From reactive to proactive solutions

Content Security

Jens Christian Høy Monrad
Ironport Systems Engineer Nordics
Agenda

- Challenges Today
- Threats and Trends
- Criminal Ecosystem
- Solutions
- Conclusion
The Evolution of Intent, A Shift to Financial Gain

Threats Are Becoming Increasingly Difficult to Detect and Mitigate

Primary Targets: Legitimate Web Sites

- Financial: Theft and Damage
- Notoriety: Viruses and Malware
- Vandalism: Basic Intrusions and Viruses

What’s Next?
Active Content: Malware Is on the Rise

# of unique Malware samples in 2006: 972K
# of unique Malware samples in 2007: 5.5M

500% increase in 12 Months
50% of traffic is “easy to classify”
Predictable traffic, Recognized domains

50% of traffic is “hard to classify”
110M sites, growing 40% annually
Mixture of legitimate sites, spyware and malware

Web Traffic
The Long Tail Gets Longer
Effect of Closing McColo - **Temporary**

SpamCop Statistics

- **McColo Shutdown**

Messages per second

- Spam Submitted
- Reports Sent

Average Spam: 31.4 msgs per second  Max Spam: 69.5 msgs per second
Total Spam (last year): 90501653 messages

Thu Apr 2 12:07:01 EDT 2009
Web Browser Ecosystem Vulnerable

SANS Top 20 2007 Security Risks
http://www.sans.org/top20/#c1

- IE and Firefox vulnerable
  “…hundreds of vulnerabilities in ActiveX controls installed by software vendors have been discovered.”

- Media Players & Browser Helper Objects (BHO)
  RealPlayer, iTunes, Flash, Quicktime, Windows Media
  Explosion of BHOs and third-party plug-ins
  Plug-ins are installed (semi) transparently by website. Users unaware an at-risk helper object or plug-in is installed … introducing more avenues for hackers to exploit users visiting malicious web sites.
“Web application vulnerabilities in open-source as well as custom-built applications account for almost half the total number of vulnerabilities being discovered in the past year. These vulnerabilities are being exploited widely to convert trusted web sites into malicious servers serving client-side exploits and phishing scams.”
Virus Sophistication Beats AV Signatures

- 182 virus tools at VX Heavens website vx.netlux.org
  Example: NGVCK (Next Generation Virus Creation Kit)
- Poly/Metamorphic tools create random variants
- Viruses download fresh copy every 24 hours
- Viruses use buddy program to reinstall virus if disinfected

A Quick & Easy Trojan Developing System

Author: Walt DiZnEy

Author's notes: EasyTrojan is a program that enables "ANYONE" to write Ready To Run Trojan Horses, using a very-easy-to-learn Trojan-Writing-Code. EasyTrojan is not intended to replace "real" programming in the developing of Trojan Horses, but it offers an invaluable help to those who don't know anything about computer languages and want to make Trojans, and also to programmers who are in a hurry and need a Quick-Ready-To-Run Trojan!

Download

<table>
<thead>
<tr>
<th>Filename</th>
<th>Size</th>
<th>Desc</th>
<th>Date</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>easyt11.zip</td>
<td>23047</td>
<td>QTBS 1.1.0</td>
<td>Dec 1993</td>
<td>a0ca972006b41089862807abe16e8ec</td>
</tr>
</tbody>
</table>
Threats and Trends
Conficker/Downadup Worm

- Microsoft MS08-067 out of band security update on Oct 23, 2008
- Vulnerability in Windows Server service allowing remote code execution using port 139 or 445
  - 2000, XP, Windows Server 2003 without authentication
  - Vista, Windows Server 2008 requires authenticated remote attacker
- Conficker spreads via
  - Scanning local network for vulnerability
  - Via local shares by password guessing administrator logins
  - Removable devices (e.g. USB drives) via autorun.inf
- Estimate approximately 9M infected PCs (F-Secure)

Computer virus shuts down Houston municipal courts

French fighter planes grounded by Conficker
Social Engineering via Social Medias
"Scareware"
Threats are also local

Finansråd: Dansk phishing-site afsløret i København

En dansk phishing-site, der lokkede kredittornumre fra godtroende PayPal kunder, er netop blevet afsløret i København.

Det er ikke usædvanligt at de danske hjemmesider, hvor kodeord, siger S

-Særligt de falske phishing-hjemmesider, så selv om det er en normal person med adressen i København, der står som registrant af domænet, behøver han ikke være ophavsmand til phishingforskøft.

Det rigtige sikkerhedsstilfælde F-Secure har undersøgt sagen
og er kommet frem til, at e-mailen er sendt via en server i
Ukraine til danske e-mailadresser.

Men det specielle i denne sag er, at de falske phishing-hjemmesider lå på en dansk server.

Skrevet af: Preben Lund
Danish Infected Sites

Infected Sites !!!

Q&A
Dette websted kan beskylde din computer.

Mutikkenesen.dk, en gratis resource for musikere på nettet.

Toyota (Ostjylland) script src=http://www.nokia1.cn

江苏商务信息服务中心—企业之窗 — [Disable some side]

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public
Criminal Ecosystem
Coordinated, Multi-Phase Attacks

Spam Engines (SMTP)

Landing pages (HTTP)

Date: Sat, 26 Aug 2007 19:06:20 -0700
From: <morgione@playstation.sony.com>
To: <brian.krebs@spnli.com>
Subject: how did you get that on film, man?

OMG, what are you doing man. This video of you is all over the net. here is where I found it...
http://www.youtube.com/watch?v=xEd4hK5jP6Q
Criminal Ecosystem
Malware Development and Distribution

Welcome to RAT Systems Crew Official website

Our team is specialised in spyware development. We are coding all types of spyware, from remote administration tools with GUI to simple keyloggers. Our main direction is to create effective and powerful spyware. Coding is not just hobby for us, its out job and style of life.

In general we're against destructive payloads and the spreading of viruses. Coding spyware is not a crime. Our team is not interested in massive infections. We are do not use our or any other spyware for illegal purposes. All our job is absolutely legal and we are not installing our or any other spyware to someone's computer without notification.
Solutions
Network Is “Locked”—Email and Web Are Open

Port 25

Content Security

Port 80
Port 443

Network Security
IronPort’s SenderBase
Faster, More Accurate Detection and Protection

Combines Email and Web Traffic Analysis

View into both email and web traffic dramatically improves detection

- 83% of spam and 80% of overall email contains URLs
- Email is a key distribution vector for web-based malware
SenderBase Network

- **Complaint Reports**
- **IP Blacklists & Whitelists**
- **Domain Blacklists & Safelists**
- **Compromised Host Lists**
- **Web site Composition Data**
- **Spam Traps**
- **Message Composition Data**
- **Global Volume Data**
- **Other Data**

- **SpamCop, SpamHaus (SBL), NJABL, Bonded Sender**
- **SpamCop, ISPs, customer contributions**
- **Message size, attachment volume, attachment types, URLs, host names**
- **Over 100,000 organizations, email traffic, web traffic**
- **Spamvertized URLs, phishing URLs, spyware sites**
- **SORBS, OPM, DSBL**
- **Downloaded files, linking URLs, threat heuristics**
- **Fortune 1000, length of sending history, location, where the domain is hosted, how long has it been registered, how long has the site been up**

**First to combine email & web data**

**Over 150 email and 50 web parameters tracked**
What SenderBase Scores Mean

-10
An IP address controlled by a spam house or a known open proxy generating massive volume of complaints and hitting many spam traps. **Definitely sending primarily spam.**

-5
Spam houses generating complaints and hitting spam traps. IP listed on one or more open proxy lists. **Still guaranteed to be spam.**

0
May be a dynamic IP (e.g., dialup) sending direct to Internet or an email marketer with poor practices, or a legitimate enterprise with an open server. **Possibly spam**

+5
Some sending history, low or moderate complaints.

+10
Long sending history, few complaints.

+10
A known enterprise, or sender who has undergone third-party certification, with no complaints and a long sending history.

+5
Possibly spam

May be a dynamic IP (e.g., dialup) sending direct to Internet or an email marketer with poor practices, or a legitimate enterprise with an open server.

0
Long sending history, few complaints.

-5
Spam houses generating complaints and hitting spam traps. IP listed on one or more open proxy lists. **Still guaranteed to be spam.**

-10
An IP address controlled by a spam house or a known open proxy generating massive volume of complaints and hitting many spam traps. **Definitely sending primarily spam.**
SenderBase Powers IronPort Email and Web Security Services

Email Reputation Filters
- Stop 80-90% of threats at the connection level
- Provide preferred availability to senders with positive reputation

IronPort Anti-Spam
- Message analysis on structure, content, and source
- Highest catch rate on new threats, proven lowest false positives (1/1,000,000)

Virus Outbreak Filters
- Quarantine outbreaks before signatures are published
- Prevent infections of desktop systems during analyze/develop/test/release A/V-signature cycle

Web Reputation Filters
- Accelerate secure web gateway by prioritizing sites based on historical behavior
- Increase A/S efficacy by rating URLs in spam

Zombie Detection (L4TM)
## SenderBase

*Reputation Filtering vs. Black Lists & White Lists*

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>REPUTATION FILTERING</th>
<th>BLACK LISTS &amp; WHITE LISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Granular Scoring</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Tailored Response</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Low Administrative Overhead</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Increased Message Throughput</td>
<td>●</td>
<td>○</td>
</tr>
</tbody>
</table>
The IronPort Story
Application-Specific Security Gateways

**BLOCK Incoming Threats:**
- Spam, Phishing/Fraud
- Viruses, Trojans, Worms
- Spyware, Adware
- Unauthorized Access

**APPLICATION-SPECIFIC SECURITY GATEWAYS**

- **EMAIL Security Gateway**
- **WEB Security Gateway**

**MANAGEMENT Controller**

- **CENTRALIZE Admin:**
  - Per-user policy
  - Per-user reporting
  - Quarantine
  - Archiving

**ENFORCE Policy:**
- Acceptable Use
- Regulatory Compliance
- Intellectual Property
- Encryption

**SenderBase**
(The Common Security Database)
Multi-Layered Defenses

C-Series Email Security

- SenderBase Reputation Filters
- Virus Outbreak Filters
- A/V (Sophos, McAfee)
- IronPort Anti-Spam

S-Series Web Security

- Web Reputation Filters
- Anti-Malware (Webroot)
- Anti-Virus (McAfee)
- IronPort URL Filters

IN

OUT

- Data Loss Prevention
- Email Encryption
- Zombie Detection (L4TM)
- Protocol Enforcement (IM, P2P)
IronPort Virus Outbreak Filters
The First Line of Defense

- Early Protection with IronPort Virus Outbreak Filters
- Exploit Hits
- Patch Issued
- AV Update Released
- AV Update Deployed to Most Hosts
- Most Hosts Patched

Time

Infected Hosts
How IronPort Virus Outbreak Filters Work

*Dynamic Quarantine In Action*

- **T = 0**
  - zip (exe) files

- **T = 5 mins**
  - zip (exe) files
  - Size 50 to 55 KB.

- **T = 10 mins**
  - zip (exe) files
  - Size 50 to 55KB
  - “Price” in the name file

- **T = 8 hours**
  - Release messages if signature update is in place

Messages Scanned & Deleted
Rapid Onset, High Variation

IronPort Virus Outbreak Filters™ is designed for this type of attack

<table>
<thead>
<tr>
<th>Sophos Virus Name</th>
<th>Outbreak First Blocked by IronPort</th>
<th>First Signature Published</th>
<th>Virus Outbreak Duration (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>W32/Feebs-Fam</td>
<td>10/13/2007 4:00</td>
<td>10/16/2007 1:49</td>
<td>69:49</td>
</tr>
<tr>
<td>W32/Feebs-BW</td>
<td>10/17/2007 4:00</td>
<td>10/17/2007 14:36</td>
<td>10:36</td>
</tr>
<tr>
<td>W32/Feebs-BX</td>
<td>10/17/2007 4:00</td>
<td>10/18/2007 1:52</td>
<td>21:52</td>
</tr>
<tr>
<td>Mal/Feebs-B</td>
<td>10/19/2007 8:00</td>
<td>10/19/2007 13:19</td>
<td>5:19</td>
</tr>
<tr>
<td>W32/Feebs-BY</td>
<td>10/20/2007 1:00</td>
<td>10/20/2007 15:25</td>
<td>14:25</td>
</tr>
</tbody>
</table>
Integrated L4 Traffic Monitor

*Wire Speed Network Layer Scanning for Malware*

Block or Monitor

Scans **all** 65,536 ports at wire speed

Catches malware attempting to bypass port 80

Tied into IronPort SenderBase

Constantly Auto Updated

Control to exempt sources and/or destinations
Conclusion
Conclusion

- Malware spreads faster than AV vendors can produce signatures
- URL Filtering only protects against known sites
- Blacklists (RBL etc.) is static and often requires user interaction
- Senderbase is a dynamic reputation filter with updates every 5 minutes, securing both e-mail and web access.
- Ironport Antispam has an industry proven low false positive rate (1/1,000,000)
- Ironport Virus Outbreak Filter helps companies to combat zero day threats
- Ironport L4TM monitor and blocks for malware trying to access www via non http(s) ports.
Links

- Cisco Realm (This makes my job look cool 😊)
  http://cisco.com/go/realm
- Senderbase
  http://www.senderbase.org
- Cisco Ironport Threat Operation Center
  http://www.ironport.com/toc/
- Cisco Security Center
  http://tools.cisco.com/security/center/
  http://www.ironport.com/report/
TRY BEFORE YOU BUY

Sign up today and receive a fully-functional IronPort appliance to test in your network, FREE for 30 days.

Visit IronPort at Cisco expo for more information on evaluations, technical inquiries and prices.