The Emerging Threat Landscape

Zulfikar Ramzan, Ph.D.
Technical Director and Architect
Security Technology and Response
Tuesday, June 03, 2008

Some Key Trends

- Underground economy and supply chain lowers bar for who can participate in cybercrime
- Lack of trust among underground economy participants may force additional organization
- Malicious software levels consistently rising
  - More malicious software in ’08 than all previous years combined
  - By all accounts, ’09 will be same
  - Good vs. bad software inflection point
- Web will continue as an attack vector because of its popularity and content richness
- Targeted attacks will likely be an issue and will necessitate defense-in-depth protection
- Attackers starting at the supply chain (infected digital picture frames)

Fraud Economy Menu & Ads

<table>
<thead>
<tr>
<th>Rank</th>
<th>Previous</th>
<th>Goods and Services</th>
<th>Current %</th>
<th>Previous %</th>
<th>Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>Bank Accounts</td>
<td>22%</td>
<td>21%</td>
<td>$10-$1000</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Credit Cards</td>
<td>13%</td>
<td>22%</td>
<td>$0.40-$20</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>Full Identity</td>
<td>9%</td>
<td>6%</td>
<td>$1-$15</td>
</tr>
<tr>
<td>4</td>
<td>N/R</td>
<td>Online Auction Site Accounts</td>
<td>7%</td>
<td>N/A</td>
<td>$1-$8</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>Scams</td>
<td>7%</td>
<td>6%</td>
<td>$2.50/wk - $50/wk (hosting); $25 (design)</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>Mailers</td>
<td>6%</td>
<td>8%</td>
<td>$1-$10</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>Email Addresses</td>
<td>5%</td>
<td>6%</td>
<td>$0.83/MB-$10/MB</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>Email Passwords</td>
<td>5%</td>
<td>8%</td>
<td>$4-$30</td>
</tr>
<tr>
<td>9</td>
<td>N/R</td>
<td>Drop (request or offer)</td>
<td>5%</td>
<td>N/A</td>
<td>10-50% of drop amount</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>Proxies</td>
<td>5%</td>
<td>6%</td>
<td>$1.50-$30</td>
</tr>
</tbody>
</table>
The Fraud Food Chain

Malware: Growing Dangerously & Dangerously Growing
For the 2nd half of ’07,

- 68% of the top 50 malicious code posed threat to confidential info
  - 3% ↑ from H1 ’07;
  - 15% ↑ from H2 ’06;
- Keystroke loggers represent 76% of the reported threats to confidential information.

The decline in all five categories could be attributable to a specific piece of malware being more targeted and having fewer capabilities (e.g., versus having all five capabilities); malware authors may be employing such techniques to make detection more difficult.

Trojan.Silentbanker

Standard banking transaction
All banking transactions are routed through the remote system.

Man in the Middle

Attacker-controlled remote system

Transactions are routed through the proxy

Locally installed malicious proxy

Attacker-controlled remote system

All banking transactions are routed through the remote system.
**Trojan.Silentbanker**

**Local Information Stealing**

- Account information is logged on the computer and then sent to the attacker.
- The attacker then uses this information to log into the account at a later date.

**Advanced Information Stealing**

- User requests login page.
- The local proxy intercepts the request with fields needed to log in.
- The attacker can then use this information to log into the user’s bank account at a later date.
- The bank sends a login page with fields needed to log in.
- The local proxy appends additional fields to it.
- When the user submits the information, it is also sent to the attacker.
- The attacker then uses this information to log into the account at a later date.
The account details are changed, redirecting the transaction to another account. The bank sends back confirmation for the transaction. The proxy modifies the account details and sends on the confirmation.

Information Stealing Authentication
Advanced Two-Factor
Trojan.Silentbanker

The user attempts a transaction, which is intercepted by the attacker. The confirmation is modified, appearing as though the transaction is going to the initial account. The bank sends a password by cell phone to complete the transaction. The attacker enters the password and then submits the final request.

Man-in-the-Middle Trojans in Action
Staged Downloaders: When it rains, it pours

For the 1st half of '07:
- 35% of computers reporting potential malicious code infections reported more than once
- Many of these likely the result of staged downloaders

Only 10% of malware samples Symantec sees actually exploit a technical vulnerability; the rest either piggyback or rely on social engineering…

Using IRS Fears to Install Malware: Backdoor.Robofo

- 0.16% of spam blocked by Symantec contained malicious code (↓ from 0.43%)
- 32% of malicious code that propagated did so over email (↑ from 30%)
Using Fear to “Copy Protect” Malware

2. The Client:
1. Does not have the right to distribute the product in any business or commercial purposes not connected with this sale.
2. May not disassemble / study the binary code of the bot builder.
3. Has no right to use the control panel as a means to control other bot nets or use it for any other purpose.
4. Does not have the right to deliberately send any portion of the product to anti-virus companies and other such institutions.
5. Commits to give the seller a fee for any update to the product that is not connected with errors in the work, as well as for adding additional functionality.

In cases of violations of the agreement and being detected, the client loses any technical support. Moreover, the binary code of your bot will be immediately sent to antivirus companies.

Web Attacks: The New Epicenter
Web browsers: many holes

- In H2 2007, 88 vulnerabilities (19 medium, 69 low) affected Mozilla browsers (↑ from 34)
- Safari (1 high, 12 medium, 9 low); IE (13 medium, 5 low); Opera (8 medium, 4 low)
- 239 Browser plug-in vulns (190 affected ActiveX, 19 QuickTime, 13 Sun Java, 11 Adobe Flash, 4 Windows Media Player, 1 Adobe Acrobat, 1 Mozilla browser extension)

MPack: Malware Commoditized

- MPack: web attack toolkit that appeared late ’06;
- Toolkit is hosted on a web server and infects pages on that server
- Page visitors get infected
- Customized: Toolkit determines exploit method on the fly based on user’s configuration (operating system, browser, etc)
- Easy to use: management console provides stats on infection rates
- Customer care: toolkit can be purchased with one-year support contract!
Web Attacker: Automated Tools Make it Easy

- Rogue distribution networks make money by using browser exploits to install downloader Trojan horse programs
- The downloaders are then used to install adware & spyware
- Reportedly pay for 0-day vulnerabilities such as WMF
- WMF vulnerability said to be purchased for ~$4K USD
- Discovered in active exploit via iframecash.biz & others
"Most days, I just sit at home and chat online while I make money," 0x80 says. "I get one check like every 15 days in the mail for a few hundred bucks, and a buncha others I get from banks in Canada every 30 days." He says his work earns him an average of $6,800 per month, although he’s made as much as $10,000. Not bad money for a high school dropout.


---

**Drive-by Pharming Overview**

- Attack concept developed by Sid Stamm, Markus Jakobsson, and me that strongly leverages prior work on JavaScript host scanning presented by Grossman at BlackHat.
- Local broadband routers (both wired and wireless) offer a web management interface for device configuration
  - Consequently, these devices contain a web server that runs a web app
- The web app is often susceptible to cross-site request forgeries (made easier since there is usually a default password that users often fail to change)
- Broadband routers govern DNS settings...
- Can change these settings from a remote location; victim only has to view web page containing malicious JavaScript to become infected
Drive-by Phishing Flow

Drive-by Pharming Flow

- Web Browser
- Broadband/Wireless Router
- Web Browser
- Good DNS Server
- Rogue DNS Server
- Click Me!!!
- 66.6.66.6
- 129.79.78.8
- www.bank.com
- 129.79.78.8
- www.bank.com
- 66.6.66.6
- <script src="http://192.168.1.1/...?..."></script>

Drive-by Pharming In the Wild

- Used an HTML IMG Tag (No JavaScript!)
- Took advantage of virtual hostnames (no need to guess router’s IP)
- Exploited router used by large Mexican ISP to pharm Mexican bank
- Added DNS entries directly (no separate DNS server needed)
- Router was particularly susceptible to Drive-by Pharming since admin password not required to change router settings.

Attacks always get better; they never get worse
Old US National Security Agency Saying
Symantec Global Intelligence Network
What Information does the GIN Contain?

The Global Intelligence Network contains several key types of information about Internet-based threats:
- Attack Intelligence
- Malicious Code and Security Risk Intelligence
- Fraud Intelligence
- Vulnerability Intelligence
- Exposure Intelligence

The various types of intelligence both come from and power many of Symantec’s products

GIN Production Information Sources

Where does the intelligence come from?
The Global Intelligence Network is comprised of information collected from a number of sources, both internal and external. The internal sources are a combination of customer-facing and Symantec-internal products and services:
- Norton AntiVirus (NAV)
- Norton Internet Security (NIS)
- Norton 360 (N360)
- Norton Confidence Online (NCO)
- Symantec Endpoint Protection
- DeepSight
- Symantec Honeypots (AQS)
- Brightmail Anti-Spam
- Phish Report Network (PRN)
- Internal Research Projects
- Managed Threat Analysis (MTA)
- Managed Security Services.
The Road Ahead

Future Watch

- Web will grow as an attack vector
- Online games – interesting to watch out for
- Election-related attacks!
- Leveraging social networking sites and other staged attacks
- Continued commoditization and "business process" innovation
- Targeted Attacks
- Pre-shipped Malware

Good news: Closely monitoring the threat landscape and studying its evolution allows us to counteract these threats

Thanks!

Zulfikar Ramzan
Zulfikar_Ramzan@symantec.com

More info: Search for 'Symantec Internet Security Threat Report' or 'Symantec Security Response Blog' or 'Crimeware Book'

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.