Current state of online banking Trojans

Candid Wueest
Symantec Global Security Response
Agenda

- Background
- New features
- Webinject MITB
- Automated fraud
- Mobile banking
- C&C infrastructure
- Conclusion
Video of a typical infection

Usually you don’t see anything!
Different Motive – Different Attack

Hacktivism

Money

Espionage

“Cyber War”
Ransomware – lock your computer

Enter any 11-digit prime number to continue.
Old methods like phishing still work too

Asking for creditcard for a tax refund
Banks - that’s where the money is
So what is it all about?

Not a new Problem!

– 2003: Infostealer.Bancos very active
– Virus Bulletin article in 2005

But how bad is it today?

– Zeus (Citadel, Ice IX, Murofet, Licat, Gameover)
  > 1 Million Zeus infection/year
– SpyEye, Carberp, Tatanarg, Shylock, Cridex, Bebloh
Distribution

- Some are local – some are global
- Shylock in UK, Carberp in Russia, Tinba in Turkey and Bebloh Germany
- Some target 300 URLs – in total 7 common families targeted 683 URLs
Easy Toolkits
# Tatanga/Tatanarg GUI

<table>
<thead>
<tr>
<th>TOP 10 Country Alive</th>
<th>Short Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spain</strong> 337 81.2%</td>
<td><strong>Total bots</strong> 1311 (9 new)</td>
</tr>
<tr>
<td><strong>United States</strong> 11 2.65%</td>
<td><strong>Alive bots</strong> 415 31.66%</td>
</tr>
<tr>
<td><strong>Germany</strong> 9 2.17%</td>
<td><strong>Dead bots</strong> 896 (102) 68.34%</td>
</tr>
<tr>
<td><strong>United Kingdom</strong> 7 1.69%</td>
<td><strong>Online bots</strong> 103 7.86%</td>
</tr>
<tr>
<td><strong>Mexico</strong> 6 1.45%</td>
<td><strong>Recovered bots</strong> 18 (0) 2.01%</td>
</tr>
<tr>
<td><strong>Brazil</strong> 6 1.45%</td>
<td><strong>Down. exe for recover today</strong> 0 0%</td>
</tr>
<tr>
<td><strong>Czech Republic</strong> 5 1.2%</td>
<td><strong>Malware infected</strong> 1075 (5) 82%</td>
</tr>
<tr>
<td><strong>Russian Federation</strong> 5 1.2%</td>
<td><strong>ZeuS infected</strong> 1 (0) 0.08%</td>
</tr>
<tr>
<td><strong>Israel</strong> 5 1.2%</td>
<td><strong>AV Protected</strong> 713 (5) 54.39%</td>
</tr>
<tr>
<td><strong>France</strong> 4 0.96%</td>
<td><strong>Honey pots</strong> 21 1.6%</td>
</tr>
</tbody>
</table>
Infection vector

The usual suspects:

- Webattack toolkits
  - Filtering victims by IP
  - May check for mouse activity
  - Rented as a service
  - Seeded in social networks

- Email with attachments

- Email with malicious link
  - Especially after data breaches

Artificial intelligence is no match for natural stupidity.
DriveBy Download infections

- browse

Legitimate Web site

- Malicious Script
  - hacked website
  - Misconfigured server
  - Weak password
  - Banner Ads
  -...

Browser is analysed
- 308 Plug-in vulnerabilities (2011)
- 351 Browser vulnerabilities (2011)

No user interaction required
Common financial Bot features

- Keylogger
- Form grabbing HTTP/S
- Steal cookies, certs and stored passwords
- Screenshots
- Socks Proxy
- Search for local files
- TCP Sniffer
- Send back screen resolution/user agent for cloning
- Inject into system processes
Adapted features

General Bot functionality evolved a bit:

• Can run as Guest account (e.g. Zeus)
• Local re-encryption, binding to machine
• Change encryption of config to thwart automated analysis
  – For example replace RC4 with AES
• Only steal once from a bot
• Red herings by virtual machine detection
• VNC with invisible remote desktop
Automated anonymous AV checks

Example: Scan4you

- **We in base have 35 antiviruses:** Kaspersky, Solo, McAfee, BitDefender, Panda, F-Prot, Avast!, VirusBlokAda, ClamAV, Vexira, Norton, DrWeb, AVG, ESET NOD32, G DATA, Quick Heal, A-Squared, IKARUS, Microsoft Security Essentials Antiviruses, Norman, AntiVir (Avira), Sophos, Rising, ArcaVir, COMODO, F-Secure, VirusBuster, eTrust, Trend Micro, AhnLab V3 Internet Security, BullGuard, VIPRE, Zoner AntiVirus, K7 Ultimate.

- **Domain check on presence in black list:** ZeuS domain blocklist, ZeuS IP blocklist, ZeuS Tracker, MalwareDomainList (MDL), Google Safe Browsing (FireFox), PhishTank (Opera, WOT, Yahoo! Mail), hpHosts, SPAMHAUS SBL, SPAMHAUS PBL, SPAMHAUS XBL, MalwareUrl, SmartScreen (IE7/IE8 malware & phishing Web site), Norton Safe Web, Panda Antivirus 2010, (Firefox Phishing and Malware Protection), SpamCop.net and RFC-Ignorant.Org.
Different Ideas: Neloweg Firefox Extension

- Creates new WSCIInstallNameSpace to load its DLL with Winsock2
- With Firefox present it will drop a FF extension (.xpi)
- Bot interaction is done within the browser by the FF extension
- Enables „webinjects“ and steals stored passwords

```javascript
var actions=new actions();
window.addEventListener("load",function(){myExtension.init()},false)
window.addEventListener("unload",function(){myExtension.uninit()},false)
window.addEventListener("load",function(){myExtension.init()},false);
var wrk=Cc["@mozilla.org/windows-registry-key;1"].createInstance(Ci.
var nsIE=Cc["@mozilla.org/process/environment;1"].getService(Ci.nsIE
var nsIL=Cc["@mozilla.org/file/local;1"].createInstance(Ci.nsILocalF
var CMD_TICKIT="!tickit!";
var CMD_EXEC_FILE="!cmd!";
var CMD_BLOCK_URL="!block!";
var CMD_SCREEN_URL="!screen!";
```
Webinjects – MITB Attacks

- Add or remove HTML elements - simple and powerful!
- Syntax shared between multiple Trojans, e.g. Zeus & SpyEye
- Hooking: nspr4.dll, wininet.dll, WS2_32.dll
- Trojans may change IE settings to allow mixed content without warning
- Some use Web services to be independent from Bot

```
[data_before] ....... [data_end]

[data_inject] malicious [data_end]

[data_after] ....... [data_end]
```
Webinject MITB

Log-on process is ignored*!
1) Transactions are swapped or generated
2) Data from the bank is sanitized
3) Money mule data is inserted from the C&C
* It could steal credentials for offline fraud

Stress is when you wake up screaming and you realize you haven't fallen asleep yet.
Webinjects

- Custom Webinjects are sold for $10-100

SpyEye 1.3.48 Private

[...]
Full installation including all injects mentioned above: 100 LR or WS

**Custom Inject** coding for your own needs: **50LR** (Per Inject)

We sell already made webinjects for Zeus/Spyeye. We can develope

**webinjects to your needs** if you provide logins for testing it. Injects can be made on for any country and any language if you provide details for it.

Injests are sold encrypted and you can`t modify them.

[...]
Price for one inject is now **60 WMZ/LR**

Updated/modify of injects 20 lr each.
Webinjects: Obfuscation Tricks

- Display a maintenance or „please wait“ window
- Cleanup the balance and transaction history (balance replacer)
- Add a fake chat window or fake contact info
- Block access to security websites
The simple ones steal CCs
Automated MITB Transactions

The smart ones make automated transactions on the client

• Steal a percentage of the highest balance or a fixed amount
  – Usually less then 5K to stay under money laundry detection

• Money mule accounts are loaded on-the-fly from C&C server

• Some simulate user behavior (browsing, menu clicking) in order to fool anomaly detection

This can bypass, virtual keyboards, anti-keylogger, OTP iTAN, mTAN (when no transaction verification is done)
Social Engineering Tricks

Let the user beat the system:

• Perform a „test“ transaction (Tatanarg)
• Revert a „false“ transaction (Zeus)
• Change corresponding mobile number and let user confirm it

Dear user,
there has been a transaction error
Please revert the following transaction
in order to unblock your account.
Mobile Authentication

• Mobile Transaction Authentication Number (mTAN)
  – Popular method for online banking, often only used for authentication
• Zeus & SpyEye mobile modules
• Main Trojan will ask for mobile number and model
• Forward all SMS to C&C server

Annuls transaction signing, as user does not see it!
Mobile Banking

• Some banks have started to deploy mobile banking solutions
  – Complete transactions from your mobile
  – OutOfBand authentication is no longer OOB if mobile is used!
  – Devices are often unprotected

Example:

• Pose as standalone OTP generator and ask for credentials
Command & Control Infrastructure

A simple PHP webfront is still the most common C&C server
Usually HTTP/S traffic with encrypted content (XOR, RC4, AES, ...)

But we have seen:

• Zeus operator that used stolen cloud service as C&C server
• Zeus operator that used a hidden TOR service as C&C server
• Zeus variant that uses P2P network

-> much harder to shutdown!
Protect your assets

From the „advertisement“

Citadel - Module MiniAV ($ 100)

- Allows you to **clean your PC** from someone else's bot Malware,
- the module is activated every 4 hours and **remove all of the Zeus**-modification systems, such as Zeus1, 2, Ice9, etc.
- Vitality of your build go up a few times, it is recommended to those who have met in my logs wrong gates and uses traffic exchanges. In the near future will add a signature to remove feykav and substitution issue.
Conclusion

Banking Trojans didn’t change much, because they still work!

• ManInTheBrowser with webinjects is very powerful
• More stealth & obfuscation features
  – Encryption, C&C protection, P2P, ...
• More automation
  – Dynamic money mule loading, transaction swapping, ...
• More social engineering
  – Because there is no patch for it ;-)

The banks added a lot of fraud protection on the backend
Which questions are still open?

CANDID_WUEEST@SYMANTEC.COM