Pinkslipbot: A deep look at how malicious code adapts and evolves

Guilherme Venere
Malware Researcher
Anti Malware Operation Team
Know Your Enemy

- Server-side polymorphic worm. EXE and DLL modules
- First seen around 2007
- Features common backdoor functionalities
- Spread method
  - Compromised webpages with injected code
  - Network shares (exploits included!)
  - AutoRun (mostly old variants)
  - Spam E-mail attachments (old variants)
- No known source code available
- Very effective in local corporate networks due to spread methods
  - This received attention from the media last year
    http://www.bankinfosecurity.com/breach-may-have-targeted-jobless-a-3655
- Actively developed over the years
• Outbreaks follow defined pattern
• Interim time used for development
• Major code change around 2009 improved effectiveness
• But that had its consequences: too much attention!
• Low profile lately.
  • Major code change in sight?

**Total Reported Infections (2011)**

- United States: 39%
- United Kingdom: 15%
- India: 11%
- Spain: 11%
- Australia: 7%
- Netherlands: 6%
- Germany: 6%
- Brazil: 5%
- Japan: 4%
- Chile: 3%
- Other countries: 2%
This Google Maps view shows reported infections by Pinksbot in 2011.
Pinkslipbot network model

hostrmeter.com:31666
up002.cn
adserv.co.in
up004.cn
up01.co.in
up02.co.in
upa01.in
nt14.in
incitylocal.com
www.cdcddcdcc2121cdsfdfd.com

ppcimg.in
du01.in
du02.in
yimg.com.ua
citypromo.info
bgstat.in
redserver.com.ua:31666
spotrate.info
karnadya.com.my
flwest.com
falahuddarain.com
silfersystem.com
gemini.com.co

yimg.com.ua
corpgift.in
soros.in.ua
googstat.info
abirvalg.co.in
69.175.80.89:21
195.3.145.32:8080

w1.webinspector.biz
a.rtbn2.cn
c.rtbn2.cn
www.cdcddcdcc2121cdsfdfd.com
ijk.cc
w1.madway.net
w1.rstk.us

109.95.114.252
nt202.cn
up002.cn
adserv.co.in
up004.cn
www.cdcddcdcc2121cdsfdfd.com
lrc.zief.pl:65520

June 14, 2012
• Packer/Obfuscation varies wildly
• Some samples with strings in Russian
• Samples were small (~14KB-45KB)
• Configuration uses Rolling-XOR encryption called SXOR by virus authors
• Spread methods included spam with zipped DOC attachments
  • Default password ‘Hello999World777’
• Infection count low
• Group behind it is not well organized yet
• Many samples using custom packer
• Client side polymorphism
• Wild variety of code seen in samples
• Apparently the group behind Pinkslipbot attempt major rework of code
  • Seems they were not successful
Pinkslipbot – Q2 2010

• File obfuscation start to look like those used by Zeus
• Starts to use server-side polymorphism
• Almost no changes since 2009
  • Reverted to old code
• Users of the following banks were targeted:

```plaintext
aCashmanWebCash db '/cashman/;web-cashplus.com;treas-mgt.frostbank.com;business-eb.ib'
                         ; DATA XREF: .data:004065D8\t0
 db 'anking-services.com;treasury.pncbank.com;access.jpmorgan.com;ktt.'
 db 'key.com;onlineserv/CM;premierview.membersunited.org;directline4bi'
 db 'z.com;onb.webcashmgmt.com;tmconnectweb;moneymanagergps.com;ibc.kl'
 db 'ikbca.com;directpay.wellsfargo.com;express.53.com;itreasury.regio'
 db 'ns.com;itreasurypr.regions.com;cpw-achweb.bankofamerica.com;busin'
 db 'essaccess.citibank.citiigroup.com;businessonline.huntington.com',0
 align 10h
```
• **Major code change.** Base for today’s version
  - EXE keep DLL alive in processes
• Adds features to steal digital certificates
• Download BackDoor-EXI, fully featured backdoor
• Pinkslipbot begins to disable AV by changing NTFS ACL permissions
• Change in network infrastructure to bulletproofed servers in Ukraine
• Stolen data sent to FTP server
• Able to infect HTML files (.asp, .pl, .php, .htm, .cfm) with `<script>` code
• Users of the following banks were targeted:
• Starts to use UPX + second-level obfuscator
• Social Engineering: AutoRun variant uses folder icons
• DLL component and configuration now comes embedded in EXE resource section
• Users of the following banks were targeted:

<table>
<thead>
<tr>
<th>Year</th>
<th>Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
</tr>
</tbody>
</table>
First variants featuring user-mode rootkits
Used to protect the main EXE and to hijack IE functions

- ntdll.dll!NtQuerySystemInformation
- ntdll.dll!NtResumeThread
- kernel32.dll!GetProcAddress
- WININET.dll!InternetCloseHandle
- WININET.dll!HttpOpenRequestA
- WININET.dll!InternetReadFile
- WININET.dll!InternetQueryDataAvailable
- WININET.dll!HttpSendRequestA
- WININET.dll!HttpSendRequestW
- WININET.dll!InternetReadFileExA
- iphlpapi.dll!GetTcpTable
- iphlpapi.dll!AllocateAndGetTcpExTableFromStack
- WS2_32.dll!connect
- WS2_32.dll!send
- WS2_32.dll!WSASend
- WS2_32.dll!WSAConnect
- ADVAPI32.dll!RegEnumValueW
- ADVAPI32.dll!RegEnumValueA
- USER32.dll!TranslateMessage
- USER32.dll!GetClipboardData
- USER32.dll!CharToOemBuffA
• Intense development cycle
• Not very effective in customer networks
• Hints that they might be targeting specific AV features
• First stolen digital certificates being used in binaries
• Change in SXOR encryption for configuration file
  • New heavy encryption layer added
Pinkslipbot – Q3/Q4 2011

Digital Signature Details

Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: [redacted]
Issued by: Autoridad Certificadora del IDSE
Valid from: 4/18/2010 to 4/19/2012

2009 2010 2011 2012

June 14, 2012
• Obfuscator looks more and more like that used by Zeus variants
• Virus activity under control
• Activity from update server:

Unique samples from yimg.com.ua
Future (Current) Developments

- New variant showing up week prior to this conference
  - New obfuscation, same as many Zbot variants
  - Doubled number of affected banks
  - Change in behavior:
    - DLL module is directly injected in memory (no file on disk!)

- Future developments
  - Improved rootkit
  - More anti-AV features
  - Change in spread method

- Interaction with other malware families
  - Partner with another backdoor or integrate in its own code
  - Code integration with Zeus
Acknowledgments

• McAfee Labs Threat Advisory
• McAfee Labs Sample Database Team
• Personal Communication (McAfee Labs): Abhishek Karnik, Mark Olea, Srinivasa Kanamatha, François Paget
• For contributions during preparation of this report:
  • Jacomo Dimmit (Team Cymru)
  • Ivo Peixinho (Brazilian Federal Police)

Guilherme_Venere@mcafee.com
@gvenere