The missing link between cybercrime gangs

Yurii Khvyl (ikh@csis.dk)
Senior Malware Analyst at CSIS eCrime and Research & Intelligence Unit
Agenda - overview

Episode 1: The quest begins
- Overview and abstract: Neverquest?
- Code and protocol analysis
- Prevalence and geographic spread

Episode 2: Dead in the waters
- 3 million credentials in the water from PONY to Neverquest
- What’s PONY about? (demo)
- Web injects (search and replace)

Episode 3: Glimpse at infrastructure
- Server infrastructure
- Panel and money mule accounts, potential loss of millions

Episode 4: The Missing Link …
Abstract

- Neverquest is also known as Vawtrak/Snifula
- Yet another Crime as a Service
- Ursniff was the foundation which later evolved into Gozi
- Gozi reemerged as “Gozi Prinimalka” (Hang Up)
- Neverquest was born based on that evolution in Trojan banking development
- It was first discovered in mid 2013
- In December 2014 we found Neverquest to implement Tor2web to hide C&C
Overview: Neverquest

- Banker-trojan
- Browser hooking
- Site Redirects
- Webinjects
- MITB
- Kills AV
- Harvests browser data
Neverquest – the missing link

Abstract

• Uses PrDGA (Pseudo-random DGA) for fallback domains except for Tor2Web
• A common distribution method are spam mails claiming to be e.g. UPS, eFax, United Airlines etc, attached a .doc file with embedded macros that upon enabling, fires the payload. Alternatively being delivered through AnglerEK as part of a cocktail (Bedep)
• First stage downloads PONY, while second stage is Neverquest with various modules and injects depending on the project ID.
• Neverquest currently supports the most comprehensive list of specific targets spanning globally and across several campaigns

12/06/2016
Abstract

- Upon execution, Neverquest drops a random %uww into %ProgramData%.
- Neverquest then executes the dropped DLL using regsvr32.exe /s [PATH] by adding a run key to registry.
- Next it enrolls the host into the BOTnet using a projectID with an encoded cookie value.
- Neverquest probably has the largest and most comprehensive target list of all Trojan bankers.

12/06/2016
Abstract

- Some weeks back (mid February 2016) it added several new targets related to banks in Israel: bankleumi.co.il, bankhapoalim.co.il, telebank.co.il.
- Several Neverquest campaigns have recently pushed the Point of Sale (PoS) malware “Abaddon” (small binary approx. 5-6KB)
- Latest new project/campaignID is Project 238
- Yet again we see new targets, including investment retirement services such as Vanguard and Paychex.
- Infected users should fear for their entire retirement savings being stolen.
Current versions of Neverquest uses several layers to protect itself from detection and to trouble analysis e.g.:

- Anti-Emulator
- Anti-Debugger
- Anti-Analysis
- Anti-Antimalware
- Garbage Collection
- Hashing
- Encryption/Decryption
- Code injection
- Compression/Decompression
Protocol

- The C&C responds with a list of items. After the first HTTP request from the infected client the server will typically respond with a configuration file and may also respond with a list of commands that the client will then execute.

<table>
<thead>
<tr>
<th>Offset</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>x00\x10</td>
<td>OK Download + Execute</td>
</tr>
<tr>
<td>x03</td>
<td>Download Module</td>
</tr>
<tr>
<td>x1C</td>
<td>Update</td>
</tr>
<tr>
<td>X05</td>
<td>Search files</td>
</tr>
</tbody>
</table>

- For some time Neverquest makes use of a linear congruential generator (LCG) method added a pseudo random number generator (PRNG) to produce the key used to encrypt the data.
- On top of that data, it’s now being compressed with LZMAT library.
Neverquest – the missing link
Distribution and prevalence – all campaigns (1 month)

NEVERQUEST INFECTIONS

USA  England  Japan  Canada  Germany  France
Neverquest – the missing link

Distribution and prevalence – all campaigns (1 year)

[Map showing distribution and prevalence globally]
Credentials lost PONY

DATA STOLEN BY PONY THE PAST 6 MONTHS
• Requirements should be authenticated for the user to be logged in the system
• Bug in auth_cookie generation

```php
function authenticate($login, $password)
{
    $this->user_id = $row['user_id'];
    $this->update_auth_cookie($row['user_id'], mixed_sha1(12345*microtime()));
    $this->login = $login;
    return true;
}
```

```
echo microtime();
0.92580500 1445414565
```
Neverquest – the missing link

Largest and latest decrypted configuration
ProjectID #8 approx. 2MB
More than 300 targets alone in that project
The targets campaign #13
All unique Neverquest targets = 1054 – oh my
Neverquest – the missing link

```php
url for test
https://[:10.0.0.1]/c_api/v1/bot/60/3836567439/info?client=test_2&token=9ba34a544e

sample answer:
{"isBotOnline":0,"Browser":"Firefox 31","arch":"x86 32bit","last_time":"2015-03-30 06:03:02","Browser":null,"OpenTabs":0,"LastPage":null,"Stats":null}

https://[:10.0.0.1]/c_api/v1/bot/85/2145880484/info?client=asket&token=4755b8a0ac8e8fdca853c7e27f69d

https://[:10.0.0.1]/c_api/v1/bot/283/4045932770/info?client=asket&token=86c940572132fa1f4d6e099cf9f1

/}
define('SERVER_BASE_URL', 'https://[:10.0.0.1]/');
define('BASIC_AUTH', 'root:');
define('CLIENT_ID', 'asket');
define('SERVER_TOKEN', '2fcdb2d25d22e');
```
<table>
<thead>
<tr>
<th>ID</th>
<th>Login info</th>
<th>Bank</th>
<th>IP</th>
<th>Last activity</th>
<th>Assigned</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1061</td>
<td>502397167</td>
<td>TSB (business)</td>
<td>86.156.47.30</td>
<td>08:12:15 (01.12)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1096</td>
<td>stoyan.kuman</td>
<td>HSBC (business)</td>
<td>77.102.236.220</td>
<td>22:11:54 (30.11)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1103</td>
<td>3450703753</td>
<td>Santander (business)</td>
<td>86.26.196.208</td>
<td>19:11:57 (30.11)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1107</td>
<td>rjazancovs</td>
<td>TSB (business)</td>
<td>80.43.21.14</td>
<td>18:11:31 (30.11)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1085</td>
<td>dancer99</td>
<td>HSBC (business)</td>
<td>87.102.6.206</td>
<td>18:11:19 (30.11)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1106</td>
<td>shanpaull</td>
<td>HSBC (business)</td>
<td>86.156.47.30</td>
<td>18:11:12 (30.11)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1106</td>
<td>8143429637</td>
<td>Santander (business)</td>
<td>2.24.168.121</td>
<td>11:11:12 (30.11)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1105</td>
<td>hox172</td>
<td>HSBC (business)</td>
<td>109.170.200.48</td>
<td>20:11:04 (29.11)</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
</tbody>
</table>

86080|fbhatti3133 (Business) | 83.244.197.194 | 14:07:15 (10.07); 18?? GBP, try send 2kk to China
171577|rachspk (business) | 91.206.177.8 | 11:07:57 (13.07); - | 40kk
86080|fbhatti3133 (Business) | 83.244.197.194 | 14:07:15 (10.07); - | 18??
407851|logoslin (business) | 46.182.58.1 | 13:07:20 (09.07); - | 15kk
16410|voltaire (business) | 77.239.131.78 | 16:07:43 (07.07); - | 2kk
172794|ssahotay (business) | 145.78.21.6 | 14:07:42 (07.07); - | 30kk
305857|simonp (business) | 37.252.30.41 | 17:06:57 (19.06); - | 2kk
25637|glenda49 (west (business) | 217.45.218.37 | 11:06:36 (08.06); - | 5kk balance ;
37183|sheila (business) | 134.36.21.217 | 13:06:40 (05.06); - | 6kk

514 | 176082|dianneh | RBS (business) | 86.188.160.194 | 13:11:36 (24.11) | -        | +      | 500k balance, inter -UK, pod chaps dropov pod kroupoe net,skip pokal
1087 | fire wolf1 | HSBC (business) | 81.154.53.172 | 11:11:47 (24.11) | -        | +      |         |
1098 | 0909510588 | Santander (business) | 82.27.47.55 | 15:11:40 (22.11) | -        | +      |         |
262  | 615111787   | TSB (business) | 94.197.113.24 | 22:11:29 (21.11) | -        | +      | 17к на борту, не дал данные для добавить дроп
795  | jkleebb     | coutts.com | 86.140.203.22 | 18:11:23 (21.11) | -        | +      | -25k Balance
1084 | 942990333   | lloydsbank.co.uk (business) | 78.33.152.124 | 13:11:27 (18.11) | -        | +      |         |
1097 | 3191896990  | Santander (business) | 50.203.97.190 | 08:11:37 (18.11) | -        | +      |         |
1095 | kirtontc     | HSBC (business) | 86.157.73.72 | 15:11:41 (17.11) | -        | +      |         |
The Missing Link (Gootkit, Tinba and Neverquest)

- At least two campaigns related to Neverquest shares infrastructure with Shifu, Tinba and Gootkit
- In those two campaigns we have a 100% identical list of corporate banking targets with primary focus on the UK but also on Qatar, Hong Kong, and United Arab Emirates

<table>
<thead>
<tr>
<th></th>
<th>Tinba</th>
<th>Gootkit</th>
<th>Neverquest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>4d1ad74191725927d76b44b0388b6de6</td>
<td>4d86ae4ac5f5bec6939e6270bfc9216e8</td>
<td>67EED9D7AAB4C7E32343CE8CD1EF0F54</td>
</tr>
<tr>
<td>Corporate targets</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>All targets</td>
<td>52,20%</td>
<td>41,90%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Neverquest – the missing link