Threat Prevention with AMP (Advanced Malware Protection)

Gary Spiteri
gaspiter@cisco.com
Cisco Systems
Agenda

- The Malware Analysis Challenge
- Endpoint Malware Analysis
- Network Malware Analysis
- Host and Endpoint Correlation
- ZeroAccess Investigation (Supplemental Slides)
THE MALWARE ANALYSIS CHALLENGE
The Event Horizon

Firewall

IDS/IPS

AMD

Antivirus

Device/Endpoint

‘Event Horizon’
The Industrialisation of Hacking

<table>
<thead>
<tr>
<th>Year</th>
<th>Type</th>
<th>Goal</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1985</td>
<td>VIRUSES</td>
<td>Glory</td>
<td>Noise</td>
</tr>
<tr>
<td>1995</td>
<td>MACRO VIRUSES</td>
<td>Profit</td>
<td>Stealth</td>
</tr>
<tr>
<td>2000</td>
<td>WORMS HACKERS</td>
<td>Profit</td>
<td>Stealth</td>
</tr>
<tr>
<td>2005</td>
<td>SPYWARE / ROOTKITS</td>
<td>Profit</td>
<td>Stealth</td>
</tr>
<tr>
<td>2010</td>
<td>APTs MALWARE</td>
<td>Profit</td>
<td>Stealth</td>
</tr>
</tbody>
</table>
Survey
What does environment look like?
What are the countermeasures?

Write
Craft context-aware malware to penetrate *this* environment

Test
Validate malware works, can evade countermeasures

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.
## Breaches Happen in Hours….

But Go Undetected For Weeks/Months

<table>
<thead>
<tr>
<th>Event Sequence</th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Attack to Initial Compromise</td>
<td>10%</td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Initial Compromise to Data Exfiltration</td>
<td>8%</td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Discovery</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%</td>
<td>2%</td>
</tr>
<tr>
<td>Discovery to Containment/Restoration</td>
<td>0%</td>
<td>1%</td>
<td>9%</td>
<td>32%</td>
<td>38%</td>
<td>17%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Timespan of events by percent of breaches - Source: Cisco Managed Threat Defense

In 60% of breaches, data is stolen in hours.

85% of breaches are not discovered for weeks.
The Pervasiveness of Malicious Traffic

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-Threat Malware</td>
<td>100%</td>
</tr>
<tr>
<td>Hijacked Infrastructure</td>
<td>96%</td>
</tr>
<tr>
<td>Sites without Content</td>
<td>92%</td>
</tr>
<tr>
<td>Suspect FTP</td>
<td>88%</td>
</tr>
<tr>
<td>Suspect VPN</td>
<td>79%</td>
</tr>
<tr>
<td>Pornography</td>
<td>50%</td>
</tr>
</tbody>
</table>
Correlating Weak Signals Into Indicators Of Compromise

- Correlate Weak Signals into Indicators of Compromise
- Malware Propagation detected by IPS
- User Privilege Gain detected by IPS
- DNS to malware site detected by Security Intelligence
- Malware File Download detected by Malware Cloud Lookup
- CNC Traffic detected by IPS
“How would you do security differently if you knew you were going to be compromised?”

Martin Roesch
Sourcefire
Think differently about Security

**Before**
- Reduce attack surface
- Detect reconnaissance

**During**
- Detect and prevent

**EVENT HORIZON**

**Retrospective security**

---

**CONTEXTUAL AWARENESS**
ENDPOINT MALWARE ANALYSIS
Sourcefire’s Approach to Advanced Malware Protection

- Sourcefire AMP is not an Anti-virus solution
- Malware Analysis is a Big Data problem
- Collect as much information about Malware from the network and endpoint
- Aggregate this data into a cloud to take advantage of super-scale and collective intelligence
- Use machine learning and decision trees to process data and continuous datamine history
- Use this data to detect threats in realtime and retrospectively
- Use “Real-boxing” as the primary analysis system over Sand-boxing
Components of FireAMP
Visibility and Control

Lightweight Connector
• Watches for move/copy/execute
• Traps fingerprint & attributes

Mobile Connector
• Watches for apps
• Traps fingerprint & attributes

Web-based Manager

- Transaction Processing
- Analytics
- Intelligence
Sensor / Connector Integration

Network-based: AMP for firePOWER™

Detection
Analysis
Blocking

Device-based: fireAMP™

Desktop
Virtual
Mobile

Detection
Analysis
Blocking
Remediation

Collective Threat Intelligence

SOURCEfire
continuous analysis

Presentation_ID
Cisco and/or its affiliates. All rights reserved.
Cisco Public
Cloud Detection Engines

- One-to-One Signature
- Advanced Analytics
- Machine Learning
- Fuzzy Fingerprinting
- Dynamic Analysis
One-to-One Signature Engine

- SHA256 Based Signature lookup
- Very fast Look Up (less then 200 milliseconds)
- Very fast distribution (realtime instantaneous)
- One-to-One matching
- Dispositions:
  - Known Good
  - Known Bad (block / quarantine)
  - Known Unknown (neither Good or Bad)
  - Never Seen Before
- Takes advantage of massive automated processing of third-party feeds and the 3+ million endpoint immunet community
Generic Signature Engine (ETHOS)

- Known as the Fuzzy Fingerprint
- One-to-Many matching
- Algorithmic detection engine
- Applied to Good and Bad Files
- Captures an infection and all variants
- Enables the Cloud to data-mine characteristics of good files and bad files
- Uses automated created of generic signatures
Machine Learning Engine (SPERO)

- Fast Heuristic Engine
- Classifies the PE from over 400 characteristics including:
  - PE Header
  - Referred DLLs
  - Common Object File Format (COFF) attributes
- Enables the Cloud to data-mine characteristics of good files and bad files
- Uses “Big Data” techniques to distinguish Good files from Bad files
Advanced Analytics Engine

- Takes a Global Intelligence approach (as opposed to file-centric approach)
- Uses patterns in all of the other engines collecting data
- Can identify new threats that normally can’t be detected
- Helps enhance ETHOS and SPERO by pushing a file from “may be malicious” to “malicious”
- Example: Drop Kick
  - If a File of Unknown disposition creates (drops) more malicious files than good files -> Make this file malicious

---

Presentation_ID
Cisco and/or its affiliates. All rights reserved.
Cisco Public
Device Flow Correlation

- Applications are tracked for first 100 connections
- Outbound and Inbound TCP/UDP
  - Localhost / Port / Protocol / Timestamp -> DestIP / Port / Protocol
- URL’s are tracked
- Domains are tracked (HTTP)
- Associated files downloaded over HTTP are tracked
- Internal network and external network monitored
- Can actively block connections against the VRT or custom black lists
- Detect and Block CNC and Attack Sites
Connectors

File Query (Connector ID, SHA, SPERO, ETHOS, DFC)

Response Disposition

File Query (Connector ID, SHA, SPERO)

Response Disposition

Retrospective Query (PING2)

Changed Disposition

Sourcefire Cloud

One-to-One
Signature-based, 1st line of defense

Fuzzy Fingerprinting (ETHOS)
Algorithms identify polymorphic malware

Machine Learning (SPERO)
Analyzes 400+ attributes for unknown malware

Device Flow Correlation
Examines and associates flows with applications

Advanced Analytics
Combines data from lattice with global trends
Data Produced

- **File Convictions**
  - Good
  - Bad
  - Unknown

- **File Trajectory**
  - How the file moves across the organisation over time
  - Patient Zero

- **Device Trajectory**
  - How files behave on an endpoint over time
  - Just like an Analyst’s Handbook

- **File Analysis**
  - Information on the nature of the file

- **Indicators of Compromise**
The AMP Private Cloud

- **FireAMP Cloud-in-a-(virtual) Box:**
  Virtual appliance that compresses FireAMP cloud portal and management into a single on-premises solution

- **Proxied Cloud:**
  Private Cloud will function as an anonymized proxy between connectors and our Public Cloud for file disposition look ups

- **Scale:**
  Each Private Cloud instance will support up to 10K connectors
**Connectors**

**File Query, Enterprise First / Unique**
*(Connector ID, SHA, SPERO, ETHOS)*

- SPERO, ETHOS (Locally evaluated)
- Response Disposition

**File Query, Previously Seen in Ent.**
*(Connector ID, SHA, SPERO, ETHOS)*

- SPERO, ETHOS (Locally evaluated)
- Response Disposition

**PING2 Query**

- Changed Disposition

---

**On-premise Appliance**

**Upstream File Query**
*(Device ID, SHA)*

- Response Disposition

**PING2 Query**

- Retrospective Queue

- Changed Disposition

---

**Sourcefire Cloud**

**Retrospective Queue**

**SHA Conviction**
Low Prevalence Reports

- Reports on Low Prevalence Executables
- Helps Identify Weak Signal Events
Elastic Search

- Quickly search entire FireAMP cloud based on any string length
NETWORK MALWARE ANALYSIS
## Detection Capabilities

### Sourcefire Cloud

<table>
<thead>
<tr>
<th>Security Intelligence IP Reputation, URL Category Updates</th>
<th>L2/L3</th>
<th>Connection Logs, Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Cloud Lookups (AMP), Sandbox, Trajectories</td>
<td>Files</td>
<td>File Types, File Transfers</td>
</tr>
<tr>
<td>Application Definitions, App Detectors</td>
<td>AppID</td>
<td>Server, Client and Web Apps</td>
</tr>
<tr>
<td>Vulnerability Updates, OS Definitions</td>
<td>FireSIGHT</td>
<td>Discovery Events – Hosts, Users, OS, Services, Vulnerabilities</td>
</tr>
<tr>
<td>Snort Rule Updates</td>
<td>Snort</td>
<td>IDS/IPS Events – Snort Rule IDs</td>
</tr>
</tbody>
</table>
Policy Constructs

- **NGIPS** – content inspection
- **FireSIGHT** – context awareness
- **Security Intelligence** - blacklist control
- **Comprehensive access control**
  - By network zone, VLAN, IP, port, protocol, application, user, URL, Geo
- **Seamlessly integrated**
  - With IPS policies
  - File control policies
  - Malware policies
Event Types

- **Connection Events** – Source, Destination, Port, User, URL, App, Proto, User
- **Discovery Events** – OS, Client App, Service, Server, Usernames
- **Intrusion Events** – Snort Rule ID, Impact, Source, Destination, Packet Level
- **File Events** – Filename, File Type, Direction, Client App, Protocol
- **Correlation Events** – White List / Black List compliance
- **Security Intelligence Events** – IP Reputation
- **Malware Events** – Malware Cloud Lookups, FireAMP Endpoint events
- **Network File Trajectories** – Tracking of Files as they traverse the network
Context through FireSIGHT

- **FireSIGHT discovers** Host, Application and User information in **realtime**, continuously, **passively**
- Derives a worst-case **Vulnerability Map** of the monitored Network
- **Correlates** all Intrusion Events to an **Impact** of the attack against the target
- **Drastically** reduces False Positives, eliminates False Negatives

<table>
<thead>
<tr>
<th>IMPACT FLAG RATING</th>
<th>ADMINISTRATOR ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Flag 1" /></td>
<td>Act Immediately, Vulnerable</td>
</tr>
<tr>
<td><img src="image" alt="Flag 2" /></td>
<td>Investigate, Potentially Vulnerable</td>
</tr>
<tr>
<td><img src="image" alt="Flag 3" /></td>
<td>Good to Know, Currently Not Vulnerable</td>
</tr>
<tr>
<td><img src="image" alt="Flag 4" /></td>
<td>Good to Know, Unknown Target</td>
</tr>
<tr>
<td><img src="image" alt="Flag 0" /></td>
<td>Good to Know, Unknown Network</td>
</tr>
<tr>
<td><img src="image" alt="Flag B" /></td>
<td>Good to Know, Blocked</td>
</tr>
</tbody>
</table>
Dynamic Analysis: Process Overview

- File Detected on FirePOWER
  - Calculates hashes
  - Saves a copy if policy dictates*

- Hash metadata sent to AMP Cloud
- AMP Cloud Response: E.g.
  - Disposition = Unknown
  - Threat Score = Unknown *

- File is sent to VRT Services Cloud for Dynamic Analysis* (if policy dictates)

- Dynamic analysis:*
  - Analysis queue Status
  - Error Status
  - Threat Score

- Sourcefire Cloud Services
- Updates
- FireAMP Cloud (Metadata / Hashes)
- VRT Dynamic Analysis Cloud* (Files)
HOST AND ENDPOINT CORRELATION
Sourcefire AMP Detection Systems

- 1-to-1 File Matching from the cloud (Network and Endpoint)
- IP Reputation Matching from the cloud (Network - Security Intelligence Feed, Endpoint - Device Flow Correlation)
- SPERO Fuzzy File Matching from the cloud (Network and Endpoint)
- Vulnerability-facing Traffic Rules (Network)
- Malware Propagation Detections Rules (Network)
- CnC Blacklist Rules (Network)
- Cloud-based machine learning engines (supports the Network and Endpoint)
- Custom File Detections (Endpoint)
- Custom File Blocking (Network)
- Application Control (Network)
- Application Execution Blocking (Endpoint)
- File Quarantine (Endpoint)
- Network File Trajectory (Network)
- Device Trajectory (Endpoint)
- File Trajectory (Endpoint)
- Cloud-based Sandboxing (supports the Network and Endpoint)
- Indication of Compromise correlation (Network and Endpoint)
- Passive Device Discovery (Network)
- URL Detection and Control (Network)
Host and Event Correlation

- Today we have many different ‘event’ sources in Defense Center. For example:
  - IPS events *(Snort)*
  - FireAMP events *(endpoint)*
  - Malware events *(network)*
  - Security Intelligence *(network + endpoint)*

- Different events can tell an analyst different things about the state of a host or the network
  - Has it been targeted a type of network attack *(snort)*
  - Has it downloaded malware? *(Snort, FireAMP, Malware)*
  - Has it executed malware *(FireAMP)*
  - Has it connected to a CNC server *(Snort, FireAMP, SI)*

- This feature combines these event sources and correlates them based on the hosts involved with the events
Indicators of Compromise Table

- Shows all IOCs set on all Hosts over the network
  - Workflow: Hosts with the most IOCs set (most likely compromised) - Good dashboard widget for this as well
  - Actions you can take on this table:
    - View the Host Profile
    - Mark the IOC as resolved
    - Drill into the triggering event(s)

- Events can different sources all sit in this table
  - Example: CNC via SI, CNC via FireAMP, CNC via Snort

- New Host Icon used for when host has displayed IOCs
Example IOC

- **IOC Tag Category:** “CNC Connected”
- **Description:** “This host may be under remote control”
- **What could set this tag?**
  - **Security Intelligence:** A host connects to a device marked as a CNC server
  - **IPS event:** An IPS event from the category “Malware-CNC” is triggered by this host
  - **FireAMP event:** FireAMP detects that a device may have connected to a CNC server via DFC
IOC Host Profile View

Host Profile

- **IP Addresses**: 10.51.1.04 (wolfe.englab.sourcefire.com)
- **NetBIOS Name**: mango.englab.sourcefire.com (0)
- **MAC Addresses (TTL)**:
  - 00:00:33:13:88:00 (COMDA ENTERPRISES CORP.) (254)
  - BA:EA:5E:3D:DE:F7 (61)
  - 00:50:56:90:70:8A (VMware, Inc.) (62)

- **Host Type**: Router
- **Last Seen**: 2013-09-20 06:40:44
- **Current User**: View

Indications of Compromise (3) = 3

1. **Exploit Kit**: Intrusion Event - exploit-kit
   - Description: The host may have encountered an exploit kit
   - First Seen: 2013-09-17 16:46:28
   - Last Seen: 2013-09-20 06:35:31

2. **CnC Connected**: Security Intelligence Event - CnC
   - Description: The host may be under remote control
   - First Seen: 2013-09-17 16:52:11
   - Last Seen: 2013-09-20 03:55:45

3. **CnC Connected**: Intrusion Event - malware-cnc
   - Description: The host may be under remote control
   - First Seen: 2013-09-17 20:09:23
   - Last Seen: 2013-09-19 17:32:49

Systems (4) ▼

- **Google**: Chromium 3701.81.2
- **Source**: FireSIGHT
IOC Table

Indications of Compromise by Host

- Impact 2 Attack
- Impact 2 Intrusion

No Search Constraints (Edit Search)

Jump to:

IP Address | Category | Event Type
---|---|---
10.5.1.19 | Impact 2 Attack | Impact 2 Intrusion
10.10.108 | Impact 2 Attack | Impact 2 Intrusion Event - attempted-admin
10.5.61.152 | Impact 2 Attack | Impact 2 Intrusion Event - attempted-user
10.5.22.191 | Impact 2 Attack | Impact 2 Intrusion Event - attempted-user
10.5.12.72 | Impact 2 Attack | Impact 2 Intrusion
10.5.25.10 | Impact 2 Attack | Impact 2 Intrusion
10.5.22.162 | Impact 2 Attack | Impact 2 Intrusion
10.22.75.18 | C&C Control

Impact 2 Intrusion Event - attempted-user:
The host was attacked and is potentially vulnerable.

Triggering Event Summary:

Source: Security Intelligence Events

<table>
<thead>
<tr>
<th>Initiator IP</th>
<th>Responder IP</th>
<th>Security Intelligence Category</th>
<th>Application Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.22.75.18</td>
<td>54.230.192.199</td>
<td>C&amp;C</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Link to original event(s)
IOC Dashboard Widget

- Because IOCs enable a quick way of classifying a host’s potentially compromised state, having this data on a dashboard is desirable.

<table>
<thead>
<tr>
<th>Host</th>
<th>Number of IOCs set against the host</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.61.104</td>
<td>6</td>
</tr>
<tr>
<td>10.5.31.73</td>
<td>6</td>
</tr>
<tr>
<td>10.22.35.10</td>
<td>4</td>
</tr>
<tr>
<td>10.1.3.210</td>
<td>3</td>
</tr>
<tr>
<td>10.1.3.128</td>
<td>3</td>
</tr>
<tr>
<td>10.1.3.127</td>
<td>3</td>
</tr>
<tr>
<td>10.1.3.126</td>
<td>3</td>
</tr>
<tr>
<td>10.1.3.208</td>
<td>3</td>
</tr>
<tr>
<td>10.1.3.206</td>
<td>3</td>
</tr>
<tr>
<td>10.1.3.200</td>
<td>3</td>
</tr>
</tbody>
</table>

Click to expand
Supplemental Slides
ZeroAccess Investigation
Note Chrome makes 3 network connections, and then Java downloads a malicious file in 3 parts, moves the file and then runs the file, triggering 3 IOCs and further infection to the target endpoint.
FireAMP correlates Java being compromised, creating a malicious file and then executing it.
Here is the connection Chrome made to a malicious web site, hosting a web page with an embedded java exploit that compromised the version of Java installed on this endpoint.
Upon executing, the malware went to Google’s public DNS server 8.8.8.8
It also connected to a publically available geolocation script to discover the geo of the infected endpoint as part of its enrollment to the CnC.
Once it enrolls and downloads more components, the malware pulls down a version of Flash which it will exploit to root the endpoint further.
Once rooted by Flash, rundl32 makes more network connections, and a new malicious payload is downloaded.
Right-clicking on Java and selecting File Trajectory allows the analyst to check where this vulnerable version of Java, which is currently being compromised, is also installed.
By searching for connections to Google’s public DNS, an analyst can determine endpoints and files making this suspicious traffic to discover new infected endpoints.
Searching for connections to j.maxmind.com, an analyst can also determine endpoints making this suspicious traffic to discover new infected endpoints.