Høgskolen i Gjøviks notatserie, 2011 nr. 3

An Analysis of SpyEye Detection and Removal Tools.

Hanno Langweg

Benjamin Daniel Adolphi

Svein Engen

Faculty of Computer Science and Media Technology

Høgskolen i Gjøvik
2011

ISSN: 1890-5196 ISBN: 978-82-91313-68-9

An Analysis of SpyEye Detection and Removal Tools

1 Management Summary

On 2011-02-15, several Norwegian banks observed malware attacks on their online banking interfaces. Following the observation, customers were advised to download and run SpyEye malware detection and removal tools to find out if their machines were affected and to remove the malware in case an infection was confirmed.

We can confirm that the detection tool detects presence of SpyEye malware on a personal computer. We can also confirm that the removal tools we tested do remove SpyEye malware from a personal computer.

We are concerned that removal is not complete in all cases and we are concerned that the detection and removal tools are susceptible to manipulations of their user interface by future variants of SpyEye malware.

2 Investigators

Hanno Langweg, Dr. rer. nat., Associate Professor in Information Security, HiG
Benjamin Daniel Adolphi, M.Sc. student in information security, HiG
Svein Roger Engen, M.Sc. student in information security, HiG

3 Background

On 2011-02-15, several Norwegian banks observed malware attacks on their online banking interfaces. Following the observation, customers were advised to download and run SpyEye malware detection and removal tools to find out if their machines were affected and to remove the malware in case an infection was confirmed.

4 Hypothesis

4.1 Detection Hypothesis

SpyEye detection tools offered by Norwegian banks can detect presence of SpyEye on a personal computer and can reliably notify the user of the personal computer of the detection result.

4.2 Removal Hypothesis

SpyEye removal tools recommended by Norwegian banks can remove SpyEye from a personal computer and can reliably notify the user of the personal computer of the removal result.

5 Method

We assume that the SpyEye malware sample that we use does not show different behavior in a virtualized environment as compared to a physical environment.

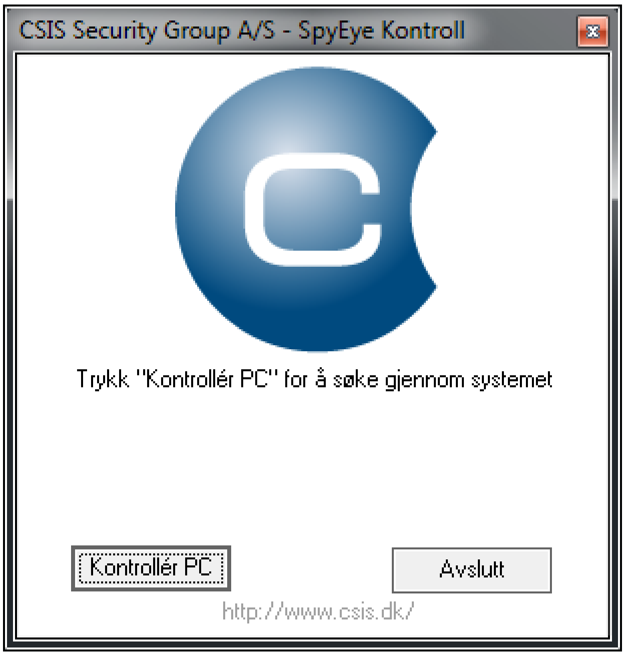
5.1 Analysis Environment

Two virtual machines were used. The first virtual machine had Microsoft Windows 7 64 Bit (all recommended operating system updates installed as of 2011-02-25). The virtual machine monitor was VirtualBox, the host system was Linux (Ubuntu 10.10 with kernel 2.6.35-27-generic).
The second virtual machine had Microsoft Windows 7 64 Bit SP1 (all recommended operating system updates installed as of 2011-02-25). The virtual machine monitor was VirtualBox, the host system was Linux (Gentoo with kernel 2.6.37).
Two user accounts were used. Account A was an administrator account used to install and execute detection and removal tools if they required it. Account B was a normal user account with no additional privileges. The malware was executed only with account B. All other programs were executed with account B unless they explicitly required to be executed with an administrator account.

5.2 Executable Files

SpyEye malware sample `build__who.exe` supplied by Promon AS 2011-02-25.
Detection tool `SpyEyeDetect_DnBNOR.exe` downloaded from https://www.dnbnor.no/portalfront/dnbnor/tools/spyeyedetect/SpyEyeDetect_DnBNOR.exe 2011-02-25 18:25. Timestamp was 2011-02-22 12:11:57. Versions for Nordea and SpareBank 1 differed only in the timestamp of the digital signature on the file. Postbanken linked to the DnBNOR version.
Removal tool `Norman_Malware_Cleaner.exe` downloaded from http://www.norman.com/personal/malware_cleaner_online_banking/ 2011-02-25 18:25. Timestamp was 2011-02-24 03:23:55. This tool was linked from NorSIS, DnBNOR, Postbanken, SpareBank 1 and Nordea.
Removal tool `Norman_Malware_Cleaner.exe` version as of 2011-02-18 supplied by Promon AS 2011-02-25.
Removal tool Norton Power Eraser `NPE.exe` downloaded from http://security.symantec.com/nbrt/npe.asp?lcid=1044 2011-02-26 22:20. Timestamp was 2010-12-10 01:59:08. This tool was linked from Terra.
Removal tool TrendMicro HouseCall `HousecallLauncher64.exe` downloaded from http://go.trendmicro.com/housecall7/HousecallLauncher64.exe 2011-02-25 18:25. Timestamp was 2011-02-21 06:20:51. This tool was linked from Terra.

5.3 Analysis of Detection Tool



CSIS Security Group A/S - SpyEye Kontroll

Trykk "Kontrollér PC" for å søke gjennom systemet

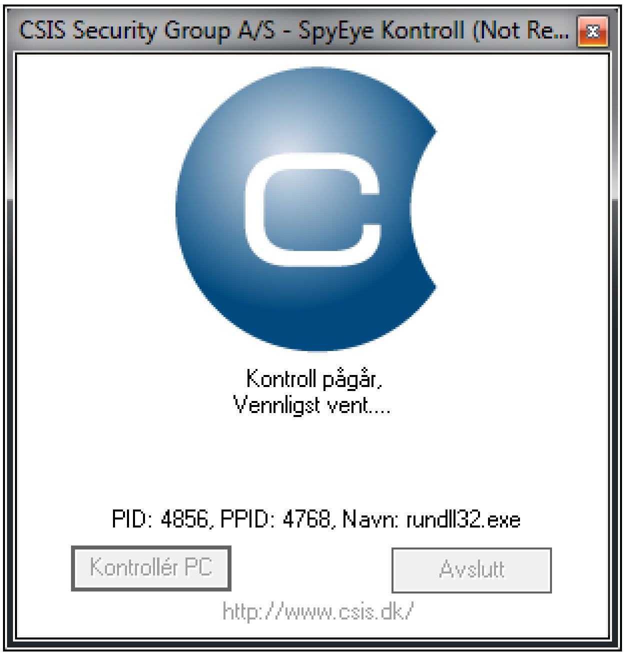
We first executed the detection tool on a clean machine that was not infected with the SpyEye malware.
The detection tool identified itself as originating from CSIS Security Group A/S with a valid digital signature verified by the Microsoft Windows operating system.
It offered the user two choices:

- "Kontrollér PC": Start examination of the personal computer for SpyEye.

- "Avslutt": Close the program.

Clicking on "Kontrollér PC" started the examination which took less than 20 seconds to complete.

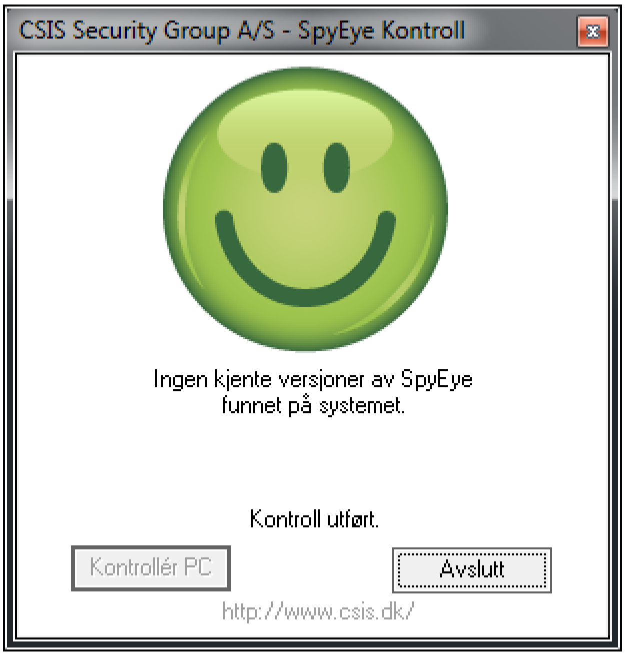
While examination was in progress, the program did not respond to user activity and displayed the names and process identifiers of active processes.
After examination was completed, the result was shown to the user.
In case no infection with SpyEye could be found, a green smiley was displayed, accompanied by the message that no known versions of SpyEye had been found on the system.



CSIS Security Group A/S - SpyEye Kontroll (Not Re...

Kontroll pågår,
Vennligst vent....

PID: 4856, PPID: 4768, Navn: rundll32.exe



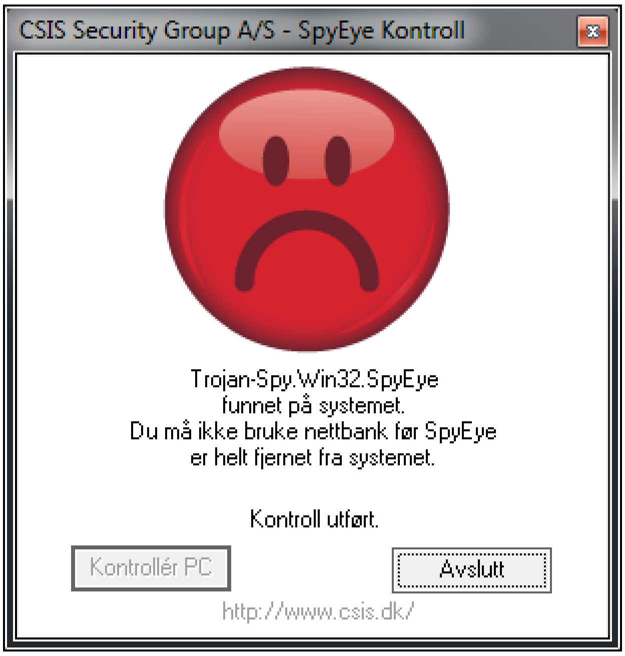
Ingen kjente versjoner av SpyEye
funnet på systemet.

Kontroll utført.

It was possible for other processes without administrator rights to manipulate the display of the examination result. This could be used by malware to display a negative examination result and hence to discourage the user from running a removal tool.

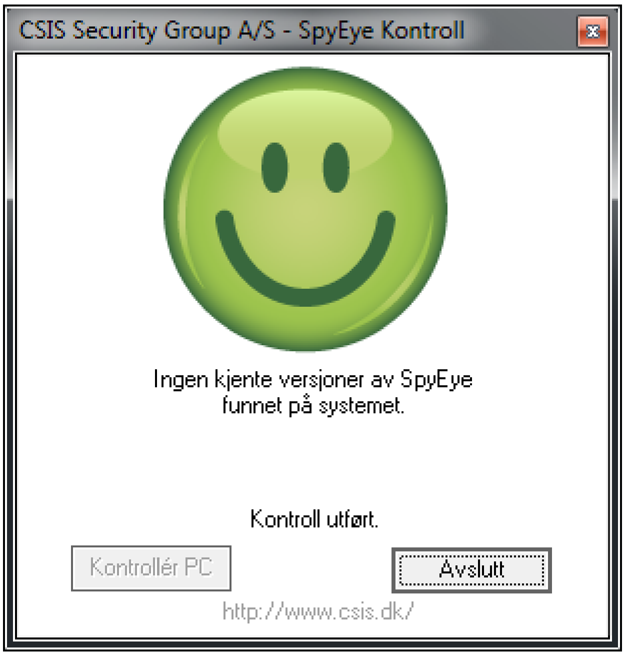
Technically, the window displaying the results consists of several common window controls, among them three Static controls containing the company logo, a green smiley, and a red smiley. Two further static controls contain the results of the examination and possible recommendations to the user.
It was possible to send simple window messages to the Static controls to show a differently colored smiley and to show a modified text message to the user.
The source code needed to manipulate display of the detection result was less than a hundred lines and was developed by experienced developers in less than an hour.

After execution of the detection tool on a clean machine, we infected a machine with the SpyEye malware and performed the exact same steps with the detection tool as we had on the clean machine.
The detection tool found the machine to be infected and displayed a red smiley and a warning message.
The smiley and the text message could be modified by our sample program so that the result of the examination of the user's computer looked like on a clean machine.



Trojan-Spy.Win32.SpyEye
funnet på systemet.
Du må ikke bruke nettbank før SpyEye
er helt fjernet fra systemet.

Kontroll utført.



Ingen kjente versjoner av SpyEye
funnet på systemet.

Kontroll utført.

5.4 Analysis of Removal Tools

We reset our machines to a defined clean state, verified that they had no network connection, and infected them as a normal user without administrative privileges by executing the build__who.exe file.

5.4.1 Norman Malware Cleaner

The Norman Malware Cleaner has to be executed with administrative privileges. It examines running processes, threads and files on the computer and tries to clean files if an infection is found.

We were able to manipulate the user interface of the removal tool. Hence, we could simulate activity of the tool and make the user believe that no infection was present or that an infection had been cleaned up. To do this, we put a button on top of the "Start scan" button and captured all mouse clicks directed at that button. When the button was clicked, we simulated output in a list view control on top of the "Scan results" list view control. The user would believe that the removal tool had operated successfully while it had been idle all the time.

In the next step we assessed the effectiveness of the removal tool. Scanning all processes and the file system of the computer took ca. 80 minutes. The removal tool detected presence of " W32/Malware.QOOC " (a SpyEye variant). As a consequence, one process was terminated, a registry value was removed, and a file was deleted from the system. The malware configuration file C:\mydnswatch\config.bin remained in the file system.

We logged on as an administrator using Windows' "Switch user" feature and verified manually that removal had taken place in the file system and the user's registry hive.

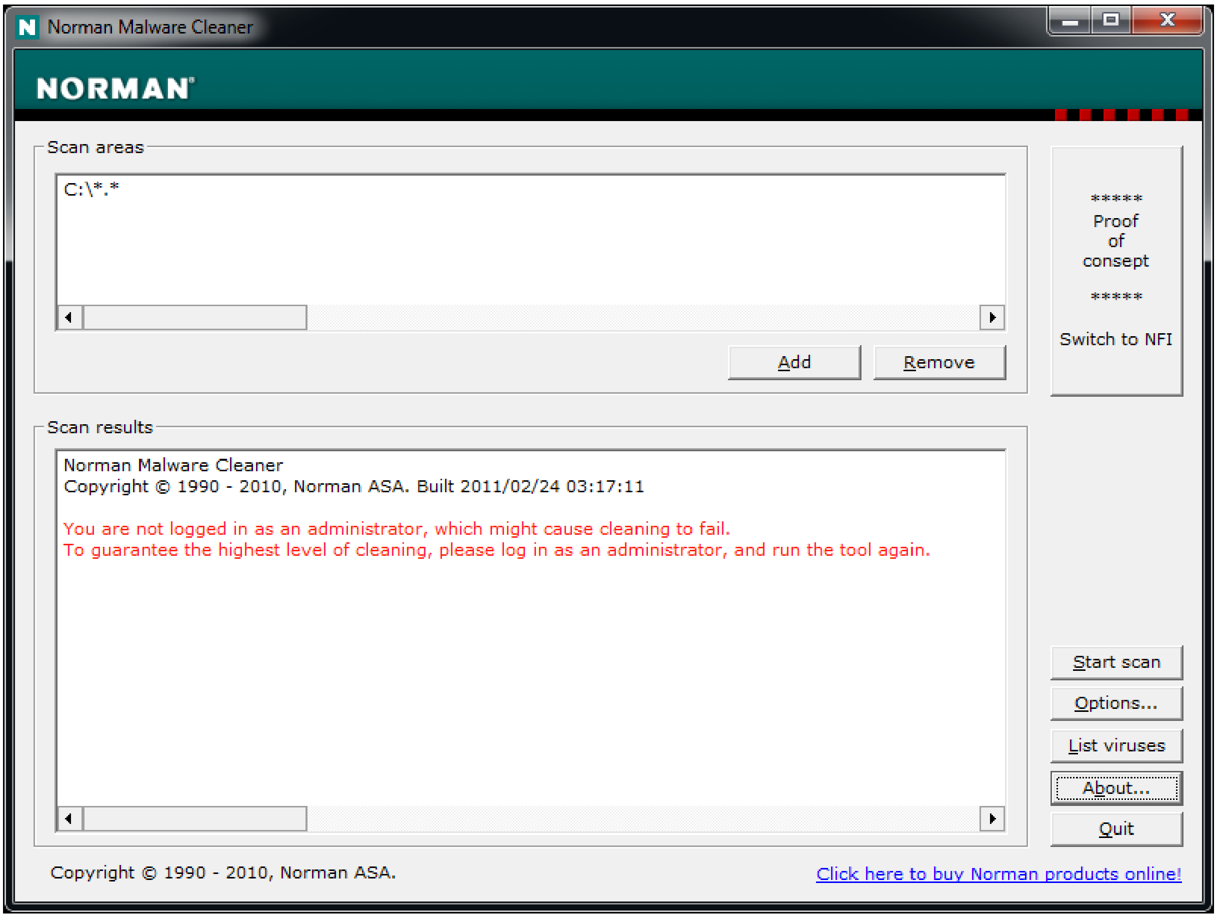
As regards the active processes, the CSIS SpyEye detection tool still warned about the machine being infected. This indicates that there still was at least one thread that had been infected by SpyEye that was not terminated by the Norman Malware Cleaner.

Logging off as a normal user and logging on again terminated all processes and restarted only those processes that had been configured with auto-start extensibility points. The CSIS SpyEye detection tool did then not warn about an infection. We logged on as an administrator using Windows' "Switch user" feature and verified manually that removal had taken place in the file system and the user's registry hive.

We concluded that SpyEye had been removed from the file system and the user's registry, but that removal was incomplete with respect to active processes. It left the possibility for SpyEye variants to establish themselves in the file system again before the current operating system session is shut down.

Results of the 2011-02-25 and the 2011-02-18 version differed with respect to removal of the registry value. The value was removed by the 2011-02-25 version and was not removed by the 2011-02-18 version.

An additional finding was undocumented functionality of the removal tool.



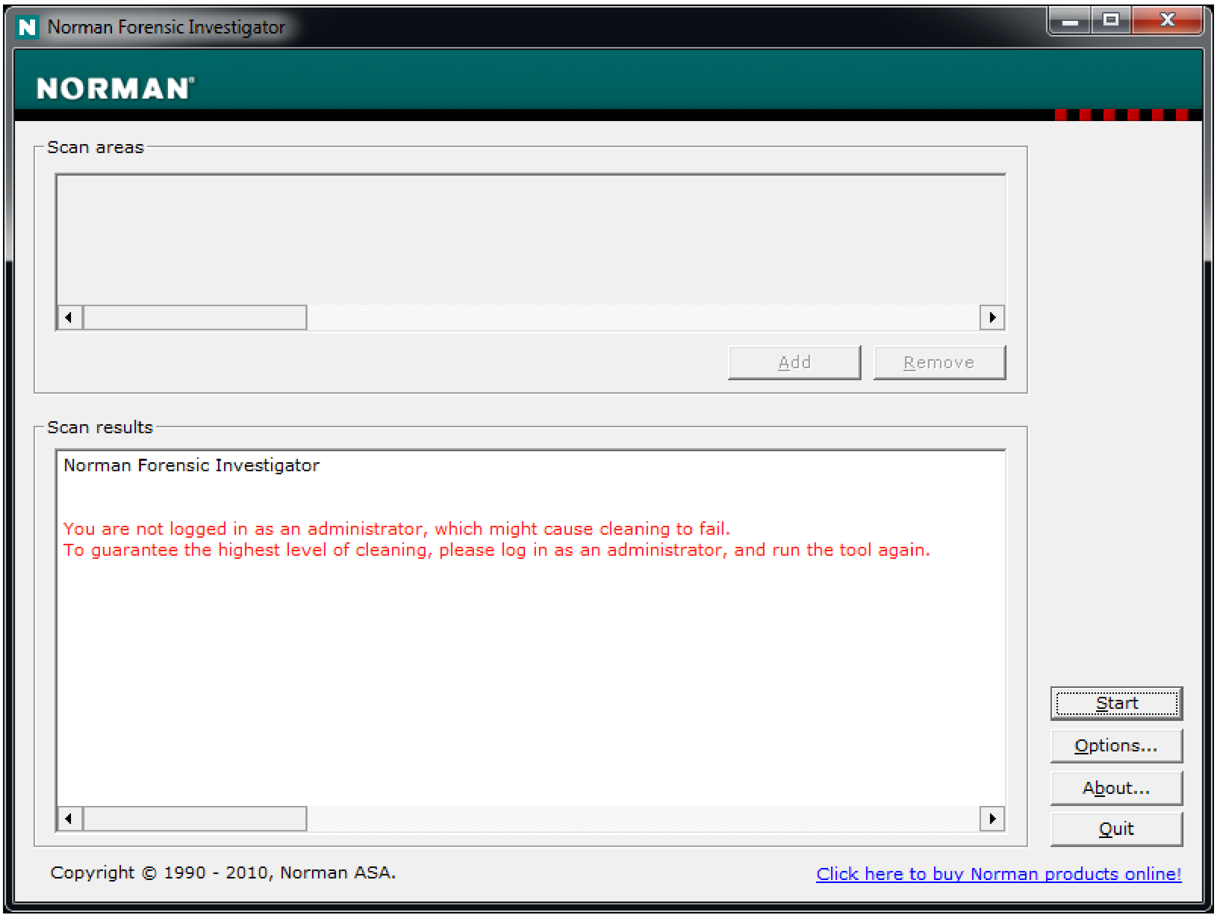
C:\*.*

```
Norman Malware Cleaner
Copyright © 1990 - 2010, Norman ASA. Built 2011/02/24 03:17:11

You are not logged in as an administrator, which might cause cleaning to fail.
To guarantee the highest level of cleaning, please log in as an administrator, and run the tool again.
```

Copyright © 1990 - 2010, Norman ASA.

Norman Malware Cleaner had a hidden disabled button titled "*****Proofofconsept*****Switch to NFI". When we enabled and showed the button and clicked it, Norman Malware Cleaner changed its behavior to Norman Forensic Investigator.


Norman Forensic Investigator
NORMAN
Scan areas
Add
Remove
Scan results
Start
Options...
About...
Quit
Copyright © 1990 - 2010, Norman ASA.
Click here to buy Norman products online!

Norman Forensic Investigator

You are not logged in as an administrator, which might cause cleaning to fail.
To guarantee the highest level of cleaning, please log in as an administrator, and run the tool again.

The functionality was probably not harmful, because Norman offered a program called "Norman Forensic Investigator" also as a standalone download. However, hidden functionality in programs deployed to the general public is contrary to best practices in software development.

5.4.2Promon Shield Launcher with Norman Malware Cleaner

We tested the Norman Malware Cleaner in a modified version. This version was provided by Promon AS. The Promon Shield Launcher was supposed to improve the security of a program against malware attacks.

We were able to manipulate the user interface of the removal tool in the same way as with the version executed without the Promon Shield Launcher. Hence, we could simulate activity of the tool and make the user believe that no infection was present or that an infection had been cleaned up. To do this, we put a button on top of the "Start scan" button and captured all mouse clicks directed at that button. When the button was clicked, we simulated output in a list view control on top of the "Scan results" list view control. The user would believe that the removal tool had operated successfully while it had been idle all the time.

In the next step we assessed the effectiveness of the removal tool. Scanning all processes and the file system of the computer took ca. 80 minutes. The behavior and effects of the removal tool did not change significantly as compared to the version without the Promon Shield Launcher.

5.4.3 Norton Power Eraser

We run the Norton Power Eraser with administrative privileges and with an active network connection. It downloaded code from the internet and recommended a reboot. We rebooted the machine.
We deactivated the network connection and deployed the SpyEye malware sample.
We run the Norton Power Eraser and it requested an internet connection for it to work properly. We refused to establish an internet connection, because we run our tests in a controlled environment and did not want to change the conditions for Norton Power Eraser. Hence, detection and removal was not performed.

5.4.4 TrendMicro House Call

We run TrendMicro House Call with administrative privileges and with an active network connection. It downloaded code from the internet.
We deactivated the network connection and deployed the SpyEye malware sample.
We run TrendMicro House Call and it concluded after ca. six minutes that the machine was infected with a SpyEye variant. We chose the recommended fix option. House Call advised that removal would only be completed after a reboot of the machine.
We confirmed that SpyEye was present in file system and registry before the reboot. It was no longer present in the file system after reboot. The registry value remained.
We did not test specifically whether user interface elements could be obscured or modified by other processes.

6 Results

6.1 Detection Tool

The SpyEye detection tool offered by Norwegian banks did detect our SpyEye malware sample. Display of the detection result could be manipulated by other processes, including malicious processes that the tool was designed to detect.

6.2 Removal Tools

6.2.1 Norman Malware Cleaner

The Norman Malware Cleaner removed our SpyEye malware sample from the file system and registry and its presence as a process could not be detected after the machine was restarted. User input could be prevented from reaching the removal tool and display could be manipulated and by other processes, including the malware processes that the tool was designed to detect and remove.

6.2.2 Promon Shield Launcher with Norman Malware Cleaner

The effectiveness and level of user interface protection of the Norman Malware Cleaner in combination with Promon Shield Launcher was not better than without Promon Shield Launcher.

6.2.3 Norton Power Eraser

Owing to the missing network connection, Norton Power Eraser refused scanning and removal.

6.2.4 TrendMicro House Call

The TrendMicro House Call removed our SpyEye malware sample from the file system and its presence as a process could not be detected after the machine was restarted.

7 Discussion

The SpyEye detection tool was designed to be run on possibly infected machines. Hence, it is unfortunate that its display can be manipulated with low effort. Users cannot trust a negative detection result, because variants of or additions to current SpyEye samples could forge a green smiley and accompanying text message.

A presumed negative detection result would discourage users from taking further action, e.g., running a time-consuming malware removal tool.

Malware removal tools are designed to be run on possibly infected machines. Hence, it is unfortunate that a user interface can be manipulated with low effort. Users cannot be sure whether or not the tool really was active, because variants of or additions to current SpyEye samples could block user input from reaching the tool and could forge messages of successful removal.

Removal of the SpyEye sample was effective with both Norton Malware Cleaner and TrendMicro House Call. It is unfortunate that there still were indications of infected processes preceding a reboot of the machine. Variants of the malware could re-infect the machine in the time span between completion of removal and reboot.

The lack of removal of the registry value by TrendMicro HouseCall is a possible security vulnerability, because malware that will be placed at the location referenced by the registry value will be automatically executed when the user logs on the next time.

Undocumented functionality in a publicly distributed product is against common best practices and should be avoided. It might be that the undocumented features contain security vulnerabilities and interfere with the intended operation of the product.

7.1 Detection Hypothesis

SpyEye detection tools offered by Norwegian banks can detect presence of SpyEye on a personal computer and can reliably notify the user of the personal computer of the detection result.

We can confirm that the detection tool detects presence of SpyEye malware on a personal computer. We cannot confirm that the detection tool reliably notifies the user of the detection result.

7.2 Removal Hypothesis

SpyEye removal tools recommended by Norwegian banks can remove SpyEye from a personal computer and can reliably notify the user of the personal computer of the removal result.

We can confirm for two of three recommended removal tools that they can remove SpyEye malware from a personal computer. We cannot confirm that removal is complete. We cannot confirm that Norton Power Eraser can remove SpyEye malware, because we did not supply a required network connection during scanning and removal. We cannot confirm that removal tools reliably notify the user of the removal result.

8 Recommendations

The SpyEye detection tool should not be offered to customers as it is of little value on infected machines. Bank customers should be encouraged to run a malware removal tool instead. A malware removal tool will also include a detection step.

Security software manufacturers should improve user interface security of those products that are designed to be run on possibly infected machines. A simple solution to this would be running a malware removal tool in a separate operating system session, i.e., by explicitly logging off and on again with an administrator account instead of elevating a process in a normal user session. This would protect execution from malware that does not have access to administrator privileges.

Tools intended to be run in possibly hostile environments should be self-contained and should not require an active network connection during detection and removal. There should be an option to cache installation files.

Undocumented functionality should be removed from a product before distribution to the public. It is best practice to ensure this by automated means, e.g., by using compiler switches.

9 Acknowledgements

SpyEye malware sample was provided by Promon AS.

We are indebted to Katrin Franke at Høgskolen i Gjøvik who provided valuable feedback during investigation and on drafts of this report.

Høgskolen i Gjøvik conducted this analysis as part of its base funded research activity and did not receive financial support from any third party.

10 Appendix

10.1 Virus description of SpyEye malware

Source: http://www.norman.com/security_center/virus_description_archive/w32_spyeye
Retrieved 2011-02-26