DDoS IRC Bot Malware (GoLang) Being Distributed via Webhards

asec.ahnlab.com/en/30755

January 19, 2022

While monitoring the distribution source of malware in Korea, the ASEC analysis team has discovered that DDoS IRC Bot strains disguised as adult games are being installed via webhards. Webhards are platforms commonly used for the distribution of malware in Korea, where njRAT and UDP Rat were distributed in the past.

UDP RAT Malware Being Distributed via Webhards

The cases that are recently being discovered are similar to the case discussed in the post above, and it appears that the same attacker is continuing to distribute the malware. For starters, the malware is being distributed under the guise of adult games. Additionally, the DDoS malware was installed via downloader and UDP Rat was used.

One difference is that the previous downloader malware was developed using C#, but now GoLang is used instead. The publicly released open-source Simple-IRC-Botnet (DDoS IRC Bot malware developed with GoLang) was also used along with UDP Rat.

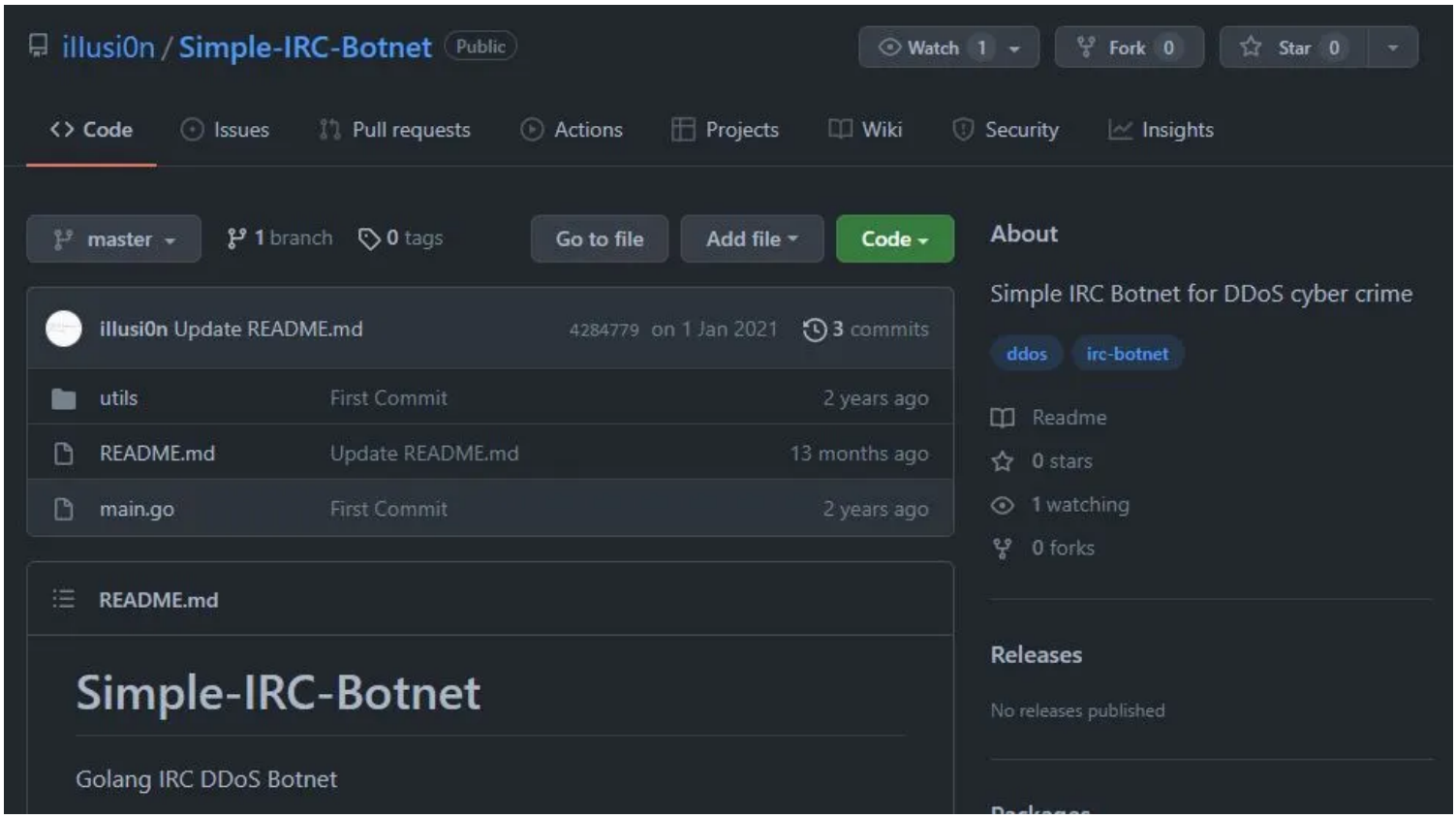

Figure 1. Open-source Simple-IRC-Botnet

The GoLang is used by various attackers and its usage is increasing recently due to various strengths it has: its low development difficulties and its cross-platform support. Following such a trend, cases that use GoLang are increasing in Korat malware strains that target Korean users.

As shown in the figure below, malware disguised as an adult game is uploaded to the webhard.

Figure 2. Compressed file that contains malware distributed on the webhard

While it is uncertain whether the person who uploaded this game is the attacker, similar posts are distributing the same malware using compressed files. Note that the games differ but the malware inside the compressed files is the same as what will be discussed below.

Figure 3. Other posts uploaded by the attacker

The adult games used for attacks contain the following path name. This means that they were distributed through the compressed files with the following names.

– [19 Korean version] Naughty Mage's EXXXXX Life
– [19 Korean version] The Reason She Became a Slave
– [19 Korean version] Refraining of Heavenly Walk
– [19 Korean version] Exchange Diary of Violation
– [19 Korean version] Girl From Tea Ceremony Club
– [19 Korean version] Curse of Lilia
– [19 Korean version] Academy with Magical Girls
– [19 Korean version] Monster Fight
– [19 Korean version] Dreamy Lilium
– [19 Korean version] Enraged Department Manager
– [19 Korean version] Fancy Days of Sayuri
– [19 Korean version] Sleif Corporation
– [19 Korean version] Country Girl Exposure
– [19 Korean version] Sylvia and Master of Medicine
– [19 Korean version] Assassin Asca
– [19 Korean version] How to Reform Your Girlfriend
– [19 Korean version] Creating Utopia with Subjugation Skill
– [19 Korean version] Uriel and Belial
– [19 Korean version] The Case of Chairperson Kana
– [19 Korean version] Princess Round
– [19 Korean version] Flora and the Root of the World Tree
– [19 Korean version] Midnight Exposure
– [19 Korean version] Modern Day Elf
– [19 Korean version] Research Data of Homunculus

Upon decompressing the downloaded zip file, the following files appear. Normally, users would run the "Game_Open.exe" file shown below to play the game.

Figure 4. Malware disguised as Game_Open.exe file

But “Game_Open.exe” is not a launcher that runs the game. It is an executable that runs the additional malware. To be more precise, it changes the “PN” file existing in the same path as “scall.dll” and runs it. Then it copies the original game executable “index” to “Game.exe” to run it. As such, users would assume that the game is being run normally.

Figure 5. Actual game program run by malware

Once the process above is complete, the “Game_Open.exe” file becomes hidden. After hidden, users would run “Game.exe” which is a copy of game program launcher. Note that “PN” file that was changed to “scall.exe” and executed is malware. It first moves “srt” file existing in the same path to C:\Program Files\EdmGen.exe.

Figure 6. Malware created in Program Files path

It then registers “EdmGen.exe” to the task scheduler using the following command to have it run periodically.

> “C:\Windows\System32\cmd.exe” /c SCHTASKS /CREATE /SC ONSTART /NP /TN “Windows Google” /TR “C:\Program Files\EdmGen.exe”

“EdmGen.exe” (“srt” file) that is executed by the process shown above runs the normal program vbc.exe and injects malware into the program. The malware that is injected to vbc.exe and executed is also a downloader type discussed in the previous ASEC blog post. One difference is that it was developed with GoLang instead of C#.

The malware can periodically access the C&C server as shown below to obtain the URL of malware that will be downloaded to install additional malware.

Figure 7. Routine of injected Golang downloader

- Download URL for Additional Malware: hxxp://node.kibot[.]pw:8880/links/01-13
- Creation Path of Downloaded Malware: C:\Down\discord_[random characters]\[malware name]

Previously, the type of additionally installed malware was UDP Rat DDoS. Yet for this case, there was also Simple-IRC-Botnet developed with GoLang.

It is also a type of DDoS Bot malware, but it uses IRC protocols to communicate with the C&C server. Unlike UDP Rat that only supported UDP Flooding attacks, it can also support attacks such as Slowris, Goldeneye, and Hulk DDoS.

Figure 8. Routine function of Golang DDoS IRC Bot malware

Golang DDoS IRC Bot connects to a particular IRC server when it is run and enters the attacker’s channel. It can perform DDoS attacks on a target if the attacker sends commands from the channel.

– IRC Server List Used by Golang DDoS IRC Bot Malware
210.121.222[.]32:6667
157.230.106[.]25:6667
89.108.116[.]192:6667
176.56.239[.]136:6697

Figure 9. Command to enter attacker's IRC channel

Figure 10. DDoS commands that can be sent by the attacker through IRC channel

As shown in the examples above, the malware is being distributed actively via file sharing websites such as Korean webhards. As such, caution is advised when approaching executables downloaded from a file-sharing website. It is recommend for the users to download products from the official websites of developers.

[File Detection]
Trojan/Win.Korat.C4914970 (2022.01.16.00)
Trojan/Win.Korat.R465157 (2022.01.16.00)
Trojan/Win.Korat.C4914985 (2022.01.16.00)
Downloader/Win.Korat.C4914968 (2022.01.16.00)
Downloader/Win.Korat.C4914972 (2022.01.16.00)
Downloader/Win.Korat.C4914976 (2022.01.16.00)
Downloader/Win.Korat.C4914977 (2022.01.16.00)
Downloader/Win.Korat.C4914979 (2022.01.16.00)
Downloader/Win.Korat.C4914980 (2022.01.16.00)
Downloader/Win.Korat.C4914997 (2022.01.16.00)
Trojan/Win.IRCGo.C4915003 (2022.01.16.00)
Trojan/Win.IRCGo.C4915004 (2022.01.16.00)
Trojan/Win.IRCGo.C4915005 (2022.01.16.00)
Backdoor/Win.UDPRat.R465188 (2022.01.16.00)

[IOC]
File
– Game Launcher
affbad0bedccbf1812599fbce847d917
b21ad73be72280ae30d8c5556824409e
889289d9d97f7c31925a451700b4b7ac
2a7de90437c66b3f2304630c3324e2de
f14c51ca5d7afc1128cceca5d5a5694b
41320f572cdf14abc1401a72a24a621d
d38803b3f7c0faac71a3e572e9214891
5d97a32e47dfa54dd1bebde208252b88
12baeacfd0ac2d66c5959d6305a4fe50

– Launcher

b621005a147ef842fbc7198c8431724c
ba43e4c84da7600881ed5ccac070e001
b6ad8550dcd317a49c6e563a1188d9f0
db2db486b828182c827e4fdfc292e143
4c1777b5763bc7655d1ca89ae4774470
2357c1c6027f21094fa62a35300a96ae
28566a08334f37d7a8d244c393e9ad33
4b3eff9f394ebd2231c5c0b980c62e63
74834f29dd5d244742879c2d800e8a53
4b3eff9f394ebd2231c5c0b980c62e63

– Downloader

42a344fbad7a56e76c83013c677330ac
6b029fc7a0f480b7dd6158bba680e49b
5a74ea453f0b424770fdddaf470f5eae
12c97b2481efe448b93b72b80eb96563
1f993f08ed40f6b03db7f78ab8e087a5
005247fa9b312eb449150b52b38e0a4c
1f2147b2a0caeb43a9a3bcaf42808581
63ff6d1bb53cdd2d7b7fca856826c8b6

– UDP Rat

bff341b0c95eda801429a4b5c321f464
0fd264b12ea39e39da7807a117718429
af486a4e9fdc62ac31f8424a787a460c
2160629e9def4c9482b4fb642c0cd2d8
51cfd6c6390ce99979350a9a21471d30
194fb8590e1218f911870c54b5830f16
7b73a4e6e504800e256495861d0c9f78
57568755bac3f20fffb970a3c6386a43
55b6e07ff120b6c2e784c8900333aa76
bc18d787c4d886f24fa673bd2056e1ed
5be1ab1d5385d5aeadc3b498d5476761
1bc93ee0bd931d60d3cd636aa35176e3
a2fc31b9c6a23e0a5acc591e46c61618
977c52d51d44a0a9257017b72cfafab1
98e4f982363c70bd9e52e5a249fce662

– Golang DDoS IRC Bot

7f3bd23af53c52b3e84255d7a3232111
00b9bf730dd99f43289eac1c67578852
90bfa487e9c5e8fe58263e09214e565b
2fe8262d0034349a030200390b23b453
8053b24878c4243d8eda0ccae8905ccb

C&C Server

– Downloader Malware

hxxp://organic.kibot[.]pw:2095/links/12-20
hxxp://node.kibot[.]pw:2095/links/12-20
hxxp://node.kibot[.]pw:2095/links/12-25
hxxp://node.kibot[.]pw:8880/links/12-28
hxxp://miix.kibot[.]pw:8880/links/12-28
hxxp://node.kibot[.]pw:8880/links/12-28
hxxp://node.kibot[.]pw:8880/links/01-13

– UDP Rat

195.133.18[.]27:1234
195.133.18[.]27:8080
195.133.18[.]27:9997

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

TAGGED AS:DDOS, GO, GOLANG, IRC, UDPRAT, WEBHARD

Categories:Malware Information

Tagged as:DDOS, Go, Golang, IRC, udprat, webhard