Global vision.
Local knowledge.

Cisco Connect Dubrovnik
Croatia, 28\textsuperscript{th} March 2019
It’s not the 99% what meters but the 1% that is missed

Szilard Csordas
IT Security Consultant
28th of March, 2019
"know your enemy and know yourself\n
Sun Tzu – military strategist
Vulnerabilities

- Weakness in system
- Configuration error, missing patch, design flaw, etc.
- Signature security defend attacks (exploiting) against vulnerabilities. Examples IPS, Anti-Virus
Why Tuning Matters

- **50% - 75% Effective**
  - IPS Detection Capabilities Enabled
  - Recon / Protocol Abuse / etc.

- **Requires Tuning**
  - Vendor Signatures
    - Heart Bleed / General Java Vuln / Exploit Kit
    - Flash Vuln, et.
  - Your Vulnerabilities
    - Server, Host, Configuration Issues

- **Default Detection**
- **Vendor Feeds**
- **Your Vulnerabilities**
Cisco Security Portfolio

Over $7 billion invested in industry-leading security solutions

<table>
<thead>
<tr>
<th>Network</th>
<th>SD-Perimeter</th>
<th>NGFW UTM Web Security</th>
<th>Security Analytics NGIPS</th>
<th>Customer SOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Endpoint</td>
<td>VPN RA &amp; Device Visibility</td>
<td>MFA / SSO BYOD SD-Perimeter Email Security</td>
<td>EPP / EDR</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Cloud</td>
<td></td>
<td>SIG / CASB Workload Protection</td>
<td>Security Analytics</td>
<td>File Investigations</td>
</tr>
</tbody>
</table>

Trusted Access  Threat Defense

Customer SOC

Cisco Threat Intel

Talos
Are We affected

Cisco Threat Response

Locating the evil

Cisco AMP for endpoints
Best of Breed
Versus
Defense in Depth
Endpoint Security: A Broad & Fragmented Market

- EPP
- EDR
- Secure Access
- User Authentication /Identity
- Sandboxing
- Behavioral Monitoring
- End User Protection via DNS
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
AMP History

Founded in 2008

In 2011 acquired by Sourcefire

In 2014 acquired by Cisco
CLOUD SUPPORT, COMMUNITY PROTECTION

Immunet® is a malware and antivirus protection system that utilizes cloud computing to provide enhanced community-based security. Join the Immunet Community today and help make the internet safer for everyone.
State of Cisco Endpoint Security Business

- **5,000+** Endpoint Customers
- **11M+** Endpoints
- AMP Everywhere **76,000+** customers
- **Forrester** Endpoint Suite "Strong Performer"
- Gartner MQ EPP "Visionary"
- NSS Labs "Recommended"
- Protection, Detection and Response in Single Agent
- Apple Partnership
- MSS Ready
- Architecture: Network, Endpoint, Cloud
- Global Customer Success
- Cisco Partner Ecosystem
- Broad OS, Platform Support
- TALOS
Value of Retrospective Security

Retrospective Detections

- **Realtime**
- **Retrospective**

<table>
<thead>
<tr>
<th>Month</th>
<th>18-Jan</th>
<th>18-Feb</th>
<th>18-Mar</th>
<th>18-Apr</th>
<th>18-May</th>
<th>18-Jun</th>
<th>18-Jul</th>
<th>18-Aug</th>
<th>18-Sep</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100%</td>
<td>90%</td>
<td>80%</td>
<td>70%</td>
<td>60%</td>
<td>50%</td>
<td>40%</td>
<td>30%</td>
<td>20%</td>
</tr>
</tbody>
</table>
## Capabilities Summary: NextGen Endpoint Security

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

<table>
<thead>
<tr>
<th>Exploitation</th>
<th>Post-Exploitation</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Corruption</td>
<td>Shellcode</td>
<td>Obfuscated</td>
</tr>
<tr>
<td>Return-Oriented Programming</td>
<td>Code Injections</td>
<td>Packer-based</td>
</tr>
<tr>
<td>Heap Spraying</td>
<td>Process Hollowing</td>
<td>Adware</td>
</tr>
<tr>
<td>Reflective Loading</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- Session Manager Subsystem (smss.exe)
- Client/Server Runtime Subsystem (csrss.exe)
- Local Security Authority Subsystem (lsass.exe)
- Windows Logon Application (winlogon.exe)
- Windows Start-up Application (wininit.exe)

Protects system processes from being compromised through memory injection attacks by other processes.

Evaluates desired process/thread access, truncates potentially dangerous access from the desired access list before invoking the original system call.
mimikatz (powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Modules informations

mimikatz (powershell) # exit

Bye!

msv :
[00000003] Primary
  * Username : victim1
  * Domain : victim1-PC
  * NTLM : 1bb3a8f6a6fe1b07262ac174bc44ee
  * SHA1 : fb35c8b445d59e8b42fb89d78a0a5f94638b104
[00010000] CredentialKeys
  * NTLM : 1bb3a8f6a6fe1b07262ac174bc44ee
  * SHA1 : fb35c8b445d59e8b42fb89d78a0a5f94638b104

tspkg :
wdigest :
  * Username : victim1
  * Domain : victim1-PC
  * Password :
Malicious Activity Protection

- Runtime protection against abnormal behaviors of running programs
- Monitor processes reading, writing, renaming, deleting files in rapid succession (ransomware)

1. User executes a file
2. A file or a process starts encrypting files on disk
3. Ransomware behavior is attributed and blocked or quarantined (per policy)
Configuring Engines

Malicious Activity Protection
Quarantine will block & remove the offending file.

System Process Protection
Enabled / Disabled only, extends SelfProtect to system processes

Exploit Prevention (ExPrev)
Enabled / Disabled only – all protected applications will be protected
Anti-Virus & Custom Blocklist

• Offline Anti-Virus engine for Windows: TETRA
• On-prem Anti-Virus update Server
• Custom File Blocking
  • Simple:
    • SHA256 hash
  • Advanced:
    • MD5 hash
    • PE section-based signatures
    • File Body-based signatures
    • Extended signature format (offsets, wildcards, regex)
    • Logical signatures
    • Icon signatures
Cloud IOCs = Detect Likely Breaches

- Surface suspicious behavior on a host, a combination of events with malicious intent
- No automated blocking, trigger investigations
- Driven by Cisco Research team

Example threat detections:
- Word document launching shell
- Powershell downloaded a file
- Registry keys modified to persist
- WMI executed on a remote system
Device Flow Correlation

• A kernel-level view into Network I/O that allows blocking or alerting on network activity tracked back to the initiating process (dropper detection)

• Relies on Cisco Talos Intelligence/IP Reputation Data for blocking of connections to known:
  • C&C hosts
  • Phishing hosts
  • Botnet hosts, etc

• Custom user-defined IP whitelists and blacklists
Endpoint IOCs = Hunt for Threats

- Security analyst specifies artifacts to look for using OpenIOC format
- Search is executed across individual hosts and results are displayed in the AMP Console
- Can be resource intensive
- Search parameters:
  - FileItem
  - RegistryItem
  - EventLogItem
  - ProcessItem
  - ServiceItem
  - https://www.iocbucket.com

Scan results retuned to AMP Console
Cognitive Intelligence

Polymorphic & Emerging Threats
- Cross-product correlation for malware detection
- Predicting evolving threat infrastructure

Agentless Malware Detection
- File-less, memory-only malware
- Process and network behavioral analysis

Web Proxy as a Sensor
- Behavioral Breach Detection
- Detection of infections bypassing the perimeter

Encrypted Traffic Analytics
- Netflow & ETA analytics
- Behavioral Breach Detection

- Anomaly Detection
- Behavioral Analytics
- Host Categorization

- Threat Classification
- Threat Actor Models
- Global Risk Map

22B Network Flows Per Day
15M Protected Devices
1500 Customers

- 12 years of research
- 80 ML scientists and engineers
- 60+ patents & filings
- 200+ publications
How It Works - Architectural Approach

Global Risk Map

Network Analysis
- Anomaly Detection
- Threat Detection
- Classification, Attribution

Endpoint Analysis
- Behavioral Analysis
- Command Lines
- Static Analysis

Cross-Layer Analytics
(Network and Endpoint Telemetry Correlation)
Graph Definition
perfect for malware that often repackages the binary, but keeps connecting to the same C&C domains

\[ B_u : \text{bipartite graph of binary - domain connections} \]

- Edge between domain and a binary (represented by SHA256) \( \Leftrightarrow \) binary created a connection to the given domain
- Seeds are binaries we know are malicious
- Other graph definitions are also possible
Command Line Argument Clustering to uncover evasive malware and morphing threats

- It enables automated generation of Cloud IOCs at scale
- these arguments are often associated with various malware families
- can represent known or unknown malware families
  - [‘/Initialize’, ‘/Hidden’]
- IOC is generated for the malicious clusters
  - IOC can be used in real time by the endpoint to detect/stop execution of the malicious binary
- BLOG – Command line argument clustering

Event Details

2018-08-14 19:48:11 UTC

OpenIOC: W32.Generic.1682.cam.ioc

Description: A process was launched with a specific set of command line arguments which have been heuristically associated with known malware/adware. This indicates that there is high likelihood that a known malware or adware was executed on the host and it needs to be further investigated to determine the response needed.
Classified Auto-generated Cloud IOC: W32.Dealply2.ioc

Description: Command-lines similar to those seen with DealPly Adware were detected. DealPly is a possibly unwanted application which claims to improve online shopping experience. It is often bundled into other legitimate installers and is hard to uninstall. In addition, activities like injection of advertisements into popular browsers make it similar to adware.
Static File Analysis

- Most from PE header
  - Imported libraries, functions, exported functions
  - DLL characteristics, linker version, OS version, machine type
  - Statistics about sections (number of sections, size of code, size of image, entropy, etc.)
    - Statistics about resources (number of resources, type, size, etc.)
- Strings extracted from the whole PE file
- Packer detection
Advanced Malware Protection for Endpoints

Device Trajectory
CLIENT03-PC.techtorial.local

2017-03-18 13:30:55 CET
Outgoing connection from notepad.exe, Microsoft® Windows® Operating System 6.1.7600.16385 (c4232dd..07e102) [PE_Executable] at 192.168.35.13 TCP Port 49243 to 192.168.36.11 Port 8080.

Unknown disposition.

Benign process distribution.

At 2017-03-18 13:30:55 CET
Parent file SHA-1: f00aa51c2ed8b2f656318fd01ee1cf5441011a4.
Parent file MD5: d378fbb70923139d6a4ff46864aa61c.
Parent file size: 179712 bytes.
AMP 4 endpoint – Device trajectory

2017-03-18 13:27:01 CET

powershell.exe, Microsoft® Windows® Operating System 6.1.7600.16385 [6c05e11..47aeC7][PE_Executable] was Executed by cmd.exe, Microsoft® Windows® Operativsystem 6.1.7601.17514 (17f746d..2402ae)[PE_Executable].

Benign disposition.
Benign parent disposition.

File full path: c:\windows\system32\windowspowershell\v1.0\powershell.exe
File SHA-1: 04c5d2bda9a0f3fa8a45702d4256ce442d8c4d.
File MD5: 92f4e405db16ac55d97e3be3fe3b132fa.
File size: 452608 bytes.
Parent file SHA-1: e66c8f12d87c4d388f09b4f69bed2e91682920b5.
Parent file MD5: ad7b9c14083b52bc532fba5948342b98.
Parent file size: 302592 bytes.

Command line


Environment variables

USERNAME CLIENT03-PC$
netsh.exe firewall disable - openIOC

Device Trajectory

CLIENT01-PC.techorial.local

[ System ]
cab6c61.tmp [CAB]
chrome.exe [PE]
vpnuui.exe [PE]
iptray.exe [PE]
cmd.exe [PE]
sysssetup.exe [PE]
vmswareres....exe [PE]
vmtosol.exe [PE]
d.t [PE]
whoami.exe [PE]
netsh.exe [PE]
cmd.exe [PE]
l2p.t [PE]
werfault.exe [PE]
a9807.tmp [PDF]
net1.exe [PE]
net.exe [PE]
w7e852.tmp [PE]
zppaudbjr.exe [PE]
tior.exe [PE]
mag69a3.tmp [PE]
acord32.exe [PE]
sedybi.exe [PE]
explorer.exe [PE]

2017-03-17 02:23:11 CET

netsh.exe ([661f5d4..169943]) [PE_Executable] was Executed by cmd.exe, Microsoft® Windows® Operating System 6.1.7601.17514 ([17f746..2402ae]) [PE_Executable].

Benign disposition.
Benign parent disposition.
File full path: c:\windows\syswow64\netsh.exe
Parent file SHA-1: ee8c8f12d87c4d388f09b4f69bed2e91682920b5.
Parent file MDS: ad7b9c14083b522bc532fb5a94834b98.
Parent file size: 302592 bytes.

Command line

netsh firewall set opmode mode=disable

Enviroment variables

USERNAME victim
new „backupservice” user with admin priviledges

Event Details
Parent file MD5: 63dd6fbaabf881385899fd39df13dce3.
Parent file size: 55808 bytes.

Command line
CWD
CMD C:\Windows\system32\netl user backupservice EvilPass12 /add

Environment variables
Path C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
USERNAME mrbrown
Event Details

2019-03-15 00:38:25 CET

System Process protected **Isass.exe**, Microsoft®
Windows® Operating System 10.0.14393.187

9403e9fe...9d677983 [PE_Executable].

by PE

**Event Details**

2019-03-15 00:46:19 CET

The Connector is being uninstalled.

Reason: Process module is not clean and not signed

File full path: C:\Windows\System32\Isass.exe

File SHA-1: de02364202b1770e46cc79ee1fb971522ce39c0.

File MDS: 6f8e95716c1a27ff2fe96d30b147ff1c1.

File size: 57400 bytes.

File age: 0 seconds.

File signed by Microsoft Windows Publisher with certificate serial
33000000cc4ee86d1a15af49950000000000cc from
ARP scan I
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.

Result of sessionGopher


SessionGopher

Brandon Arvanaghi
Twitter: @arvanaghi | arvanaghi.com

[+] Digging on MRBROWN-PC ...
Microsoft Remote Desktop (RDP) Sessions
Source : MRBROWN-PC\mrbrown
Hostname : 192.168.34.7
Username : BUDLAB\mrorange
PutTY Sessions
Source : MRBROWN-PC\mrbrown
Session : linux1
Hostname : linux1
SecOps

- EPP
- NGIPS
- DNS Security
- Etc

- File Analysis
- Domain reputation
- IP reputation
- Etc

- EPP logs
- NGIPS logs
- DNS logs
- Etc

- Etc
Summary - How CTR brings it all together?
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.
Use Case:
Investigate Phishing with Malware Delivery
1. Receive Retrospective Alert via Email

From: IronPort C100V Alert <alert@cisco-ros.com>
Date: January 14, 2019 at 08:26:59 EST
To: <nedross@cisco.com>
Subject: Info <AMP> esa1.hc2926-99.iphm.com:AMP Retrospective Alert:8528com62962102584486292345678910111213141516171819202122.html attachment verdict changed from VERDICT UNKNOWN to MALICIOUS

The Info message is:

Retrospective verdict received for 8528com62962102584486292345678910111213141516171819202122.html.

SHA256: 13dc071014c82e5615198a698ea70b9b3caf454179af0939434bdaa453d

Verdict: MALICIOUS
Spyname: W32.13DC071014-95.SBX.TG

Total users affected: 5
----------------- Affected Messages -----------------

Message 1
MID : 53998
Subject : [FILE ANALYSIS PENDING]Thank you
From : noreply@domainwithnovalue.com
To : alain@ciscothreatresponse.com, javed@ciscothreatresponse.com, hsimpson@ciscothreatresponse.com, ravi@ciscothreatresponse.com, michael@ciscothreatresponse.com
File name : 8528com62962102584486292345678910111213141516171819202122.html
Parent SHA256 : unknown
Parent File name : unknown
Date : 2019-01-14T11:34:44Z

-----------------------------------------------
Pasted whole retrospective email

Retrospective verdict received for 8528com62962102584486292345678910111213141516171819202122.html.
SHA256: 13dc071014c82e56151918a698ea70b9b3caf45179af09394a34bd2aa453dfa
Verdict: MALICIOUS
2. Analyze Outbreak

- 5 email recipients
- 1 ESA
- 1 endpoint

1 endpoint encounter
Five recipients received email
### 3. Observe Targets

7 Targets received file

<table>
<thead>
<tr>
<th>EMAIL ADDRESS</th>
<th>EMAIL ADDRESS</th>
<th>EMAIL ADDRESS</th>
<th>EMAIL ADDRESS</th>
<th>EMAIL ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:javed@ciscothreatresponse.com">javed@ciscothreatresponse.com</a></td>
<td><a href="mailto:hsimpson@ciscothreatresponse.com">hsimpson@ciscothreatresponse.com</a></td>
<td><a href="mailto:javed@ciscothreatresponse.com">javed@ciscothreatresponse.com</a></td>
<td><a href="mailto:hsimpson@ciscothreatresponse.com">hsimpson@ciscothreatresponse.com</a></td>
<td><a href="mailto:javed@ciscothreatresponse.com">javed@ciscothreatresponse.com</a></td>
</tr>
<tr>
<td>VLNESA15658201_420D08BF005D49C5A730-D6FE24895791</td>
<td>VLNESA15658201_420D08BF005D49C5A730-D6FE24895791</td>
<td>VLNESA15658201_420D08BF005D49C5A730-D6FE24895791</td>
<td>VLNESA15658201_420D08BF005D49C5A730-D6FE24895791</td>
<td>VLNESA15658201_420D08BF005D49C5A730-D6FE24895791</td>
</tr>
<tr>
<td>Email Security Appliance</td>
<td>Email Security Appliance</td>
<td>Email Security Appliance</td>
<td>Email Security Appliance</td>
<td>Email Security Appliance</td>
</tr>
<tr>
<td>d959e7a4-98c3-4818-b0e2-a3f1bb49a109</td>
<td>d959e7a4-98c3-4818-b0e2-a3f1bb49a109</td>
<td>d959e7a4-98c3-4818-b0e2-a3f1bb49a109</td>
<td>d959e7a4-98c3-4818-b0e2-a3f1bb49a109</td>
<td>d959e7a4-98c3-4818-b0e2-a3f1bb49a109</td>
</tr>
<tr>
<td><a href="mailto:michael@ciscothreatresponse.com">michael@ciscothreatresponse.com</a></td>
<td><a href="mailto:michael@ciscothreatresponse.com">michael@ciscothreatresponse.com</a></td>
<td><a href="mailto:michael@ciscothreatresponse.com">michael@ciscothreatresponse.com</a></td>
<td><a href="mailto:michael@ciscothreatresponse.com">michael@ciscothreatresponse.com</a></td>
<td><a href="mailto:michael@ciscothreatresponse.com">michael@ciscothreatresponse.com</a></td>
</tr>
<tr>
<td><a href="mailto:alain@ciscothreatresponse.com">alain@ciscothreatresponse.com</a></td>
<td><a href="mailto:alain@ciscothreatresponse.com">alain@ciscothreatresponse.com</a></td>
<td><a href="mailto:alain@ciscothreatresponse.com">alain@ciscothreatresponse.com</a></td>
<td><a href="mailto:alain@ciscothreatresponse.com">alain@ciscothreatresponse.com</a></td>
<td><a href="mailto:alain@ciscothreatresponse.com">alain@ciscothreatresponse.com</a></td>
</tr>
<tr>
<td>Windows 7, SP 1.0</td>
<td>Windows 7, SP 1.0</td>
<td>Windows 7, SP 1.0</td>
<td>Windows 7, SP 1.0</td>
<td>Windows 7, SP 1.0</td>
</tr>
<tr>
<td>HOSTNAME</td>
<td>HOSTNAME</td>
<td>HOSTNAME</td>
<td>HOSTNAME</td>
<td>HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Pivot to AMP to Analyze Trajectory
Threat Response Allows Pivot Investigation of Hash and Tracing Emails

319988b9603d5f29545fd7194ab4af8dafa1197e6fc45236b45004914a9eef

Investigation 1 of 1 enrichments complete

What can I search for?

Investigate Clear Reset

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

Relations Graph Showing 9 nodes
5. Pivot on Target for More Options

Targeted by 1 unique threat, 11 times in the last 3 days

Hostname
HSIMPSON-WIN7.CISCOTHEA...

AMP Computer GUID
6eb83ec-2108-4f37-9e7e-

IP Address
192.168.243.108

MAC Address
00:50:56:88:8f:52

Copy to Clipboard
Add to Investigation
Add to New Case

EU-Threat-Grid
Browse 192.168.243.108
Search 192.168.243.108

Global-Umbrella-Defense
IP view for 192.168.243.108

Talos Intelligence
Search for this IP

US-AMP-for-Endpoints
Search for this IP

US-Threat-Grid
Browse 192.168.243.108
Search 192.168.243.108

Sightings Timel

My Environment

13 Sightings in My Environment
First: Jan 14, 2019
Last: Jan 14, 2019
6. Drill Deeper

Observe victim has connected with another known malicious IP via 2 files on this machine

Add files to block list via pivot menu
I am a Cisco Security customer using Cisco Threat Response

My team can:

• Answer questions faster about observables.

• Block and unblock domains from Cisco Threat Response.

• Block and unblock file executions from Cisco Threat Response.

• Hunt for an observable associated with a known actor and immediately see organizational impact.

• Save a point in time snapshot of our investigations for further analysis.

• Document our analysis in a cloud casebook from all integrated or web-accessible tools, via an API.

• Integrate Cisco Threat Response easily into existing processes and custom tools.
Cisco Threat Response is included
...with select Cisco Security product licenses

You’re already entitled to Threat Response if you have...

- Cisco AMP for Endpoints
- Cisco Threat Grid
- Cisco Umbrella
- Cisco Email Security
- Cisco NGFW/NGIPS

Not a customer yet?
Request your free trial of Cisco AMP for Endpoints... and try both solutions right now!

www.cisco.com/go/amp
Please, fill out the survey!