Defeating Blended Threat
with Cisco Content Security Solution
Cisco Solution Summit

Brian Cotaz
Consulting Systems Engineer
July 15, 2015
The Blended Threat
The Reality
Organizations Are Under Attack

- Cybercrime is lucrative, barrier to entry is low
- Hackers are smarter and have the resources to compromise your organization
- Malware is more sophisticated
- Organizations face tens of thousands of new malware samples per hour

- Phishing, Low Sophistication
- Hacking Becomes an Industry
- Sophisticated Attacks, Complex Landscape

- 95% of large companies targeted by malicious traffic
- 100% of organizations interacted with websites hosting malware

- Viruses 1990–2000
- Viruses 2000–2005
- Spyware and Rootkits 2005–Today
- APTs Cyberware Today +
Creating Increasingly Exposed Users and Organizations

- Advanced Malware
- IPv6 Spam
- Blended Threats
- Rootkits
- APTs
- Worms
- Trojan Horse
- Targeted Attacks

Email is the #1 Threat Vector

Malware Infections
Acceptable Use Violations
Data Loss

Cisco
## Most dangerous threats

<table>
<thead>
<tr>
<th>Approach</th>
<th>Tactic</th>
<th>Impact</th>
<th>Threat vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watering hole</td>
<td>Infect or inject a trusted site</td>
<td>Conduct reconnaissance on a target</td>
<td>Target users through compromised links</td>
</tr>
<tr>
<td>Spear phishing</td>
<td>Leverage social engineering</td>
<td>Deliver an exploit that will attack</td>
<td>Compromises system control, personal data and authorizations</td>
</tr>
<tr>
<td>Dropper</td>
<td>Gain access through DLL injection and control firewalls, antivirus, etc</td>
<td>Deliver malware with stealth and self-deleting programs</td>
<td></td>
</tr>
</tbody>
</table>
Sample attack: Joe CFO case

Meet Joe. He is heading to a well deserved vacation.

He’s catching up on email using the airport Wi-Fi while he waits for his flight.
Joe just got an email from his vacation resort.

Joe,  

Thank you for choosing us. We look forward to seeing you.  

Before your arrival, please verify your information here:  
www.vacationresort.com  

Best,  
Resort Team
Instinctively, he clicks on the link. No problem, right? Everything looks normal.

The site may even be a trusted site, or maybe a site that is newly minted.

Joe,

Thank you for choosing us. We look forward to seeing you.

Before your arrival, please verify your information here:

www.vacationresort.com

Best,

Resort Team
Joe opens the link and the resort video plays.

Although he doesn’t know it, Joe’s machine has been compromised by a flash based video exploit.

The malware now starts to harvest Joe’s confidential information:

- Passwords
- Credentials
- Company access authorizations
Attckers:

Shifts in the attack vectors

PDF and Flash steady
Java drop 34%

Silverlight rise 228%
Attacks:
A growing appetite to leverage targeted phishing campaigns

Example: Snowshoe SPAM attack

SPAM up 250%
Attackers:

Malvertising is on the rise: low-limit exfiltration makes infection hard to detect

In October 2014, there is a spike of 250%
Users becoming complicit enablers of attacks

- Untrustworthy sources
- Clickfraud and Adware
- Outdated browsers

<table>
<thead>
<tr>
<th></th>
<th>IE requests running latest version</th>
<th>Chrome requests running latest version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>vs 64%</td>
<td></td>
</tr>
</tbody>
</table>
Feeding the Beast

43% Opened an email I suspected was spam
11% Clicked on a link in an email I suspected was spam
15% Opened a spam email, to learn more about the offered products or services

Source: MAAWG
Cisco Content Security Solution
To Defeat Those Blended Threats Requires Greater Intelligent and Visibility across Attack Continuum

Attack Continuum

Before
Discover
Enforce
Harden

During
Detect
Block
Defend

After
Scope
Contain
Remediate

Email
Web
Endpoint
Mobile
Virtual
Cloud
Network

Point-in-time
Continuous
Cisco Content Security Security integration with Threat Intelligence
Built on unmatched collective security analytics

- 180,000+ file samples per day
- FireAMP™ community
- Advanced Microsoft and industry disclosures
- Snort and ClamAV open source communities
- Honeypots
- Sourcefire AEGIS™ program
- Private and public threat feeds
- Dynamic analysis

<table>
<thead>
<tr>
<th>Threat Intelligence</th>
<th>Research Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6 million global sensors</td>
<td>180,000+ file samples per day</td>
</tr>
<tr>
<td>100 TB of data received per day</td>
<td>FireAMP™ community</td>
</tr>
<tr>
<td>150 million+ deployed endpoints</td>
<td>Advanced Microsoft and industry disclosures</td>
</tr>
<tr>
<td>600+ engineers, technicians, and researchers</td>
<td>Snort and ClamAV open source communities</td>
</tr>
<tr>
<td>35% worldwide email traffic</td>
<td>Honeypots</td>
</tr>
<tr>
<td>13 billion web requests</td>
<td>Sourcefire AEGIS™ program</td>
</tr>
<tr>
<td>24x7x365 operations</td>
<td>Private and public threat feeds</td>
</tr>
<tr>
<td>40+ languages</td>
<td>Dynamic analysis</td>
</tr>
</tbody>
</table>
Cisco Advanced Malware Protection
Built on Unmatched Collective Security Intelligence

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
4.3 billion web blocks per day
40+
languages
1.1 million incoming malware
samples per day
AMP Community
Private/Public Threat Feeds

Talos Security Intelligence
AMP Threat Grid Intelligence
AMP Threat Grid Dynamic
Analysis
10 million files/month
Advanced Microsoft
and Industry Disclosures
Snort and ClamAV Open Source
Communities
AEGIS Program

Automatic updates
in real time

AMP
Advanced Malware Protection

Cisco Collective
Security Intelligence Cloud

Cisco® Collective
Security Intelligence

AMP
Advanced Malware Protection

Cisco Collective
Security Intelligence Cloud

Cisco
Collective
Security Intelligence

AMP
Advanced Malware Protection
Delivers the First Line of Detection

One-to-One Signature  Fuzzy Finger-printing  Machine Learning  Advanced Analytics  Dynamic Analysis

Reputation Filtering and File Sandboxing
Real-Time Sandbox: Defend Blended Threats
Analysis for Zero-Day Defense

Real-Time Emulation
Cisco Advanced Malware Protection

Point-in-Time Protection

Retrospective Security

File Reputation and Sandboxing

Continuous Analysis
And Continues to Analyze What Happened

Breadth and Control points:
- Email
- Endpoints
- Web
- Network
- IPS
- Devices

Telemetry Stream

File Fingerprint and Metadata
File and Network I/O
Process Information
Talos + Threat Grid Intelligence

Continuous feed

1100001110001110  1001  1101 1110011  0110011  101000  0110 00  0111000  111010011  101  1100001
110
1000111010011101  1100001110001110

Continuous analysis
Marketing Message Classification

Privacy Policy

At Buy.com, your privacy is a top priority. Please read our privacy policy details. All information collected from you will be shared with Buy.com and its affiliate companies.
Graymail

The Graymail solution will provide:

- Protection against malicious threats masquerading as unsubscribe links
- A uniform interface for all subscription management to end-users
- Better visibility to the email administrators and end-users into such emails
End User Experience
Safe Unsubscription Status: Success
URL Defense: Defend Blended Threats

Email Contains URL

Cisco® Talos

- Rewrite
- Send to Cloud
- Defang/Block
  - BLOCKED www.playboy.com
  - BLOCKED www.proxy.org

Replace

“This URL is blocked by policy”

URL Reputation and Categorization
Web Interaction Tracking: Defend Blended Threats

URL Rewritten

Users Click Rewritten URL

Rewritten URL Report

- The top malicious URLs
- Users clicked
- Date/time, rewrite reason, URL action

List of users accessing rewritten URLs

- Based on Email ID
- Based on LDAP group
- Based on IP Address

Add malicious URLs to blacklist

- Stop 0-Day
- Dynamic Intelligence
- Educate users
Missed-Spam Analysis

- Administrator can set rate limit for individual senders
- Majority of Offer spam uses Snowshoe techniques
- Snowshoe spam – technique used by spammers to cover their tracks, go under the radar. Its objective is to defeat traditional Anti-Spam techniques.
- Short campaigns – morphs fast – constantly changing

<table>
<thead>
<tr>
<th>Anti-Sender Reputation</th>
<th>Anti-Content Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Never use the same IP to send more than x amount of spam in more than y period of time.</td>
<td>▪ Never use the same series of words</td>
</tr>
<tr>
<td>▪ Never send the same spam from the same IP.</td>
<td>▪ Never reuse the same images</td>
</tr>
<tr>
<td>▪ Never use the same series of words</td>
<td>▪ Never use the same URL</td>
</tr>
</tbody>
</table>

- Not “new” techniques, however, usage has increased
- Fine line to balance catch rate and false positive

**Categories of Missed Spam**
(Customer submissions since Jan/14)

- Offer
- Seminar
- Diplomas
- Mkt Svcs
- Casino
- Link
- Malware
- Luxury
- Stocks
- Scam
- Phish
- Drug
- Lottery
- Job
- Loan
- Dating
- Insurance
- Offer

细线平衡捕获率和误报率
The Spam Landscape

Increase in “Snowshoe” spam

<table>
<thead>
<tr>
<th>Sender Type</th>
<th>Nov 2013</th>
<th>Apr 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other sender</td>
<td>53%</td>
<td>46%</td>
</tr>
<tr>
<td>Marketing sender</td>
<td>38%</td>
<td>37%</td>
</tr>
<tr>
<td>Snowshoe sender</td>
<td>7%</td>
<td>15%</td>
</tr>
<tr>
<td>Freemail sender</td>
<td>2%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Spam broken down by Sender Type
Anti-Snowshoe
Steps to Take in Battling Spam

“Maintain leadership in antispam efficacy through ever-changing threat landscape to protect our customers and keep ahead of the competition”

Sensor footprint expansion for early awareness of snowshoe campaigns

Increase automation and automatic classification of emails for faster response

Better defense against snowshoe spam through enhanced contextual analysis
Thank you