Crimeware on the Net

The “Behind the scenes” of the new web economy

Iftach Ian Amit
Director, Security Research – Finjan

BlackHat Europe, Amsterdam 2008
Who Am I? (iamit)

• Iftach Ian Amit  
  – In Hebrew it makes more sense…
• Director Security Research @ Finjan
• Various security consulting/integration gigs in the past  
  – R&D  
  – IT
• A helping hand when needed… (IAF)
Today’s Agenda

• Terminology
• Past vs. Present – 10,000 feet view
• Business Impact
• Key Characteristics – what does it look like?
  – Anti-Forensics techniques
  – Propagation methods
• What is the motive (what are they looking for)?
• Tying it all up – what does it look like when successful (video).
• Anything in it for us to learn from?
  – Looking forward on extrusion testing methodologies
Some Terminology

- **Crimeware** – what we refer to most malware these days is actually crimeware – malware with specific goals for making $$$ for the attackers.

- **Attackers** – not to be confused with malicious code writers, security researchers, hackers, crackers, etc... These guys are the Gordon Gecko’s of the web security field. The buy low, and capitalize on the investment.

- **Smart (often mislead) guys** write the crimeware and get paid to do so.
How Do Cybercriminals Steal Business Data?

Criminals’ activity in the cyberspace

Federal Prosecutor: “Cybercrime Is Funding Organized Crime”
Criminals target sensitive business data using crimeware

- Brand damage
- Financial theft
- Data theft
- Password theft
- Identity theft
- Compromised computers to steal resources
- Employee productivity loss

Federal Prosecutor: “Cybercrime Is Funding Organized Crime”
How much is business data worth to criminals?

- Financial Report: $5,000
- Product Design: $1,000
- Trojan Log: $300
- CreditCard + PIN: $500
- Driving License: $150
- SocialSecurity #: $100
- Valid CreditCard: $20
Key Characteristics of Crimeware

Financially motivated criminals are utilizing new methods to infect PCs with crimeware that steals sensitive data.

**Propagation Methods**
Hosted on compromised legitimate and Web 2.0 sites over the globe with frequent location changes.

**Anti-Forensic Methods**
Evade signature-based detection by utilizing code obfuscation and controlled exploits visibility in the wild.

URL and Reputation-based filtering solutions will not block these sites.

Anti-Virus signatures will not match today’s malicious code.
Anti Forensics

• Code Obfuscation
  – Not the one you are used to…

• Single serve exploits
  – One per customer please

• Geographical preference
  – More on this later when we talk $$$…
Dynamic Code Obfuscation

Javascript Encoder

This script will encode javascript to make it more difficult for people to read and/or steal. Just follow the directions below.

1. Enter your javascript (no HTML) in the box below.
2. Select the Code Key you want.
3. Press the Encode button.

```javascript
//exploits combination
if ($browser[name] == "MSIE") {
    if ($browser[os] != "Windows NT 5.0") {
        AddIP("Oday"); include 'crypt.php'; include 'megapack1.php';
    }
    if ($browser[os] == "Windows NT 5.0") {
        AddIP("jar"); include 'ms06-044_w2k.php'; include 'megapack1.php';
    }
}
```

3. Click the "Encode" button.
4. Select all the text that appears in the box below and paste it into your HTML page where you would want the script to be. The pasted code should appear all on one line in your editor, unless you have word-wrap on. Do not add any linebreaks (by pressing Enter) or the script may not work.

Select All...

<SCRIPT LANGUAGE="JavaScript">document.write(unescape("%3C%73%70%77%71%73%73%77%70%74%20%6C%61%66%67%75%61%67%65%20%61%66%67%75%61%73%73%72%69%70%74%22%3E%66%75%68%43%
```
Dyn. Code Obf. – the neosploit way (2.0.15)
Obfuscation and IFRAMES

- Have become in 2007 the main driving tools for distributing malware and malicious code in general.
  - They are even signatured by AV – while as we see the obfuscation or IFRAME itself may NOT be malicious…

<table>
<thead>
<tr>
<th>Position</th>
<th>Last month</th>
<th>Malware</th>
<th>Percentage of reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Mal/Iframe</td>
<td>50.8%</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Mal/ObfJS</td>
<td>19.2%</td>
</tr>
<tr>
<td>3</td>
<td>New</td>
<td>Trojan/DRClick</td>
<td>14.6%</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>Trojan/Unif</td>
<td>3.0%</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>Trojan/Decdec</td>
<td>2.4%</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>Trojan/Fujif</td>
<td>1.6%</td>
</tr>
<tr>
<td>7</td>
<td>Re-entry</td>
<td>Trojan/Pintadd</td>
<td>0.9%</td>
</tr>
<tr>
<td>8</td>
<td>Re-entry</td>
<td>Trojan/Zlobar</td>
<td>0.8%</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>Mal/RunDF</td>
<td>0.6%</td>
</tr>
<tr>
<td>10</td>
<td>Re-entry</td>
<td>VBS/Haptimer</td>
<td>0.5%</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
<td>5.6%</td>
</tr>
</tbody>
</table>

Source: top 10 web threats in 2007
Crimeware Profile

Crimeware binaries and their URL locations are changing every hour.
Location, Location, Location

- Have you been to our fine establishment before?
  - You can only get the “good” stuff once…

- Where do you come from?
  - You may not be worth the exposure…

```php
index.php
// checks and saves user's IP hashed with browser
// to avoid future browser's hangup
function CheckAddUser() {
  ...
  $rcount = mysql_num_rows($res);
  if ($rcount > 0) {
    // found data, prevent view
    echo ":[
    exit;
  } else {
    // not found, add
    $query = "INSERT INTO ".$dbstats."_users VALUES
    ('".$ipua."')";
    mysql_query($query);
  }
}

settings.php:
$BlockDuplicates=1; // send exploits only once
$CountReferers=1; // make referrer's statistics
$OnlyDefinedCountries=0; // send exploits only to countries in the list
$CountryList="RU US UA"; // 2-letter codes ONLY! (see readme for details)

Source: Mpack 0.94 source code
Crimeware Toolkits
A glimpse into the code

- Modern toolkits are provided in their binary form, with licensing mechanisms, built in obfuscation, configuration files, user management (for supporting multiple attackers under the same kit), and DB functionality.
- The snippets here are taken from a disassembly of Neosploit version 2.0.15 (first time analysis – in.cgi)
Neosploit code

```assembly
loc_8049BE8:
    sub    esp, 8
    push   [ebp+var_84]
    push   [ebp+var_2C]
    push   offset a?o6PURU
    lea    ebx, [ebp+var_338]
    push   ebx
    call   _sprintf
    add    esp, 0Ch
    push   [ebp+var_84]
    push   [ebp+var_2C]
    push   offset aStartwvf
    lea    ebx, [ebp+var_338]
    push   ebx
    push   offset aData
    push   offset exp_quicktime_opera

sub    esp, 0Ch
push   [ebp+timer]
    call   get_ip_hash
add    esp, 10h
    cmp    eax, [ebp+var_468]
    jnz    loc_8049ABE

loc_8049ABE:
    sub    esp, 18h
    push   [ebp+var_4AC]
    push   offset exp_wvf
    call   js_crypter_put
    mov    [esp+4E8h+var_4E8], offset aStartquicktime
    push   offset exp_superbuddy_is_decoded
    push   0D90FC7h
    push   0CAh
    push   offset exp_superbuddy
    call   decode_data
    add    esp, 18h
    push   0
    push   offset exp_superbuddy
    call   js_crypter_put
    mov    [esp+4E8h+var_4E8], offset aStartsuperbudd
    call   add_function
    push   offset exp_audiofile_is_decoded
    push   0A1E716h
    push   145h
    push   offset exp_audiofile
    call   decode_data
    add    esp, 18h
    push   0
    push   offset exp_audiofile
    call   js_crypter_put
    mov    [esp+4E8h+var_4E8], offset aStartaudiofile
    call   add_function
    push   offset exp_gom_is_decoded
    push   1F040Ah
    push   0D9h
    push   offset exp_gom
    call   decode_data
    add    esp, 18h
    push   0
    push   offset exp_gom
    call   js_crypter_put
    mov    [esp+4E8h+var_4E8], offset aStartgom
    call   add_function
    push   offset exp_wvf_is_decoded
    push   84C0B8h
    push   10Dh
    push   offset exp_wvf
    call   decode_data
    add    esp, 18h
    push   0
    push   offset exp_wvf
    call   js_crypter_put
    mov    [esp+4E8h+var_4E8], offset aStartwvf
```

...
Propagation techniques

• How did THAT code turned out on THAT site
  – Anyone remember bankofindia.com?

• Helpful HTML tags (infamous iframes…)

• And of course, bling… $$$
On My Site? No way!
Way... It's all business

- You can get paid to put a snippet of HTML on your site that will spur “installations” (= infections). Guaranteed high “install” rate, updated code (remember the toolkit), bypass of security measures...

- “The number of legitimate Web sites compromised by attackers has surpassed those purposefully created by attackers” – Jan 22\textsuperscript{nd}, Websense security labs.
Evasive attacks – increasing the infection rates

User Access to an infected website

Infected site identifies browser version and records user IP, country, etc...

IP lookup to identify if the user already visited the site

Delivery of Malicious code according to browser version, OS, and country if this is the first visit
What’s the end game?

- Holy grail of web attacks: successful installation of crimeware Trojan (aka – rootkit+keylogger+otherstuff)
Local Crimeware Effect

• Crimeware analysis showing a sampler of how financial crime is being performed.

• Don’t let your eyes off the ball… (the SSL icon?)
Play-by-play…

Client identification

Privacy Policy

We respect your privacy. Schwab will use the information you provide to verify your identity, and may later use the information you submit to notify you about products and services that you may find useful. Please read our privacy policy about online security. Our policy is always available for your review on the home page of our web site.
And in reality (movie)...

[Crimeware video showing XXX-bank being targeted.]
The last nail in the coffin of “trusted websites”

- To conclude – the recent example of website exploitation to distribute crimeware:
  - Using all the techniques detailed in this talk
  - Single point of contact (no data is being pulled from external domains – all self hosted on the compromised webserver)
  - Still financially motivated
  - And to top it all – baffling the security community with how the attack took place to begin with to infect the hosting servers.

- Now let’s talk about a website’s “reputation”…
Where are we going to?

- Time for predictions:
  - We are starting to see criminals exploit (pun intended) the full potential of “web2.0”
  - Think trojans that conduct all of their communications over ‘legitimate’ channels over loosely coupled web2.0 services
  - Google’s mashup editor, and yahoo’s pipes are great examples of what can be done in terms of back-channel management of data…
So how do I use this?

- **Extrusion Testing**
  - The ugly half-brother of pen-testing
  - Gaining a lot of momentum
  - Uses tried-and-tested methods (social engineering, passive external fingerprinting, work the CEO’s secretary rather than the security administrator…)

- **Arsenal includes:**
  - Toolkits (told you these things are useful)
  - Updated exploits to recent vulnerabilities
  - Custom infection (you don’t want to end up being blocked by an AV when you do have a chance to get in) – not for the faint of heart.
  - Chutzpa (someone come up with an English phrase for it!)
Future directions of web security

- Assuming of course the previous video worked...
- For the full Monty look for our talk on insecurity of widgets and gadgets.
- Another direction – think Web2.0 enabled Trojans...

[Widgets & Gadgets video showing a possible attack vector]
Feel free to drop me a line at iamit@finjan.com