Web Security.

Not the one you are used to…

Iftach Amit – Director of Security Research, Finjan
• So let me tell you about this cool new Cross Site Scripting
  – (In the industry we call it XSS!!!)

• Right…
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”
The Business Impact of Crimeware

How much is business data worth to criminals?

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Report</td>
<td>$5,000</td>
</tr>
<tr>
<td>Product Design</td>
<td>$1,000</td>
</tr>
<tr>
<td>Trojan Log</td>
<td>$300</td>
</tr>
<tr>
<td>CreditCard + PIN</td>
<td>$500</td>
</tr>
<tr>
<td>Driving License</td>
<td>$150</td>
</tr>
<tr>
<td>SocialSecurity #</td>
<td>$100</td>
</tr>
<tr>
<td>Valid CreditCard</td>
<td>$20</td>
</tr>
</tbody>
</table>
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.
Let’s get down to business

• How they do it
  – Is there anything in it for us?
    • (hell yeah!)

• First things first:
  – Obfuscated code
    • (again – not the one you are used to…)
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. Add your javascript code to the textarea box above.
2. Select the "Code Key" you wish to use.
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.

```javascript
//exploits combination
if (!$_SERVER["HTTP_ACCEPT"] == "text/html") {
    if ($_SERVER["HTTP_USER_AGENT"] == "Windows NT 5.0") {
        AddIP("Oday");
        include 'crypt.php';
    }
    include 'megapack1.php';
}
```
Crimeware Toolkits

[Images of various interfaces and data tables related to crimeware toolkits]
Crimeware binaries and their URL locations are changing every hour
On My Site? No way!
Way… It’s all business

• You will get paid to put a snippet of HTML code on your site that will spur “installations” – infections. Guaranteed high “install” rate, updated code (remember the toolkit), bypass of security measures…
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.
We like cool movies...
So how do I use this?

• Extrusion Testing
  – The ugly 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!)
More video

• Assuming of course the previous one worked…
Q&A

• You know the drill…