



Ransomware Detection and Analysis with Advanced Malware Protection (AMP)

György Ács
Cisco Systems



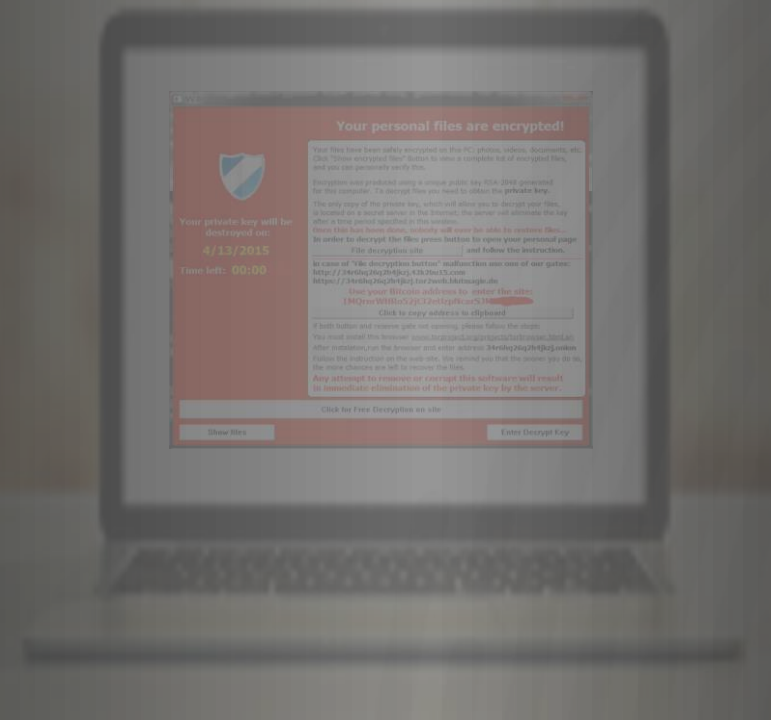
Agenda

- Modern malware: ransomware
 - What can be done?
 - Ransomware analysis examples
-



Ransomware: Easy Profits

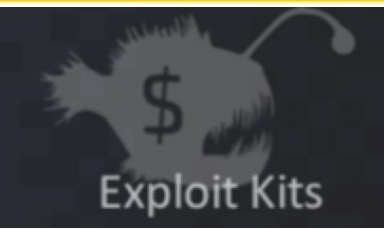
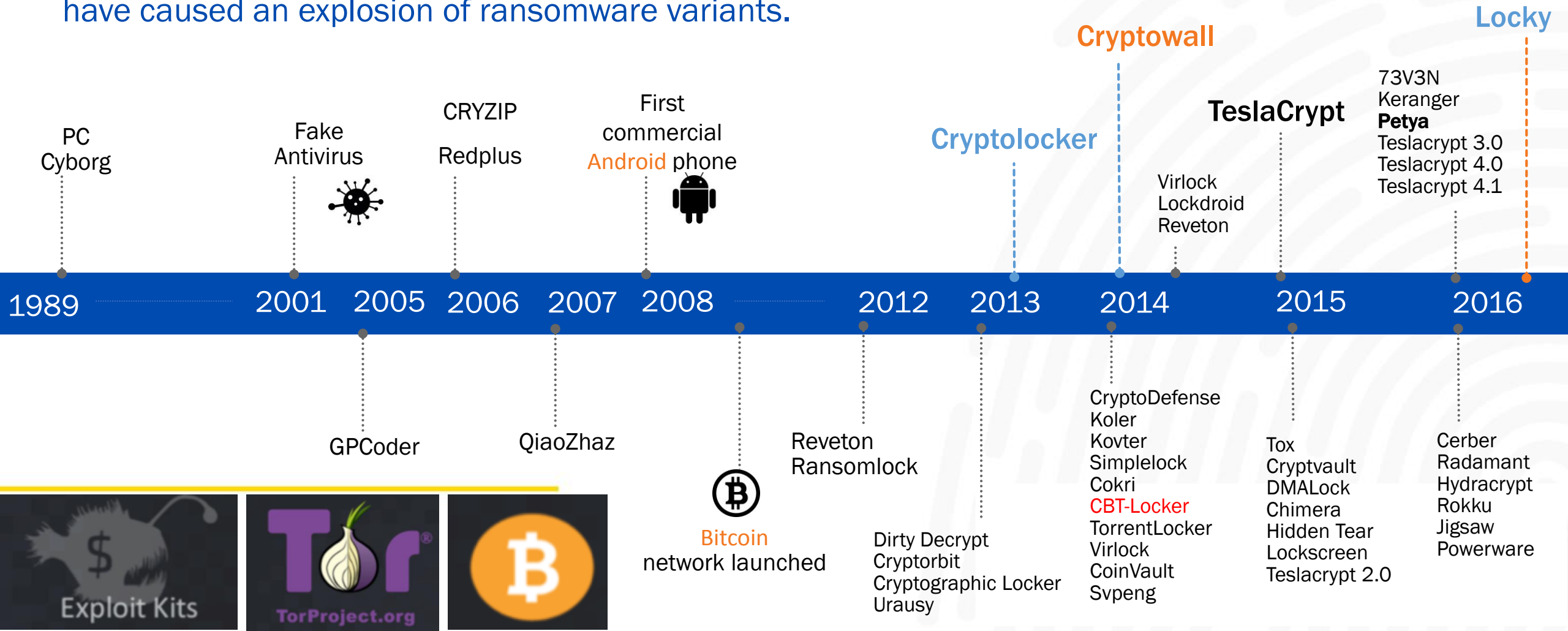
- **Most profitable** malware in history
- Lucrative: Direct payment to attackers!
- Cyber-criminals collected **\$209 million in the first three months of 2016** by extorting businesses and institutions to unlock computer servers.
- At that rate, **ransomware** is on pace to be a **\$1 billion a year** 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.



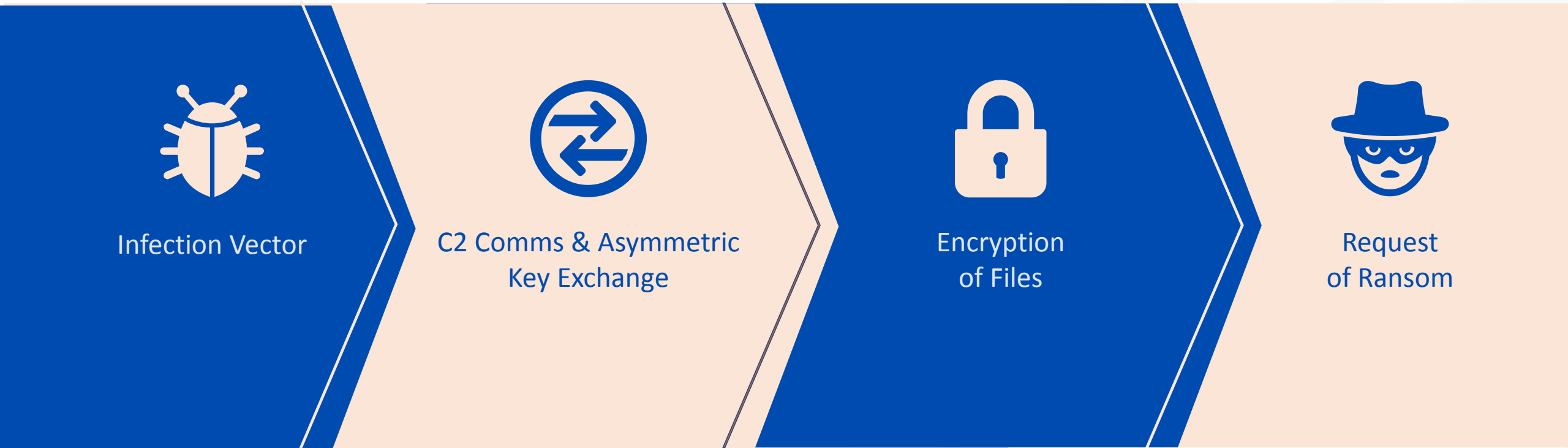


How Does Ransomware Work?



Typical Ransomware Infection

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



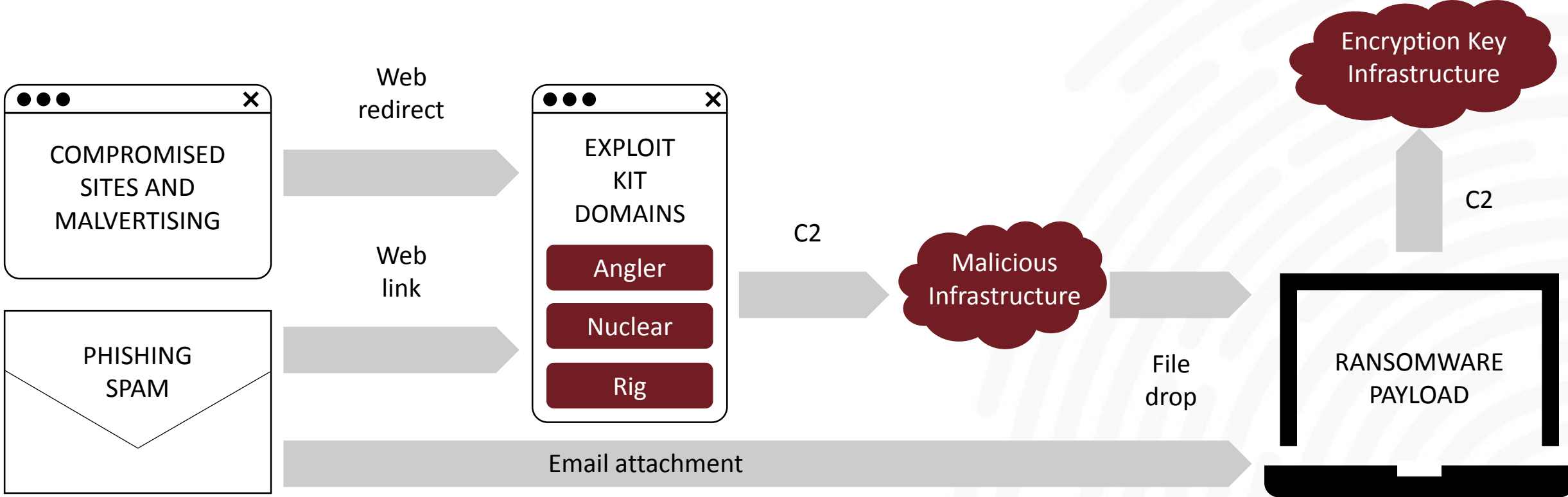
Ransomware frequently uses web and email

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



Most Ransomware Relies on C2 Callbacks



Encryption Key

Payment MSG

NAME*	DNS	IP	NO C2	TOR	PAYMENT
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

*Top variants as of March 2016



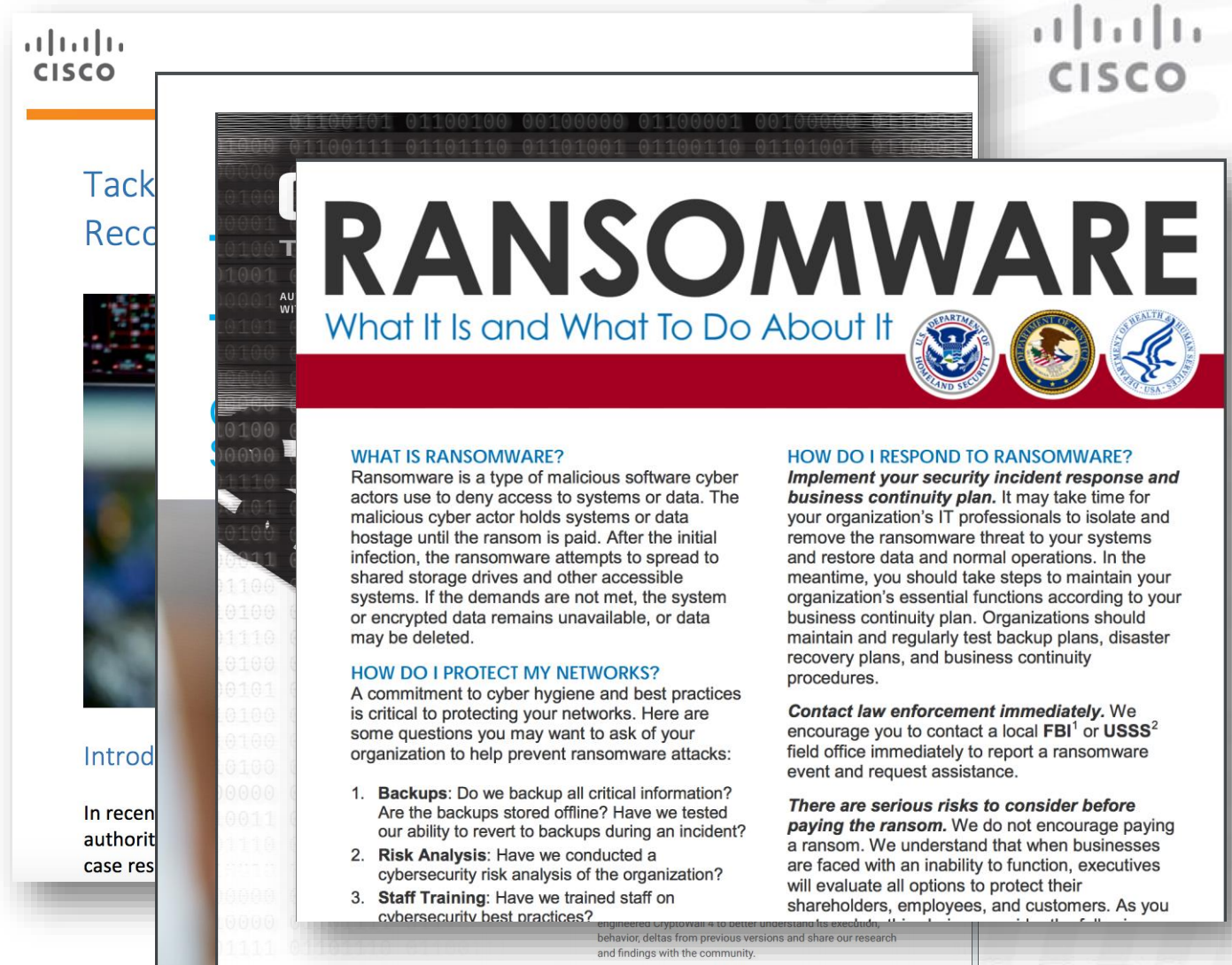


What can be done?



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)



The image shows a document titled "RANSOMWARE: What It Is and What To Do About It" from Cisco Security. The document is a white page with a red header bar. The Cisco logo is in the top left and right corners. The title "RANSOMWARE" is in large, bold, black letters. Below the title, the subtitle "What It Is and What To Do About It" is in blue. There are three circular logos from the U.S. Department of Homeland Security, U.S. Department of Justice, and U.S. Department of Health & Human Services. The document is divided into sections: "WHAT IS RANSOMWARE?", "HOW DO I PROTECT MY NETWORKS?", and "HOW DO I RESPOND TO RANSOMWARE?". The "WHAT IS RANSOMWARE?" section explains that ransomware is a type of malicious software that denies access to systems or data. The "HOW DO I PROTECT MY NETWORKS?" section lists three key practices: Backups, Risk Analysis, and Staff Training. The "HOW DO I RESPOND TO RANSOMWARE?" section emphasizes the importance of having a security incident response and business continuity plan, and encourages contacting law enforcement immediately. The document also includes a warning: "There are serious risks to consider before paying the ransom." The Cisco SEC logo is at the bottom right.

RANSOMWARE
What It Is and What To Do About It

WHAT IS RANSOMWARE?
Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I PROTECT MY NETWORKS?
A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?

HOW DO I RESPOND TO RANSOMWARE?
Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact a local FBI¹ or USSS² field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you

<http://blogs.cisco.com/security/ransomware-the-race-you-dont-want-to-lose>

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)

  voicemail23WMZ.html (17 KB) [Preview](#)

 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



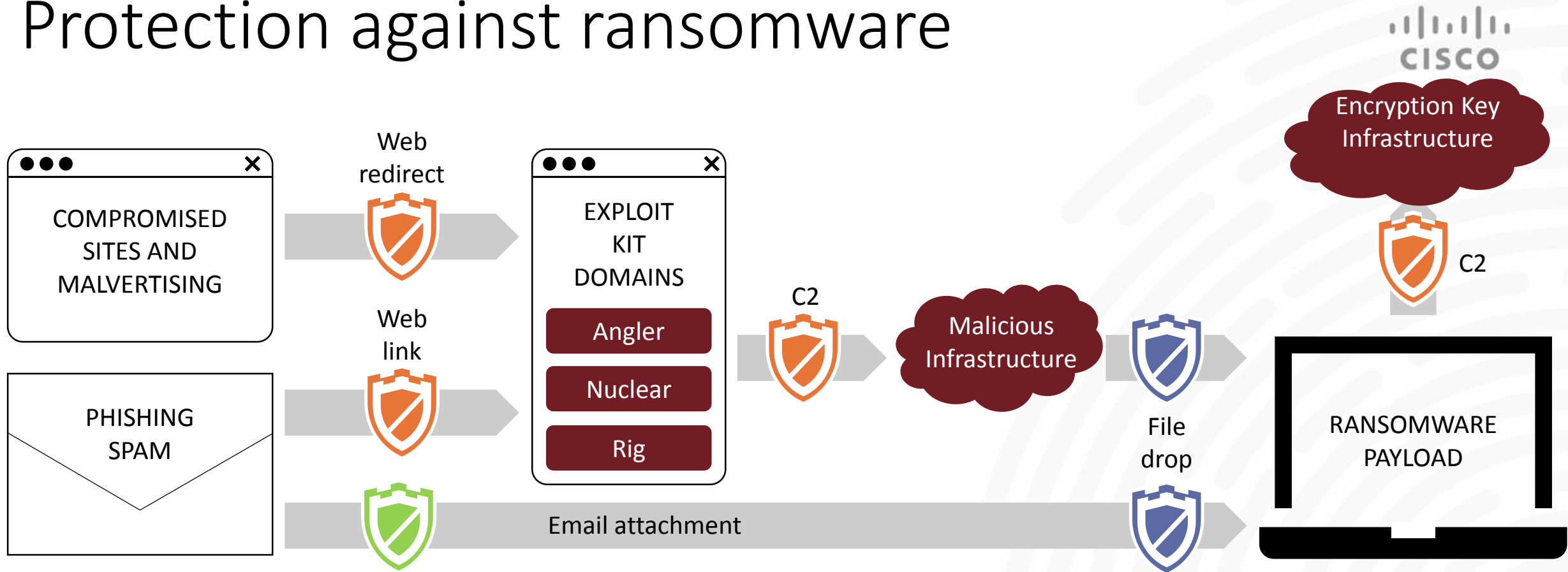
AMP

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




CISCO  SEC

Protection against ransomware



 Blocked by
DNS Security

 Blocked by
Cisco AMP for Endpoints or
Network

 Blocked by
Email Security

CISCO  SEC

AMP: Advanced Malware Protection



Network-based AMP



Firepower Management Center



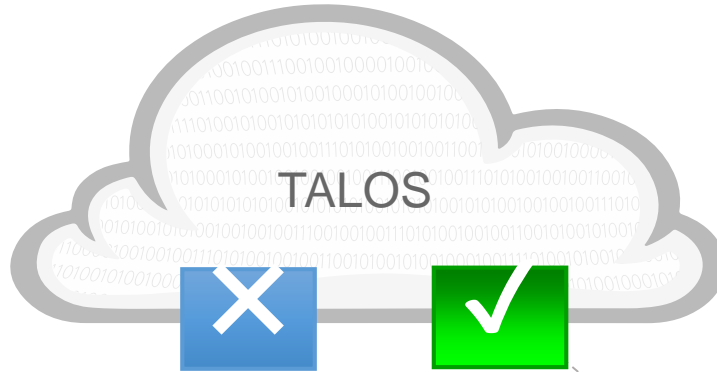
Firepower or ASA FirePower Services



AMP Malware license



No agent needed



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**)



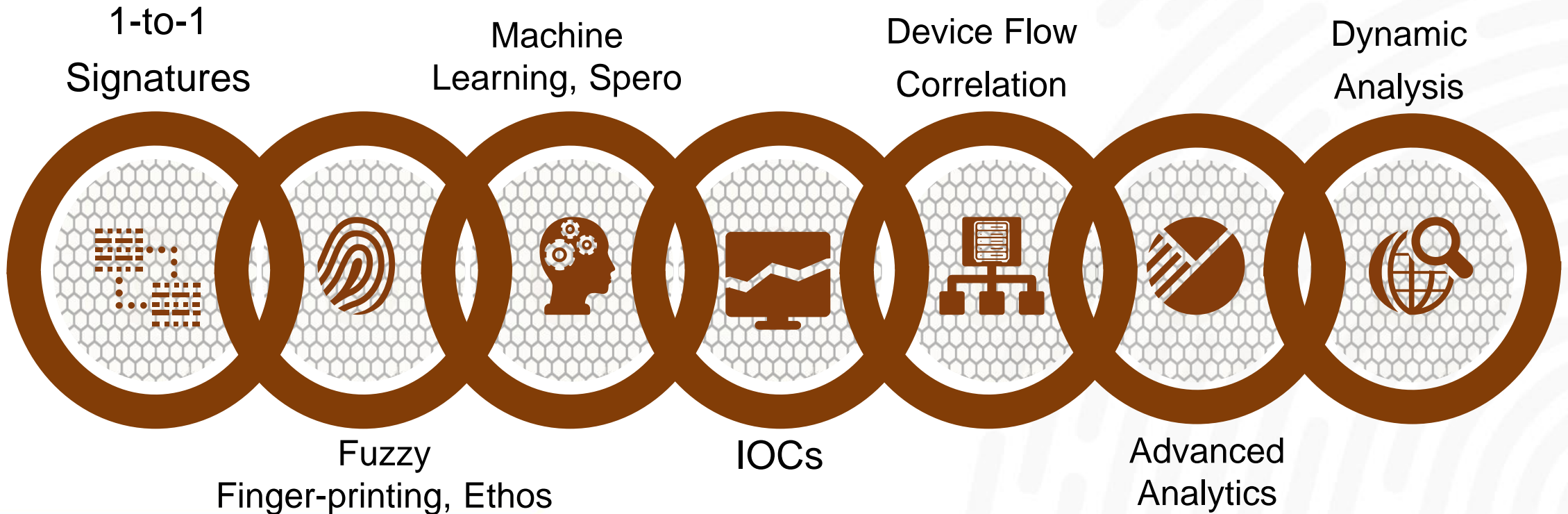
Get Your Head Out of the Sandbox



Plan A: The Protection Framework



All prevention solution < 100% protection

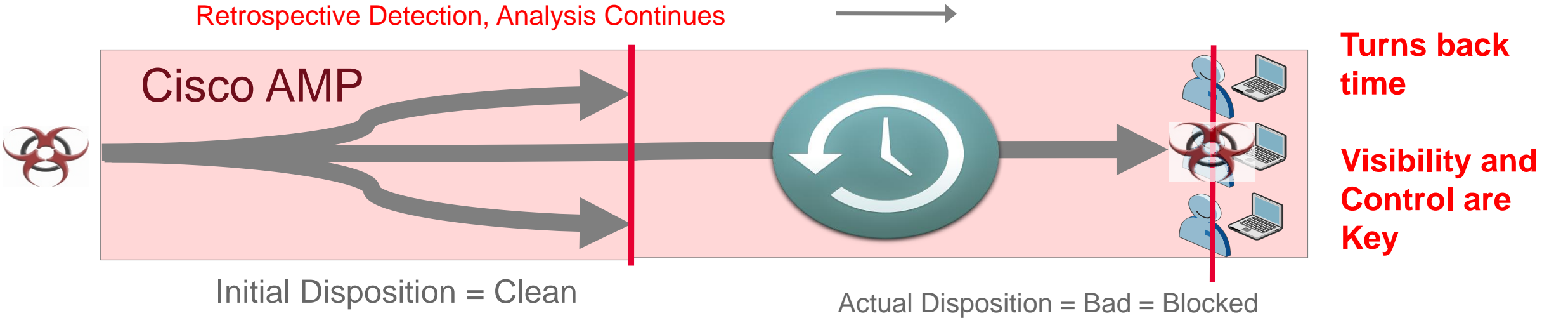
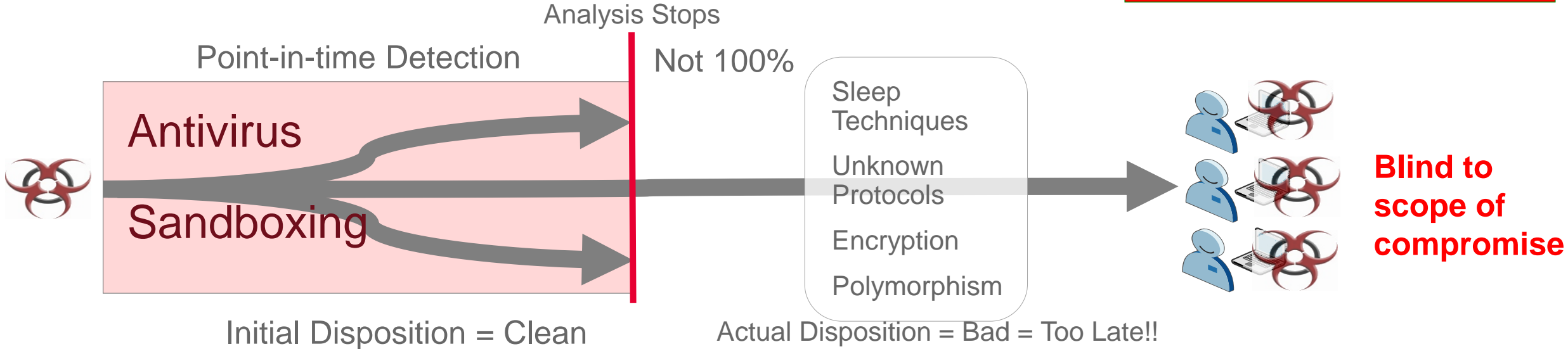


Reputation Filtering and File Sandboxing



Plan B: Retrospective Security

• When you can't detect 100%, visibility is critical



Ransomware analysis examples



CryptoLocker



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

The screenshot displays a file explorer window with a list of files, many of which have been renamed with a ".pdf.encrypted" extension. A context menu is open over one of the files, showing options such as "File Analysis", "File Trajectory", and "File Fetch". A blue callout box points to the file list with the text "renamed with a '.pdf.encrypted'". To the right, an "OpenIOC: W32.Cryptolocker.ioc" notification is visible, providing a description of the malware's behavior and the time it was detected. A second blue callout box points to the notification with the text "renamed with a '.pdf.encrypted' extension".

[System]
re wandi south s... [OLE2]
explorer.exe [PE]
\$rcv5vzu.pdf.encr... [PDF]
\$replgze.pdf.encr... [PDF]
\$rg3f72v.pdf.encr... [PDF]
\$rhmf79q.msg.e... [OLE2]
\$rkdyxs.pdf.ency... [PDF]
dewatering licens... [PDF]
\$rlijkd3.pdf.ency... [PDF]
\$rl22ip6.pdf.encr... [PDF]
\$r6rrun0.pdf.encr... [PDF]
\$rmt4gd4.pdf.enc... [PDF]

\$rcv5vzu.pdf.encr... [PDF]
\$replgze.pdf.er...
\$rg3f72v.pdf.er...
\$rhmf79q.msg...
\$rkdyxs.pdf.enc...
dewatering lice...
\$rlijkd3.pdf.enc...
\$rl22ip6.pdf.er...
\$r6rrun0.pdf.er...
\$rmt4gd4.pdf.e...
sup...@austi...
\$...5r7.pdf.er...
...lvbxb.pdf.er...
treatment_an...
re wandi south...
\$rxw05hg.pdf.e...
p6a4svww.cab.e...
explor...
p6a4ptww.cab.e...
\$rw36g2b.pdf.f...
\$rxqp4ks.pdf.er...
\$rv13r1l.pdf.er...
re wandi south...
\$romwqeh.pdf.f...
\$roios2i.pdf.enc...
\$rmiw7uy.pdf.e...
patio document...
cce04082015.p...
dewatering ma...
\$rkjco73.pdf.encr... [PDF]
\$rllvof.pdf.ency... [PDF]

5d0da70..cdc3ca

Disposition: Unknown

Filename: \$rcv5vzu.pdf.encrypted

Copy SHA-256

Search

View Full SHA-256

File Analysis

File Trajectory

File Fetch

Simple Detection

Application Blocking

Whitelist

Back

Forward

Reload

OpenIOC: W32.Cryptolocker.ioc

Description: This IoC detects a version of cryptolocker that injects malicious code into explorer.exe. The malicious code renames victim's files with a .encrypted file extension before encrypting them.

At 04:41:45, Tue Feb 2 2016 UTC

renamed with a ".pdf.encrypted"

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

[\[less details \]](#)

Parent file SHA-1: cea0890d4b99bae3f635a16dae71f69d137027b9.

Parent file MD5: 8b88ebbb05a0e56b7dcc708498c02b3e.

Parent file size: 2616320 bytes.

Parent file signed by Microsoft Corporation with certificate serial
33000000b011af0a8bd03b9fdd0001000000b0 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

Indicator	Categories	Severity	Confidence
7ev3n Ransomware Detected	malware	100	100
Chuingam Ransomware Detected	malware	100	100
CryptoDefense Ransomware Detected	malware	100	100
CryptoFortress Ransomware Detected	malware	100	100
CryptoJoker Ransomware Detected	malware	100	100
Esy Ransomware Detected	infection persistence malware	100	100
Generic Ransomware Detected	malware	100	95
Hydra Ransomware Detected	malware	100	100
Locked Ransomware Detected	malware	100	100
Locky Ransomware Detected	malware	100	100
NanoLocker Ransomware Detected	malware	100	100
PClock Ransomware Detected	malware	100	100
Ransomware CryptoLocker Detected	malware	100	100
<p>Descriptio... 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.</p>			
Ransomware CryptoLocker Variant Detected	malware	100	100
TeslaCrypt 2.2 Ransomware Detected	infection persistence malware	100	100
TeslaCrypt 3.0 Ransomware Detected	mawlware	100	100
TeslaCrypt 3.1 Ransomware Detected	malware	100	100

Analysis Report

[Resubmit](#)

ID	4fa958d6d53b70c1bc8c5f1c170ed2bb	Filename	724026eeb1d4789f77f1c6dea493cd8d.exe
OS	2600.xpsp.080413-2111	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	2/3/16 08:25:01	Analyzed As	exe
Ended	2/3/16 08:31:15	SHA256	791b4b565431078fa7d183719d71021cad76b9b442d108ba173a8e6f53e2855a
Duration	0:06:14	SHA1	3d752bc268726e077607b7afbb6f94e8f4b5b33d
Sandbox	phl-work-25 (pilot-d)	MD5	724026eeb1d4789f77f1c6dea493cd8d
		Tags	tag

Warnings

- Executable Failed Integrity Check

Behavioral Indicators

Threat Score: 100

Shadow Copy Deletion Detected

Severity: 100 Confidence: 100

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.

Categories weakening**Tags** crypto, ransomware, file, system[Report Error](#)

Command Line	Process Name	Process ID
vssadmin.exe Delete Shadows /All /Quiet	vssadmin.exe	2036 (vssadmin.exe)

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: 60 Confidence: 70

Process Disables the Phishing Filter of Internet Explorer 8

Severity: 50 Confidence: 60

Potential Code Injection Detected

Severity: 50 Confidence: 50

DNS Traffic

⊕ Query Type: A, Query Data: okshizyju.otyiruqaewt.org

Stream: 2 Query: 3593

TTL: - Timestamp: +50.637s

⊕ Query Type: A, Query Data: ozogytof.otyiruqaewt.org

Stream: 2 Query: 3633

TTL: - Timestamp: +70.598s

⊕ Query Type: A, Query Data: ivalo.otyiruqaewt.org

Stream: 2 Query: 5047

TTL: - Timestamp: +192.057s

⊕ Query Type: A, Query Data: efymtbu.otyiruqaewt.org

Stream: 2 Query: 6002

TTL: - Timestamp: +135.928s

⊕ Query Type: A, Query Data: upipohacuhw.otyiruqaewt.org

Stream: 2 Query: 6552

TTL: - Timestamp: +288.092s

⊕ Query Type: A, Query Data: adixatugo.otyiruqaewt.org

Stream: 2 Query: 7707

TTL: - Timestamp: +227.521s

⊕ Query Type: A, Query Data: asoviv.otyiruqaewt.org

Stream: 2 Query: 8146

TTL: - Timestamp: +55.54s

⊕ Query Type: A, Query Data: egkkedaqup.otyiruqaewt.org

Stream: 2 Query: 9201

TTL: - Timestamp: +237.601s

⊕ Query Type: A, Query Data: jgog.otyiruqaewt.org

Stream: 2 Query: 9288

TTL: - Timestamp: +105.981s

⊕ Query Type: A, Query Data: olozirkwez.otyiruqaewt.org

Stream: 2 Query: 10986

TTL: - Timestamp: +303.32s

⊕ Query Type: A, Query Data: itumeq.otyiruqaewt.org

Stream: 2 Query: 11648

TTL: - Timestamp: +146.181s

⊖ 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.

Answer Code	Query Data	Query Type	Query ID	Network Stream
NXDOMAIN	obiwdgozybo.otyiruqaewt.org	A	35418	Stream 2
NXDOMAIN	adepulaty.otyiruqaewt.org	A	61862	Stream 2
NXDOMAIN	egkkedaqup.otyiruqaewt.org	A	9201	Stream 2
NXDOMAIN	bpesaju.otyiruqaewt.org	A	42319	Stream 2
NXDOMAIN	ajujenasyjo.otyiruqaewt.org	A	59124	Stream 2
NXDOMAIN	irururyrqf.otyiruqaewt.org	A	18551	Stream 2
NXDOMAIN	inawocupi.otyiruqaewt.org	A	54987	Stream 2
NXDOMAIN	okshizyju.otyiruqaewt.org	A	3593	Stream 2
NXDOMAIN	ilyk.otyiruqaewt.org	A	27068	Stream 2
NXDOMAIN	oraxoru.otyiruqaewt.org	A	55397	Stream 2
NXDOMAIN	kcydoxev.otyiruqaewt.org	A	33784	Stream 2
NXDOMAIN	icyvfpet.otyiruqaewt.org	A	24488	Stream 2
NXDOMAIN	icopotomyce.otyiruqaewt.org	A	58393	Stream 2
NXDOMAIN	adixatugo.otyiruqaewt.org	A	7707	Stream 2
NXDOMAIN	aqywu.otyiruqaewt.org	A	59808	Stream 2
NXDOMAIN	ybodkwu.otyiruqaewt.org	A	57276	Stream 2

Angler exploit kit, Teslacrypt, Cryptowall

<http://blog.talosintel.com/2015/12/cryptowall-4.html>



VV 0

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files press button to open your personal page

and follow the instruction.

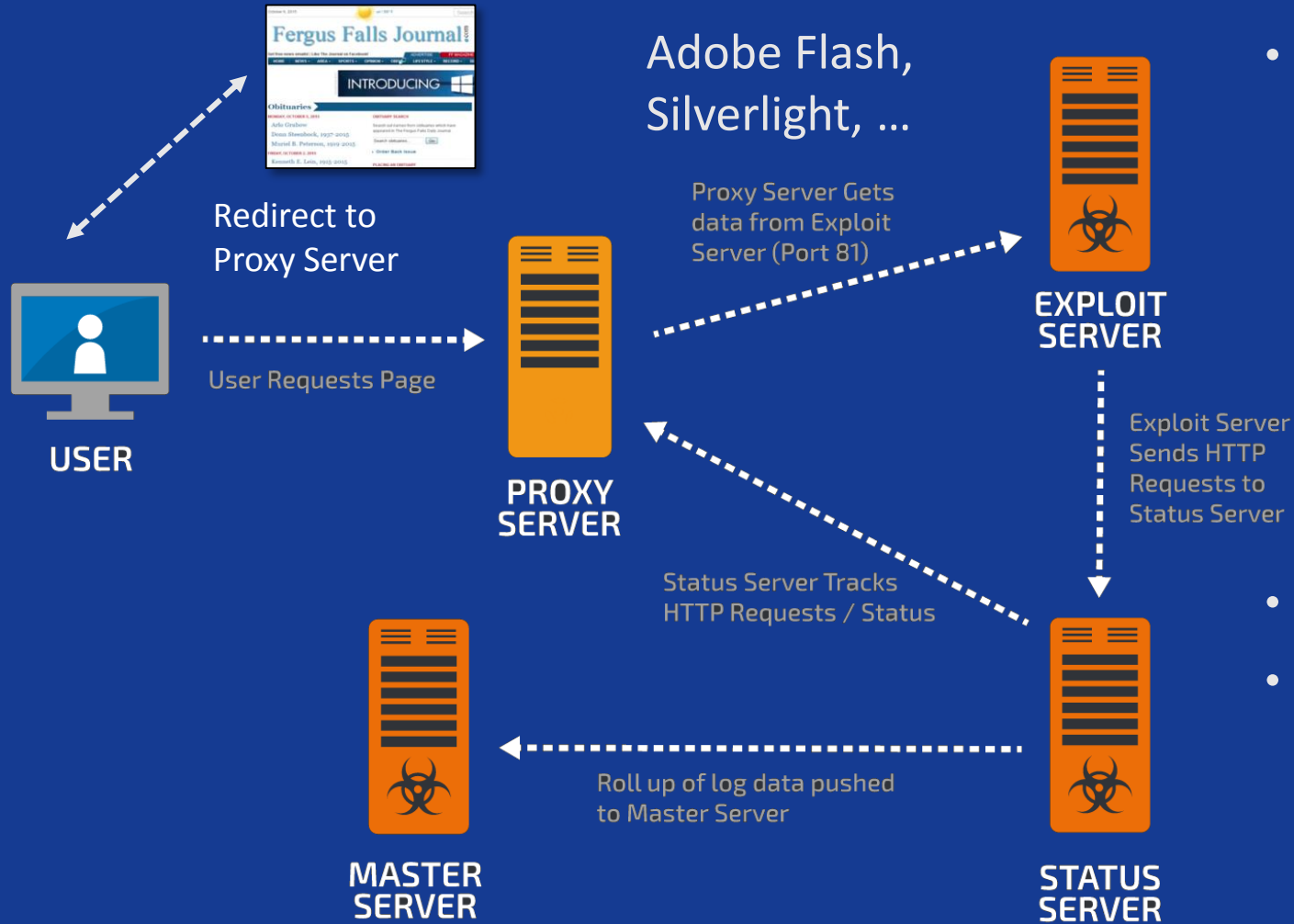
in case of "File decryption button" malfunction use one of our gates:
<http://34r6hq26q2h4jkzj.42k2bu15.com>
<https://34r6hq26q2h4jkzj.tor2web.blutmagie.de>

Use your Bitcoin address to enter the site:
1MQrnWHRo52jt32eUzpNcarSJM

if both button and reserve gate not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

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

TeslaCrypt



TeslaCrypt

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



Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

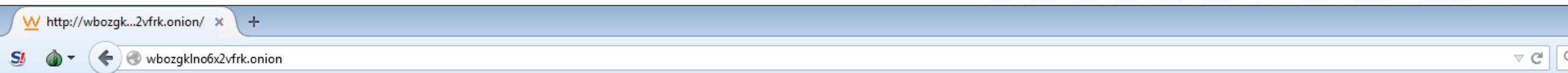


TeslaCrypt: Victory



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

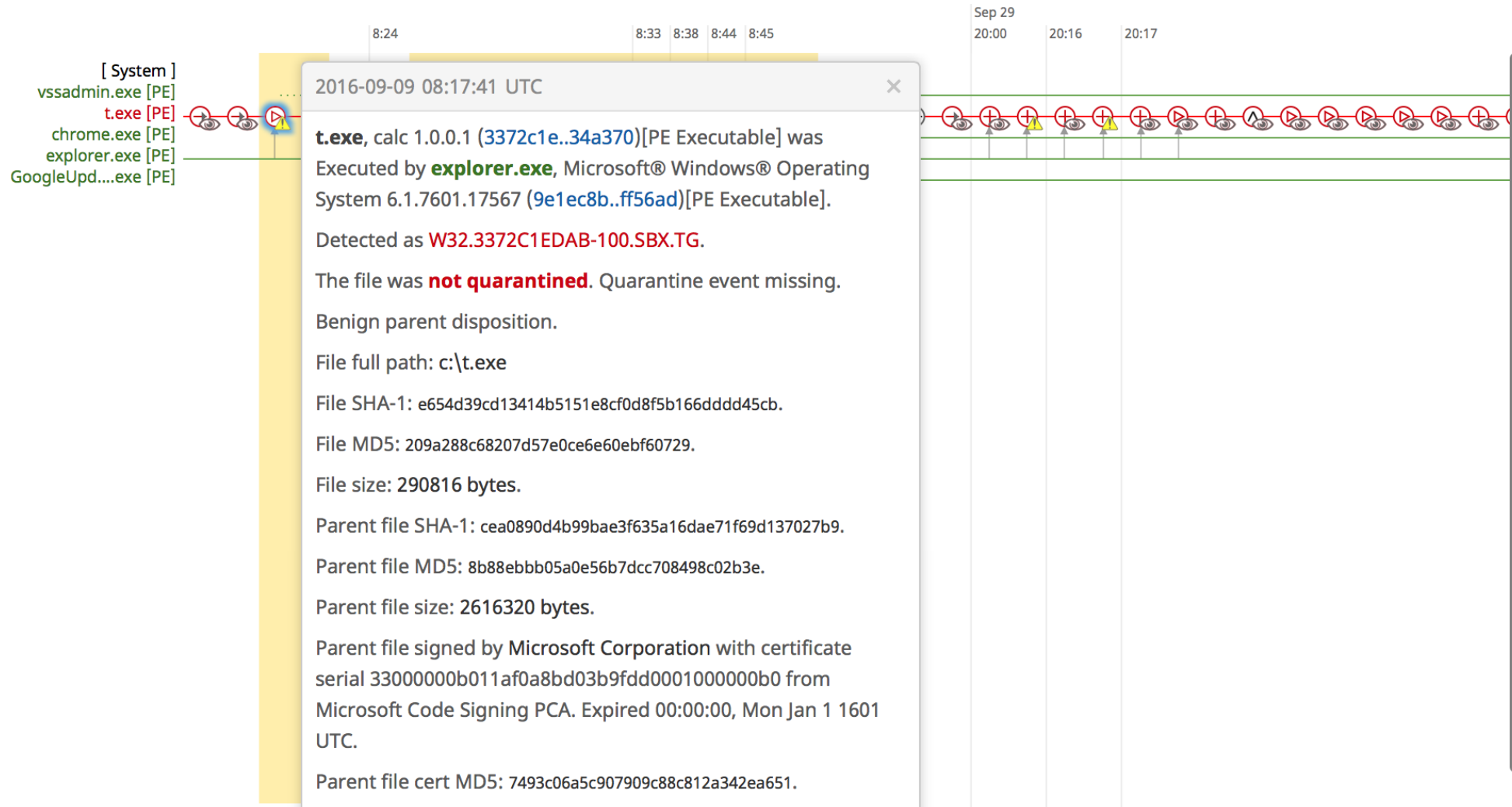
master key for decrypt 440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE

wait for other people make universal decrypt software

we are sorry!

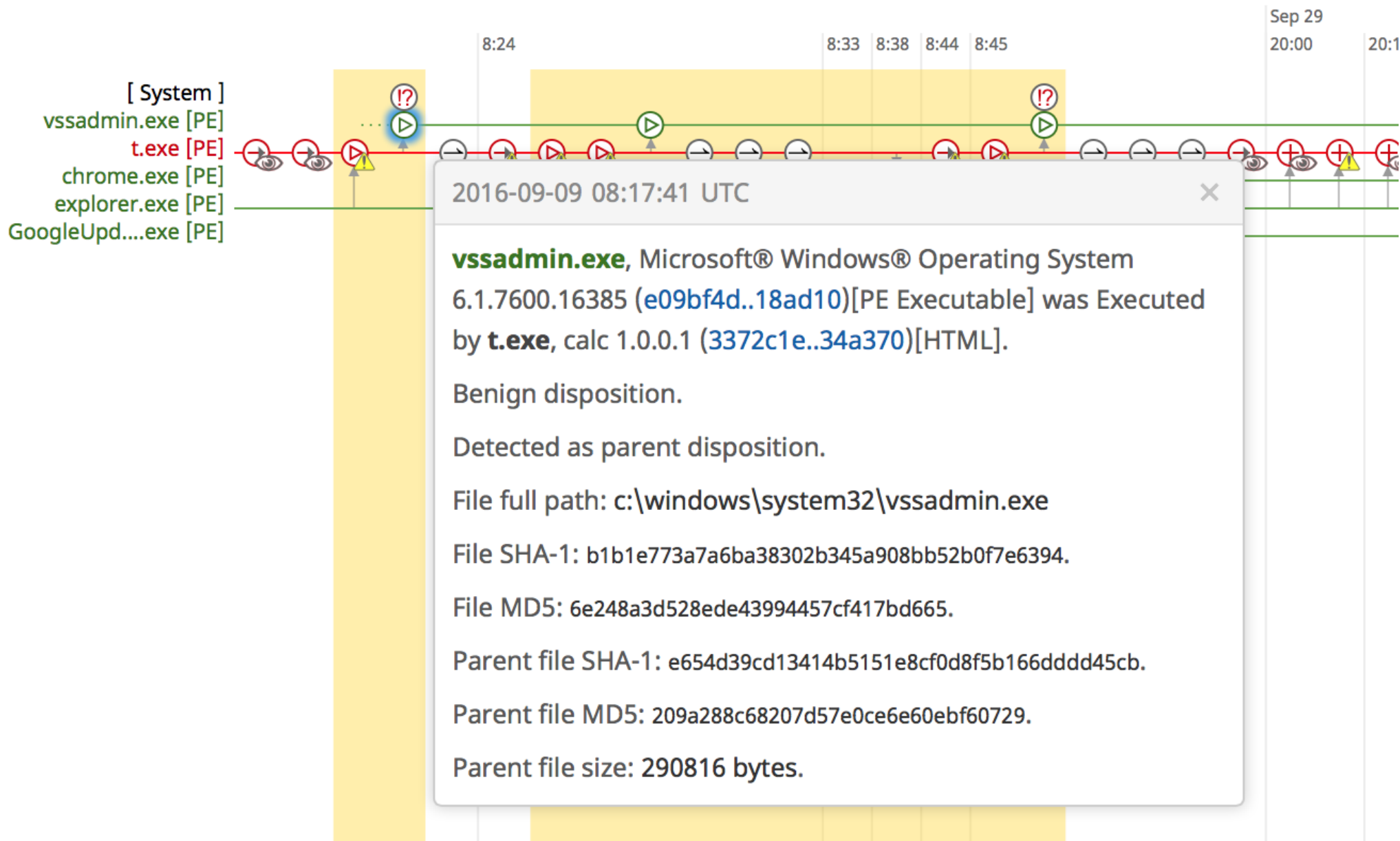
Device Trajectory

For Demo_TeslaCrypt



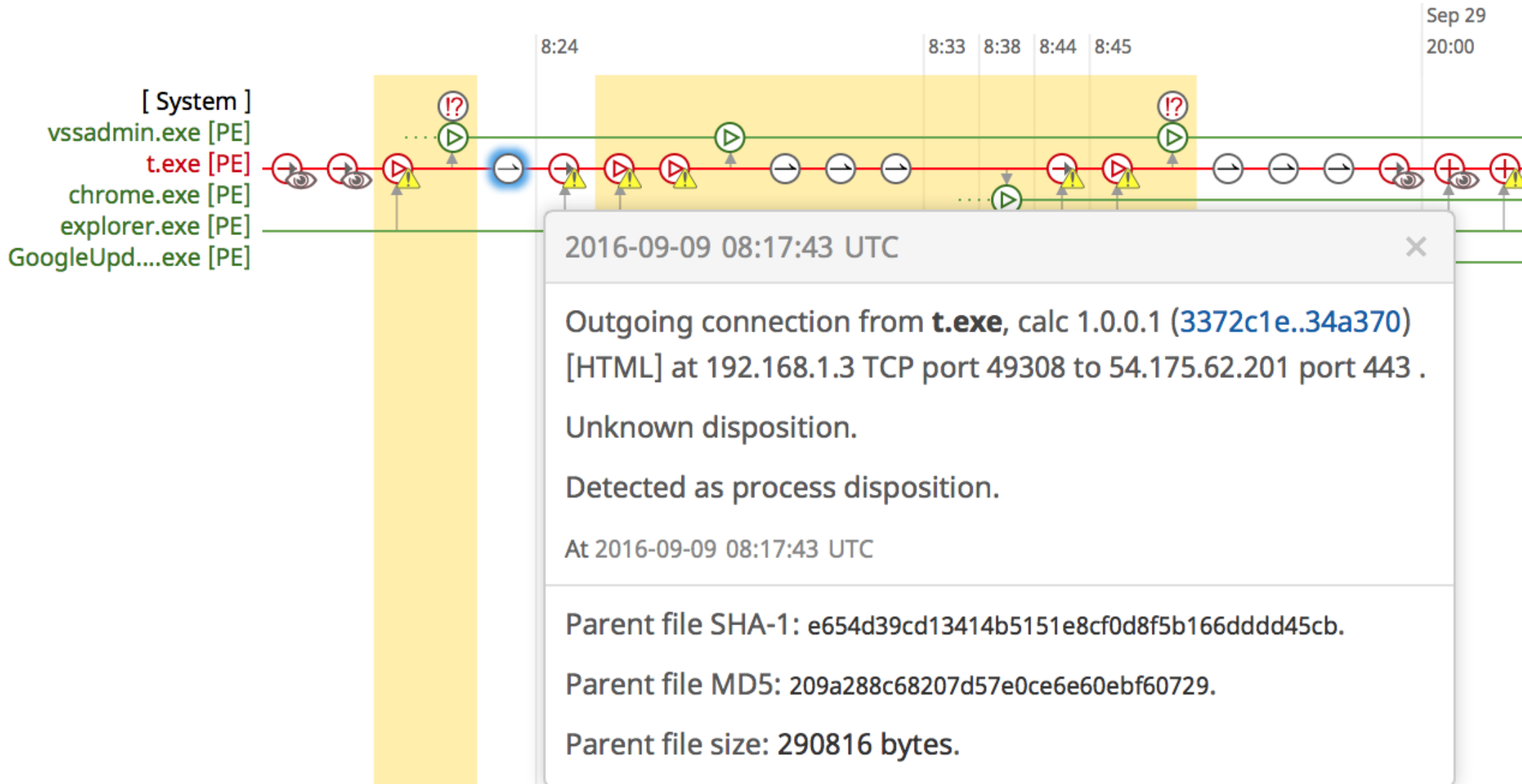
Device Trajectory

For Demo_TeslaCrypt



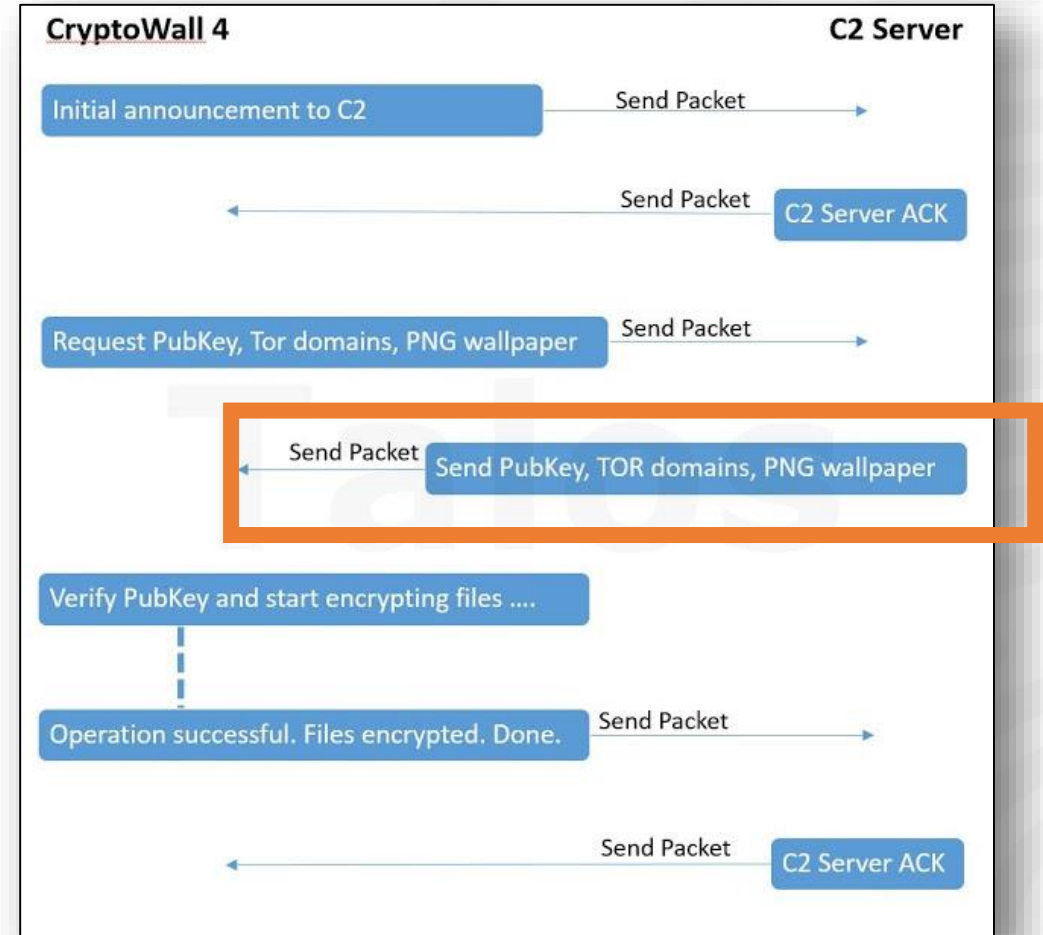
Device Trajectory

For Demo_TeslaCrypt



Cryptowall

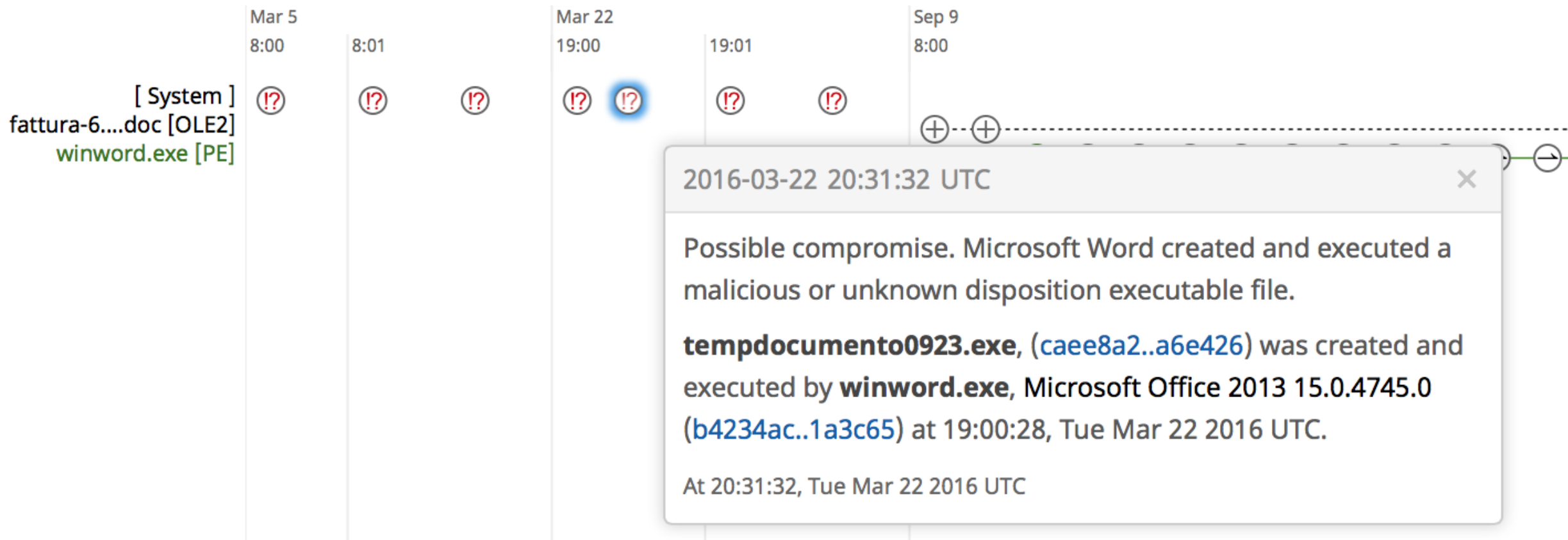
- Version 4: Deletes all **shadow copies**, encrypts the filenames
- **2048 byte RSA** public key encryption
- Decryption software's initial price: \$500
- if it cannot retrieve the public RSA encryption key from the C2 server it **will not "harm"** the victim's computer.
- excludes certain regions from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





Device Trajectory

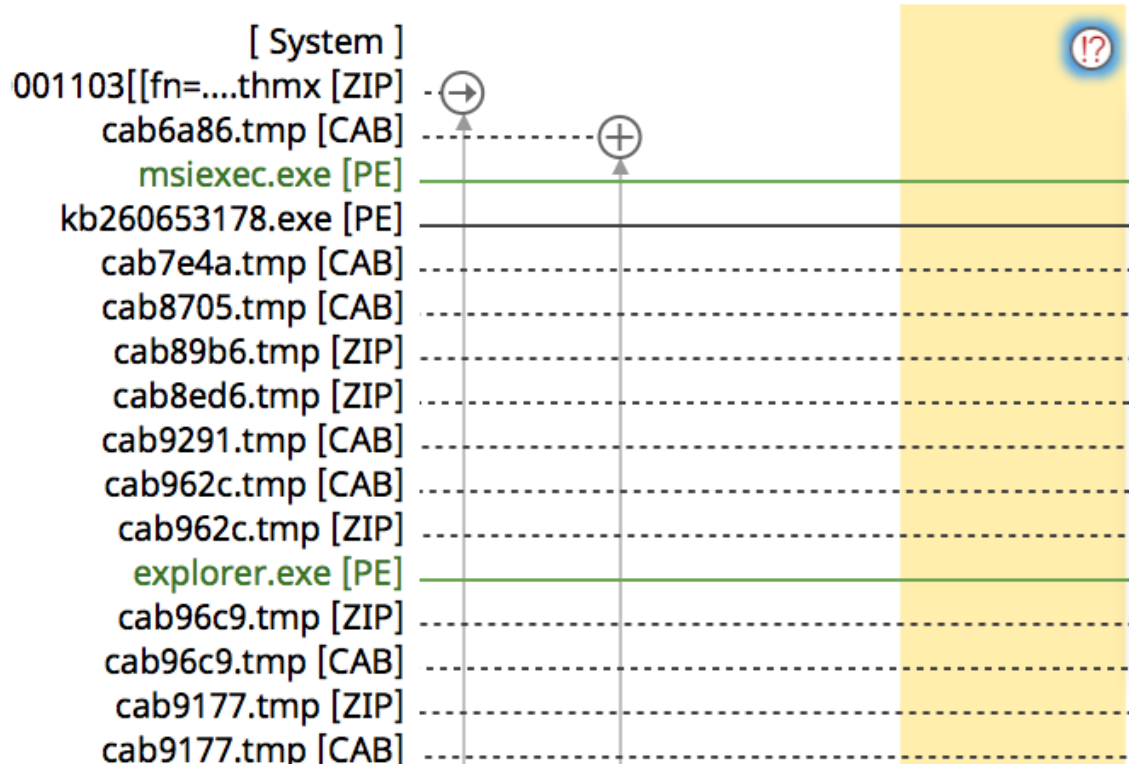
For Demo_CryptoWall





Device Trajectory

For Demo_CryptoWall



2016-09-29 21:46:28 UTC

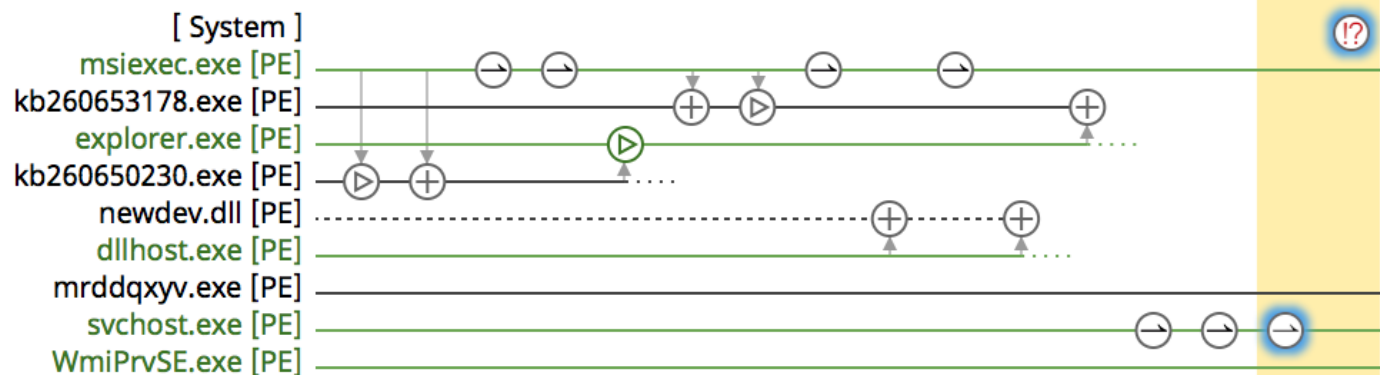
Possible compromise. Microsoft Word created and executed a malicious or unknown disposition executable file.

tempdocumento0923.exe, ([caee8a2..a6e426](#)) was created and executed by **winword.exe**, Microsoft Office 2013 15.0.4745.0 ([b4234ac..1a3c65](#)) at 20:00:28, Thu Sep 29 2016 UTC.

At 21:46:28, Thu Sep 29 2016 UTC

Device Trajectory

For Demo_CryptoWall



2016-09-29 20:01:25 UTC

OpenIOC: W32.SvchostHitWordpressURL.ioc

Description: Svchost.exe accessed a Wordpress URL - this is anomalous and indicative of a process injection.

At 20:01:25, Thu Sep 29 2016 UTC

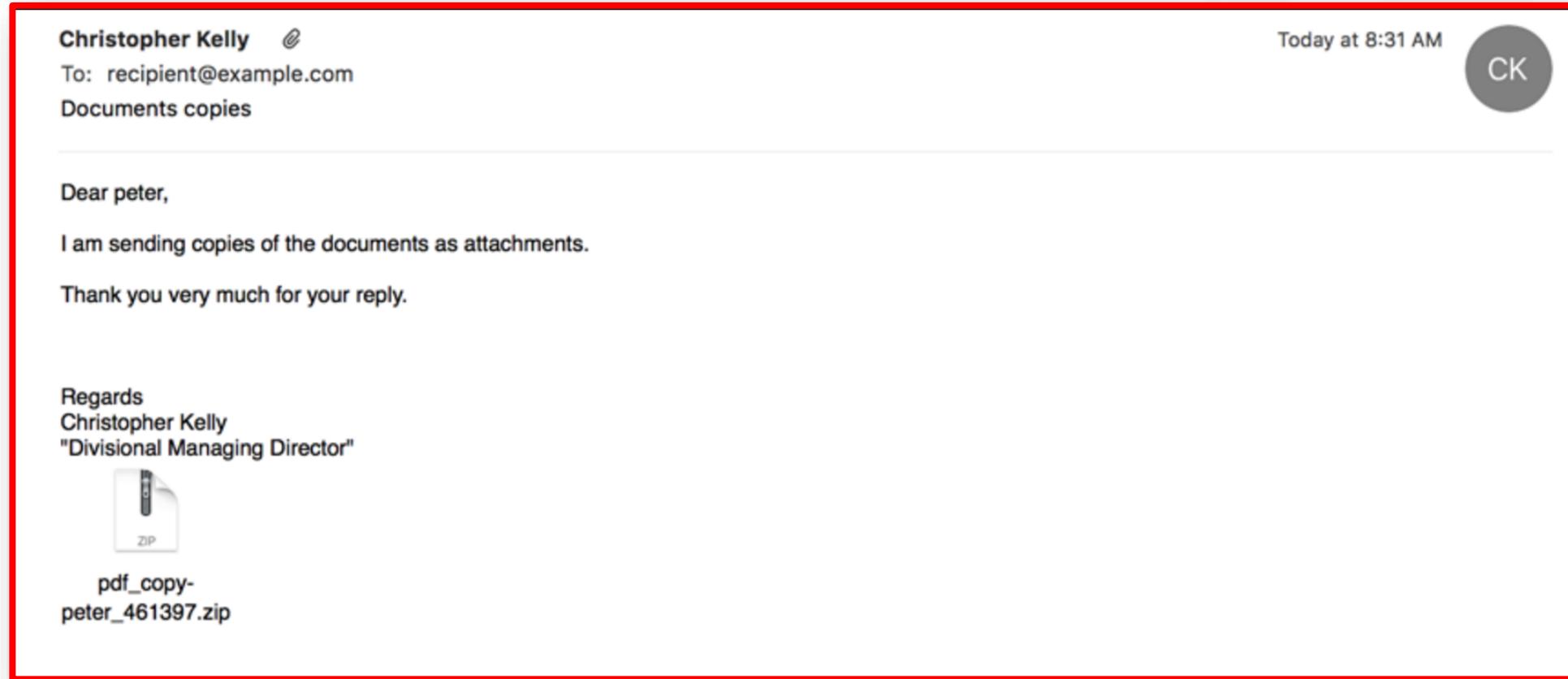
Behavioral Indicators

Threat Score: 100

+ Cryptowall Communications Detected	Severity: 100 Confidence: 100
+ Ransomware Backup Deletion Detected	Severity: 100 Confidence: 100
+ Registry Modification Disabled System Restore	Severity: 100 Confidence: 100
+ Shadow Copy Deletion Detected	Severity: 100 Confidence: 100
+ Artifact Flagged Malicious by Antivirus Service	Severity: 100 Confidence: 95
+ Excessive Suspicious Activity Detected	Severity: 90 Confidence: 100
+ Registry Persistence Mechanism Refers to an Executable in a User Data Directory	Severity: 90 Confidence: 100
+ Excessive Number of DNS Queries	Severity: 70 Confidence: 100
+ Artifact Flagged by Antivirus	Severity: 80 Confidence: 80
+ Process Modified an Executable File	Severity: 60 Confidence: 100
+ Process Modified File in a User Directory	Severity: 70 Confidence: 80
+ Process Disabled Internet Explorer Proxy	Severity: 70 Confidence: 70
+ Process Modified Autorun Registry Key Value	Severity: 80 Confidence: 60
+ Process Modified Trusted Root Certificates	Severity: 60 Confidence: 60
+ DNS Query Returned Non-Existent Domain	Severity: 25 Confidence: 75
+ Possible Double Flux Nameserver Detected [Beta]	Severity: 35 Confidence: 50
+ URL Resulted in 404 or Empty File	Severity: 25 Confidence: 25
+ Ransomware Queried Domain	Severity: 25 Confidence: 25
+ Outbound HTTP POST Communications	Severity: 25 Confidence: 25
+ Outbound Communications to Nginx Web Server	Severity: 25 Confidence: 25
+ Executable Imported the IsDebuggerPresent Symbol	Severity: 20 Confidence: 20

Locky/ Zepto

- 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

[Resubmit](#)

ID 36d038b1d1326983a4aa253973d06fe2
OS 2600.xpsp.080413-2111
Started 6/29/16 13:36:19
Ended 6/29/16 13:42:10
Duration 0:05:51
Sandbox phl-work-11 (pilot-d)

Filename swift 6d2.js
Magic Type JavaScript
Analyzed As js
SHA256 00e475ae83002930c6a9dd9c4223fd710c3a29a4c1c3775413d58e9e23e5c0b2
SHA1 7907255b6fd0d5600d4d9c311d72003d308b4fda
MD5 15ae1614b42526956a3855071553b056
Tags

Behavioral Indicators

Threat Score: 95

Process Modified Desktop Wallpaper	Severity: 100 Confidence: 95
A Script Established Direct IP Communications	Severity: 90 Confidence: 90

Windows Picture And Fax Viewer Used To Display Decoy Image	Severity: 70 Confidence: 100
Process Modified an Executable File	Severity: 60 Confidence: 100
An HTTP Request Was Made to a Numeric IP Address	Severity: 75 Confidence: 80
Process Created an Executable in a User Directory	Severity: 60 Confidence: 95
Outbound HTTP GET Request	Severity: 75 Confidence: 75
Process Modified File in a User Directory	Severity: 70 Confidence: 80
Process Modified AUTOEXEC.BAT	Severity: 80 Confidence: 70
A Script File Established Network Communications	Severity: 70 Confidence: 80
Process Disabled Internet Explorer Proxy	Severity: 70 Confidence: 70
Command Exe File Execution Detected	Severity: 50 Confidence: 80
File Downloaded to Disk	Severity: 30 Confidence: 90
Potential Code Injection Detected	Severity: 50 Confidence: 50
DNS Response Contains Low Time to Live (TTL) Value	Severity: 35 Confidence: 20
Outbound HTTP POST Communications	Severity: 25 Confidence: 25
Outbound Communications to Nginx Web Server	Severity: 25 Confidence: 25



One more thing ...



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](#)
Last Seen 2016-03-28 20:27:57 on [198.19.19.38](#)
Event Count 2
Seen On 3 hosts (2 displayed)
Seen On Breakdown 2 senders → 2 receivers (1 → 1 displayed)

Trajectory



Retrospective Alert

- Events Transfer Block Create Move Execute Scan Retrospective Quarantine
- Dispositions Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2016-03-28 19:04:39	Transfer	14.144.144.66	198.19.19.38	Job-Obscene-Salary.xls	Unkn...	Malware Cloud ...	HTTP	Chrome		Retrospective Event, Mon Mar...
2016-03-28 20:27:57	Retrospectiv...				Malw...					

Result of Dynamic Analysis



Dynamic Analysis Summary

Report ●●●● (100) 2016-03-27 12:56:03 (Windows XP - SP3/i386)

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

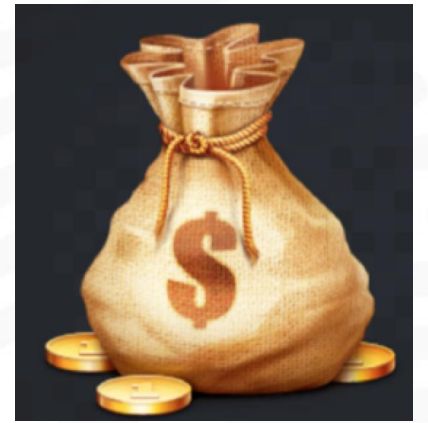
Threats

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



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.
- Quick solutions: OpenDNS; AMP, Email Security, NGFW
- Time-to-detect : [TTD] **13 hours** vs 100-200 days,
- NSS Labs : 91.8 % [**>3min**]



Thank you

György Ács
Cisco Systems
gacs@cisco.com

