Think Outside the Sandbox
Cisco AMP (Advanced Malware Protection)
Think Outside the Sandbox
Cisco AMP (Advanced Malware Protection)

Mahmoud Rabi
Consulting Systems Engineer - Security
Today’s advanced malware is not just a single entity

It is an **Ecosystem** that hides in plain sight

Missed by Point-in-time Detection
The Industrialisation of Hacking

- **Goal: Glory, mode: Noise**
- **Goal Profit, mode: Stealth**

- **VIRUSES** (1985)
- **MACRO VIRUSES** (1995)
- **WORMS** (2000)
- **SPYWARE / ROOTKITS** (2005)
- **MALWARE** (2010)

**APT**: Advanced Persistent Threats
How Hacking is done today

Survey
- What does environment look like?
- What are the countermeasures?
- Identify weak/vulnerable assets.

Write
- Craft context-aware malware to penetrate this environment

Test
- Validate malware works, can evade countermeasures and stay undetected

Execute
- Use malware. Move laterally, establish secondary access,

Accomplish
- The mission: Extract data, destroy, plant evidence, compromise.

Each stage may generate a Weak Signal indicating malicious activity.

We must find these signals in the noise.
Can you correlate multiple events to indicate a compromise?

- Machine Owned!
- File Propagation
- User Privilege Gain
- DNS Resolving
- Direct IP Connection
- Call Back
- Droppers
- EXE file download
- Malware detected
- Rootkit
It’s Time to Think Outside the Sandbox!
Point-in-time Detection Evasion Technique

Analysis Stops Not 100%

Antivirus

Sandboxing

Initial Disposition = Clean

Actual Disposition = Bad Too Late!!

Sleep Techniques
Unknown Protocols
Encryption
Polymorphism

Blind to scope of compromise
"Would you do **Security** differently “*if* ” you knew you would be compromised?”
It is no longer a question of “if” you will be breached...

It is a matter of “when”.
Think Differently about Security

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network
Endpoint
Mobile
Virtual
Cloud
Email & Web

Point-in-time
Continuous
Cisco AMP Delivers Three Advantages

1. A better approach
2. More comprehensive protection
3. Address the full attack continuum

BEFORE | DURING | AFTER

Content | Network | Endpoint

Point-in-Time Detection | Retrospective Security

Cisco Collective Security Intelligence
Cisco Has The Best-In-Class Security Asset To Deliver Against These Requirements

Cisco Collective Security Intelligence

Automatic Updates every 3-5 minutes

**Cisco SIO**

- Email
- Endpoints
- Web
- Networks
- IPS
- Devices

- 1.6 million global sensors
- 100 TB of data received per day
- 150 million+ deployed endpoints
- 600+ engineers, technicians, and researchers

- 35% worldwide email traffic
- 13 billion web requests
- 24x7x365 operations
- 40+ Languages

**Sourcefire VRT® (Vulnerability Research Team)**

- 300,000+ File Samples per Day
- FireAMP™ Community, 3+ million
- Advanced Microsoft and Industry Disclosures
- Snort and ClamAV Open Source Communities
- Honeypots
- Sourcefire AEGIS™ Program
- Private and Public Threat Feeds
- Dynamic Analysis

**AMP Advanced Malware Protection**
Cisco AMP Delivers A Better Approach

Point-in-Time Detection

File Reputation & Behavioral Detection

Retrospective Security

Continuous Protection

Unique To Cisco AMP
Cisco AMP Defends With Reputation Filtering And Behavioral Detection

Reputation Filtering
- One-to-One Signature
- Fuzzy Finger-printing
- Machine Learning
- Indications of Compromise

Behavioral Detection
- Dynamic Analysis
- Advanced Analytics
- Device Flow Correlation
Reputation Filtering Is Built On Three Features

1. Unknown file's signature is analyzed and sent to the cloud
2. File's signature is not known to be malicious and is admitted
3. Unknown file's signature is analyzed and sent to the cloud
4. File's signature is known to be malicious and is prevented from entering the system
Reputation Filtering Is Built On Three Features

1. Fingerprint of file is analyzed and determined to be malicious
2. Malicious file is not allowed entry
3. Polymorphic form of the same file tries to enter the system
4. The fingerprints of the two files are compared and found to be similar to one another
5. Polymorphic fingerprint is denied entry based on its similarity to known malware
Reputation Filtering Is Built On Three Features

1. Unknown file’s metadata is sent to the cloud to be analyzed
2. Metadata is recognized as possible malware
3. File is compared to known malware and is confirmed as malware
4. A second unknown file’s metadata is sent to cloud to be analyzed
5. Metadata is similar to known clean file, possibly clean
6. File is confirmed as a clean file after being compared to a similarly clean file

Machine Learning Decision Tree

- Possible malware
- Confirmed clean file
- Confirmed malware
- Possible clean file
Behavioral Detection Is Built On Four Features

1. Unknown file is analyzed, indications of self-replication are found
2. These indications of self-replication are communicated to the cloud
3. Unknown file is also performing independent external transmissions
4. The transmission behavior is also sent to the cloud
5. These actions are reported to user to identify the file as possible malware

Collective Security Intelligence Cloud
Behavioral Detection Is Built On Four Features

1. Unknown files are uploaded to the cloud where the Dynamic Analysis Engine executes them in sandboxes.
2. Two files are determined to be malware, one is confirmed as a clean file.
3. Malicious signatures are updated to the Intelligence cloud and broadcasted to user base.
Behavioral Detection Is Built On Four Features

1. Device Flow Correlation monitors the source and destination of I/O traffic on a network.
2. Two unknown files are seen communicating with a particular IP address.
3. One is communicating information outside the network, the other is receiving commands from the IP.
4. Collective Security Intelligence Cloud recognizes the external IP as a confirmed, malicious site.
5. Unknown files are identified as malware because of the association.

Collective Security Intelligence Cloud

IP: 64.233.160.0
Cisco AMP Delivers A Better Approach

Point-in-Time Detection

File Reputation & Behavioral Detection

Retrospective Security

Continuous Protection

Unique to Cisco AMP
Putting It All Together

Collective Security Intelligence

Event History

Who
What
Where
When
How

Discover, Enforce, Harden
Detect, Block, Defend

BEFORE
DURING
Putting It All Together

Who
What
Where
When
How

Discover, Enforce, Harden
Detect, Block, Defend
Scope, Contain, Remediate

BEFORE
DURING
AFTER
Cisco AMP Defends With Retrospective Security

- Retrospection
- Attack Chain Weaving
- Behavioral Indications of Compromise
- Trajectory
- Breach Hunting
Retrospective Security Is Built On…

1. Performs analysis the first time a file is seen
2. Persistently analyzes the file over time to see if the disposition is changed
3. Giving unmatched visibility into the path, actions or communications that are associated with a particular piece of software
Retrospective Security Is Built On...

Behavioral Indications of Compromise uses Retrospection to monitor systems for suspicious and unexplained activity.

1. An unknown file is admitted into the network.
2. The unknown file copies itself to multiple machines.
3. Duplicates content from the hard drive.
4. Sends duplicate content to an unknown IP address.

Leveraging the power of Attack Chain Weaving, AMP is able to recognize patterns and activities of a given file, and identify an action to look for across your environment rather than a file fingerprint or signature.
Retrospective Security Is Built On…

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unknown file is downloaded to device</td>
</tr>
<tr>
<td>2</td>
<td>Fingerprint is recorded and sent to cloud for analysis</td>
</tr>
<tr>
<td>3</td>
<td>The unknown file travels across the network to different devices</td>
</tr>
<tr>
<td>4</td>
<td>File trajectory automatically records time, method, point of entry, systems impacted and prevalence of the file</td>
</tr>
<tr>
<td>5</td>
<td>Sandbox analytics determines the file is malicious and notifies all devices</td>
</tr>
<tr>
<td></td>
<td>File trajectory provides greater visibility into the extent of an infection</td>
</tr>
</tbody>
</table>

Collective Security Intelligence Cloud

![Diagram showing the flow of file trajectory and the interaction with devices and cloud]

- Mobile
- Network
- Virtual Machine
- Computer
- Mobile
- Computer
- Mobile
- Virtual Machine
Retrospective Security Is Built On…

1. Unknown file is downloaded to a particular device
2. The file moves around the device, executing different operations. Meanwhile, device trajectory records the root cause, lineage and actions of the files on a machine.
3. That data pinpoint the exact cause and extent of the compromise on the device.
Cisco’s AMP Everywhere Strategy Means Protection Across the Extended Network

- **AMP for Networks**
- **AMP for Endpoints**
- **AMP on ASA Firewall with FirePOWER Services**
- **AMP on Web & Email Security Appliances**
- **AMP Private Cloud Virtual Appliance**
- **AMP for Cloud Web Security & Hosted Email**
- **AMP Threat Grid**
  - Dynamic Malware Analysis + Threat Intelligence Engine

Advanced Malware Protection
### Deployment Options

<table>
<thead>
<tr>
<th>Email and Web; AMP on ASA CWS</th>
<th>AMP for Networks (AMP on FirePOWER Network Appliance)</th>
<th>AMP for Endpoints</th>
<th>AMP Private Cloud Virtual Appliance</th>
</tr>
</thead>
</table>

### Method

| License with ESA, WSA, CWS, or ASA customers | Snap into your network | Install lightweight connector on endpoints | On-premise Virtual Appliance |

### Ideal for

| New or existing Cisco CWS, Email/Web Security, ASA customers | IPS/NGFW customers | Windows, Mac, Android, VMs | High Privacy Environments |

### Details

**Email and Web; AMP on ASA CWS**

- ESA/WSA: Prime visibility into email/web
- CWS: Web and advanced malware protection in a cloud-delivered service
- AMP capabilities on ASA with FirePOWER Services

**AMP for Networks (AMP on FirePOWER Network Appliance)**

- Wide visibility inside network
- Broad selection of features - before, during and after an attack

**AMP for Endpoints**

- Comprehensive threat protection and response
- Granular visibility and control
- Widest selection of AMP features

**AMP Private Cloud Virtual Appliance**

- Private Cloud option for those with high privacy requirements
- For endpoints and networks

---

There are several ways you can deploy AMP.
Cisco Advanced Malware Protection
Possible compromise. Adobe Acrobat Reader created and executed a malicious or neutral disposition executable file.

a.exe, (92a6e18..655a7a) was created and executed by AcroRd32.exe, Adobe Reader 9.3.3.177 (825b7b2..2e4f82) at 19:03:12, Mon Feb 16 2015 UTC.

At 22:01:49, Mon Feb 16 2015 UTC
AMP for Endpoint Analysis – Adobe Acrobat Reader Compromise
# ThreatGRID AMP – Behavioral Indicators

## Behavioral Indicators

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port</th>
<th>Protocol</th>
<th>Network Stream</th>
<th>Artifact ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>74.122.246.154</td>
<td>80</td>
<td>HTTP</td>
<td>Stream 4</td>
<td>36</td>
</tr>
</tbody>
</table>

**Categories**
- file
- network
- artifact

**Tags**
- dropper
- executable

### Outbound HTTP GET Request
- **Severity**: 75
- **Confidence**: 75

### Process Modified File in a User Directory
- **Severity**: 80
- **Confidence**: 80

### Process Disabled Internet Explorer Proxy
- **Severity**: 70
- **Confidence**: 70

### Potential Sandbox Detection - Enumeration of ProductID
- **Severity**: 60
- **Confidence**: 60

### Process Created an Executable in a User Directory
- **Severity**: 80
- **Confidence**: 80

### Command Exe File Execution Detected
- **Severity**: 50
- **Confidence**: 50

### Potential Code Injection Detected
- **Severity**: 50
- **Confidence**: 50

### Executable with Encrypted Sections
- **Severity**: 30
- **Confidence**: 30

### Outbound Communications to Nginx Web Server
- **Severity**: 25
- **Confidence**: 25

### Executable Imported the IsDebuggerPresent Symbol
- **Severity**: 20
- **Confidence**: 20

---

**Threat Score**: 90
Network AMP Indications of Compromise and Correlation

Indications of Compromise

Hosts by Indication

- Threat Detected...sfer
- Excel Compromised...eAMP
- Excel launched shell
- Threat Detected...uted
- Impact 1 Intrus...user
- Impact 1 Intrus...dmin
- Impact 2 Intrus...ack
- Impact 2 Intrus...dmin
- Dropper Infect...eAMP
- Intrusion Event...cnc
- Security Intel... Cnc
- Suspected Botnet...eAMP
- Adobe Reader la...hell
- PDF Compromise...eAMP
- Java launched shell
- Java Compromised...eAMP
- QuickTime Compromised...eAMP
- QuickTime launch...hell
- PowerPoint Compromised...eAMP
- PowerPoint launch...hell

Indications by Host

Top File Types

- PDF
- SWF
- MSCAB
- ZIP
- GZ
- MAIL
- RTF
- JARPACK
- MSEXE

Top File Names

Files by Disposition

- Clean
- Unavailable
- Unknown
- Malware
NSS Labs Breach Detection Systems SVM
Cisco AMP is a Leader in Security Effectiveness and TCO and offers Best Protection Value

NSS Labs Security Value Map (SVM) for Breach Detection Systems

Cisco Advanced Malware Protection
Best Protection Value
99.0% Breach Detection Rating
Lowest TCO per Protected Mbps
Other Products Do Not Provide Retrospective Security After a Breach

Cisco Connect 2015
Thank you.