SR B26: Find Botnets & Other Malware Using the Malicious Activity Assessment

Piero DePaoli & Eric Schwake
Product Marketing
Malware Activity
The Big Numbers for 2011

5.5B Attacks blocked by Symantec
403M Unique variants of malware
4,595 Web attacks per day
4,989 New vulnerabilities
8 Zero-day vulnerabilities

+81%
+41%
+36%
-20%
-43%
Why is Malware Continuing to Rise?

- Attack tool kits continue to flourish
- Increase efficacy of known vulnerabilities

*Figure A.9*

**Malicious Web Site Activity: Attack Toolkit Trends, 2011**

*Source: Symantec*
Why is Malware Continuing to Rise?

• Web attacks are increasing

Figure A.8

Average Sites Blocked Each Month

Source: Symantec.cloud
Which Website is More Dangerous?

18+
WARNING! ADULTS ONLY!
EXPLICIT MATERIAL FOR VIEWING
BY ADULTS 18 YEARS OF AGE OR OLDER
YOU MUST BE AT LEAST 18 YEARS OLD TO ACCESS THIS SITE!

Continue to Site

wwwalborgbackground.net

SR B26: Malicious Activity Assessment
Most Harmful Websites by Categories

Figure A.15

Malicious Web Activity:
Malicious Code By Number Of Infections Per Site, 2011

<table>
<thead>
<tr>
<th>Rank</th>
<th>Categories Of Web Sites</th>
<th>Average Number Of Threats Found On Infected Web Sites</th>
<th>Major Threat Type Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Religion/ Ideologies</td>
<td>115</td>
<td>Fake Antivirus: 82%</td>
</tr>
<tr>
<td>2</td>
<td>Hosting/ Personal hosted sites</td>
<td>39</td>
<td>Trojans: 43%</td>
</tr>
<tr>
<td>3</td>
<td>Pornography</td>
<td>25</td>
<td>Trojans: 44%</td>
</tr>
<tr>
<td>4</td>
<td>Entertainment and Music</td>
<td>21</td>
<td>Fake Antivirus: 42%</td>
</tr>
<tr>
<td>5</td>
<td>Business/ Economy</td>
<td>17</td>
<td>Fake Antivirus: 62%</td>
</tr>
<tr>
<td>6</td>
<td>Technology/ Computer and Internet</td>
<td>17</td>
<td>Fake Antivirus: 54%</td>
</tr>
<tr>
<td>7</td>
<td>Travel</td>
<td>16</td>
<td>Fake Antivirus: 46%</td>
</tr>
<tr>
<td>8</td>
<td>Sports</td>
<td>13</td>
<td>Fake Antivirus: 69%</td>
</tr>
<tr>
<td>9</td>
<td>Automotive</td>
<td>11</td>
<td>Fake Antivirus: 41%</td>
</tr>
<tr>
<td>10</td>
<td>Shopping</td>
<td>9</td>
<td>Fake Antivirus: 63%</td>
</tr>
</tbody>
</table>

Source: Symantec

- Sites with poor security become easy targets for malware authors
- Some businesses understand that customers will visit sites that infect them
Targeted Attacks Have Expanded
Advanced Targeted Threats

Your Assumptions are Wrong
Only large corporations, governments and defense industries are targeted for attack
Organizations of All Sizes at Risk of Targeted Attacks

13,518

2,500+
Targeted Attacks by Sector

- Government & Public Sector: 25%
- Manufacturing: 15%
- Finance: 14%
- IT Services: 6%
- Chemical & Pharmaceutical: 6%
- Transport & Utilities: 6%
- Non-Profit: 6%
- Marketing & Media: 3%
- Education: 3%
- Retail: 3%

SR B26: Malicious Activity Assessment

SYMANTEC VISION 2012
Assumption #2

Only CEOs and senior managers are targeted
Targeted Attacks by Job Function

- C-Level: 25%
- Senior: 6%
- R&D: 8%
- Sales: 12%
- Media: 10%
- Shared Mailbox: 9%
- PA: 12%
- Recruitment: 6%

SR B26: Malicious Activity Assessment
Targeted Attacks by Job Function

58%

Sales
Media
Shared Mailbox
PA
Recruitment
Assumption #3

A targeted attack is a single attack
Use Case: Taidoor

- One target was attacked for 9 straight months
- In June, attacks occurred almost once a day
The Malicious Activity Assessment
The Key Questions We’ll be Asking

1. Are you concerned about employees becoming infected via drive-by downloads? Do you know if this is happening, and on which endpoints?

2. Are you concerned about new threats -- Web 2.0 attacks, spear phishing, and APTs?

3. Are you concerned endpoints on your network may get infected due to lack of antivirus installed, or not being patched & configured to corporate standards?

4. Can you effectively report on the volume of malicious activity on your network?

5. Are you able to quickly identify infected clients and remediate before further disruption?

6. Can you inspect your network for botnets, both dormant and active, and quickly remediate issues?
Malicious Activity Assessment Basics

Goal

- Identify the presence of installed malware & botnet activity

How

- Passive monitoring of live customer traffic using Symantec Web Gateway
- 7 to 14 day engagement
- Run by Symantec or Symantec Partners
Malicious Activity Assessment

Customer Benefits

Understand the volume and impact of malicious activities

Identify key areas for improved protection and response

Leverage new sources of security intelligence -- Insight
Malicious Activity Assessment

Customer Requirements

- Gain executive commitment to assessment process and outcomes
- Secure IT Staff to participate (install requires < 1 day of technical resource)
- Identify and configure SPAN Port or Tap for bi-directional passive monitoring
- Key stakeholder participation in presentation of results
Discover Connections to Malicious IPs ...

- Provided from Symantec Global Intelligence Network
- Sources:
  - 75M+ Norton Community Watch Users
  - Symantec Honey pots
  - Symantec Web Crawlers
  - Symantec DeepSight
- Policy based blocking
  - User/Group/IP
  - Severity
  - Category

<table>
<thead>
<tr>
<th>Latest Detection</th>
<th>Spyware Name</th>
<th>Severity</th>
<th>Category</th>
<th>Detection Type</th>
<th>Clients</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/23/2010 08:33</td>
<td>demo.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>147</td>
<td>244</td>
</tr>
<tr>
<td>09/23/2010 09:30</td>
<td>securewebsitename.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>104</td>
<td>190</td>
</tr>
<tr>
<td>09/23/2010 09:30</td>
<td>pineapple.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>104</td>
<td>112</td>
</tr>
<tr>
<td>09/23/2010 09:44</td>
<td>xjmx.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>26</td>
<td>6,266</td>
</tr>
<tr>
<td>09/23/2010 09:36</td>
<td>naver.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>21</td>
<td>1,253</td>
</tr>
<tr>
<td>09/23/2010 09:45</td>
<td>dmcmn.baidu.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>21</td>
<td>831</td>
</tr>
<tr>
<td>09/23/2010 08:00</td>
<td>dere-01.fdl.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>15</td>
<td>260</td>
</tr>
<tr>
<td>09/22/2010 21:10</td>
<td>yellowbouquet.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>14</td>
<td>52</td>
</tr>
<tr>
<td>09/22/2010 02:20</td>
<td>eyemall.co.kr</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>11</td>
<td>510</td>
</tr>
<tr>
<td>09/22/2010 16:28</td>
<td>brotherssoft.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>9</td>
<td>894</td>
</tr>
<tr>
<td>09/22/2010 12:06</td>
<td>154.71.11.69</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware IP</td>
<td>8</td>
<td>40</td>
</tr>
<tr>
<td>09/22/2010 16:11</td>
<td>itc.cn</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware IP</td>
<td>8</td>
<td>28</td>
</tr>
<tr>
<td>09/23/2010 09:46</td>
<td>taobao.cn</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>7</td>
<td>219</td>
</tr>
<tr>
<td>09/23/2010 08:48</td>
<td>leadhostext.com</td>
<td>Critical</td>
<td>Critical Spyware Web Site</td>
<td>Malware URL</td>
<td>7</td>
<td>77</td>
</tr>
</tbody>
</table>
Discover Infected Endpoints ...

- Infected Endpoints
  - Malware by name
  - Virus download source
  - ‘Call Home’ component
  - Can range in severity

- Network Signatures
- Any Port/Protocol
- Actionable Reporting
Discover Botnets ...

- Inspects all traffic in/out the network
- Detects Bot patterns
  - Command & Control
  - IP scanning
  - Spamming
- Correlates Behaviors
  - Single patterns Suspect
  - Active Bots are Blocked
  - Dormant bots Inactive

<table>
<thead>
<tr>
<th>Bot IP/Hostname</th>
<th>Status</th>
<th>Latest Detection</th>
<th>Bot Activities</th>
<th>Hits</th>
<th>C&amp;C (Command &amp; Control)</th>
</tr>
</thead>
<tbody>
<tr>
<td>129.210.140.246</td>
<td>Active</td>
<td>04/01/2010 04:04</td>
<td>2 Types</td>
<td>2.122</td>
<td>5 controllers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>129.210.140.246</td>
<td>Active</td>
<td>03/31/2010 03:58</td>
<td>IP Scanning</td>
<td>7.810</td>
<td></td>
</tr>
<tr>
<td>129.210.129.89</td>
<td>Active</td>
<td>02/31/2010 20:42</td>
<td>2 Types</td>
<td>8.626</td>
<td>29 controllers</td>
</tr>
<tr>
<td>129.210.15.14</td>
<td>Active</td>
<td>03/31/2010 17:03</td>
<td>3 Types</td>
<td>132.660</td>
<td>1 controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>129.210.129.89</td>
<td>Active</td>
<td>01/25/2010 12:29</td>
<td>IP Scanning</td>
<td>213.174.149.74</td>
<td></td>
</tr>
<tr>
<td>129.210.15.14</td>
<td>Active</td>
<td>03/31/2010 17:01</td>
<td>IP Scanning</td>
<td>86.692</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Spam Activities</td>
<td>45.871</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>129.210.210.42</td>
<td>0</td>
<td>09.121.103.122</td>
<td>Roubais, France</td>
<td>Botnet C&amp;C</td>
<td></td>
</tr>
<tr>
<td>129.210.140.246</td>
<td>0</td>
<td>09.121.25.99</td>
<td>Roubais, France</td>
<td>Botnet C&amp;C</td>
<td></td>
</tr>
<tr>
<td>129.210.236.7</td>
<td>1140</td>
<td>77.604.111</td>
<td>Gloucester, U.K.</td>
<td>Botnet C&amp;C</td>
<td></td>
</tr>
<tr>
<td>129.210.216.106</td>
<td>0</td>
<td>09.121.25.99</td>
<td>Roubais, France</td>
<td>Botnet C&amp;C</td>
<td></td>
</tr>
<tr>
<td>129.210.210.96</td>
<td>0</td>
<td>109.174.144.60.8</td>
<td>Novosibirsk, Russia</td>
<td>Botnet C&amp;C</td>
<td></td>
</tr>
<tr>
<td>129.210.175.113</td>
<td>20047</td>
<td>88.36.96.34</td>
<td>Bergamo, Italy</td>
<td>Botnet C&amp;C</td>
<td></td>
</tr>
</tbody>
</table>

SR B26: Malicious Activity Assessment
Sample Customer Report
Assessment Overview

• Configured Symantec Web Gateway
  – Monitors the download of malware
  – Monitors user access to known malicious sites
  – Identifies malware and botnet infected machines on the network and reports potential attacks
  – Monitors <Internet, IM, TCP, and FTP> traffic

• Data Monitored
  – Passive monitoring from Sep 8th 15:00 to Sep 16th 15:00 (8 days/168 hours)
  – Raw Traffic Processed 1,216.79 GB
  – URL’s Inspected 65,580,574
  – Downloads Inspected 363,786
  – Client Machines Monitored 6,361
Executive Summary

- Malware URL and IP Detections
  - 1,230
- Malware Download Detections
  - 2
- Phone Home Detections
  - 708 Active Bots (1), Suspected Bots Under Watch (5)
    ※assuming that the infected machine had been shutdown during week.
- Active Infected Client Detections
  - 1 Critical (1), Major (0), Minor (0)
- Potential Attacks
  - Spyware 0
  - IP Scanning 2
  - Spamming 0
Assessment Result – Infection Sources

Infection Sources 1,230

sis.amazon.com
Trojan.Malscript!html
HTML contains malicious Java scripts
America

liveweb.archive.org
Adware.Istbar or W32.Virut.W
It opens a back door and may download potentially malicious files on to the compromised computer.
America

Ykimg.com
Bloodhound.Exploit.13
(Buffer overflow attack)
Chinese Video Site
China

Turboupdate.com
Trojan Horse
Korea

Uf.tistory.com
SecurityRisk.Downldr
America

220.136.231.29
W32.Downadup.B
Taiwan
Assessment Result – Infections by Malware Name
Active bot x1

Infections by Malware Name

Active bot communicates with C&C server 708 times through port 80
## Assessment Result – Botnet Report #1

**Active Bot x1, Suspected Bot x5**

### Botnet Report

**Active Bots**  
Must investigate ASAP

**Suspected Bots**  
Should monitor continuously  
Should specify the machine usage and scan the machines by the latest virus definition

<table>
<thead>
<tr>
<th>Bot IP/Hostname</th>
<th>Status</th>
<th>Latest Detection</th>
<th>Bot Activities</th>
<th>Hits</th>
<th>C&amp;C (Command &amp; Control)</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Active</td>
<td>09/16/2011 12:26</td>
<td>2 Types</td>
<td>20,272</td>
<td>3 controllers</td>
</tr>
<tr>
<td>-</td>
<td></td>
<td>09/14/2011 16:16</td>
<td>Botnet Control (C&amp;C)</td>
<td>345</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td>09/16/2011 12:26</td>
<td>IP Scanning</td>
<td>19,927</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Suspect</td>
<td>09/16/2011 09:56</td>
<td>1 Type</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Suspect</td>
<td>09/15/2011 18:04</td>
<td>1 Type</td>
<td>93</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Suspect</td>
<td>09/12/2011 16:14</td>
<td>1 Type</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Suspect</td>
<td>09/09/2011 14:05</td>
<td>1 Type</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Suspect</td>
<td>09/08/2011 21:45</td>
<td>1 Type</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td>09/08/2011 21:45</td>
<td>Botnet Control (C&amp;C)</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

© Copyright 2004-2011, Symantec Corporation. All rights reserved.
Assessment Result – Botnet Report #2
Active Bot x1 (xxx.xxxxx.co.jp)

Botnet Report

Destination Host
xxx.xxxxx.co
communicates with C&C x3

IP Scanning
xxx.xxxxx.co
run IP scanning 7 times to broader external IP ranges

Must investigate the infected machine and respond as soon as possible!!
Assessment Result – Botnet Report #3
Active Bot x1 (xxx.xxxxx.co.jp)

Botnet Report

Destination Host
xxx.xxxxx.co
communicates with C&C x3

URL requests from the active bot (xxx.xxxxx.co) are extremely high (almost 2 million times)

Destination IP address
- 67.195.140.36
  Hosting service by Yahoo / America
- 68.178.232.99
  Hosting service / America
- 94.126.40.145
  Hosting service / England

Assuming botnet activities on the hosted server

IP Scanning
xxx.xxxxx.co
run IP scanning 7 times to broader external IP ranges
Assessment Result – Botnet Report #4
Suspected Bot x5

Botnet Report

• **Machine A**
  61.195.154.6 (Japan) --- A legitimate corporation has the IP address. However the server is used for IRC relay server.

• **Machine B** (Mail Server)
  61.121.247.163 (Japan) --- Web design company
  109.70.26.36 (Russia) --- Unused server (registered by Botnet DB)
  194.85.61.78 (Russia) --- Unused server (registered by Botnet DB)

• **Machine C**
  61.121.247.163 (Japan) --- Web design company

• **Machine D**
  134.237.1.242 (Customer’s proxy)

• **Machine E**
  82.98.86.176 (Germany) --- The company provides web redirect service. The site has malware.

Suspected Bots
Should monitor continuously
Should specify the machine usage and scan the machines by the latest virus definition
Assessment Result – Potential Attacks

IP Scanning x2

Two machines are run IP scanning to broader external IP ranges.
Must investigate why the machines are doing so.
Assessment Result – Virus Downloads

xxx.xxx.xxx.xxx downloads virus twice

Virus Downloads

Trojan.GEN.2 Risk Level 1: Very Low

McAfee (Generic Downloader.ha) Founded on Aug 16th, 2010

Assuming that Virus definition on McAfee gateway may not be updated or Virus may be downloaded by the another channel.
Assessment Result – P2P Application

P2P Application on 3 clients

A total of 3 clients and 82 hits in the Peer 2 Peer category.

Top Peer 2 Peer Applications by Clients
- Ares: 1
- BitTorrent: 1
- DirectConnect: 1

Top Peer 2 Peer Clients by Hits
- xxx.xxx.xxx.xxx: 73
- xxx.xxx.xxx.xxx: 8
- xxx.xxx.xxx.xxx: 1

The machine is using BitTorrent and communicate with the server located in Germany.

The machine is using Ares
What is BitTorrent / Ares?

BitTorrent / Ares is P2P file exchange application like Kazaa and WinMx
Summary

• Investigate machines running active botnets (suspected botnet as well)
  Recommend to disconnect those machines from corporate network if that doesn’t affect to business applications and run virus scanning with the latest definition on those machines.
  ✓ Host A
  ✓ Host B
  ✓ Host C

• Investigate machines running P2P applications
  Recommend to check what applications / process are running
  ✓ Host A
  ✓ Host B

• Investigate machines which might be successfully downloaded malwares
  Assuming that Virus definition on McAfee gateway may not be updated or Virus may be downloaded by the another channel.
  ✓ Host A

• Enhance URL filtering application
  ✓ Block malicious sites

• Redesign of corporate network architecture
  Some proxy server are running and it causes difficulties to identify the infections. Client may access to internet via unauthorized network channels.
Symantec Proposal

Symantec Insight

Symantec Insight is reputation-based security technology that puts files in context, using their age, frequency, location and more to expose threats otherwise missed. Built on contributions from over 175 million systems in over 200 countries, Symantec Insight has the power to examine and track the context of files.

With the recent growth of APT and targeted attack, protecting a single layer is not sufficient. We need “multi layer protection” based on that machine is infected.

Symantec Insight™ is reputation-based security technology that puts files in context, using their age, frequency, location and more to expose threats otherwise missed. Built on contributions from over 175 million systems in over 200 countries, Symantec Insight has the power to examine and track the context of files.

With the recent growth of APT and targeted attack, protecting a single layer is not sufficient. We need “multi layer protection” based on that machine is infected.

Symantec Insight™ is reputation-based security technology that puts files in context, using their age, frequency, location and more to expose threats otherwise missed. Built on contributions from over 175 million systems in over 200 countries, Symantec Insight has the power to examine and track the context of files.

With the recent growth of APT and targeted attack, protecting a single layer is not sufficient. We need “multi layer protection” based on that machine is infected.

Consolidate management by Symantec Protection Center

WWW (Public Web Server)

Host IPS by Symantec Critical System Protection

L3 switch

Monitoring by Symantec Web Gateway

Monitoring botnet activities on mirror port

Anti-Spam by Symantec Messaging Gateway

Confidential Information

Data loss prevention by Symantec DLP

Symantec Insight™

Anti Virus by Symantec Endpoint Protection 12

Automated incident response by Symantec Workflow

SR B26: Malicious Activity Assessment

SYMANTEC VISION 2012
Customer Case Studies
Customer Success
Malicious Activity Assessment

Customer

Finance Customer
HQ: CA | Employees: 5,000

Customer Specifics

- Installed Symantec Web Gateway in Blocking mode
- Customer is currently testing SEP, CSP, MSS and Encryption
- MAA highlighted malware that McAfee did not catch at the endpoints

Customer Drivers

- Notified they were a target by Anonymous
- Immediate need to gain insight into malicious activity
- Partner delivered an MAA which uncovered vulnerabilities
- Opened-up discussions around defense and depth from Symantec
What’s Next

• Learn More:
  – Contact your Symantec Sales Representative or Symantec Partner
  – go.symantec.com/istr
  – go.symantec.com/trywebgateway
Thank you!

Piero DePaoli  
piero_depaoli@symantec.com  
+1 415 203 5991

Eric Schwake  
eric_schwake@symantec.com  
+1 541 520 6015