe [BPT] "c:\Program Files\Bpt\bpt.exe" [Dl2] C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\27.exe supportinstall.exe (installation process) webcprI.exe (installation process) wrgrcI.exe (installation process)
Exe		
Dll	**Mis-dll-01**	C:\windows\system32\aklsp.dll (VX2)
Run	**Mis-run-01** **Mis-run-02** **Mis-run-04** **Mis-run-05** **Mis-run-06** **Mis-run-07**	[upsfctl] HKLM\software\microsoft\windows\currentversion\run\Upsfctl “C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\gpginst.exe” [BPT] "c:\Program Files\Bpt\bpt.exe" [Random] C:\Windows\%Random%.exe [vmss] C:\WINDOWS\System32\vmss\vmss.exe [wsxsvc/dvx] C:\WINDOWS\System32\wsxsvc\wsxsvc.exe [Dl2] C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\27.exe
Bho		
Reg	**Mis-reg-01** **Mis-reg-02** **Mis-reg-03** **Mis-reg-04**	HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar = res://C:\WINDOWS\TEMP\se.dll/sp.html HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = about:blank HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant = about:blank

		HKLM\Software\Microsoft\Internet Explorer\Main,HomeOldSP = about:blank

Hosts		
Hosts	**Host-01**	69.20.16.183 auto.search.msn.com
	Host-02	69.20.16.183 search.netscape.com
	Host-03	69.20.16.183 ieautosearch
	Host-04	127.0.0.1 www.igetnet.com
	Host-05	127.0.0.1 code.ignphrases.com
	Host-06	127.0.0.1 clear-search.com
	Host-07	127.0.0.1 r1.clrsch.com
	Host-08	127.0.0.1 sds.clrsch.com
	Host-09	127.0.0.1 status.clrsch.com
	Host-10	127.0.0.1 www.clrsch.com
	Host-11	127.0.0.1 clr-sch.com
	Host-12	127.0.0.1 sds-qckads.com
	Host-13	127.0.0.1 status.qckads.com
	Host-14	82.179.166.164 lender-search.com
	Host-15	82.179.166.165 hot-searches.com

Not all of the defined spyware components were present one or more times in the experiment. During pilot experiments, different variants of components were discovered and put into a category that they originated from, like the BHO in VX2.

There are different kinds of processes when assessing spyware. Some are directly transmitting personal information to an external server and others are processes that are updating existing software on a computer. By blocking certain process one can prevent a whole installation of spyware. As mentioned before, some spyware relies on first installing a small piece of code to the computer before it downloads the rest of the spyware program, and by killing such processes the entire spyware program may be prevented from getting installed on a victim's computer.

Appendix B - 3rd party software defined as spyware/adware

http://www.winpatrol.com/stats.html
- MyWay/MyBar
- ISTBar
- 180Solutions
- Gator/Claria/Gain (CMESys, GMT, Trickler)
- WebRebates
- Internet Optimizer

http://sarc.com/avcenter/venc/data/adware.surfsidekick.html
- SurfSideKick
- FlashEnhancer
- BroadCastPC/BTV
- BlazeFind

http://www.processlibrary.com/
- P2p networking
- Altnet (asm.exe)
- Claria/Gain/Gator
- AdRoar
- Isearch Desktop Search (ffisearch.exe)

http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453074383
- TopSearch (BHO)
- WebCPR
- Flashtrack/flashenhancer
- ISearchTech SideFind
- BookedSpace

http://www.liutilities.com/products/wintaskspro/processlibrary/powerscan/
- ISearchTech PowerScan

http://www.pcsympathy.com/article379.html
- Bundleware connected to VX2

Not spyware
http://www.doxdesk.com/parasite/Cydoor.html
Cydoor

The above URLs states the following about the spyware and adware:
istsvc.exe “is an advertising program by Integrated Search Technologies. This process monitors your browsing habits and distributes the data back to the author's servers for analyses. This also prompts advertising pop-ups. This program is a registered security risk and should be removed immediately.”

optimize.exe “is a virus which is installed by consent from websites, and attempts to dial expensive pornography servers. This program is a registered security risk and should be removed immediately.”

sais.exe “is an advertising program by 180 solutions Spyware. This process monitors your browsing habits and distributes the data back to the author's servers for analysis. This also prompts advertising pop-ups. This program is a registered security risk and should be removed immediately.”

powerscan.exe “is an advertising program by Integrated Search Technologies. This process comes packaged with a search toolbar for Internet Explorer, but monitors your browsing habits and distributes the data back to the author's servers for analyses. This

also prompts advertising pop-ups. This program is a registered security risk and should be removed immediately."

webrebates0.exe "is an advertising program. This process monitors your browsing habits and distributes the data back to the author's servers for analysis. This also prompts advertising pop-ups. This program is a registered security risk and should be removed immediately."

Webcpr "has the ability to track your Web surfing habits, purchases, and display pop-up advertisements on your computer. This program has the ability to download and execute third party programs on your computer without your knowledge or consent."

farmmext.exe "is a process associated with the Transponder parasite. It monitors your online activities and opens pop-ups based on it. This process should be removed to protect your personal privacy."

nls.exe "is an advertising program by Webrebates. This process monitors your browsing habits and distributes the data back to the author's servers for analysis. This also prompts advertising pop-ups. This program is a registered security risk and should be removed immediately."

cashback.exe "is an advertising program. This process monitors your browsing habits and distributes the data back to the author's servers for analysis. This also prompts advertising pop-ups. This program is a registered security risk and should be removed immediately."

Asm.exe "monitors your browsing habits and distributes the data back to the author's servers for analysis."

Btv "is an adware program that downloads movie and advertisement clips. It assigns the user a global user ID and tracks aggregate Internet use patterns to better target advertisements. The advertisements are downloaded in the background and can be scheduled to run at any time, regardless of whether the computer is online or offline."

ArUpdate.exe "monitors your browsing habits and distributes the data back to the author's servers for analysis."

Gmt.exe "gathers information regarding personal Internet usage for transmission back to an online location"

Cmesys, "this Adware pops up advertisements as well as analyses computer usage."

P2p networking.exe, "this process monitors your browsing habits and distributes the data back to the author's servers for analysis."

TopSearch.dll "is a library file needed by the Kazaa.exe application for spyware operations."

IST Sidefind is reported to "Change browser settings other than homepage, without user permission."

ffisearch.exe "is a process which belongs to the the FFIsearch Spyware (stored in the %systemroot%\isrvs\ directory) is installed on your computer and will monitor your browsing habits and send information back to it's servers."

BlazeFind "installs itself as a Browser Helper Object and redirects search queries."

BookedSpace “is an adware program that displays pop-up windows with advertisements while browsing the Internet.”

Vmss.exe / wsxsvc.exe “is a part of the Delfin Media Viewer. It is acting as an adware displaying ads on your desktop.”

Bpt.exe is related to BroadCastPC (http://www.superadblocker.com/B/BPT.EXE-1566.html).

Spyware (except cookies and simple registry entries) are defined from resources and monitoring behavior.

MyBar	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Non-process – Embedded – Toolbar/BHO
Security	Permission – Transfer – URL
Privacy	BHO/Hijacker – EULA – Browser history
ISTBar	
Distribution	Active – Drive-by downloads – No interaction – Reinstalls itself
Behavior	Process – Terminate – Pop-up/web browser configuration
Security	Hidden – Transfer - Encrypted
Privacy	Trackware – EULA – Bowser history
180Solutions	
Distribution	Active – Drive-by downloads – No interaction – Reinstalls itself
Behavior	Process – Terminate – Logging
Security	Hidden – Transfer - Encrypted
Privacy	Trackware – None – Locations
Gator/Gain/Claria	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Terminate – Logging
Security	Permission – Transfer – Encrypted
Privacy	Trackware – EULA – Browser history
WebRebates	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Auto restart – Logging
Security	Permission – Transfer – Encrypted
Privacy	Trackware – EULA – Browser history
WebCPR	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Auto restart – Logging
Security	Permission – Transfer – Encrypted
Privacy	Trackware – EULA – Browser history
Internet Optimizer	
Distribution	Active – Drive-by downloads – No interaction - Uninstaller
Behavior	Process – Terminate – Pop-up/Logging
Security	Hidden – Transfer – Encrypted
Privacy	Trackware/BHO/Hijacker – EULA – Browser history
SurfSideKick	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Terminate – Logging
Security	Permission – Transfer – Encrypted
Privacy	Adware – EULA – Browser history
BroadCastPC	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Terminate – Logging
Security	Permission – Transfer – Encrypted
Privacy	Adware – EULA – Browser history
YSB	
Distribution	Active – Drive-by downloads – No interaction – Embedded

Behavior	Non-process – Embedded – Toolbar/BHO
Security	Hidden – Transfer – Encrypted
Privacy	BHO/Hijacker – EULA – Browser history
P2p networking	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Terminate – Logging
Security	Permission – Transfer – Encrypted
Privacy	Adware – EULA – Browser history
Altnet	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Terminate – Logging
Security	Permission – Transfer – Encrypted
Privacy	Trackware – EULA – Browser history
AdRoar	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Terminate – Logging
Security	Permission – Transfer – Encrypted
Privacy	Trackware – EULA – Browser history
Isearch Desktop Search	
Distribution	Active – Drive-by downloads – No interaction – Terminable
Behavior	Process – Terminate - Logging
Security	Hidden – Transfer – Encrypted
Privacy	Trackware – EULA – Browser history
ISearch Power Scan	
Distribution	Active – Drive-by downloads – No interaction – Terminable
Behavior	Process – Terminate – Pop-up/Logging
Security	Hidden – Transfer – Encrypted
Privacy	Adware – EULA – Browser history
IST SideFind	
Distribution	Active – Drive-by downloads – No interaction – Uninstaller
Behavior	Non-process – Embedded – Toolbar/BHO/Redirections
Security	Hidden – Transfer – Encrypted
Privacy	BHO/Hijacker – EULA – Browser history
FlashEnhancer/Track	
Distribution	Active – Bundle – No interaction – Uninstaller
Behavior	Process – Embedded/Auto restore – Toolbar/BHO
Security	Permission – Transfer – Encrypted
Privacy	BHO/Hijacker – EULA – Browser history
VX2	
Distribution	Active – Drive-by downloads – No interaction – Embedded
Behavior	Non-process – Embedded - Logging
Security	Hidden – Transfer – Encrypted
Privacy	LSP – EULA – Browser history

The bundled spyware are most of the same characteristics, since it origins from the same source, and the user plays an active part when installing the spyware by accepting the EULA. Some of the bundled spyware has its own uninstaller, but when tested these did not remove all the instances of the spyware or had no effect at all. Drive-by spyware that installs through ActiveX doesn't notify the user or give the user

any options whether to install the software or not. If the security settings in the IE browser are set to low, accept all ActiveX controls, signed and unsigned.

There are no options for avoid installing spyware when a user installs the free version of Grokster, therefore no interaction whether to install the spyware or not are present.

The EULAs for each 3rd party software have not been analyzed since Groster's EULA states that these software may accompanied Grokster.

There is some uncertainty in this picture of spyware; first of all, the spyware comes in a lot of variants, secondly the information about the spyware that has been used as references may not be correct, and the monitoring period of the spyware may not be representative for it. No Browser history or personal information seemed to be sent un-encrypted on the network in the time the traffic monitor was active (10 minutes), but this doesn't mean that the spyware do encrypt all the information that are sent.

Some spyware programs log and store the log file locally, which may be collected by other intruders or shared accidentally on the network, and represent a privacy issue if the log contains sensitive personal information and is not encrypted.

Appendix C – Spyware detections, removals, and blockings

Ad-Aware

Ad-aware		Bundle		
Detected	Removed	Blocked	Amount	
12	10	0	34	Process
2	1	0	10	Exe
5	2	0	16	Dll
9	6	0	18	Run
1	1	0	3	Bho
21	21	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

Ad-aware		Drive-by		
Detected	Removed	Blocked	Amount	
6	3	0	10	Process
1	1	0	1	Exe
3	3	0	5	Dll
5	4	0	5	Run
0	0	0	0	Bho
21	21	0	25	Reg
10	9	0	10	Cookie
0	0	0	2	Host

	Reference system
Processes	**IsP-pro-01 IsS-pro-01 180-pro-01 CyF-pro-01 WeR-pro-01 WeR-pro-02 Mis-pro-03 Mis-pro-04 Mis-pro-06 Mis-pro-09**
Exe	**WeR-exe-01**
Dll	**ISF-dll-01 ISF-dll-02 ISF-dll-03 BoS-dll-01 IsY-dll-01**
Run	**IsP-run-01 IsS-run-01 180-run-01 CyF-run-01 WeR-run-01**
Bho	
Reg	**IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 Cws-reg-01 Cws-reg-02 Cws-reg-03 BoS-reg-01 Win-reg-01 Win-reg-02 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04 WeR-reg-01 WeR-reg-02 WBI-reg-04**
Cookie	**Cookie-01 Cookie-04 Cookie-05 Cookie-06 Cookie-07 Cookie-08 Cookie-10 Cookie-11 Cookie-13 Cookie-15**
Host	**Host-14 Host-15**

SpywareGuard

SpywareGuard		Bundle		
Detected	Removed	Blocked	Amount	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
3	3	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	**Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15**
Exe	**Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-**

	exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

SpywareGuard		Drive-by		
Detected	**Removed**	**Blocked**	**Amount**	
0	0	0	8	Process
0	0	0	1	Exe
0	0	0	4	Dll
0	0	0	6	Run
1	1	0	1	Bho
0	0	0	20	Reg
0	0	0	6	Cookie
0	0	0	0	Host

	Reference system
Processes	WeR-pro-01 WeR-pro-02 CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01 Mis-pro-08 Mis-pro-09
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	WeR-run-01 CyF-run-01 IsP-run-01 IsS-run-01 180-run-01 Mis-run-04
Bho	ISF-bho-01
Reg	WeR-reg-01 WeR-reg-02 IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 Win-reg-01 Win-reg-02
Cookie	Cookie-01 Cookie-05 Cookie-04 Cookie-07 Cookie-08 Cookie-15
Host	

Spybot S&D

Spybot S&D		Bundle		
Detected	**Removed**	**Blocked**	**Amount**	
10	10	0	34	Process
6	6	0	10	Exe
10	9	0	16	Dll
8	8	0	18	Run
2	2	0	3	Bho
17	32	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	**Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15**
Exe	**Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02**
Dll	**Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01**
Run	**Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02**
Bho	**Myw-bho-01 FlE-bho-01 AdR-bho-01**
Reg	**Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02**
Cookie	
Host	

Spybot		Drive-by		
Detected	**Removed**	**Blocked**	**Amount**	
3	2	0	8	Process
0	0	0	1	Exe
0	0	0	4	Dll
4	3	0	6	Run
1	1	0	1	Bho
13	13	0	20	Reg
5	4	0	9	Cookie
0	0	0	0	Host

	Reference system
Processes	CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01 WeR-pro-01 WeR-pro-02 Mis-pro-08 Mis-pro-09
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	CyF-run-01 IsP-run-01 IsS-run-01 180-run-01 WeR-run-01 Mis-run-04
Bho	ISF-bho-01
Reg	ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsP-reg-01 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04 sB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 Win-reg-01 Win-reg-02 WeR-reg-01 WeR-reg-02
Cookie	Cookie-05 Cookie-13 Cookie-04 Cookie-06 Cookie-07 Cookie-11 Cookie-16 Cookie-08 Cookie-15
Host	

Outpost

Outpost		Bundle		
Detected	**Removed**	**Blocked**	**Amount**	
10	0	18	30	Process
0	0	0	8	Exe
0	0	2	7	Dll
0	0	8	16	Run
0	0	2	3	Bho
0	0	2	28	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Gat-reg-01 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

Outpost		Drive-by		
Detected	Removed	Blocked	Amount	
1	0	6	7	Process
0	0	1	1	Exe
0	0	3	4	Dll
0	0	5	5	Run
0	0	1	1	Bho
0	0	7	17	Reg
0	0	0	9	Cookie
0	0	0	0	Host

	Reference system
Processes	Mis-pro-09 WeR-pro-01 WeR-pro-02 CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	WeR-run-01 CyF-run-01 IsP-run-01 IsS-run-01 180-run-01
Bho	ISF-bho-01
Reg	Cws-hij-01 Cws-hij-02 Cws-hij-03 WeR-reg-01 WeR-reg-02 IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04
Cookie	Cookie-01 Cookie-05 Cookie-06 Cookie-07 Cookie-08 Cookie-10 Cookie-11 Cookie-12 Cookie-13
Host	

ZoneAlarm

ZoneAlarm		Bundle		
Detected	Removed	Blocked	Amount	
10	0	18	30	Process
0	0	0	8	Exe
0	0	2	7	Dll
0	0	8	16	Run
0	0	2	3	Bho
0	0	2	28	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01

	Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Gat-reg-01 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

ZoneAlarm		Drive-by		
Detected	Removed	Blocked	Amount	
0	0	9	9	Process
0	0	1	1	Exe
0	0	6	6	Dll
0	0	7	7	Run
0	0	2	2	Bho
0	0	21	21	Reg
0	0	7	7	Cookie
0	0	0	0	Host

	Reference system
Processes	180-pro-01 180-pro-02 CyF-pro-01 WeR-pro-01 WeR-pro-02 IsP-pro-01 IsS-pro-01 Mis-pro-09 Mis-pro-08
Exe	WeR-exe-01
Dll	180-dll-01 CyF-dll-01 ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	180-run-01 180-run-02 CyF-run-01 WeR-run-01 IsP-run-01 IsS-run-01 Mis-run-04
Bho	ISF-bho-01 CyF-bho-01
Reg	CyF-reg-01 CyF-reg-02 CyF-reg-03 WeR-reg-01 WeR-reg-02 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsP-reg-01 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04
Cookie	Cookie-05 Cookie-04 Cookie-06 Cookie-07 Cookie-01 Cookie-08 Cookie-15
Host	

XP Firewall sp1

XP FW sp1		Bundle		
Detected	Removed	Blocked	Amount	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

XP firewall sp1		Drive-by		
Detected	**Removed**	**Blocked**	**Amount**	
0	0	0	9	Process
0	0	0	1	Exe
0	0	0	6	Dll
0	0	0	7	Run
0	0	0	2	Bho
0	0	0	21	Reg
0	0	0	7	Cookie
0	0	0	0	Host

	Reference system
Processes	180-pro-01 180-pro-02 CyF-pro-01 WeR-pro-01 WeR-pro-02 IsP-pro-01 IsS-pro-01 Mis-pro-09 Mis-pro-08
Exe	WeR-exe-01
Dll	180-dll-01 CyF-dll-01 ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	180-run-01 180-run-02 CyF-run-01 WeR-run-01 IsP-run-01 IsS-run-01 Mis-run-04
Bho	ISF-bho-01 CyF-bho-01
Reg	CyF-reg-01 CyF-reg-02 CyF-reg-03 WeR-reg-01 WeR-reg-02 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsP-

	reg-01 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04
Cookie	Cookie-05 Cookie-04 Cookie-06 Cookie-07 Cookie-01 Cookie-08 Cookie-15
Host	

Norton Antivirus

Norton AV		Bundle		
Detected	Removed	Blocked	Amount	
8	6	0	34	Process
3	3	0	10	Exe
4	4	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

Norton		Drive-by		
Detected	Removed	Blocked	Amount	
5	5	0	11	Process
1	1	0	1	Exe
3	3	0	6	Dll
0	0	0	7	Run
0	0	0	0	Bho
0	0	0	27	Reg
0	0	0	9	Cookie
0	0	0	3	Host

Processes	CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01 WeR-pro-01 WeR-pro-02 Mis-pro-08 Mis-pro-05 Mis-pro-09 IDS-pro-01 IDS-pro-02
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01 BoS-dll-01 Mis-dll-01
Run	CyF-run-01 IsP-run-01 IsS-run-01 180-run-01 WeR-run-01 Mis-run-04 IDS-run-01
Bho	
Reg	IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 WeR-reg-01 WeR-reg-02 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04 BoS-reg-01 WBI-reg-01 WBI-reg-02 WBI-reg-03 WBI-reg-04 Mis-reg-01 Mis-reg-02 Mis-reg-03 Mis-reg-04
Cookie	Cookie-01 Cookie-02 Cookie-03 Cookie-04 Cookie-05 Cookie-06 Cookie-07 Cookie-08 Cookie-09
Host	Host-01 Host-02 Host-03

IE-Spyad

IE-Spyad		Bundle		
Detected	Removed	Blocked	Amount	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15

Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

IE-Spyad		Drive-by		
Detected	**Removed**	**Blocked**	**Amount**	
0	0	8	8	Process
0	0	1	1	Exe
0	0	4	4	Dll
0	0	6	6	Run
0	0	1	1	Bho
0	0	22	22	Reg
0	0	9	9	Cookie
0	0	2	2	Host

Processes	WeR-pro-01 WeR-pro-02 CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01 Mis-pro-08 Mis-pro-09
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	WeR-run-01 CyF-run-01 IsP-run-01 IsS-run-01 180-run-01 Mis-run-04
Bho	ISF-bho-01
Reg	WeR-reg-01 WeR-reg-02 Cws-reg-01 Cws-reg-02 Cws-reg-03 IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 Win-reg-01 Win-reg-02
Cookie	Cookie-01 Cookie-02 Cookie-03 Cookie-04 Cookie-05 Cookie-06 Cookie-07 Cookie-08 Cookie-09
Host	Host-14 Host-15

Patch OS

Patch OS sp2		Bundle		
Detected	**Removed**	**Blocked**	**Amount**	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	**Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15**
Exe	**Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02**
Dll	**Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01**
Run	**Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02**
Bho	**Myw-bho-01 FlE-bho-01 AdR-bho-01**
Reg	**Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02**
Cookie	
Host	

Patch OS sp2		Drive-by		
Detected	**Removed**	**Blocked**	**Amount**	
0	0	0	7	Process
0	0	0	1	Exe
0	0	0	4	Dll
0	0	0	5	Run
0	0	0	1	Bho
0	0	0	19	Reg
0	0	0	8	Cookie
0	0	0	13	Host

	Reference system
Processes	WeR-pro-01 WeR-pro-02 CyF-pro-01 180-pro-01 IsP-pro-01 IsS-pro-01 Mis-pro-09
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	WeR-run-01 CyF-run-01 180-run-01 IsP-run-01 IsS-run-01
Bho	ISF-bho-01
Reg	WeR-reg-01 WeR-reg-02 BoS-reg-01 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 IsP- reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04
Cookie	Cookie-01 Cookie-02 Cookie-04 Cookie-05 Cookie-08 Cookie-10 Cookie-14 Cookie-15
Host	Host-01 Host-02 Host-03 Host-04 Host-05 Host-06 Host-07 Host-08 Host-09 Host-10 Host-11 Host-12 Host-13

WinSnort

WinSnort		Bundle		
Detected	Removed	Blocked	Amount	
5	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
1	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-

	reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

WinSnort		Drive-by		
Detected	**Removed**	**Blocked**	**Amount**	
3	0	0	9	Process
0	0	0	1	Exe
2	0	0	7	Dll
0	0	0	6	Run
0	0	0	0	Bho
0	0	0	20	Reg
0	0	0	8	Cookie
0	0	0	3	Host

	Reference system
Processes	CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01 WeR-pro-01 WeR-pro-02 Mis-pro-08 Mis-pro-03 Mis-pro-09
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01 BoS-dll-01 Mis-dll-01
Run	CyF-run-01 IsP-run-01 IsS-run-01 180-run-01 WeR-run-01 Mis-run-04
Bho	
Reg	IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsY-reg-04 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 BoS-reg-01 WeR-reg-01 WeR-reg-02 BoS-reg-01
Cookie	Cookie-05 Cookie-13 Cookie-04 Cookie-06 Cookie-11 Cookie-01 Cookie-08 Cookie-15
Host	Host-01 Host-02 Host-03

Internet Explorer ActiveX

IE		Bundle	ActiveX	
Detected	**Removed**	**Blocked**	**Amount**	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

IE ActiveX		Drive-by		
Detected	**Removed**	**Blocked**	**Amount**	
0	0	8	8	Process
0	0	1	1	Exe
0	0	4	4	Dll
0	0	6	6	Run
0	0	1	1	Bho
0	0	19	19	Reg
0	0	0	4	Cookie
0	0	0	0	Host

Processes	Mis-pro-09 Mis-pro-09 WeR-pro-01 WeR-pro-02 CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	Mis-run-04 CyF-run-01 IsP-run-01 180-run-01 IsS-run-01 WeR-run-01
Bho	ISF-bho-01
Reg	WeR-reg-01 WeR-reg-02 Win-reg-01 Win-reg-02 IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04

Cookie	**Cookie-01 Cookie-05 Cookie-09 Cookie-08**
Host	

SpywareBlaster ActiveX

SpywareBlaster		Bundle	ActiveX	
Detected	**Removed**	**Blocked**	**Amount**	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	**Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15**
Exe	**Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02**
Dll	**Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01**
Run	**Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02**
Bho	**Myw-bho-01 FlE-bho-01 AdR-bho-01**
Reg	**Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02**
Cookie	
Host	

SpywareBlaster		Drive-by	ActiveX	
Detected	Removed	Blocked	Amount	
0	0	8	8	Process
0	0	1	1	Exe
0	0	4	4	Dll
0	0	6	6	Run
0	0	1	1	Bho
0	0	22	22	Reg
0	0	0	6	Cookie
0	0	2	2	Host

Processes	WeR-pro-01 WeR-pro-02 CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01 Mis-pro-08 Mis-pro-09
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	WeR-run-01 CyF-run-01 IsP-run-01 IsS-run-01 180-run-01 Mis-run-04
Bho	ISF-bho-01
Reg	WeR-reg-01 WeR-reg-02 Cws-reg-01 Cws-reg-02 Cws-reg-03 IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 Win-reg-01 Win-reg-02
Cookie	Cookie-01Cookie-05 Cookie-06 Cookie-07 Cookie-08 Cookie-15
Host	Host-14 Host-15

AVG

AVG Free		Bundle		
Detected	Removed	Blocked	Amount	
3	1	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02

Dll	**Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01**
Run	**Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02**
Bho	**Myw-bho-01 FlE-bho-01 AdR-bho-01**
Reg	**Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02**
Cookie	
Host	

AVG Free		**Drive-by**		
Detected	**Removed**	**Blocked**	**Amount**	
0	0	0	7	Process
0	0	0	1	Exe
0	0	0	1	Dll
0	0	0	3	Run
0	0	0	0	Bho
0	0	0	12	Reg
0	0	0	4	Cookie
0	0	0	13	Host

Processes	**WeR-pro-01 WeR-pro-02 IsP-pro-01 IsS-pro-01 Mis-pro-03 Mis-pro-04 Mis-pro-09**
Exe	**WeR-exe-01**
Dll	**IsY-dll-01**
Run	**WeR-run-01 IsP-run-01 IsS-run-01**
Bho	
Reg	**Win-reg-01 Win-reg-02 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 WeR-reg-01 WeR-reg-02 IsP-reg-01 IsY-reg-01 IsY-reg-02 IsY-reg-03**
Cookie	**Cookie-01 Cookie-05 Cookie-08 Cookie-09**
Host	**Host-01 Host-02 Host-03 Host-04 Host-05 Host-06 Host-07 Host-08 Host-09 Host-10 Host-11 Host-12 Host-13**

Internet Explorer Cookie

IE		Bundle	Cookie	
Detected	Removed	Blocked	Amount	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

IE cookie block		Drive-by		
Detected	Removed	Blocked	Amount	
0	0	0	8	Process
0	0	0	1	Exe
0	0	0	4	Dll
0	0	0	6	Run
0	0	0	1	Bho
0	0	0	22	Reg
0	0	9	9	Cookie
0	0	0	2	Host

Processes	WeR-pro-01 WeR-pro-02 CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01 Mis-pro-08 Mis-pro-09
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	WeR-run-01 CyF-run-01 IsP-run-01 IsS-run-01 180-run-01 Mis-run-04
Bho	ISF-bho-01
Reg	WeR-reg-01 WeR-reg-02 Cws-reg-01 Cws-reg-02 Cws-reg-03 IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04 Win-reg-01 Win-reg-02
Cookie	Cookie-01 Cookie-02 Cookie-03 Cookie-04 Cookie-05 Cookie-06 Cookie-07 Cookie-08 Cookie-09
Host	Host-14 Host-15

SpywareBlaster Cookie

SpywareBlaster		Bundle	Cookie	
Detected	Removed	Blocked	Amount	
0	0	0	34	Process
0	0	0	10	Exe
0	0	0	16	Dll
0	0	0	18	Run
0	0	0	3	Bho
0	0	0	49	Reg
0	0	0	0	Cookie
0	0	0	0	Host

	Reference system
Processes	Alt-pro-01 Alt-pro-02 Alt-pr0-03 Bpc-pro-01 Bpc-pro-02 Bpc-pro-03 Gat-pro-01 Gat-pro-02 Gat-pro-03 p2p-pro-01 WeC-pro-01 WeC-pro-02 WeR-pro-01 WeR-pro-02 Mis-pro-13 Mis-pro-14 Myw-pro-01 Bpc-pro-04 Ssk-pro-01 Ssk-pro-02 Ssk-pro-03 Ssk-tmp-01 AdR-pro-01 AdR-pro-02 AdR-pro-03 Mis-pro-14 Mis-pro-10 Mis-pro-11 Mis-pro-12 Mis-pro-07 Mis-pro-01 Mis-pro-06 Mis-pro-13 Mis-pro-15
Exe	Alt-exe-01 Alt-exe-02 Bpc-exe-01 Bpc-exe-02 Gat-exe-01 Gat-exe-02 WeC-exe-01 WeR-exe-01 FlE-exe-01 FlE-exe-02
Dll	Alt-dll-01 Alt-dll-02 Alt-dll-03 Alt-dll-04 Alt-dll-05 Alt-dll-06 Alt-dll-07 Alt-dll-08 P2p-dll-01 Myw-dll-01 Myw-dll-02 Top-

	dll-01 Ssk-dll-01 Ssk-dll-02 FlE-dll-01 AdR-dll-01
Run	Alt-run-01 Bpc-run-01 Bpc-run-02 Bpc-run-03 Gat-run-01 Gat-run-02 P2p-run-01 WeC-run-01 WeR-run-01 Ssk-dll-01 FlE-run-01 AdR-run-01 AdR-run-02 Mis-run-05 Mis-run-06 Mis-run-07 Mis-run-01 Mis-run-02
Bho	Myw-bho-01 FlE-bho-01 AdR-bho-01
Reg	Alt-reg-01 Alt-reg-02 Alt-reg-03 Alt-reg-04 Alt-reg-05 Alt-reg-06 Alt-reg-07 Alt-reg-08 Alt-reg-09 Alt-reg-10 Alt-reg-11 Alt-reg-12 Alt-reg-13 Alt-reg-14 Alt-reg-15 Gat-reg-01 P2p-reg-01 P2p-reg-02 P2p-reg-03 P2p-reg-04 P2p-reg-05 P2p-reg-06 Myw-reg-01 Myw-reg-02 Myw-reg-03 Myw-reg-04 Myw-reg-05 Myw-reg-06 Myw-reg-07 Myw-reg-08 Myw-reg-09 Myw-reg-10 Myw-reg-11 Myw-reg-12 Myw-reg-13 Myw-reg-14 WeC-reg-01 WeR-reg-01 WeR-reg-02 Ssk-reg-01 Ssk-reg-02 FlE-reg-01 FlE-reg-02 FlE-reg-03 AdR-reg-01 AdR-reg-02 AdR-reg-03 Dpr-reg-01 Dpr-reg-02
Cookie	
Host	

SpywareBlaster		Drive-by	Cookie block	
Detected	Removed	Blocked	Amount	
0	0	0	8	Process
0	0	0	1	Exe
0	0	0	4	Dll
0	0	0	6	Run
0	0	0	1	Bho
0	0	0	19	Reg
0	0	5	9	Cookie
0	0	0	0	Host

Processes	Mis-pro-09 Mis-pro-09 WeR-pro-01 WeR-pro-02 CyF-pro-01 IsP-pro-01 IsS-pro-01 180-pro-01
Exe	WeR-exe-01
Dll	ISF-dll-01 ISF-dll-02 ISF-dll-03 IsY-dll-01
Run	Mis-run-04 CyF-run-01 IsP-run-01 180-run-01 IsS-run-01 WeR-run-01
Bho	ISF-bho-01
Reg	WeR-reg-01 WeR-reg-02 Win-reg-01 Win-reg-02 IsP-reg-01 ISF-reg-01 ISF-reg-02 ISF-reg-03 ISF-reg-04 ISF-reg-05 ISF-reg-06 ISF-reg-07 IsY-reg-01 IsY-reg-02 IsY-reg-03 IsB-reg-01 IsB-reg-02 IsB-reg-03 IsB-reg-04
Cookie	Cookie-01 Cookie-02 Cookie-03 Cookie-04 Cookie-05 Cookie-06 Cookie-07 Cookie-08 Cookie-09
Host	

Appendix D - Countermeasure configuration

Countermeasure	Type	Intention	Configuration / setup
ZoneAlarm	Firewall	Blocking of illegitimate connections	Internet Zone Security: High Trusted Zone security: Medium Expert rules: none Privacy: Cookie control: medium (Block cookies from tracking sites/3rd party cookies, disable web bugs, remove private header information). Ad blocking: high (block banner ads, pop-up, animation, block javascript, block vbscript, and block embedded objects (java, ActiveX).
Outpost	Firewall	Blocking of illegitimate connections	Enable auto configuring of rules, disable content blocking, disable image blocking, disable "block advertising objects", and make sure of that there are no blocked sites entries.
Windows Firewall (SP1)	Firewall	Blocking of illegitimate connections	By using the default settings no additional configuring are required.
Ad-aware	Spyware removal tool	Remove any spyware infections	Update the definition file and run the "deep scan". The time it takes to run the scan should not be counted for.
Spybot	Spyware removal tool	Remove any spyware infections	Update the definition file and scan the computer.
WinSnort	Intrusion Detection System (IDS)	Detect any spyware traffic	Update rules, download the "bleeding-all" rules from "http://www.bleedingsnort.com/staticpages/index.php?page=allsigs", and include these within the etc/snort.conf file, and disable the uPnP service detection in the "scan rule" located in the rules folder. WinPcap 3.0 protocol must be installed. The IDS will be configured to detect any malware/spyware and alike on the network, logging the traffic and alert when such traffic occurs. The appropriate command line should be achieved by studying the manual accompanied WinSnort.
AVG Free	Anti-virus software	Detect and remove viruses	Update the definition file; take action if illegitimate files are detected, and run a scan on the computer.
Norton AntiVirus	Anti-virus software	Detect and remove viruses	Update the definition file; take action if illegitimate files are detected, and run a scan on the computer.
SpywareBlaster - cookie	Spyware blocking	Block tracking cookies	Update the latest definition file, and check "prevent spyware/tracking cookies" at the Internet Explorer tab.
SpywareBlaster - ActiveX	Spyware blocking	Block harmful	Update the latest definition file, and check "prevent the installation of ActiveX-based

		ActivX controls	spyware, dialers, etc." at the Internet Explorer tab.
Internet Explorer - cookie	Privacy policy	Block tracking cookies	Choose "block all" cookies at the privacy settings in Internet Explorer (IE).
IE-Spyad	Site blocking	Block suspicious web sites	IE-Spyad requires no additional configuring after the installation.
Patch OS	Patching	Patch known weaknesses	Run Windows Update, choose only the updates of high priority.
Internet Explorer - Java / ActiveX	Security policy	Block ActiveX controls	Disable all ActiveX (signed and unsigned) and disable the usage of scripts on ActiveX controls at the security settings and Internet in the IE.
SpywareGuard	Spyware blocking	Detect and block spyware infections	Update the definition file, ensure that "Real-Time Scanning", "Download Protection", and "Browser Hijack Protection" are enabled at "Options".

Appendix E - Spyware Registry Construction -bundle

-Filtered interesting entries with RegMon (www.sysinternals.com)

Setup.exe

SetValue HKCR\CLSID\{44EC053A-400F-11D0-9DCD-00A0C90391D3}
SetValue HKCR\ADM25.ADM25.1
SetValue HKCR\ADM25.ADM25
SetValue HKCR\CLSID\{1D3BCE37-7834-4579-8169-E67681420A98}
SetValue HKCR\ADM4.ADM4.1
SetValue HKCR\ADM4.ADM4
SetValue HKCR\CLSID\{DEF37997-D9C9-4A4B-BF3C-88F99EACEEC2}
SetValue HKCR\CLSID\{1D3BCE37-7834-4579-8169-E67681420A98}
SetValue HKCR\CLSID\{E813099D-5529-47F4-9B37-4AFAFCB00A43}
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AltnetPoints Manager SUCCESS
"C:\Program Files\Altnet\Points Manager\Points Manager.exe -s "

adm4005.exe

SetValue HKCR\ADM.ADM.1
SetValue HKCR\ADM.ADM
SetValue HKCR\CLSID\{C15B7EA2-A360-43E8-A591-5FAEDC7C4E1D}

p2psetup.exe

SetValue HKCR\WebP2PInstaller.Installer.1
SetValue HKCR\WebP2PInstaller.Installer
SetValue HKCR\CLSID\{1D6711C8-7154-40BB-8380-3DEA45B69CBF}
SetValue ? HKLM\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{1D6711C8-7154-40BB-8380-3DEA45B69CBF}

P2P Networking.exe

SetValue HKCR\CLSID\{C91E8926-D4BE-4685-99F4-0D996B96BAC0}
SetValue HKCR\CLSID\{CC7A6223-3759-4075-8CEA-971F5CFC0ED2}

asm.exe

SetValue HKCR\SigningModule.SigningModule.1
SetValue HKCR\CLSID\{E813099D-5529-47F4-9B37-4AFAFCB00A43}
SetValue HKCR\SigningModule.SigningModule
SetValue HKCR\CLSID\{9BBCF06C-DCD7-495D-80DF-CDD5399D0FF8}
SetValue HKCR\CLSID\{3646C2BD-3554-49CA-8125-44DEEFB881DE}

FSG.exe

SetValue HKLM\Software\CLASSES\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}
SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Trickler SUCCESS ""c:\programfiler\grokster\fsg_4203.exe""

fsg_4203.exe

SetValue HKLM\Software\CLASSES\CLSID\{21FFB6C0-0DA1-11D5-A9D5-00500413153C}

mySetp.exe

SetValue HKCR\CLSID\{0494D0D2-F8E0-41ad-92A3-14154ECE70AC}

SetValue HKCR\CLSID\{0494D0D9-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKCR\CLSID\{0494D0D3-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKCR\CLSID\{0494D0DE-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKLM\Software\Microsoft\Internet Explorer\Toolbar\{0494D0D9-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKCR\CLSID\{0494D0D1-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKCR\MyWayToolBar.NetscapeStartup.1
SetValue HKCR\MyWayToolBar.NetscapeStartup
SetValue HKCR\CLSID\{0494D0D7-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKCR\MyWayToolBar.NetscapeShutdown.1
SetValue HKCR\MyWayToolBar.NetscapeShutdown
SetValue HKCR\CLSID\{0494D0D5-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKCR\MyWayToolBar.SettingsPlugin.1
SetValue HKCR\MyWayToolBar.SettingsPlugin
SetValue HKCR\CLSID\{0494D0DB-F8E0-41ad-92A3-14154ECE70AC}
SetValue HKCR\CLSID\{014DA6C9-189F-421a-88CD-07CFE51CFF10}

983723.exe
SetValue HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Wast
SUCCESS "C:\WINDOWS\wast2.exe 2"

wast2.exe
SetValue HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Wast
SUCCESS "C:\WINDOWS\wast2.exe 2"

WCprI.exe
SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WebCpr0
SUCCESS "C:\Programfiler\Web_Cpr\WebCpr0.exe"

WRGrCI.exe
SetValue
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WebRebates0
SUCCESS "C:\Programfiler\Web_Rebates\WebRebates0.exe"
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\djtopr1150.exe SUCCESS
""C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\djtopr1150.exe""

Points Manager.exe
SetValue HKCR\CLSID\{3f4d4f88-0198-4921-b630-957f3eb814e0}

btv_1001.exe
SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\BTV
SUCCESS "c:\Program Files\BTV\btv.exe"
SetValue
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\BtvC
SUCCESS ""c:\Program Files\BTV\btvclean.exe""

breg.exe
SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Breg
SUCCESS ""c:\Program Files\Common Files\Java\breg.exe""
SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\BTV
SUCCESS "C:\Program Files\BTV\btv.exe"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Breg
SUCCESS ""c:\Program Files\Common Files\Java\breg.exe""
SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\BTV
SUCCESS "C:\Program Files\BTV\btv.exe"

WebCpr0.exe
SetValue HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\ins\2000
SUCCESS 0x7D0
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WebCpr0
SUCCESS ""C:\Programfiler\Web_Cpr\WebCpr0.exe""

WebRebates0.exe
SetValue HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\ins\1150
SUCCESS 0x48F
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WebRebates0
SUCCESS ""C:\Programfiler\Web_Rebates\WebRebates0.exe""

gpginst.exe
SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Upsfctl
SUCCESS "C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\gpginst.exe"

cpr_in.exe
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdRoarUpdat
e SUCCESS "C:\WINDOWS\ARUpdate.exe"

GLJ2E.tmp
SetValue HKLM\Software\Microsoft\Internet Explorer\Toolbar\{BDF6CE3D-
F5C5-4462-9814-3C8EAC330CA8} SUCCESS
SetValue HKCR\AdRoar.Band.1
SetValue HKCR\AdRoar.Band
SetValue HKCR\CLSID\{BDF6CE3D-F5C5-4462-9814-3C8EAC330CA8}

explorer.exe
DeleteValueKey HKCU\SOFTWARE\Microsoft\Internet
Explorer\UrlSearchHooks\{CFBFAE00-17A6-11D0-99CB-00C04FD64497}
SUCCESS
SetValue HKCR\CLSID\{CA0E28FA-1AFD-4C21-A8DC-70EB5BE2F076}
SetValue
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SurfSideKick
2 SUCCESS "C:\Programfiler\SurfSideKick 2\Ssk.exe"
SetValue HKLM\SOFTWARE\Microsoft\Internet
Explorer\UrlSearchHooks\{CA0E28FA-1AFD-4C21-A8DC-70EB5BE2F076}
SUCCESS ""

IEXPLORE.EXE
SetValue HKCU\Software\Microsoft\Internet
Explorer\Toolbar\WebBrowser\{01E04581-4EEE-11D0-BFE9-00AA005B4383}
SUCCESS 81 45 E0 01 EE 4E D0 11 ...
SetValue HKCU\Software\Microsoft\Internet
Explorer\Toolbar\WebBrowser\{0E5CBF21-D15F-11D0-8301-00AA005B4383}
SUCCESS 21 BF 5C 0E 5F D1 D0 11 ...

```
SetValue HKCU\Software\Microsoft\Internet
Explorer\Toolbar\WebBrowser\{0494D0D9-F8E0-41AD-92A3-14154ECE70AC}
SUCCESS D9 D0 94 04 E0 F8 AD 41 ...
SetValue HKCU\Software\Microsoft\Internet
Explorer\Toolbar\WebBrowser\ITBarLayout SUCCESS 11 00 00 00 4C 00 00
00 ...
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdRoarUpdat
e SUCCESS "C:\WINDOWS\ARUpdate.exe"
```

Appendix F - Spyware File Construction – bundle

-Filtered interesting operations with FileMon (www.sysinternals.com)

grokstersetup.exe
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg History.IE5 \index.dat
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat

GROKST~1.EXE
SET INFORMATION
C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\altnet\Setup.exe
WRITE C: SUCCESS Offset: 0 Length: 24576
SET INFORMATION C:\PROGRA~1\Grokster\CD_INS~1.EXE
WRITE C: SUCCESS Offset: 0 Length: 65536
CD_INS~1.EXE
WRITE C:\WINDOWS\System32\cd_clint.dll
SET INFORMATION C:\Programfiler\Grokster\cd_install_371.exe
DELETE C:\Programfiler\Grokster\cd_install_371.exe
SET INFORMATION C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\983723.exe
WRITE C: SUCCESS Offset: 0 Length: 65536
SET INFORMATION C:\PROGRA~1\Grokster\FSG.exe
WRITE C: SUCCESS Offset: 0 Length: 65536
SET INFORMATION C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\mySetp.exe

WRITE C: SUCCESS Offset: 0 Length: 65536
SET INFORMATION
C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\SUPPOR~1.EXE
WRITE C: SUCCESS Offset: 0 Length: 65536
SET INFORMATION C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\btv_1001.exe

WRITE C: SUCCESS Offset: 0 Length: 65536
SET INFORMATION C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\gpginst.exe
WRITE C: SUCCESS Offset: 0 Length: 65536
SET INFORMATION C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\SSK_B5.EXE

WRITE C: SUCCESS Offset: 0 Length: 28672

QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
QUERY INFORMATION C:\Programfiler\Grokster\TopSearch.dll
READ C:\Programfiler\Grokster\TopSearch.dll

Setup.exe
WRITE C:\program files\altnet\download manager\admdloader.dll
WRITE C:\program files\altnet\download manager\admdata.dll
WRITE C:\program files\altnet\download manager\admfdi.dll

WRITE C:\program files\altnet\download manager\adm25.dll
WRITE C:\program files\altnet\download manager\adm4005.exe
WRITE C:\program files\altnet\download manager\adm4.dll
WRITE C:\program files\altnet\download manager\admprog.dll
WRITE C:\docume~1\terjem~1\lokale~1\temp\p2psetup.exe

p2psetup.exe

WRITE C:\WINDOWS\Downloaded Program Files\WebP2PInstaller.dll
WRITE C:\WINDOWS\System32\P2P Networking\MARSHAL.DLL
WRITE C:\WINDOWS\System32\P2P Networking\P2P Networking.exe
WRITE C:\program files\altnet\download manager\asm.exe
WRITE C:\program files\altnet\download manager\asmps.dll
WRITE C:\Program Files\Altnet\Points Manager\Points Manager.exe.Manifest
WRITE C:\Program Files\Altnet\Points Manager\sysdetect.dll
WRITE C:\Program Files\Altnet\Points Manager\Points Manager.exe
WRITE C:\program files\altnet\download manager\altinst1.dll
WRITE C:\program files\altnet\download manager\altinst2.dll

READ C:\WINDOWS\System32\drivers\etc\hosts
WRITE C:\WINDOWS\WININIT.INI

FSG.exe

WRITE C:\programfiler\grokster\fsg_4203.exe
WRITE C:\Programfiler\Fellesfiler\GMT\EGNSEngine.dll
WRITE C:\Programfiler\Fellesfiler\GMT\GMT.exe
WRITE C:\Programfiler\Fellesfiler\GMT\GUninstaller.exe
WRITE C:\Programfiler\Fellesfiler\GMT\EGIEProcess.dll
WRITE C:\Programfiler\Fellesfiler\GMT\GatorRes.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\CMESys.exe
WRITE C:\Programfiler\Fellesfiler\CMEII\CMEIIAPI.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GAppMgr.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GDwldEng.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GIocl.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GIoclClient.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GMTProxy.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GObjs.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GStore.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\GStoreServer.dll
WRITE C:\Programfiler\Fellesfiler\CMEII\Gtools.dll

GMT.exe

WRITE C:\Programfiler\Fellesfiler\GMT\EGIEProcess.dll
WRITE C:\Programfiler\Fellesfiler\GMT\GatorRes.dll
WRITE C:\Programfiler\Fellesfiler\GMT\EGNSEngine.dll
WRITE C:\Programfiler\Fellesfiler\GMT\EGGCEngine.dll

CMESys.exe

QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat

mySetp.exe

WRITE C:\Programfiler\MyWay\myBar\1.bin\MY2NS.EXE
WRITE C:\Programfiler\MyWay\myBar\1.bin\MYBAR.DLL
WRITE C:\Programfiler\MyWay\myBar\1.bin\NPMYWAY.DLL

asm.exe

983723.exe
SET INFORMATION C:\WINDOWS\wast2.exe
WRITE C: SUCCESS Offset: 0 Length: 65536

Points Manager.exe

SUPPOR~1.EXE
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temp\WCprI.exe
WCprI.exe
WRITE C:\Programfiler\Web_Cpr\WebCpr1.exe
WRITE C:\Programfiler\Web_Cpr\WebCpr0.exe
WRITE C:\Programfiler\Web_Cpr\disp2000.exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\WRGrCI.exe
WRGrCI.exe
WRITE C:\Programfiler\Web_Rebates\WebRebates1.exe
WRITE C:\Programfiler\Web_Rebates\WebRebates0.exe
WRITE C:\Programfiler\Web_Rebates\disp1150.exe
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temp\WCprI.exe

btv_1001.exe
WRITE C:\Program Files\BTV\btv.exe
WRITE C:\Program Files\BTV\btvclean.exe
WRITE C:\Program Files\BTV\breg_inst.exe
breg_inst.exe
WRITE C:\Program Files\Common Files\Java\breg.exe

p2psetup.exe
WRITE C:\WINDOWS\System32\P2P Networking\P2P Networking.exe
P2P Networking.exe
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat

SSK_B5.EXE
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\i2B.tmp *
i2B.tmp
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\SskUpdater.exe
SskUpdater.exe
QUERY INFORMATION C:\Programfiler\SurfSideKick 2\Ssk.exe SUCCESS Length: 94208
WRITE C: SUCCESS Offset: 0 Length: 65536
DELETE
C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\SskUpdater.exe
QUERY INFORMATION C:\WINDOWS\System32\WS2_32.dll
QUERY INFORMATION C:\WINDOWS\System32\WS2HELP.dll
QUERY INFORMATION C:\WINDOWS\system32\rpcss.dll
QUERY INFORMATION C:\WINDOWS\System32\uxtheme.dll
QUERY INFORMATION C:\WINDOWS\System32\MSCTF.dll
QUERY INFORMATION C:\WINDOWS\System32\imm32.dll
QUERY INFORMATION C:\WINDOWS\system32\mswsock.dll
QUERY INFORMATION C:\WINDOWS\System32\wshtcpip.dll
QUERY INFORMATION C:\WINDOWS\System32\Shdocvw.dll

QUERY INFORMATION
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.10.0_x-ww_f7fb5805\comctl32.dll
QUERY INFORMATION C:\WINDOWS\WindowsShell.Manifest

QUERY INFORMATION C:\WINDOWS\system32\Apphelp.dll
QUERY INFORMATION C:\WINDOWS\AppPatch\sysmain.sdb

Ssk.exe
WRITE C:\Programfiler\SurfSideKick 2\SskBho.dll
WRITE C:\Programfiler\SurfSideKick 2\SskCore.dll
QUERY INFORMATION C:\WINDOWS\System32\winrnr.dll
QUERY INFORMATION C:\WINDOWS\System32\rasadhlp.dll
QUERY INFORMATION C:\WINDOWS\System32\Shdocvw.dll
QUERY INFORMATION
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.10.0_x-ww_f7fb5805

explorer.exe
QUERY INFORMATION C:\Programfiler\SurfSideKick 2\ SUCCESS
Attributes: D
READ C:\WINDOWS\system32\SHELL32.dll
READ C:\WINDOWS\System32\stdole2.tlb
READ C:\WINDOWS\System32\shdocvw.dll

wast2.exe
SET INFORMATION C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\cpr_in.exe
WRITE C:\$ConvertToNonresident SUCCESS Offset: 262144 Length: 16384
cpr_in.exe

IEXPLORE.EXE
SET INFORMATION C:\Programfiler\MyWay\myBar\Cache\files.ini
SET INFORMATION C:\WINDOWS\System32\shell32.dll
SET INFORMATION C:\WINDOWS\System32\url.dll
SET INFORMATION C:\WINDOWS\System32\mshtml.dll
SET INFORMATION C:\Programfiler\Internet Explorer\iexplore.exe
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@myway[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@myway[2].txt
READ C:\Programfiler\MyWay\myBar\Cache\files.ini
WRITE C:\Programfiler\MyWay\myBar\Cache\files.ini
QUERY INFORMATION C:\Programfiler\MyWay\myBar\1.bin\MYBAR.DLL

WebCpr0.exe
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat

WebRebates0.exe
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
QUERY INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat

gpginst.exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\srtin.exe
srtin.exe:1964
WRITE C:\WINDOWS\System32\wsxsvc\wsxsvc.exe

btv.exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\73.exe\73.exe
73.exe
WRITE C:\Program Files\Bpt\BPT.exe

svchost.exe e.g.
WRITE C:\WINDOWS\Prefetch\MYSETP.EXE-1A24A9F9.pf
WRITE C:\WINDOWS\Prefetch\SSK_B5.EXE-1EB63483.pf
WRITE C:\WINDOWS\Prefetch\IEXPLORE.EXE-0805A066.pf

Appendix G - Registry entries Drive-by downloads

- \Current Version\Run & \Current Version\Run Once

istsvc.exe
SetValue
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\IST Service SUCCESS "C:\Programfiler\ISTsvc\istsvc.exe"

mofnj.exe
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\yWlWb4 SUCCESS "C:\WINDOWS\mofnj.exe"

optimize.exe:2772
SetValue
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Internet Optimizer SUCCESS ""C:\Documents and Settings\Terje Mjømen\Internet Optimizer\optimize.exe""

sais.exe:3176
SetValue
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\sais SUCCESS "c:\programfiler\180solutions\sais.exe"

iinstall.exe:3480
SetValue
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\PowerScan SUCCESS "C:\Programfiler\Power Scan\powerscan.exe"

webrebates.exe:3836
SetValue
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WebRebates0 SUCCESS
"C:\Programfiler\Web_Rebates\WebRebates0.exe"

webrebates.exe:3836
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\djtopr1150.exe SUCCESS
""C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\djtopr1150.exe""

farmmext.exe:2904
SetValue
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\farmmext SUCCESS "C:\WINDOWS\farmmext.exe"

Appendix H - File creation Drive-by downloads

-\Current Version\Run

optimize.exe
WRITE C:\Documents and Settings\Terje Mjømen\Internet Optimizer**optimize.exe** SUCCESS
WRITE C:\Programfiler\180Solutions**sais.exe** SUCCESS
WRITE C:\Programfiler\Power Scan**powerscan.exe** SUCCESS

webrebates.exe
WRITE C:\Programfiler\Web_Rebates**WebRebates0.exe** SUCCESS

IEXPLORE.EXE
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@spylog[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@spylog[2].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@servedby.advertising[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@advertising[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@targetnet[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@servedby.advertising[2].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@targetnet[2].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@4[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@0[2].tx
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@474[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@413[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\ICD1.tmp\MediaPassX.dll
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\G9Y7SD23\MediaPassK[1].exe

DELETE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\G9Y7SD23\MediaPassC[1].dll

WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\8PAROHY3\MediaPass[1].exe
DELETE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\ICD1.tmp
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@spylog[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Skrivebord\halflife2crackfff.zip

WRITE
C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\ICD1.tmp\YSBactivex.dll
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\iinstall.exe
SET INFORMATION C:\WINDOWS\system32\config\software.LOG
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\SLU38TUF\ysb_prompt[1].php
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\SLU38TUF\ysb_prompt[1].htm
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\8PAROHY3\yoursitebar[1].xml
WRITE C:\PROGRA~1\YOURSI~1\yoursitebar.xml
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\8PAROHY3\congratulation1[1].gif
WRITE C:\WINDOWS\system\UpdInst.exe
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\OHUJWHMR\Installer[1].exe

explorer.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
WRITE C:\Documents and Settings\Terje Mjømen\Siste\halflife2crackfff.lnk
SET INFORMATION C:\WINDOWS\system32\gplul3391.dll

mshta.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat
WRITE C:\WINDOWS\update13.js
SET INFORMATION C:\WINDOWS\System32\WScript.exe

file.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat

svchost.exe e.g.
WRITE C:\WINDOWS\Prefetch\REGSVR32.EXE-25EEFE2F.pf
WRITE C:\WINDOWS\Prefetch\EXPLORER.EXE-082F38A9.pf

iinstall.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\ntuser.dat.LOG
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\8PAROHY3\istsvc[1].exe
WRITE C:\Programfiler\ISTsvc\istsvc.exe

WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\OHUJWHMR\istrecover[1].exe
WRITE C:\WINDOWS\rjcchs.exe
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\G9Y7SD23\ysb[1].dll
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\ysb.dll
WRITE C:\Programfiler\YourSiteBar\ysb.dll
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\8PAROHY 3\optimize[1].exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\optimize.exe
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\G9Y7SD23\ncase_new[1].exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\sais.exe
WRITE C:\Programfiler\180Solutions\sais.exe
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\SLU38TUF\sidefind[1].exe
WRITE C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\OHUJWHMR\powerscan[1].exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\powerscan.exe
WRITE C:\Programfiler\Power Scan\powerscan.exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\webrebates.exe
WRITE C:\Documents and Settings\Terje Mjømen\Favoritter\Technology\Anti-Virus.lnk
WRITE C:\Documents and Settings\Terje Mjømen\Favoritter\Fun & Games\Casino.lnk
WRITE C:\Documents and Settings\Terje Mjømen\Favoritter\Going Places\Air Tickets.lnk

istsvc.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\terje mjømen@xxxtoolbar[1].txt
WRITE C:\Documents and Settings\Terje Mjømen\Cookies\index.dat

rjcchs.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\ntuser.dat.LOG

tmksrvu.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat

optimize.exe
WRITE C:\Documents and Settings\Terje Mjømen\Internet Optimizer\optimize.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\ntuser.dat.LOG
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat

SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat

sais.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat

sidefind.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat

webrebates.exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\jkill.exe
WRITE C:\DOCUME~1\TERJEM~1\LOKALE~1\Temp\djtopr1150.exe
WRITE C:\Programfiler\Web_Rebates\WebRebates1.exe
WRITE C:\Programfiler\Web_Rebates\WebRebates0.exe
WRITE C:\Programfiler\Web_Rebates\disp1150.exe
SET INFORMATION C:\Programfiler\Web_Rebates\disp1150.exe

sidefind.exe
WRITE C:\Programfiler\SideFind\sfbho.dll
WRITE C:\Programfiler\Sidefind\update\sidefind.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\ntuser.dat.LOG

WebRebates0.exe
SET INFORMATION C:\Documents and Settings\Terje Mjømen\ntuser.dat.LOG
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Temporary Internet Files\Content.IE5\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Cookies\index.dat
SET INFORMATION C:\Documents and Settings\Terje Mjømen\Lokale innstillinger\Logg\History.IE5 \index.dat

UpdInst.exe
WRITE C:\WINDOWS\system32\kvdbene.dll
WRITE C:\Recycled\desktop.ini
WRITE C:\WINDOWS\system32\mfdex.dll

Appendix I – Template Metric NIST 800-55

Critical Element	2.2 Does management ensure that corrective actions are effectively implemented?
Subordinate Question	2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action?
Metric	The average time elapsed between vulnerability or weakness discovery and implementation of corrective action?
Purpose	Measures the efficiency of closing significant system weaknesses to evaluate the existence, and the timeliness and effectiveness, of a process for implementing corrective actions
Implementation Evidence	1. Do you have a tracking system for weakness discovery and remediation implementation? ? Yes ? No 2. How many system weaknesses were discovered within the reporting period (count all weaknesses that were opened and closed within the reporting period)?___ 3. How many weaknesses discovered within the reporting period were closed in 30 days____ 60 days____ 90 days____ 180 days____ 12 months____ Remain open____
Frequency	Quarterly, semiannually, annually
Formula	(Number of weaknesses x 30 + number of weaknesses x 60 + number of weaknesses x 90 + number of weaknesses x 180 + number of weaknesses x 265)(individual answers to Question 3)/Total number of weaknesses closed (Sum of all the answers to Question 3)
Data Source	Plan of Actions and Milestones (POA&M) tracking system.
Indicators	A target time must be set for corrective action implementation. Results should be compared to this target. The trend for corrective action implementation/weakness closure should be toward shorter time frames, as management becomes more aware experience of personnel and the institutionalization of a formal remedial action process. It should be noted that some corrective actions may require an extended period of time to implement.

Appendix J –Collecting information

A-1 User-friendliness		Date:
Countermeasure:	Utility/method:	Requirements:

Test #	**Time consumed**	**Comment**
1		
2		
3		
Average		

A-2 Method of detection		Date:
Countermeasure:	Utility/method:	Requirements:

Test #	**Method (rt/ctrl)**	**Comment**
1		
2		
3		
Method		

A-3 Costs		Date:
Countermeasure:	Utility/method:	Requirements:

Vendor #	**Cost**	**Comment**
1		
2		
3		
Average		

A-4 Category of spyware		Date:
Countermeasure:	Utility/method:	Requirements:

Category	**Score**	**Comment**
X1		
X2		
X3		
Score		

A-5 Spyware detection		Date:
Countermeasure:	Utility/method:	Requirements:

	Detected modifications	**Actual modifications**
Processes		
Autoruns		
Hijacks		
Executive files		
Dlls		
Cookies		
Score		

A-6 Spyware removal		Date:
Countermeasure:	Utility/method:	Requirements:

	Removed instances	**Actual instances**
Processes		
Autoruns		
Hijacks		
Executive files		
Dlls		
Cookies		
Score		

A-7 Spyware blocking		Date:
Countermeasure:	Utility/method:	Requirements:

	Blocked instances	**Actual instances**
Processes		
Autoruns		
Hijacks		
Executive files		
Dlls		
Cookies		
Score		

A-8 False positives			Date:
Countermeasure:		Utility/method:	Requirements:

Spyware	**Amount**	**Trigged (d / r / b)***	**Actual instances**
X1			
X2			
X3			
Average			

* detected / removed / blocked

Summarizing the metric scores							Date:	
Countermeasure:			Utility/method:					
Total	**A-1**	**A-2**	**A-3**	**A-4**	**A-5**	**A-6**	**A-7**	**A-8**