Advanced Malware Protection Against ransomware

György Ács
IT Security Consulting Systems Engineer
October 2016
Agenda

• Modern malware: ransomware
• What can be done?
• Ransomware analysis examples
Ransomware: Easy Profits

- Most profitable malware in history
- Lucrative: Direct payment to attackers!
- Cyber-criminals collected $209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers.
- At that rate, ransomware is on pace to be a $1 billion a year crime this year.
- Let’s take an example:
  - Looking only at the Angler exploit kit delivering ransomware
  - $60 million dollars a year in profits

- Ransomware as a Service, Tox
The Evolution of Ransomware Variants

The confluence of easy and effective encryption, the popularity of exploit kits and phishing, and a willingness for victims to pay have caused an explosion of ransomware variants.
How Does Ransomware Work?
Typical Ransomware Infection

- Problem: Customers can be taken hostage by malware that locks up critical resources – Ransomware

Ransomware frequently uses **web and email**

Ransomware takes **control** of targeted systems

Ransomware holds those systems **‘hostage’**

owner/company agrees to pay the **‘ransom’** (bitcoins) to free the system ($100-$1000, 0.5-1.5 bitcoin, deadline, demo files, “customer service”)
Most Ransomware Relies on C2 Callbacks

- Compromised sites and malvertising
- Phishing spam
- Web redirect
- Web link

EXPLOIT KIT DOMAINS
- Angler
- Nuclear
- Rig

C2

Malicious Infrastructure

File drop

Encryption Key Infrastructure

C2

Ransomware payload
Most Ransomware Relies on C2 Callbacks

<table>
<thead>
<tr>
<th>NAME*</th>
<th>DNS</th>
<th>IP</th>
<th>NO C2</th>
<th>TOR</th>
<th>PAYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locky</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>SamSam</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>TeslaCrypt</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>CryptoWall</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>TorrentLocker</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>PadCrypt</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>CTB-Locker</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>FAKBEN</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>PayCrypt</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td>DNS</td>
</tr>
<tr>
<td>KeyRanger</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td>DNS</td>
</tr>
</tbody>
</table>

*Top variants as of March 2016*
What can be done?
Recommendations

1. Build User Awareness (check the sender checking, macro)

2. Assume That Breaches Have Taken Place (a security breach is no longer a question of “if” but “when.”)

3. Prioritize Cyber-hygiene (patch, backup!, min. privilege)

Best-Practices Recommendations

- Solid patch management
- Non-native document rendering PDF + Office
- Users run as non-privileged users (no admin)
- Disable RDP
- Firewall enabled on endpoints
- Segmented and secured backups (tested)
- Encryption of backups and local documents
Build User Awareness

Undeliverable Voicemail: Error 23WMZ

Voicemail Alert

Sent: Wednesday 16 March 2016 13:28
To: Gyorgy Acs (gacs)

This message is high priority.

The attached audio message file was unable to be delivered to your voicemail account.

Regards,
Voicemail Team
Cisco Ransomware Defense Solution

• Solution to Prevent, Detect and Contain ransomware attacks

Cisco Ransomware Defense Solution is not a silver bullet, and not a guarantee. It does help to:

• Prevent ransomware from getting into the network where possible
• Stop it at the systems before it gains command and control
• Detect when it is present in the network
• Work to contain it from expanding to additional systems and network areas
• Performs incident response to fix the vulnerabilities and areas that were attacked

This solution helps to keep business operations running with less fear of being taken hostage and losing control of critical systems
Architectural Force Multiplier
Cisco Protects from the Network to the Endpoint to the Cloud

Email Security
On Promise or In the Cloud
Blocks 99% of Spam, 1 in 1 million false positive rate

Umbrella
Security from the cloud
Blocks 95% of threats before they cause damage

Next-Gen Firewall
Prioritizes threats
Automates response
Improved malware protection
Fully integrated management

AMP
See a threat once, block it everywhere
Most effective solution for known and emerging advanced threats

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Protection against ransomware

COMPROMISED SITES AND MALVERTISING

PHISHING SPAM

Web redirect

Web link

EXPLOIT KIT DOMAINS

Angler

Nuclear

Rig

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Blocked by DNS Security

Blocked by Cisco AMP for Endpoints or Network

Blocked by Email Security

Encryption Key Infrastructure
AMP: Advanced Malware Protection

Network-based AMP

Firepower Management Center

Firepower or ASA FirePower Services

AMP Malware license

No agent needed

TALOS

AMP for hosts desktop (Win, MAC, Linux) and mobile devices (Android)

Private Cloud / SaaS Manager

Host-based AMP

- Small agent
- Monitors file access (move/copy/execute)
- Gathers features (fingerprint & attributes)
- Retrieves the file’s disposition (clean, malware, unknown)
The AMP Everywhere Architecture

AMP Protection across the Extended Network for an Integrated Threat Defense

AMP Threat Intelligence Cloud

- AMP on Firepower NGIPS Appliance (AMP for Networks)
- AMP on Cisco® ASA Firewall with Firepower Services
- AMP on ISR with Firepower Services
- Threat Grid Malware Analysis + Threat Intelligence Engine
- AMP Private Cloud Virtual Appliance
- AMP on Web & Email Security Appliances
- AMP on Cloud Web Security & Hosted Email
- AMP on Firepower NGIPS Appliance (AMP for Networks)

Endpoints

- Windows OS
- Android Mobile
- Virtual
- MAC OS
- CentOS, Red Hat Linux for datacenters

Remote Endpoints

AMP for Endpoints

AMP for Endpoints can be launched from AnyConnect
Plan A: The Protection Framework

All prevention solution < 100% protection

1-to-1 Signatures
Machine Learning, Spero
Device Flow Correlation
Dynamic Analysis

Fuzzy Finger-printing, Ethos
IOCs
Advanced Analytics

Reputation Filtering and File Sandboxing
Plan B: Retrospective Security

- When you can’t detect 100%, visibility is critical

- Antivirus
  - Point-in-time Detection
  - Initial Disposition = Clean
  - Analysis Stops

- Sandboxing
  - Not 100%
  - Sleep Techniques
  - Unknown Protocols
  - Encryption
  - Polymorphism

- Cisco AMP
  - Initial Disposition = Clean
  - Actual Disposition = Bad = Too Late!!
  - Retrospective Detection, Analysis Continues

- Turns back time
- Visibility and Control are Key

Actual Disposition = Bad = Blocked

Initial Disposition = Clean
Ransomware analysis examples
CryptoLocker
• CryptoLocker propagated via infected email attachments, and via an existing botnet
• malware encrypts certain types of files stored on local and mounted network drives using RSA
• private key stored only on the malware's control servers
Cryptolocker in Feb 2016 – device trajectory

renamed with a ".pdf.encrypted" extension
Outgoing connection from **explorer.exe** [common filename],
6.1.7601.17567 (9e1ec8b..ff56ad) [PE Executable] at 192.168.40.73 TCP port 53813 to 37.139.47.101 port 443.

Unknown disposition.

Benign process disposition.

At 2016-02-02 04:41:11 UTC

Parent file SHA-1: cea0890d4b99bae3f635a16dae71f69d137027b9.
Parent file MD5: 8b88ebbb05a0e56b7dcc708498c02b3e.
Parent file size: 2616320 bytes.
Parent file signed by Microsoft Corporation with certificate serial 33000000b011af0a8bd03b9fd0001000000b0 from Microsoft Code Signing PCA. Expired 00:00:00, Mon Jan 1 1601 UTC.

Parent file cert MD5: 7493c06a5c907909c88c812a342ea651.
Parent file cert SHA-1: 108e2ba23632620c427c570b6d9db51ac31387fe.

**it connected to 37.139.47.101:443**

**IP has been related to Cryptolocker**
Retrospective alert

**chrome downloaded an executable file which was then executed by explorer.exe.**

The name of the executable - `au_post_(rand).exe` seems **suspicious**. The **disposition** was unknown.
<table>
<thead>
<tr>
<th>Indicator</th>
<th>Categories</th>
<th>Severity</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>7ev3n Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Chuingam Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>CryptoDefense Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>CryptoFortress Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>CryptoJoker Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Esy Ransomware Detected</td>
<td>infection, persistence, malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Generic Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>95</td>
</tr>
<tr>
<td>Hydra Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Locked Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Locky Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>NanoLocker Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>PClock Ransomware Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Ransomware CryptoLocker Detected</td>
<td>malware</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

**Description:** CryptoLocker is a ransomware program that was released around the beginning of September 2013 and targets all versions of Windows including Windows XP, Windows 7 and Windows 8. When first run, the payload installs itself in the Documents and Settings folder with a random name, and adds a key to the registry that causes it to run on startup. It then attempts to contact one of several designated command and control servers; once connected, the server then generates a 2048-bit RSA key pair, and sends the public key back to the infected computer. CryptoLocker will encrypt certain files using a mixture of RSA & AES encryption. When it has finished encrypting your files, it will display a CryptoLocker payment program that prompts you to send a ransom of either $100 or $300 in order to decrypt the files.
## Behavioral Indicators

### Shadow Copy Deletion Detected

Volume Shadow Copies are snapshots of portions of a file system used for backups and System Restore points. The `vssadmin.exe` utility provides a way to remove these copies. Malware authors may delete these copies in order to make recovery and access to a target's original files more difficult. This is especially true for ransomware varieties which encrypt files since these shadow copies may still contain the files in an unencrypted state.

<table>
<thead>
<tr>
<th>Command Line</th>
<th>Process Name</th>
<th>Process ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vssadmin.exe Delete Shadows /All /Quiet</td>
<td>vssadmin.exe</td>
<td>2036 (vssadmin.exe)</td>
</tr>
</tbody>
</table>

### Excessive Suspicious Activity Detected

- **Severity:** 90  
  - **Confidence:** 100

### Process Modified a File in a System Directory

- **Severity:** 90  
  - **Confidence:** 100

### Registry Persistence Mechanism Refers to an Executable in a System Directory

- **Severity:** 90  
  - **Confidence:** 100

### Excessive Number of DNS Queries

- **Severity:** 70  
  - **Confidence:** 100

### Process Modified an Executable File

- **Severity:** 60  
  - **Confidence:** 100

### Processes Have A Circular Parent-Child Relationship

- **Severity:** 60  
  - **Confidence:** 80

### Process Modified Autorun Registry Key Value

- **Severity:** 80  
  - **Confidence:** 60

### Potential Sandbox Detection - Enumeration of ProductID

- **Severity:** 80  
  - **Confidence:** 70

### Process Disables the Phishing Filter of Internet Explorer 8

- **Severity:** 50  
  - **Confidence:** 60

### Potential Code Injection Detected

- **Severity:** 50  
  - **Confidence:** 50

---

**Threat Score:** 100

**Categories:** weakening

**Tags:** crypto, ransomware, file, system
Artifacts – DNS traffic

### DNS Traffic

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Query Data</th>
<th>TTL</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>okshizyyu.otiyruqaewt.org</td>
<td>-</td>
<td>+50.837s</td>
</tr>
<tr>
<td>A</td>
<td>ozogytof.otiyruqaewt.org</td>
<td>-</td>
<td>+70.596s</td>
</tr>
<tr>
<td>A</td>
<td>ivalo.otiyruqaewt.org</td>
<td>-</td>
<td>+192.057s</td>
</tr>
<tr>
<td>A</td>
<td>efymtbu.otiyruqaewt.org</td>
<td>-</td>
<td>+135.928s</td>
</tr>
<tr>
<td>A</td>
<td>upipohacuhw.otiyruqaewt.org</td>
<td>-</td>
<td>+288.092s</td>
</tr>
<tr>
<td>A</td>
<td>adixatug.o.tyiruqaewt.org</td>
<td>-</td>
<td>+227.521s</td>
</tr>
<tr>
<td>A</td>
<td>asoviv.otiyruqaewt.org</td>
<td>-</td>
<td>+55.54s</td>
</tr>
<tr>
<td>A</td>
<td>egkkedaqu.otyiruqaewt.org</td>
<td>-</td>
<td>+237.601s</td>
</tr>
<tr>
<td>A</td>
<td>jgoq.otiyruqaewt.org</td>
<td>-</td>
<td>+105.981s</td>
</tr>
<tr>
<td>A</td>
<td>olozirkwez.otiyruqaewt.org</td>
<td>-</td>
<td>+303.32s</td>
</tr>
<tr>
<td>A</td>
<td>itumeq.otiyruqaewt.org</td>
<td>-</td>
<td>+146.181s</td>
</tr>
</tbody>
</table>

#### DNS Query Returned Non-Existent Domain

This BI indicates that a DNS query was performed to an unregistered domain name. This could be for a domain not yet used by the author, an abandoned domain, or intentional noise from a domain generation algorithm.

<table>
<thead>
<tr>
<th>Answer Code</th>
<th>Query Data</th>
<th>Query Type</th>
<th>Query ID</th>
<th>Network Stream</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXDOMAIN</td>
<td>obiwogzybo.otiyruqaewt.org</td>
<td>A</td>
<td>35418</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>adepulaty.otiyruqaewt.org</td>
<td>A</td>
<td>61882</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>egkkedaqu.otyiruqaewt.org</td>
<td>A</td>
<td>9201</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>bpesajj.otiyruqaewt.org</td>
<td>A</td>
<td>42319</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>ajjenasyjo.otiyruqaewt.org</td>
<td>A</td>
<td>59124</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>irururyqf.otiyruqaewt.org</td>
<td>A</td>
<td>18551</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>inawocupi.otiyruqaewt.org</td>
<td>A</td>
<td>54987</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>okshizyju.otiyruqaewt.org</td>
<td>A</td>
<td>3593</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>iljy.otiyruqaewt.org</td>
<td>A</td>
<td>27088</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>oraroru.otiyruqaewt.org</td>
<td>A</td>
<td>55397</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>kcydoxev.otiyruqaewt.org</td>
<td>A</td>
<td>33784</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>icyvpet.otiyruqaewt.org</td>
<td>A</td>
<td>24488</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>icopotomyce.otiyruqaewt.org</td>
<td>A</td>
<td>58393</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>adixatug.o.tyiruqaewt.org</td>
<td>A</td>
<td>7707</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>acywsu.otiyruqaewt.org</td>
<td>A</td>
<td>59808</td>
<td>Stream 2</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>ybodkwu.otiyruqaewt.org</td>
<td>A</td>
<td>57276</td>
<td>Stream 2</td>
</tr>
</tbody>
</table>
OpenDNS – AMP Threat Grid Collaboration
Angler exploit kit, Teslacrypt, Cryptowall

http://blog.talosintel.com/2015/12/cryptowall-4.html
Angler infrastructure

- Angler
  - 90,000 victims daily
  - 40% “success” rate
  - 62%: ransomware: Cryptowall + Teslacrypt
  - A few Day0’s
  - Target: IE, No: Chrome
- RIG (webzilla)
- Nuclear:
  - domain shadowing
  - HTTP302: URL redirect
  - Referer checking

Diagram:
- USER
- Redirect to Proxy Server
- Adobe Flash, Silverlight, ...
- Proxy Server
- Proxy Server gets data from Exploit Server (Part 81)
- Exploit Server
- Exploit Server sends HTTP Requests to Status Server
- Status Server
- Status Server tracks HTTP Requests / Status
- Roll up of log data pushed to Master Server
- MASTER SERVER
TeslaCrypt

- Imitates CryptoLocker screen
- Pay in Bitcoin
- Not asymmetric (RSA2048) keys used
- Encryption: AES CBC 256-bit
TeslaCrypt: Victory

http://www.talosintelligence.com/teslacrypt_tool/

- TeslaCrypt 0.x - Encrypts files using an AES-256 CBC algorithm
- TeslaCrypt 2.x - Same as previous versions, but uses EC to create a weak Recovery key. The application is able to use factorization to recover the victim's global private key.
- TeslaCrypt 3 & 4 - The latest versions. Able to decrypt thanks to the C&C server EC private key which was recently released.

Project closed
master key for decrypt 440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE
wait for other people make universal decrypt software

we are sorry!
Device Trajectory
For Demo_TeslaCrypt

2016-09-09 08:17:41 UTC

`t.exe`, calc 1.0.0.1 (3372c1e..34a370) [PE Executable] was
Executed by `explorer.exe`, Microsoft® Windows® Operating
System 6.1.7601.17567 (9e1ec8b..ff56ad) [PE Executable].
Detected as W32.3372C1EDAB-100.SBX.TG.
The file was not quarantined. Quarantine event missing.
Benign parent disposition.
File full path: c:\t.exe
File SHA-1: e654d39cd13414b5151e8cf0d8f5b166ddd45cb.
File MD5: 209a288c68207d57e0ce66e60bf60729.
File size: 290816 bytes.
Parent file SHA-1: ceb0890d4b99baf3635a16daa71f691d37027b9.
Parent file MD5: 8888ebbb05a0e6b7dc708498c02b3e.
Parent file size: 2616320 bytes.
Parent file signed by Microsoft Corporation with certificate
serial 330000000b011a08bd03b9fdd0001000000b0 from
Microsoft Code Signing PCA. Expired 00:00:00, Mon Jan 1 1601
UTC.
Parent file cert MD5: 7493c06a5c907909c88c812a342ea651.
Vssadmin: delete shadow copy

2016-09-09 08:17:41 UTC

**vssadmin.exe**, Microsoft® Windows® Operating System 6.1.7600.16385 (e09bf4d..18ad10)[PE Executable] was Executed by t.exe, calc 1.0.0.1 (3372c1e..34a370)[HTML].

Benign disposition.

Detected as parent disposition.

File full path: c:\windows\system32\vssadmin.exe

File SHA-1: b1b1e773a7a6ba38302b345a9088bb52b0f7e6394.

File MD5: 6e248a3d528ede43994457cf417bd665.

Parent file SHA-1: e654d39cd13414b5151e8cf0d8f5b166ddd45cb.

Parent file MD5: 209a288c68207d57e0ce6e60ebf60729.

Parent file size: 290816 bytes.
**Device Trajectory**
For Demo_TeslaCrypt

[Image of a timeline with various processes and an alert message]

**Alert Message**

---

**Outgoing connection from t.exe, calc 1.0.0.1 (3372c1e..34a370) [HTML] at 192.168.1.3 TCP port 49308 to 54.175.62.201 port 443.**

Unknown disposition.

Detected as process disposition.

At 2016-09-09 08:17:43 UTC

**Parent file SHA-1:** e654d39cd13414b5151e8cf0d8f5b166ddd54cb.

**Parent file MD5:** 209a288c68207d57e0ce6e60ebf60729.

**Parent file size:** 290816 bytes.
---

**C2 communication**
Cryptowall

- Version 4: Deletes all shadow copies, encrypts the filenames
- 2048 byte RSA public key encryption
- Decryption software's initial price: $500
- If it cannot retrieve the public RSA encryption key from the C2 server, it will not "harm" the victim's computer.
- Excludes certain regions from infection (Russia +...)
Cryptowall: File encryption

Temporary AES key can only be decrypted with the private RSA key.

From C&C server:
- Encrypted AES256 key
- Other data
- Encrypted 1.jpg
- random.xyz

1.jpg

Temp. AES256 key

RSA public key
Word creates and executes an exe
Accesses Wordpress -> process injection
### Behavioral Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Severity</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptowall Communications Detected</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Ransomware Backup Deletion Detected</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Registry Modification Disabled System Restore</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Shadow Copy Deletion Detected</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Artifact Flagged Malicious by Antivirus Service</td>
<td>100</td>
<td>95</td>
</tr>
<tr>
<td>Excessive Suspicious Activity Detected</td>
<td>90</td>
<td>100</td>
</tr>
<tr>
<td>Registry Persistence Mechanism Refers to an Executable in a User Data Directory</td>
<td>90</td>
<td>100</td>
</tr>
<tr>
<td>Excessive Number of DNS Queries</td>
<td>70</td>
<td>100</td>
</tr>
<tr>
<td>Artifact Flagged by Antivirus</td>
<td>80</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified an Executable File</td>
<td>60</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified File in a User Directory</td>
<td>70</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified File in a User Directory</td>
<td>70</td>
<td>100</td>
</tr>
<tr>
<td>Process Disabled Internet Explorer Proxy</td>
<td>70</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified Autorun Registry Key Value</td>
<td>80</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified Trusted Root Certificates</td>
<td>60</td>
<td>100</td>
</tr>
<tr>
<td>DNS Query Returned Non-Existing Domain</td>
<td>75</td>
<td>100</td>
</tr>
<tr>
<td>Possible Double Flux Nameserver Detected [Beta]</td>
<td>35</td>
<td>50</td>
</tr>
<tr>
<td>URL Resulted in 404 for Empty File</td>
<td>65</td>
<td>100</td>
</tr>
<tr>
<td>Ransomware Queried Domain</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>
Locky/Zepto

http://blog.talosintel.com/2016/06/gotta-be-swift-for-this-spam-campaign.html
Locky

- **extension**: .locky
- **RSA and AES algorithms (Windows CryptoAPI)**

- Email/ phishing [137,731 emails per 4 days]
- Spam spike -> spam level like in 2010
- **Doc or Javascript, attachment**: swift [XXX|XXXX].js X: numbers
- Please allow macro: “if the data encoding is incorrect.”
- Deletes shadow copies, ‘wscript.exe’ send HTTP GET requests to C2 domains
## Analysis Report

<table>
<thead>
<tr>
<th>ID</th>
<th>36d03b1d326983a4aa253973d06fe2</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>2800.xpse.080413-2111</td>
</tr>
<tr>
<td>Started</td>
<td>6/29/16 13:36:19</td>
</tr>
<tr>
<td>Ended</td>
<td>6/29/16 13:42:10</td>
</tr>
<tr>
<td>Duration</td>
<td>0:05:51</td>
</tr>
<tr>
<td>Sandbox</td>
<td>phl-work-11 (pilot-d)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filename</th>
<th>swift 6d2.js</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magic Type</td>
<td>JavaScript</td>
</tr>
<tr>
<td>Analyzed As</td>
<td>js</td>
</tr>
<tr>
<td>SHA256</td>
<td>00e475ae83002930c6a9dd9c4223fd710c3a29a4c1c3775413d58e9e23e5c0b2</td>
</tr>
<tr>
<td>SHA1</td>
<td>7907255b6fd0d5600d4d9c311d72003d308b4fda</td>
</tr>
<tr>
<td>MD5</td>
<td>15ae1614b42526956a3855071553b056</td>
</tr>
<tr>
<td>Tags</td>
<td><img src="tag" alt="tag" /></td>
</tr>
</tbody>
</table>

## Behavioral Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Severity</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Modified Desktop Wallpaper</td>
<td>100</td>
<td>95</td>
</tr>
<tr>
<td>A Script Established Direct IP Communications</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td>Command Exe File Deletion Detected</td>
<td>75</td>
<td>100</td>
</tr>
<tr>
<td>Windows Picture And Fax Viewer Used To Display Decoy Image</td>
<td>70</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified an Executable File</td>
<td>60</td>
<td>100</td>
</tr>
<tr>
<td>An HTTP Request Was Made to a Numeric IP Address</td>
<td>75</td>
<td>100</td>
</tr>
<tr>
<td>Process Created an Executable in a User Directory</td>
<td>60</td>
<td>95</td>
</tr>
<tr>
<td>Outbound HTTP GET Request</td>
<td>75</td>
<td>75</td>
</tr>
<tr>
<td>Process Modified File in a User Directory</td>
<td>70</td>
<td>80</td>
</tr>
<tr>
<td>Process Modified AUTOEXEC.BAT</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>A Script File Established Network Communications</td>
<td>70</td>
<td>80</td>
</tr>
<tr>
<td>Process Disabled Internet Explorer Proxy</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>Command Exe File Execution Detected</td>
<td>50</td>
<td>80</td>
</tr>
<tr>
<td>File Downloaded to Disk</td>
<td>30</td>
<td>90</td>
</tr>
<tr>
<td>Potential Code Injection Detected</td>
<td>35</td>
<td>50</td>
</tr>
<tr>
<td>DNS Response Contains Low Time to Live (TTL) Value</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>Outbound HTTP POST Communications</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>Outbound Communications to Nginx Web Server</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>
One more thing ...
Host Analysis

![Image of Cisco Firepower Management Center for VMWare and Network File Trajectory for 3381eff5...213c415e]

- **Current User**: mordsc (LDAP)
- **Host Profile**:
  - IP Addresses: 198.19.19.38
  - NetBIOS Name: vFTD (2)
  - MAC Addresses (TTL): 00:50:56:00:00:01 (VMware, Inc.) (254)
  - Host Type: NAT Device
  - Last Seen: 2016-04-22 21:51:09

- **Indications of Compromise**:
  - ChC Connected: Security Intelligence Event - ChC
    - First Seen: 2016-03-30 18:40:28
    - Last Seen: 2016-04-02 22:23:04
  - Impact 2 Attack: Impact 2 Intrusion Event - attempted-admin
    - First Seen: 2016-04-02 13:55:22
  - Malware Detected: Threat Detected in File Transfer
    - First Seen: 2016-04-02 11:17:21
    - Last Seen: 2016-04-02 11:59:30

- **Threat Score**: Very High
- **Detection Name**: W32.3381EFF572-100...X.TG
Retrospective Alert

Network File Trajectory for 948ad120...fa40f778

File SHA256: 948ad120...fa40f778
File Name: Job-Obscene-Salary.xls
File Size (KB): 51.0000
File Type: MSOLE2
File Category: Office Documents
Current Disposition: Malware
Threat Score: Very High
Detection Name: W32.948AD12043-100 SBX TG

First Seen: 2016-03-28 19:04:39 on 14.144.144.66
Event Count: 2
Seen On: 3 hosts (2 displayed)
Seen On Breakdown: 2 senders → 2 receivers (1 → 1 displayed)

Trajectory:
Mar 28
14.144.144.66
198.19.19.38

Events
- Time: 2016-03-28 19:04:39
  - Event Type: Transfer
  - Sending IP: 14.144.144.66
  - Receiving IP: 198.19.19.38
  - File Name: Job-Obscene-Salary.xls
  - Disp.: Unknown
  - Action: Malware
  - Protocol: HTTP
  - Client: Chrome
  - Web App: Unspecified

- Time: 2016-03-28 20:27:57
  - Event Type: Retrospect...
### Dynamic Analysis Summary

<table>
<thead>
<tr>
<th>Report</th>
<th>Score</th>
<th>Date/Time</th>
<th>OS</th>
<th>Threat Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100</td>
<td>2016-03-27 12:56:03</td>
<td>Windows XP - SP3/i386</td>
<td>Office Document Launches a Powershell</td>
</tr>
</tbody>
</table>

Showing the report for the highest score because no report with a matching score was found.

### Threats

- Office Document Launches a Powershell (100)
- A Document File Established Network Communications (90)
- Office Document Contains a VBA Macro (56)
- PowerShell Used With Encoded Command (42)
- Potential Code Injection Detected (25)
- DNS Query Returned Non-Existent Domain (18)
Summary
AMP and Ransomware

- Most profitable malware, targeting corporates
- Main goal: focus on protection, but quick detections and countermeasures [retrospective analysis] can minimize the costs.
- AMP: Time-to-detect: [TTD] 13 hours vs 100-200 days,
- NSS Labs: 91.8% [>=3min]