Internet Security Threat Report Volume XII

Dean Turner - Director, Global Intelligence Network
Symantec Security Response
October 11, 2007
Today’s Discussion

- Symantec Global Intelligence Network™
- Today’s Threat Landscape - Overview
- Global Reach
- Targets
- Methods
- Fraud
- Spam
- Critical Priorities and Steps
Symantec™ Global Intelligence Network

3 Symantec SOCs
80 Symantec Monitored Countries
40,000+ Registered Sensors in 180+ Countries
8 Symantec Security Response Centers

> 6,000 Managed Security Devices + 120 Million Systems Worldwide + 30% of World’s email Traffic + Advanced Honeypot Network
Threat Evolution Timeline

1986
- Brain, 1986
- Michaelangelo infects the MBR & overwrites data, 1991
- BugTraq provides forum for admins, security pros & attackers to share vuln & exploit info, 1993
- Melissa, 1999
- Love Letter, 2000
- Code Red, 2001
- Nimda, 2001
- RD Bot, 2002
- Spybot, 2003
- Gaobot, 2004
- Ongoing...

1998
- Trinoo, 1997
- Tribal Flood, 1998
- Double Click first to use tracking cookies, 1996
- Unknown vulns found actively exploited in the wild to install Adware, Spyware, Bots and Crimeware
- WMF 2005
- MS Office Exploits & Trojans

2000
- Attacks begin in earnest using Bots. CNN, Yahoo, eBay and Datek knocked offline for hours, 2000
- Spam Explodes
- Bots & Botnets
- DDoS Attacks
- Bots Explode
- Paid Vulnerability Research

2002
- Likely due to increasing use of botnets to send spam, 2002
- Rootkits On the Rise
- Unknown vulns found actively exploited in the wild to install Adware, Spyware, Bots and Crimeware
- 2005 Sony DRM
- 2005 Elitebar
- 2006 Many threats

2004-present
- Online fraud fueled by criminal economy
- Malware predominately used for stealing information or providing unauthorized access
- Widespread drive-by downloads & install via web browser exploits
- Both legitimate and black markets for buying new vulns
- Online fraud fueled by criminal economy
- Malware predominately used for stealing information or providing unauthorized access
- Widespread drive-by downloads & install via web browser exploits
- Both legitimate and black markets for buying new vulns

2007
- Concept Virus for MS Office, 1995
- Concept Virus for MS Office, 1995
- BugTraq provides forum for admins, security pros & attackers to share vuln & exploit info, 1993
- Melissa, 1999
- Love Letter, 2000
- Code Red, 2001
- Nimda, 2001
It’s a Market Economy…

- Professional crime requires professional tools
- Increasingly commercialized
- PFR, Development spec., QA, RTM
- GTM - Pricing, distribution, support
...and business is booming!

- In the first half of 2007, 212,101 new malicious code threats were reported to Symantec. This is a 185% increase over the second half of 2006.
Attacks in Stages

- Multi-staged attacks use a small and quiet initial compromise to establish a beachhead from which subsequent attacks are launched.
- Later stages of an attack can be changed to suit the attacker's needs.

1. Spam containing link to compromised server
2. User visits legitimate site
3. Redirection
4. Downloader installed through browser vulnerability
5. Download and install additional threats
Change in Tactics and Targets

- Why go to you when you'll come to them?
- Fertile ground
- Difficult to police
Increasing Regional Focus

- Threats are being tailored to specific regions and countries
- Some malicious code types are more prevalent in certain regions than others
Between January 1st and June 30th Germany was the top country for malicious activity (raw numbers) with 19% of the overall proportion. The U.K. ranked second with 11%.

When accounting for Internet populations, Israel was the top country with 19% followed by Poland with 11%. Worldwide, seven of the top ten countries in this metric were located in EMEA.

<table>
<thead>
<tr>
<th>Overall Rank</th>
<th>Previous Rank</th>
<th>Country</th>
<th>Overall Proportion</th>
<th>Previous Overall Proportion</th>
<th>Malicious Code Rank</th>
<th>Spam Zombies Rank</th>
<th>Command-and-Control Server Rank</th>
<th>Phishing Websites</th>
<th>Bot Rank</th>
<th>Attack Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Germany</td>
<td>19%</td>
<td>19%</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>United Kingdom</td>
<td>11%</td>
<td>10%</td>
<td>1</td>
<td>10</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>France</td>
<td>9%</td>
<td>11%</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>Italy</td>
<td>8%</td>
<td>8%</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>7</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>Spain</td>
<td>8%</td>
<td>8%</td>
<td>6</td>
<td>6</td>
<td>13</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Poland</td>
<td>5%</td>
<td>5%</td>
<td>9</td>
<td>2</td>
<td>11</td>
<td>6</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>India</td>
<td>4%</td>
<td>2%</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>14</td>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>Netherlands</td>
<td>4%</td>
<td>4%</td>
<td>7</td>
<td>17</td>
<td>6</td>
<td>3</td>
<td>12</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>Turkey</td>
<td>3%</td>
<td>3%</td>
<td>12</td>
<td>5</td>
<td>5</td>
<td>20</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>Russia</td>
<td>3%</td>
<td>3%</td>
<td>25</td>
<td>9</td>
<td>9</td>
<td>4</td>
<td>11</td>
<td>15</td>
</tr>
</tbody>
</table>
Globally, during the current reporting period Symantec observed an average of 52,771 active bot network computers per day, a 17% decrease from the last half of 2006. 35% of daily active bots were observed in EMEA. Symantec identified 2,084,189 bot infected PC’s in EMEA.

Command and control servers decreased during this period to 4,622 - a 3% decrease. EMEA has 25% of the world’s command and control servers with Germany having the highest percentage within the region at 25%.

<table>
<thead>
<tr>
<th>Regional Rank</th>
<th>Previous Regional Rank</th>
<th>Country</th>
<th>Percentage of Regional Bots</th>
<th>Previous Percentage of Regional Bots</th>
<th>Percentage of Worldwide Bots</th>
<th>Average Lifespan (days)</th>
<th>Command-and-Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>Germany</td>
<td>23%</td>
<td>16%</td>
<td>9%</td>
<td>1</td>
<td>25%</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>Spain</td>
<td>15%</td>
<td>14%</td>
<td>6%</td>
<td>2</td>
<td>2%</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>France</td>
<td>11%</td>
<td>16%</td>
<td>5%</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>Italy</td>
<td>9%</td>
<td>6%</td>
<td>4%</td>
<td>3</td>
<td>6%</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>United Kingdom</td>
<td>9%</td>
<td>11%</td>
<td>4%</td>
<td>3</td>
<td>11%</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>Israel</td>
<td>6%</td>
<td>5%</td>
<td>3%</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>Poland</td>
<td>6%</td>
<td>8%</td>
<td>3%</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>Portugal</td>
<td>2%</td>
<td>2%</td>
<td>1%</td>
<td>4</td>
<td>0%</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>Turkey</td>
<td>2%</td>
<td>3%</td>
<td>1%</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>India</td>
<td>2%</td>
<td>2%</td>
<td>1%</td>
<td>4</td>
<td>3%</td>
</tr>
</tbody>
</table>
Global Data breaches

- The Education sector accounted for the majority of data breaches with 30%, followed by Government (26%) and Healthcare (15%) - almost half of breaches (46%) were due to theft or loss with hacking only accounting for 16%.

- The retail sector was responsible for 85% of exposed identities followed by Government. Where identities were exposed, 73% were due to hacking.
Global underground economies

- Trading in credit cards, identities, online payment services, bank accounts, bots, fraud tools, etc. are ranked according to goods most frequently offered for sale on underground economy servers.

- Credit cards were the most frequently advertised item (22%) followed by bank accounts (21%).

- Email passwords sell for almost as much as a bank account.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Item</th>
<th>Percentage</th>
<th>Range of Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Credit Cards</td>
<td>22%</td>
<td>$0.50–$5</td>
</tr>
<tr>
<td>2</td>
<td>Bank Accounts</td>
<td>21%</td>
<td>$30–$400</td>
</tr>
<tr>
<td>3</td>
<td>Email Passwords</td>
<td>8%</td>
<td>$1–$350</td>
</tr>
<tr>
<td>4</td>
<td>Mailers</td>
<td>8%</td>
<td>$8–$10</td>
</tr>
<tr>
<td>5</td>
<td>Email Addresses</td>
<td>6%</td>
<td>$2/MB–$4/MB</td>
</tr>
<tr>
<td>6</td>
<td>Proxies</td>
<td>6%</td>
<td>$0.50–$3</td>
</tr>
<tr>
<td>7</td>
<td>Full Identity</td>
<td>6%</td>
<td>$10–$150</td>
</tr>
<tr>
<td>8</td>
<td>Scams</td>
<td>6%</td>
<td>$10/week</td>
</tr>
<tr>
<td>9</td>
<td>Social Security Numbers</td>
<td>3%</td>
<td>$5–$7</td>
</tr>
<tr>
<td>10</td>
<td>Compromised Unix Shells</td>
<td>2%</td>
<td>$2–$10</td>
</tr>
</tbody>
</table>
Target technologies - Web browsers

- Microsoft had the highest number of documented vulnerabilities with 39 followed by Mozilla with 34. Both these vendors also had the highest window of exposure at 5 days each.

- There were 25 vulnerabilities documented in Safari this period, a significant increase from the 4 documented in the last half of 2006. However, Safari had the shortest window of exposure at only 3 days.
Vulnerabilities in Web browser plug-ins are frequently exploited to install malicious software.

In the first half of 2007, 237 vulnerabilities affecting browser plug-ins were documented compared to 108 in all of 2006.

89% of browser plug-in vulnerabilities affected ActiveX components for Internet Explorer, an increase over the 58% in the previous period.
Symantec documented 2,461 vulnerabilities in the current reporting period, 3% fewer than the previous reporting period.

Severity classification: High severity 9%, Medium severity 51% and Low severity 40%.

Web applications constituted 61% of all documented vulnerabilities.

72% of vulnerabilities documented this period were easily exploitable compared to 79% in the previous period.

The W.O.E. for enterprise vendors was 55 days, an increase over the 47 day average in the second half of 2006.
Methods - Malicious code

- Globally, trojans continue to rise and may constitute a greater threat because they tend to exploit web browser and zero-day vulnerabilities. Trojans causing potential/attempted infections increased from 68% to 73% this period.
- The United Kingdom, Italy and Germany are the top countries for trojans and backdoors.
Methods - Data theft and data leakage

- During the current reporting period, threats to confidential information made up 65% of the volume of top 50 malicious code causing potential infections, up from 53% in the previous reporting period.

- While the volume of threats that allow remote access remained stable from the same reporting period last year, the volume of threats that log keystrokes and export user and system data have all increased - Keystroke loggers represent 86% of the report threats to confidential information.
Methods - EMEA Propagation

- Email attachment propagation is the number one propagation mechanism in EMEA at 49%.
- In countries where P2P music sharing is legal, there is a tendency for threats to favour P2P as a propagation mechanism.

<table>
<thead>
<tr>
<th>Regional Rank</th>
<th>Propagation Mechanism</th>
<th>Regional Percentage of Threats</th>
<th>Worldwide Percentage of Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>File Transfer/Email Attachment</td>
<td>49%</td>
<td>46%</td>
</tr>
<tr>
<td>2</td>
<td>File Sharing/Peer-to-Peer</td>
<td>25%</td>
<td>22%</td>
</tr>
<tr>
<td>3</td>
<td>Remotely Exploitable Vulnerability</td>
<td>21%</td>
<td>18%</td>
</tr>
<tr>
<td>4</td>
<td>File Sharing/Peer-to-Peer/Kazaa</td>
<td>21%</td>
<td>18%</td>
</tr>
<tr>
<td>5</td>
<td>File Sharing/Executables</td>
<td>20%</td>
<td>22%</td>
</tr>
<tr>
<td>6</td>
<td>File Transfer/CIFS</td>
<td>18%</td>
<td>24%</td>
</tr>
<tr>
<td>7</td>
<td>File Sharing/Peer-to-Peer/Morpheus</td>
<td>17%</td>
<td>15%</td>
</tr>
<tr>
<td>8</td>
<td>File Sharing/Peer-to-Peer/eDonkey</td>
<td>17%</td>
<td>15%</td>
</tr>
<tr>
<td>9</td>
<td>Back door/Kuang2</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>10</td>
<td>Back door/SubSeven</td>
<td>3%</td>
<td>3%</td>
</tr>
</tbody>
</table>
The Rapid Evolution of Fraud

- The old tactics won’t go away
  - Non-stop stream of new targets coming online who may not be aware of basic scam techniques
- New brand techniques
  - Leverage new, trusted brands a user will not suspect
  - Keep an eye on the 2008 elections and fraud tactics that may leverage them
- More sophisticated tricks
  - “Universal Phishing Kit” makes attacks more convincing and easy than ever
  - “Man-in-the-middle” attack where phisher shows the real phished site but through an SSL proxy
  - No need for phisher to create spoofed website, only requires PHP script & proxy as well as enticement messages

Advertising Age

Phishers Switch Brand Bait to Coke and McDonald's

Bogus Web Sweepstakes Use Identities of Nonfinancial Companies

By Kate Macarthur

Published: December 11, 2006

NEW YORK (AdAge.com) -- A November e-mail signed by a Hong Kong-based Coca-Cola sales and marketing manager incited cash for entries submitted to a link in the e-mail. Another one in March from McDonald’s Corp. and JPMorgan Chase offered a 50% discount at McDonald’s over 10 days, followed by a promotional site.

These offers didn’t signify aggressive interactive-marketing efforts. They were “phishing” -- the Mercedes-Benz ML 350 convertible.

Hijacking brands

Until recently, such bogus offers -- in which familiar brands are hijacked to dupe consumers e-mails or web offers -- were limited to banking, online-retail and other transaction-based spreading to nonfinancial consumer brands as phishers latch on to well-known and trusted brands.

And that, coming at a time when marketers are relying more and more on interactive marketing to build trust but also raises serious questions for marketers about liability and what action if any.

Telltale signs of phishing

A Coca-Cola spokeswoman said: "The Coke logo is so widely known that people are trying to use e-mail scams with scans the marketer has posted on its website. On the site, Coke explains that its name and trademark are used without prior trademark. "Overall, if it looks too good to be true, it probably is," the page says.
Fraud - Phishing

- The Symantec Probe network detected a total of 196,860 unique phishing messages, an 18 percent increase from the previous period. This translates into an average of 1,088 unique phishing messages per day.

- Financial services accounted for 79% of the unique brands that were-phished while making up 72% of the total phishing websites. The ISP sector accounted for 11% of unique brands phished and 3% of the total number of phishing websites.

- During the first six months of 2007, Symantec classified 78 of the 359 brands being phished as core brands. Core brands are those that are spoofed at least once each month by a phishing attack.

<table>
<thead>
<tr>
<th>Regional Rank</th>
<th>Previous Rank</th>
<th>Country</th>
<th>Regional Percentage</th>
<th>Previous Regional Percentage</th>
<th>Worldwide Percentage</th>
<th>Previous Worldwide Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Germany</td>
<td>22%</td>
<td>32%</td>
<td>6%</td>
<td>11%</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>United Kingdom</td>
<td>9%</td>
<td>9%</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>Netherlands</td>
<td>9%</td>
<td>5%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>Russia</td>
<td>8%</td>
<td>5%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>France</td>
<td>8%</td>
<td>8%</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>Poland</td>
<td>4%</td>
<td>3%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>Italy</td>
<td>4%</td>
<td>4%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>Spain</td>
<td>4%</td>
<td>3%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>9</td>
<td>13</td>
<td>Czech Republic</td>
<td>3%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>Denmark</td>
<td>3%</td>
<td>4%</td>
<td>1%</td>
<td>1%</td>
</tr>
</tbody>
</table>
Three phishing toolkits were responsible for 42 percent of all phishing Web sites observed by Symantec in the first half of 2007.

86% of all phishing Web sites were hosted on only 30% of IP addresses known to be phishing Web servers. Phishing toolkits are often indicated by the ability to host a large number of phishing sites on the same compromised computer.
Globally, between July 1 and December 31, 2006, spam made up 61 percent of all email traffic. 60% of all spam is in English.

Poland, Spain, Hungary and Russia - >80% of all email originating from these countries is spam.

Image spam made up 27% of all spam blocked by Symantec in the first half of 2007.
## Critical priorities and steps

<table>
<thead>
<tr>
<th>Priority</th>
<th>Recommendation</th>
</tr>
</thead>
</table>
| 1        | Data Inventory & Classification  
*Figure out where the important data lives. Start there.* |
| 2        | Encryption  
*Pick what works best for your business, critical data first.* |
| 3        | Awareness & Training  
*For travelers/remote workers, critical data handlers & everyone else.* |
| 4        | Process, Process, Process  
*Helpdesk authentication, termination process, contractor lifecycle, etc.* |
| 5        | Segmentation & Separation of Duties  
*Networks & employees-- don’t let the fox (or the hens!) watch the henhouse* |
| 6        | Know Thy Perimeter  
*Wireless audits & overall vulnerability management prevent “easy” hacks* |
| 7        | Develop Secure Applications  
*Cheapest and best means of protecting applications is to develop them securely* |
| 8        | New Technical Solutions  
*Do the basics but also consider solutions such as data leakage & lojack* |
Thank you!

Questions

Dean_turner@symantec.com