```
{
  "took" : 18,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 208,
    "max_score" : 6.200597,
    "hits" : [
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-Ew-7KAqxoxQqWu",
        "_score" : 6.200597,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK
Priority 3 11/08-155633.102111 10.2.197.24035978 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID1467 "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqOU",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK
Priority 3 11/08-154715.725482 10.2.197.24042817 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID25983 IpLen20 DgmLen475 DF AP Seq 0x81F833FE Ack
0x2F78F8A9 Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 743107
87752814  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqOo",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK
Priority 3 11/08-154722.508095 10.2.197.24042834 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID61085 IpLen20 DgmLen394 DF AP Seq 0x8919B3DA Ack
0x35924094 Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 744817
87759708  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqOs",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK
Priority 3 11/08-154723.990919 10.2.197.24042838 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID3943 IpLen20 DgmLen392 DF AP Seq 0x8A1951DF Ack 0x37331F93
Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 745191 87761203  "
```

```
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqPC",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK 
Priority 3 11/08-154732.188399 10.2.197.24042858 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID43025 IpLen20 DgmLen335 DF AP Seq 0x918FCEC9 Ack
0x3EA5B590 Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 747252
87769446  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqPH",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK 
Priority 3 11/08-154733.959290 10.2.197.24042863 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID62804 IpLen20 DgmLen354 DF AP Seq 0x93AE9DD9 Ack
0x402D7F4B Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 747700
87771238  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqPL",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK 
Priority 3 11/08-154735.446467 10.2.197.24042867 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID354 IpLen20 DgmLen396 DF AP Seq 0x9538689E Ack 0x4241205E
Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 748071 87772720  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqPQ",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK 
Priority 3 11/08-154737.277307 10.2.197.24042872 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID7312 IpLen20 DgmLen369 DF AP Seq 0x96327743 Ack 0x44189ABA
Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 748534 87774572  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqPc",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK 
Priority 3 11/08-154741.675250 10.2.197.24042884 -> 154.241.88.20180 TCP
```

```
TTL61 TOS0x0 ID9460 IpLen20 DgmLen380 DF AP Seq 0x9A9454E2 Ack 0x4828968A
Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 749634 87778971  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-Ew-7KAqxoxQqVr",
        "_score" : 5.6682158,
        "_source" : {
          "content" : " 11921 (http_inspect) DOUBLE DECODING ATTACK
Priority 3 11/08-155620.820541 10.2.197.24035936 -> 154.241.88.20180 TCP
TTL61 TOS0x0 ID14220 IpLen20 DgmLen369 DF AP Seq 0x829D5A4A Ack
0x2F4E2ABB Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP TS 880097
88300767  "
        }
      }
    ]
  }
}
```