Malicious campaign targets South Korean users with backdoor-laced torrents

welivesecurity.com/2019/07/08/south-korean-users-backdoor-torrents/

July 8, 2019

ESET researchers have discovered a malicious campaign distributing a backdoor via torrents, with Korean TV content used as a lure

Zuzana Hromcová
8 Jul 2019 - 11:30AM

ESET researchers have discovered a malicious campaign distributing a backdoor via torrents, with Korean TV content used as a lure

Fans of Korean TV should be on the lookout for an ongoing campaign spreading malware via torrent sites, using South Korean movies and TV shows as a guise. The malware allows the attacker to connect the compromised computer to a botnet and control it remotely.

The malware is a modified version of a publicly available backdoor named GoBot2. The modifications to the source code are mainly South Korea-specific evasion techniques, which are described in detail in this blogpost. Due to the campaign's clear focus on South Korea, we have dubbed this Win64/GoBot2 variant GoBotKR.

According to ESET telemetry, GoBotKR has been active since March 2018. The detections are in the hundreds, with South Korea being the most affected (80%), followed by China (10%) and Taiwan (5%).

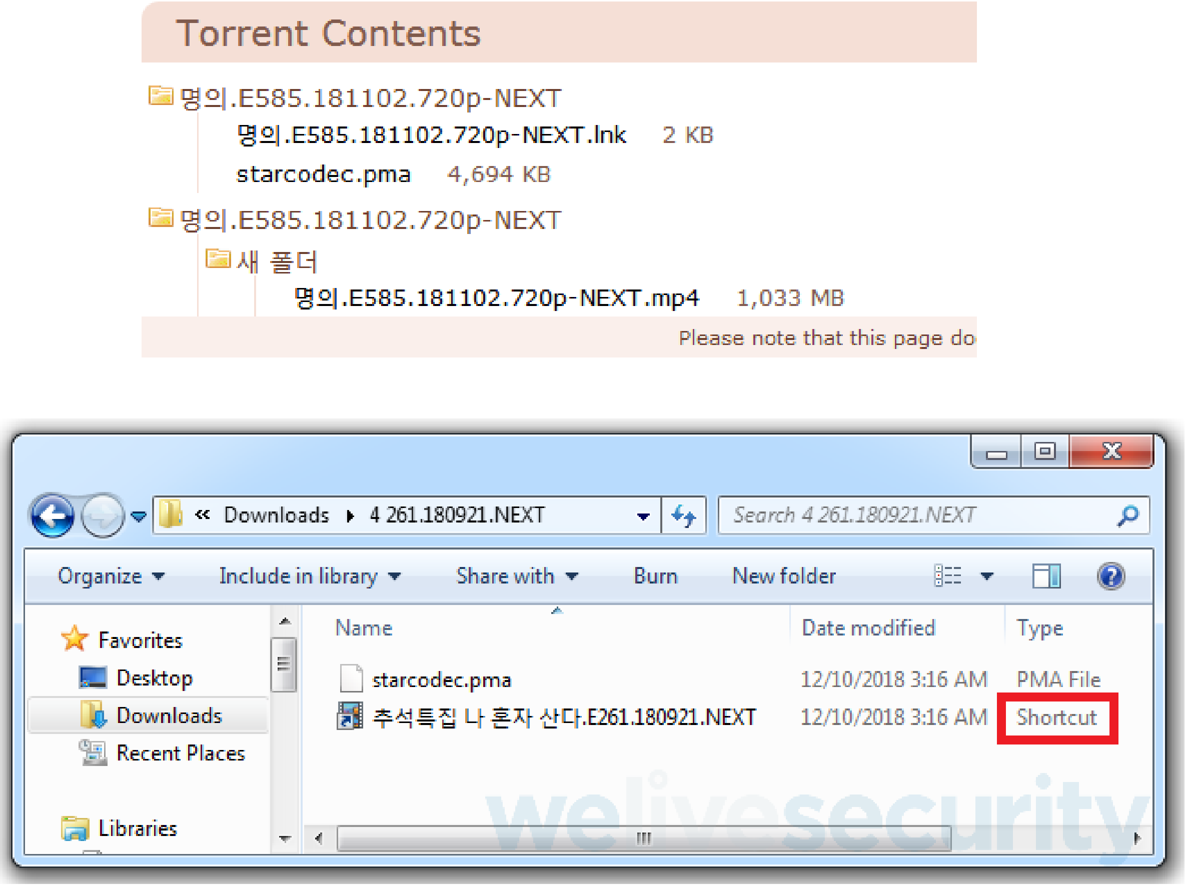
Distribution

GoBotKR has been spreading via South Korean and Chinese torrent sites, masquerading as Korean movies and TV shows, as well as some games.

The attackers behind this campaign try to trick users into executing the malware by booby-trapping the contents of the torrents with malicious files that have deceptive filenames, extensions and icons. Our analysis shows that the torrents using a movie/TV show disguise generally contain the following types of files:

1. The expected MP4 file
2. A malicious executable masked as a PMA archive file with a filename mimicking various codec installers
3. A malicious LNK file with a filename and icon mimicking the expected video file

Figure 1 shows examples of torrent contents from this malicious campaign.



Torrent Contents

명의.E585.181102.720p-NEXT
- 명의.E585.181102.720p-NEXT.lnk 2 KB
- starcodec.pma 4,694 KB

명의.E585.181102.720p-NEXT
- 새 폴더
  - 명의.E585.181102.720p-NEXT.mp4 1,033 MB

Please note that this page do

Name	Date modified	Type
starcodec.pma	12/10/2018 3:16 AM	PMA File
추석특집 나 혼자 산다.E261.180921.NEXT	12/10/2018 3:16 AM	Shortcut

Figure 1. Contents of some torrents delivering the malware (the MP4 video is not displayed on the second screenshot); the malware is executed by an LNK file with a deceptive filename and icon

So how exactly do users get compromised?

Directly opening the intended MP4 file will not result in any malicious action. The catch here is that the MP4 file is often hidden in a different directory, and users might encounter the malicious LNK file mimicking it first. Further increasing the chance of users falling for the lure is the fact that the extension of the LNK file is normally not displayed when viewed in Windows Explorer, as seen in the second screenshot in Figure 1, in the file with the Korean name.

Clicking on the deceptive LNK file executes the malware. However, it also opens the intended file (in this case a video), giving victims little reason to suspect something has gone wrong.

Renaming the malicious EXE file to a PMA file is also likely done to prevent raising suspicion of potential victims. We have also seen this technique using games as a lure, and with filenames and extensions relevant to gaming.

During our investigation, we have seen the following filenames being used for the malicious executables: starcodec.pma, WedCodec.pma and Codec.pma (movie/TV show disguise) and leak.dll (game disguise). The name “starcodec” mimics the legitimate Korean codec pack Starcodec.

Capabilities

GoBotKR was built on the basis of a backdoor named GoBot2, the source code of which has been publicly available since March 2017. Both the original and the modified version are written in GoLang, also known as Go. While still relatively rare for malware, new variants of GoLang malware are emerging, likely due to the challenges posed to analysts with the bulky nature of its compiled executables.

The functionality of GoBotKR largely overlaps with the published GoBot2 source code, with only minimal modifications. Overall, the malware is not particularly complex technically, and the implementation is rather straightforward. Most features are implemented with the use of GoLang libraries, and by executing Windows commands (such as cmd, ipconfig, netsh, shutdown, start, systeminfo, taskkill, ver, whoami, and wmic), and third-party utilities such as BitTorrent and uTorrent clients.

Collected information

Ultimately, the actors behind GoBotKR are building a network of bots that can then be used to perform DDoS attacks of various kinds (e.g. SYN Flood, UDP Flood, or Slowloris). Therefore, after being executed, GoBotKR first collects system information about the compromised computer, including network configuration, OS version information, CPU and GPU versions. In particular, it collects a list of installed antivirus software.

This information is sent to a C&C server, which helps the attackers determine which bots should be used in the respective attacks. All C&C servers that we extracted from the analyzed malware samples are hosted in South Korea and registered by the same person.

Bot commands

Once communication with the C&C server is established, the server instructs the compromised computer with backdoor commands. GoBotKR supports fairly standard botnet functions, which mostly serve three main purposes:

- allowing misuse of the compromised computer
- allowing the botnet operators to control, or further extend, the botnet
- evading detection or hiding from the user

These are the supported commands:

- carry out a DDoS attack on a specified victim
- access a URL
- execute a file, a command, a script
- update, terminate or uninstall itself
- shutdown/reboot/log off the computer

- change homepage in IE
- change desktop background
- seed torrents
- copy itself to connected removable media, and setup AutoRun function
- copy itself to public folders of cloud storage services (Dropbox, OneDrive, Google Drive)
- run a reverse proxy server
- run an HTTP server
- change firewall settings, edit hosts file, open a port
- enable/disable Task Manager
- enable/disable Windows registry editors
- enable/disable Command Prompt
- kill a process
- hide a process window

Of particular interest are two commands – seeding torrents and DDoS capability.

The “seed torrents” command allows the attackers to misuse the victimized machines for seeding arbitrary files using the BitTorrent and uTorrent programs, even if these are not already installed on the system. This may be used as a mechanism to distribute the malware further.

The “carry out a DDoS attack” command lets attackers abuse the victim’s network bandwidth to block the availability of targeted services, such as websites. According to our analysis, this is most likely the main purpose of the GoBotKR botnet.

Evasion techniques

In this section, we explore the evasion techniques used by the GoBotKR backdoor. While many techniques were already present in the publicly available source code, the authors of GoBotKR further expanded them with South Korea-specific features. This shows us that the attackers customized the malware for a specific audience, while taking extra effort to remain undetected in their campaign.

Techniques taken from GoBot2

The following detection evasion and anti-analysis techniques used by GoBotKR have been adopted from GoBot2 source code:

- The malware installs two instances of itself on the system. The second instance (watchdog) monitors whether the first instance is still active and reinstalls it if it has been removed from the system.

- The malware employs antivirus bypass techniques (it allocates large chunks of memory and delays execution of the malicious payload to prevent antivirus engines from emulating the code due to resource constraints).
- The malware can detect selected security and analytical tools, such as debuggers. If detected, it terminates itself.
- The malware terminates itself if IP information of the victim suggests one of several blacklisted organizations (e.g. Amazon, BitDefender, Cisco, ESET). It uses external legitimate websites for querying IP information and searches for hardcoded strings in this information (e.g. “cloud”, “Cisco”, “Microsoft”), rather than using API functions.
- The malware terminates itself if its file name consists of 32 hexadecimal characters, which prevents the payload from being executed in some automated sandboxes.

South Korea-specific modifications in GoBotKR

The authors of GoBotKR added three new evasion techniques, related to their focus on South Korea:

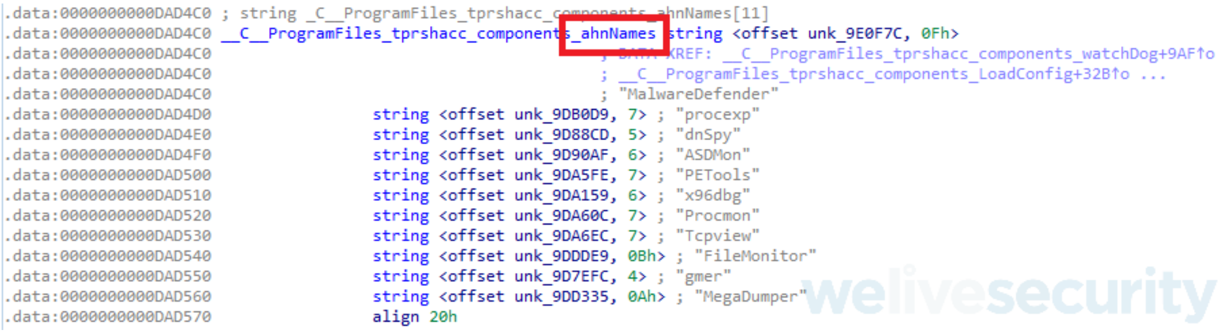
- As explained in the previous section, the malware uses IP information of the compromised computer to detect whether it is running in one of the blacklisted organizations. In GoBot2, the IP address of the victim is determined by accessing Amazon Web Services or dnsDynamic and parsing the reply.
  In the samples of GoBotKR we analyzed, these URLs are replaced with South Korean online platforms Naver and Daum.
- GoBotKR features a new evasion technique that scans running processes on the compromised system to detect selected antivirus products (listed in Table 1). If any of the products are detected, the malware terminates itself and removes some traces of its activity from the host. The list of detected processes includes products by AhnLab, a South Korean security company.

Process name substring	Associated company/product
V3Lite	AhnLab, V3 Internet Security
V3Clinic	AhnLab, V3 Internet Security
RwVnSvc	AhnLab Anti-Ransomware Tool
Ksde	Kaspersky
kavsvc	Kaspersky
avp	Kaspersky
Avast	Avast
McUICnt	McAfee

Process name substring	Associated company/product
360	360 Total Security
kxe	Kingsoft Antivirus
kwsprotect	Kingsoft Internet Security
BitDefender	BitDefender
Avira	Avira
ByteFence	ByteFence

Table 1. List of security products detected by GoBotKR

> The malware tries to detect analytical tools running on the system. It terminates itself if any of them are detected. The list is internally named “ahnNames”, which might be another reference to AhnLab.



```
.data:0000000000DAD4C0 ; string _C__ProgramFiles_tprshacc_components_ahnNames[11]
.data:0000000000DAD4C0 __C__ProgramFiles_tprshacc_components_ahnNames string <offset unk_9E0F7C, 0Fh>
.data:0000000000DAD4C0                                         ; DATA XREF: __C__ProgramFiles_tprshacc_components_watchDog+9AF↑o
.data:0000000000DAD4C0                                         ; __C__ProgramFiles_tprshacc_components_LoadConfig+32B↑o ...
.data:0000000000DAD4C0                                         ; "MalwareDefender"
.data:0000000000DAD4D0                 string <offset unk_9DB0D9, 7> ; "procexp"
.data:0000000000DAD4E0                 string <offset unk_9D88CD, 5> ; "dnSpy"
.data:0000000000DAD4F0                 string <offset unk_9D90AF, 6> ; "ASDMon"
.data:0000000000DAD500                 string <offset unk_9DA5FE, 7> ; "PETools"
.data:0000000000DAD510                 string <offset unk_9DA159, 6> ; "x96dbg"
.data:0000000000DAD520                 string <offset unk_9DA60C, 7> ; "Procmon"
.data:0000000000DAD530                 string <offset unk_9DA6EC, 7> ; "Tcpview"
.data:0000000000DAD540                 string <offset unk_9DDDE9, 0Bh> ; "FileMonitor"
.data:0000000000DAD550                 string <offset unk_9D7EFC, 4> ; "gmer"
.data:0000000000DAD560                 string <offset unk_9DD335, 0Ah> ; "MegaDumper"
.data:0000000000DAD570                 align 20h
```

Figure 2. The malware’s blacklist of running processes is internally named “ahnNames”

In addition to the AhnLab references, the defensive techniques described in the second and third points were added into the source code as a file named AhnLab.go, according to the metadata we obtained from the malware.

Timeline

Because the malware is spreading via torrents, a lot of the samples are broken or incomplete. We were, however, able to recover C&C servers and internal version information.

Since the malware was first seen, we have detected samples with internal versions 2.0, 2.3, 2.4, and 2.5. Each of these versions comes with some minor technical improvements or differences in implementation. The versioning differs from that used in the GoBot2 source code, where an internal name “ArchDuke” is used.

Table 2 lists the different versions of GoBotKR detected by ESET systems from May 2018 to the time of writing. The timeline features the malware's internal versioning and detection dates, as PE timestamps have been cleared from the samples.

First seen	Internal version	Functionality linked to South Korea	C&C server
May 2018	2.0	No	https://jtbcsupport[.]site:7777/
Jul 2018	2.0	Yes	https://jtbcsupport[.]site:7777/
Aug 2018	2.0	Yes	https://higamebit[.]com:6446/
Sep 2018	2.3	Yes	https://kingdomain[.]site:6556/
Sep 2018	2.3	Yes	https://bitgamego[.]com:6446/
Sep 2018	2.3	Yes	https://higamebit[.]com:6446/
Sep 2018	2.3	Yes	https://helloking[.]site:6446/
Jan 2019	2.4	Yes	https://kingdomain[.]site:6556/
Jan 2019	2.5	Yes	https://kingdomain[.]site:6556/

Table 2. GoBotKR version timeline

As seen in the table, the first malware samples detected in May 2018 were not yet customized for South Korean targets and were thus almost identical to the GoBot2 source code. However, we were able to link them to newer samples because they used the same C&C server.

How to stay safe

If you suspect you might have fallen victim to this malware campaign, we recommend you scan your computer with a reliable security solution. ESET products detect and block this malware under the detection name Win64/GoBot2. You can use ESET's Free Online Scanner to check your computer for the presence of this threat and remove anything that is detected. Existing ESET customers are protected automatically.

Pirated content distributed via torrent sites is a well-known vector for spreading all kinds of malware. To steer clear of similar attacks in the future, stick to official sources when downloading content. Before launching downloaded files, pay attention to whether their extensions match the intended filetypes. To keep your computer protected, we advise you to patch regularly and use reputable security software.

Indicators of Compromise (IoCs)

ESET detection name

Win64/GoBot2

C&C servers

jtbcsupport[.]site
kingdomain[.]site
higamebit[.]com
bitgamego[.]com
helloking[.]site

SHA-1

Note that some malware samples may be corrupted due to the nature of its distribution mechanism (torrents).

Version 2.0

038C69021F4091F0B1BE3F059FCDC1C4FA8885D2
092A4F085A01E0D61418114726B9F9EF9F4683C3
11953296BBC2B26303DED2F92FB8677BD8320326
11BF60CC2B8AC0321635834820460824D76965DE
275EE3BD90996EF54DB5931CBDF35B059D379E0E
424215E74EA64FC3A55FE9C94B74AFC4EA593699
4899912880FF7B881145B72A415C7662625E062E
6560BD68CD0CA0402AB28D8ABE52909EB2BA1E10
6A58E32DFF59BAEE432E5D351EAD7C7CB939CCB7
6BE3A40D89DDCDCFA37926A29CE5BCC5FF182D12
77EAE50B8C424338C2987D6DFF52CE0F0BBBD98F
A04EB443942DD3906A883119429BF09A3601B3E0
A61D72BA8AE6A216F1D5013A05CEA8D4F96E81E1
B60DA1F89313751FAA21DD394D6D862CC8C2DBE4
B7CEAE53118890011B695E358633CCD35E8CD577
BDBA27E525D6DC698C1CF90B07F4FB85956E9C28

C31955C4D3C38591BBC8A2089F23B5558146267B
D688A58001E41A8CA22EABCA309DA9FCD2910CB3
DD18D7B0ADE5E65EFDE920C9261E8890B4105B75
E0046D91BED1B3A09243C43760599DC9D8F99953
E00F1BB85A277A8C1ED081642EF76413B2FF7EA9
EA968D757281E6BB5D9334E7F2C9ECDA69EA15A9
F9C40789C780174F6BB377AE46F49B94E402AE77
FFF263FA9E16F7945BCE21D0F6C11C75DAA241D8

Version 2.3

018927A35B2CEC08D5493CB75BAA62D6956D0109
063C462E98453AD6E4091A5AB35613CAF19DF415
082A026BD14F69AF46641ABF20520B3D2D0D6E6A
084A7E6B7DD955554FCED021DF58458C7E66EBB2
097248EB38277DA879F5D606179C746DB6BB2C54
0DBA9DDBBB12FA4FE22CD4EE16EF8DCC73B7D295
0E9D0C1A82DFB53DF9BB8B75D3A90B2236704498
0F4BB3FC6771D306565E1002B3327A9F2AED92AF
14129424593DC8B1865F491A9CA92BE753B2A7F0
16703AE741257EAF2EC76E097D17F379E3FCB29D
1BE6DB3F30B41A8777819C9D04056923C74E052E
1C4FDDDBB8402D3A1E70E5DCD4C0187C6F55ABA3
1F966B8540CF9716640DF39FA0B97FBA62200C1F
1FCE2D1735C226DC688EC191B18EF773D0B51830
2145B398927E056AFEA963CCEE39D60760F4FD21
2172B67E6E17944C74468634C1BB52269187D633
227198CB1BB02601E6E707892DC50CB9F11D1C62
25E43D900CD7AA89A209F97CC8B1E718B2E98F6B
2B0D9C7D0D9C847822283EBCB7D4E650A5DC8104
2C4B970778D8F4441EB93DA34A279E7A678E370A
2F6320819D541AE804873EA5AD3E93C0B21028F3
2F635862C92A31CE39F87262D77FC022810F40D3
31AE67F632FC6B278BD6D50D298585BF53A844DB
3356BFD26189533E8E77BFC6E59A5ED25F6BE1E2
354D5135660292C9D4DD5C394ECAAC5DC3719D8A
37902317F4B751C80C4404F6FC6A831602B9B540
3918E9F79C154F6031DA52A21F1F7477715B28BC
3B0B403BAFC72FD86EEC6474886AA7233083888F
3DD1A7A8533676FD471C69AD39DCEE0FBBE7E1FD
4186AECA8B229B51EFD559E7B839E669374673AD
426D064FDBB9AFB694F67F37942BBBD0C2E4AD69
42C4F415580B0EB17E139E92A2DA111BF6CCAF7F

```
446C3F1EFB3A44FEA98F23AEBBC925DD0C330BE6
4596E0D116A511E204A57877538EA26D174E269E
46D398B78C2DFF0118100B6507F049E867E5195F
4709995AC0FB5F32129AAD235755A8BEB9B355ED
47918740BA72FD3857F209069D6674AF8EFD411B
49A56E7A0BCF3538555078BFFA7DDBB60ADF0DDE
4C3D825798056EEF7E3FE33BDA777F9E70D4E7D4
4F4781B24879DF51652DF3FB24F156F76F78B376
4F6E7EA69CD44E5065EAD8655BC4105375D33A06
5B96C0349C07D6B37F1D3EC9F792CB5848FC48C6
5CD88B03821C3B84D7397D166233A15C0041B38B
5D93972D0352DF08DC06FF5AF120B328654B272F
5E7BEB4E8A35B234D263DDE0AED33C6C9A0D1D57
60CA70EDA899EE58AD419F513F5FB279B89C87A4
60D3445A6A15C8396356AC6F9807965A8E7BFA67
60F638CAD3116DB2FE580C31800A66836D534986
64FC3A6B5F0FA745D66DC66ED2FBC75A7C71C747
660C360B3DF4354FDAFA6454B7E19588FFE296E1
6D90CC4FF3A7F91FDFD904E73CDE3351F14EA828
6FC19EB46CAFC1A18F99119EB7353DE116F1BDFD
718957E417194A6EBD3B55C77AB3EB405E30257B
734F33BCDBF062DDEA90B2B89AF5DC4F0B292594
7688C3DCD43605BDC5E3AED03F6D87E18AEAC9AC
779366C5B356383A2286441EB84140C13000510C
7CD7334FC7CE9701A7C4FE091CC3EC01D07363D9
7DF8023457D50FF9F66CDB4C914206A163BD1713
7F95715B0BF80B7BBECC757D613084D76334101C
830F1387DFEC3D7F8D5678EED8A7C45C76B5DBE6
8368E9DEAE2F880D37232E57240CA893472C8BD3
8AFECBF940273C979D01856E1332EFF6EFE24D09
900E1C9666EECACA47DD59D908EED5480CF92953
9166AB0420C9223F23AC5C4EC5503F75505E5770
94D723C409EF4C4308113F3DBB3CB7E1084C3E12
966B722D6180AC774CFF51CFD20A1C1B966E3F43
98826BC207F1914867572561B4E0643DBE8FD8E4
9DD65F76AAF739AEF7EB9D4601ED366B3B48B121
9E6E772E41F452ED695310BCFA2B88429F12100A
9EDA0E8C2F0EDE283DC1457E4967002BDF3D376F
A9A0A33466B54A5617F986F6B160E10C5B8D81DA
AEF7725E9B945C7BCCCD7A23B1C1C1E40EEAC774
B052FC4D36F40C225397127EFB31628E8B96DC48
B563B60ED58C99199CCAB44496F858A5D42E54E7
```

```
B56A6FB4EC95793407752294782EF914EF497C8F
B57736D4F14F4E157D23C14E627A817A03C2DE24
B703848F4BC390E3E9516E3E4C746AD7C616FF96
B8F46453C1E5C03DAD1C07AB8705BE3E4F4224D2
BB7438119A8A2F79CF06BDAA14D8CACA57E05B17
BB89551AA131832395B1589C0E25D3F013A22A24
BCD2027681DD5628F0741B79B1D7C2AC4573D8E2
BD3859586D4C1701498EEFD05BB2E016848CE95D
BF42743314770340DDB5C80F22F39C6E07F74252
BFCB367868E4CFBA880E41B37241E089382F424C
C0B5CE4D03AED769DCCD5BA2BB5296C7D9F55F68
C13BED8DADA964EBF2A88786715FF83F0A1A8BCA
CBA77FE9FA0759AE0CD073D3B126F73BEB340814
CC98D9E90B7DA6E314434A246653B718ABF72FBB
CD880876565DF58EAFC033C0D207E2B2613F8C0D
CE1B68F65E2CC9A060996E58101B80C907C63377
D1D603E24FD82B6BE32B99A25A86F6CD46F3A8AF
D7423A1F56FFF460031419856FE4F7C557E1A2BF
D8ACB99F04A5EC3E355B947885E02977D6C37AF0
DA6603AC6CB47A3C448CB232EB0116BD62C7B7E4
DD1E3544F8363517556A91EBA40E85EE3638528E
DE5F6E4F559BD9FD716271AA35AFF961DF620B84
DEEC9543303C8211AD2C781F4AA936EFC191F64F
DFF022EC8223676E0D792DD126EE91B0D3059C4C
E22D6F80F0FA05446D3AF7D57EB920BA89DBEE9E
E31ABA7D0BBE49F7E66BD04379BC4837A7C91E46
E3204213E526C6ED3F8BE49D8E493DB5E92EC52A
E51519CF8C9522B4266D7CFC7125AF111DB259E7
E6AB36FE3BBDE63B28BFDF27D8890048FEA1E66D
E95A1D9E57821EBA66B421A587A014EB297DE69F
EA2BB07BB8AD5BFE1F0E92AD7B64D960600924C9
EBB140CDF75386E0FA7746910EB6596323184A7F
EDFA500254F315407783F302E85A27D8C802E4F8
EE8198049EBE16E2BA86163361FE4B5F7768FA2E
F0C6B2DEAB37A6BF78E4DF66FC4DD538F5658F6A
F15ED7BE791A2DD2446A7EF5DF748ACB474C0E98
F3DD44C8FC41D466685D8F3B9D3EA59C479230B6
F8353AB3D4D6575FD68BE1ECCF6446A5100925C9
FA22EB25A1FCBD26D5E6B88B464B61BCC4B303C2
FAEE079AABB92B4C887BA3FBEE4D1D63732D72A3
FD37E55481C7941B420950B0979586BDE2BA6B8A
FFD169CBB8E6DC9F1465AC82DDDC4C99AB59C619
```

Version 2.4

896FB40BACBF8B51A06AAF49523DE720D1C21D53
A997A5316D4936F70CDF697DF7E65796CE11B607

Version 2.5

27ED3426EA5DB2843B312E476FFFCF41BA4FDD31
C4074FCC7A600707ADCAF3DD5C0931E6CBF01B48

Registry values

The registry key used by GoBotKR is a subkey under [HKCU\SOFTWARE] with a variable name from a hardcoded list, mostly mimicking legitimate software names.

The following registry values are used:

ID
INSTALL
NAME
VERSION
REMASTER
LAST
WATCHDOC

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1189	Drive-by Compromise	GoBotKR has been distributed through torrent file-sharing websites to South Korean victims, using games or Korean movie/TV series as a lure.
Execution	T1059	Command-Line Interface	GoBotKR uses cmd.exe to execute commands.
T1064	Scripting	GoBotKR can download and execute scripts .	

Tactic	ID	Name	Description
T1204	User Execution	GoBotKR makes their malware look like the torrent content that the user intended to download, in order to entice a user to click on it.	
Persistence	T1060	Registry Run Keys / Startup Folder	GoBotKR installs itself under registry run keys to establish persistence.
T1053	Scheduled Task	GoBotKR schedules a task that adds a registry run key to establish malware persistence.	
Privilege Escalation	T1088	Bypass User Account Control	GoBotKR attempts to bypass UAC using Registry Hijacking.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	GoBotKR has used base64 to obfuscate strings, commands and files.
T1089	Disabling Security Tools	GoBotKR may use netsh to add local firewall rule exceptions.	
T1158	Hidden Files and Directories	GoBotKR stores itself in a file with Hidden and System attributes.	
T1070	Indicator Removal on Host	GoBotKR removes the Zone identifier from the ADS (Alternate Data Streams) of the file, to conceal the fact the file has been downloaded from the internet.	

Tactic	ID	Name	Description
T1036	Masquerading	GoBotKR uses filenames and registry key names associated with legitimate software.	
T1112	Modify Registry	GoBotKR stores its configuration data in registry keys. GoBotKR can modify registry keys to disable Task Manager, Registry Editor and Command Prompt.	
T1027	Obfuscated Files or Information	GoBotKR uses base64 to obfuscate strings, commands and files.	
T1108	Redundant Access	GoBotKR installs a second copy of itself on the system, which monitors and reinstalls the primary copy if it has been removed.	
T1497	Virtualization/Sandbox Evasion	GoBotKR performs several checks on the compromised machine to avoid being emulated or executed in a sandbox.	
Discovery	T1063	Security Software Discovery	GoBotKR checks for processes associated with security products and debugging tools, and terminates itself if any are detected. It can enumerate installed antivirus software using the wmic command.

Tactic	ID	Name	Description
T1082	System Information Discovery	GoBotKR uses wmic, systeminfo and ver commands to collect information about the system and the installed software.	
T1016	System Network Configuration Discovery	GoBotKR uses netsh and ipconfig to collect information about the network configuration. It has used Naver and Daum portals to obtain the client IP address.	
T1033	System Owner/User Discovery	GoBotKR uses whoami to obtain information about the victimized user. It runs tests to determine the privilege level of the compromised user.	
T1124	System Time Discovery	GoBotKR can obtain the date and time of the compromised system.	
Lateral Movement	T1105	Remote File Copy	GoBotKR attempts to copy itself into public folders of cloud storage services (Google Drive, Dropbox, OneDrive). It is also able to spread itself by instructing the compromised machine to seed torrents with the malicious file.

Tactic	ID	Name	Description
T1091	Replication Through Removable Media	GoBotKR can drop itself onto removable media and relies on Autorun to execute the malicious file when a user opens the removable media on another system.	
Collection	T1113	Screen Capture	GoBotKR is capable of capturing screenshots.
Command and Control	T1090	Connection Proxy	GoBotKR can be used as a proxy server.
T1132	Data Encoding	The communication with the C&C server is base64 encoded.	
T1105	Remote File Copy	GoBotKR can download additional files and update itself.	
T1071	Standard Application Layer Protocol	GoBotKR uses HTTP or HTTPS for C&C.	
T1065	Uncommonly Used Port	GoBotKR uses non-standard ports, such as 6446, 6556 and 7777, for C&C.	
Impact	T1499	Endpoint Denial of Service	GoBotKR has been used to execute endpoint DDoS attacks – for example, TCP Flood or SYN Flood.
T1498	Network Denial of Service	GoBotKR has been used to execute network DDoS.	
T1496	Resource Hijacking	GoBotKR can use the compromised computer's network bandwidth to seed torrents or execute DDoS.	

8 Jul 2019 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion