Threat Hunting through Network Anomaly Detection

and

the Quest For the Holy Grail

Erik Hjelmvik
@netresec

52nd TF–CSIRT meeting
Stockholm, Sweden
About Me

- Name: Erik Hjelmvik
- Company: NETRESEC
- Develop: NetworkMiner and CapLoader
- Twitter: @netresec
- Reserve: FM CERT
HEALTHY

OR

HACKED?
PCAP by @eldracote: https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-249-1/
Healthy or Hacked?

PCAP by @eldracote: https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-249-1/
SSL on TCP 5353

Frame 6: 1060 bytes on wire (8480 bits), 1060 bytes captured (8480 bits)
Ethernet II, Src: CzNicZ5P_00:0F:72 (08:58:07:00:0F:72), Dst: PcComput_11:4e:fa (08:00...
Internet Protocol Version 4, Src: 216.66.0.143, Dst: 192.168.1.130
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 74
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: TLS 1.2 (0x0303)
    Random: 58dbad61c580f7920c1d033690928a19a1b1e8f281c631a...
    Session ID Length: 32
    Session ID: 4e64b97f746f4d30810a1b45b518eaf082d2c3e89419e...
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x0303)
    Compression Method: null (0)
TLSv1.2 Record Layer: Handshake Protocol: Certificate
  Content Type: Handshake (22)
### X.509 Certificate Details

![Image of NetworkMiner Professional 2.2 interface showing X.509 certificate details.](image)

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter value</th>
<th>Source host</th>
<th>Source port</th>
<th>Source protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Subject CN</td>
<td>0ncht hedblo.industries</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Subject O</td>
<td>Issblin GBR</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Subject L</td>
<td>London</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Subject C</td>
<td>UK</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Issuer CN</td>
<td>0ncht hedblo.industries</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Issuer O</td>
<td>Issblin GBR</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Issuer L</td>
<td>London</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Issuer C</td>
<td>UK</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Hash</td>
<td>830F59685711410495B97F...</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate valid from</td>
<td>2017-03-17 06:54:04</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate valid to</td>
<td>2017-09-15 07:54:04</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate Serial</td>
<td>00AFDB10F1E2805980</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>2.5.29.14 Subject Key Identifier</td>
<td>9b c5f6 d5 f 70 a7 60f5 90 a8...</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>2.5.29.35 Authority Key Identifier</td>
<td>KeyID=9b c5f6 d5 f 70 a7 60f5 90 a8...</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>2.5.29 19 Basic Constraints</td>
<td>Subject Type=CA,Path Length...</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
<tr>
<td>Certificate valid</td>
<td>FALSE</td>
<td>216.66.0.143 [0ncht hedblo.industries]</td>
<td>TCP 5353</td>
<td></td>
</tr>
</tbody>
</table>
X.509 Certificate Details

**Certificate Details:****

- **Certificate Subject CN**: Onchtuthedblo.industries
- **Issuer**: Issblin GbR
- **Location**: London, UK
- **Hash**: 830F59685711410495B976F...
- **Valid From**: 17-03-17 06:54:04
- **Valid To**: 17-09-15 07:54:04
- **Serial**: 00AFDB10F1E2805980
- **2.5.29.14 Subject Key Identifier**: 9b c5f6 d5 f1 a7 60 f5 90 a8...
- **2.5.29.35 Authority Key Identifier**: KeyID=9b c5f6 d5 f1 a7 60 f5...
- **2.5.29.19 Basic Constraints**: Subject Type=CA, Path Length...
- **Certificate Valid**: FALSE

**Certificate Status:**

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.
SSL Blacklist

SSL Certificate Information

Subject Common Name: Onchtuthedblo.industries
Subject: C=UK, L=London, O=Issblin GbR, CN=Onchtuthedblo.industries
Issuer Common Name: Onchtuthedblo.industries
Issuer: C=UK, L=London, O=Issblin GbR, CN=Onchtuthedblo.industries
SSL Version: TLS 1.2
Fingerprint (SHA1): 830f59685711410495b976bfc6aea388bd7b8213
Status: Blacklisted (Reason: Dridex C&C, Listing date: 2017-03-26 07:41:29)

Associated malware binaries

<table>
<thead>
<tr>
<th>Timestamp (UTC)</th>
<th>Malware binary (MD5 hash)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-25 11:42:47</td>
<td>af07a28f2cf91b6f57fd5023ee21b336</td>
</tr>
</tbody>
</table>

# of referencing malware binaries: 1

Copyright © 2017 - sslbl.abuse.ch
HEALTHY OR HACKED?
GET /document.php?rnd=7691&id=5556535E1705080117240A011016011701074A070B09 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; HPNTDF)
Host: les-eglantiers.fr
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 24 Jul 2015 21:20:59 GMT
Server: Apache
X-Powered-By: PHP/5.4.41
Content-Disposition: attachment; filename=6fa.gif
Content-Length: 666682
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: image/gif

MZ?........... ?????? @ ..............................................?....... ? !?L?!?
This program cannot be run in DOS mode. $........???6????e????e???e.?e????e?..!e???
e?..e???e?..e.??e??,e???e???ex??e?..e???e?.e???e?."e???eRich????e...........PE. L...?8?
GET /document.php?rnd=7691&id=5556535E1705080117240A011016011701074A070B09 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; HPNTDF)
Host: les-eglandiers.fr
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 24 Jul 2015 21:20:59 GMT
Server: Apache
X-Powered-By: PHP/5.4.41
Content-Disposition: attachment; filename=6fa.gif
Content-Length: 6116682
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: image/gif

MZ?..........??........@..........................?..........??........???.L?!
This program cannot be run in DOS mode.$$........??6????e????e????e.?e????e.?e???e??e?e??e??e??e??e??e??e??e??e??e??e??e??e??e??e??e??e??e???eRic...
Emerging Threats sid:2020644
pcre:"/\.php\?rnd=[0-9]{3,7}&id=[0-9A-F]{44,54}$/U"
A student asked why I went through so many alert examples in class that turned out to be false positives. Why do you think I might do that?
Are you too busy to improve?

No thanks!

We are too busy

Håkan Forss @hakanforss http://hakanforss.wordpress.com
This illustration is inspired by and in part derived from the work by Scott Simmerman, “The Square Wheels Guy” http://www.performancemanagementcompany.com/
Compromise to Detection

Source: Mandiant M-TRENDS 2017
Threat Hunting

#define THREAT_HUNTING “Assuming compromise and finding intrusions”

• Method 1: IOC’s / Threat Feeds
• Method 2: Assumptions / Heuristics
I still cringe when I see people ask how they ingest feeds into alerting mechanisms. I see a lot of FP's in their future! #DFIR
Threat hunting is anomaly hunting and defining an anomaly is extremely difficult.

Anomaly Detection

#define ANOMALY_DETECTION “Finding intrusions through abnormal patterns”

Blacklist vs. Whitelist

**Blacklist**

Define $BAD$.

Alert when $BAD$ is observed.

Examples: Anti-virus, IDS, IOCs

**Whitelist**

Define $GOOD$.

Alert when observation isn't $GOOD$.

Example: Anomaly Detection
Rinse Repeat Threat Hunting

1. Look at network traffic
2. Define what’s normal
3. Remove that
4. GOTO 1.
Sometimes I **hunt** for traffic by telling Wireshark what to **ignore** so that I can examine what’s left behind. I start with a simple filter, **review** the results, add another filter, **review** the results, **and so on** until I’m left with a small amount of traffic to analyze.

*Richard Bejtlich in:*
*The Practice of Network Security Monitoring*
Network Hunting Tip #1

Fact: Malware domains are often new and have poor page rank.

PRO-TIP
Ignore “normal” traffic going to the top 1 million domains (Alexa/Umbrella).
Network Hunting Tip #2

Fact: Infected machines are sometimes controlled via a single TCP or UDP session

Look for long sessions
Network Hunting Tip #3

Fact: C2 traffic is often regular/periodic

Look for periodic flows between a pair of IPs
Fact: Malware sometimes use hard coded IPs instead of DNS.

Look for connections to IPs that haven't been resolved.
Network Hunting Tip #5

Fact: DGA botnets only register a few of the generated domains

PRO-TIP: Look for requests for non-existent domains
Network Hunting Tip #6

Fact: Botnets often use proprietary protocols on TCP 80 or 443.

PRO-TIP
Look for port/protocol mismatches
Network Hunting Tip #7

Fact: Real SSL encryption is becoming popular in botnets.

Look for invalid certificates
Blocked Phishing Certificates

Source: http://toolbar.netcraft.com/stats/certificateAuthorities
Recap: Healthy or Hacked?

- Outside top 1 million
- Long session
- Periodic
- Hardcoded IP
- NXDOMAIN
- Port/protocol mismatch
- Invalid certificate
Periodic C2 Connections

Inter-flow interval: 11 to 14 minutes
Periodic C2 Connections

![CapLoader 1.5 screenshot](image)

<table>
<thead>
<tr>
<th>Client_IP</th>
<th>Server_IP</th>
<th>Server_Port</th>
<th>Trans Flows</th>
<th>Regularity</th>
<th>Period</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.130</td>
<td>216.66.0.143</td>
<td>5353</td>
<td>1740</td>
<td>14.1</td>
<td>00:12:24</td>
<td>SSL</td>
</tr>
</tbody>
</table>
Recap: Healthy or Hacked?

🔥 Outside top 1 million

- Long session
- Periodic
- Hardcoded IP
- NXDOMAIN
- Port/protocol mismatch

N/A - Invalid certificate
## 43 engines detected this file

<table>
<thead>
<tr>
<th>Detection</th>
<th>Details</th>
<th>Behavior</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>Gen:Variant.Kazy.691637</td>
<td>AhnLab-V3</td>
<td>Trojan/Win32.Starter</td>
</tr>
<tr>
<td>ALYac</td>
<td>Gen:Variant.Kazy.691637</td>
<td>Antiy-AVL</td>
<td>Trojan/Win32.TSGeneric</td>
</tr>
<tr>
<td>Arcabit</td>
<td>Trojan.Kazy.DA8DB5</td>
<td>Avast</td>
<td>Win32:Malware-gen</td>
</tr>
<tr>
<td>AVG</td>
<td>Pakes.QTT</td>
<td>Avira</td>
<td>TR/AD.Kovter.Y.5</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Gen:Variant.Kazy.691637</td>
<td>Comodo</td>
<td>UnclassifiedMalware</td>
</tr>
<tr>
<td>Cyren</td>
<td>W32/Trojan.EOZF-5967</td>
<td>DrWeb</td>
<td>Trojan.DownLoader15.5888</td>
</tr>
<tr>
<td>Emsisoft</td>
<td>Gen:Variant.Kazy.691637 (B)</td>
<td>eScan</td>
<td>Gen:Variant.Kazy.691637</td>
</tr>
</tbody>
</table>
Fact: IDS signatures might arrive too late.

PRO-TIP

Apply updated IDS signatures to old traffic before removing PCAP from disk.
Attacker’s Advantage

Controls:
- When to attack
- What to attack
- How to attack
Defenders’ Advantage

Control:
- The battlefield
- Instrumentation
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<body>
<img src="https://www.netresec.com/images/Netresec_Logo_190x60.png?alert=true" border="0" width="95" height="30" style="float: right" />
<h1>Internal Memo on Q3 R&amp;D Goals</h1>
<p><b style="color: darkred">CLASSIFIED</b></p>
<p>Enter some interesting text here...</p>
</body>
</html>