VNC Malware (TinyNuke, TightVNC) Used by Kimsuky Group

asec.ahnlab.com/en/27346/

October 20, 2021

While monitoring Kimsuky-related malware, the ASEC analysis team has recently discovered that VNC malware was installed via AppleSeed remote control malware.

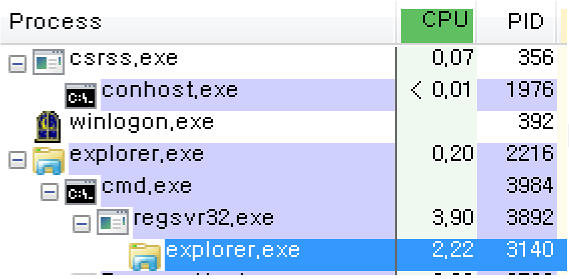
VNC, also known as Virtual Network Computing, is a screen sharing system that remotely controls other computers. Similar to the commonly-used RDP, it is used to remotely access and control other systems.

Kimsuky group installs AppleSeed backdoor on the target system after the initial compromise, then additionally installs VNC malware via AppleSeed to ultimately control the target system in a graphical environment. One of the VNC malware that is installed is TinyNuke.

1. **TinyNuke (HVNC)**

TinyNuke, also known as Nuclear Bot, is a banking malware discovered in 2016, and it includes features such as HVNC (HiddenDesktop/VNC), reverse SOCKS4 proxy, and form grabbing. Due to its source code revealed in 2017, TinyNuke is used by various attackers, and the HVNC, Reverse SOCKS4 Proxy features are partially borrowed by other malware such as AveMaria and BitRAT.

Among the various features of TinyNuke that are being distributed, only the HVNC feature is enabled. A difference between normal VNC and HVNC used by TinyNuke is that the user does not realize that the PC is infected and its screen is being controlled. The following shows the process tree when HVNC is enabled.



Process	CPU	PID
csrss.exe	0.07	356
conhost.exe	< 0.01	1976
winlogon.exe		392
explorer.exe	0.20	2216
cmd.exe		3984
regsvr32.exe	3.90	3892
explorer.exe	2.22	3140

Figure 1. Process tree upon using HVNC

explorer.exe (PID: 3140) is the child process of explorer.exe (PID: 2216), and is found in the process tree. The attacker is able to control the screen via the new explorer.exe (PID: 3140), and the GUI (Graphical user interface) of the process created while the attacker is controlling the target PC is not visible on the target PC screen. This type of VNC remote access is called HVNC (Hidden Virtual Network Computing).

Another characteristic is that it uses the reverse VNC method. VNC consists of a server and a client. It installs the VNC server on the control target system, and the user who wishes to control the system remotely uses the VNC client. It gains control of the VNC client by going through the VNC server installed on the remote control target system.

In a normal VNC environment, it attempts to access the remote control target (VNC server) via the VNC client. However, HVNC of TinyNuke attempts to access the client from the server with the reverse VNC feature. This means that when HVNC of the infected system is run, the awaiting attacker accesses the designated C&C server and uses the VNC client (server for HVNC) on the C&C server to gain remote control. It is assumed that this is to bypass firewalls such as Reverse Shell that blocks internal access from the outside and to support communication in a private IP environment.

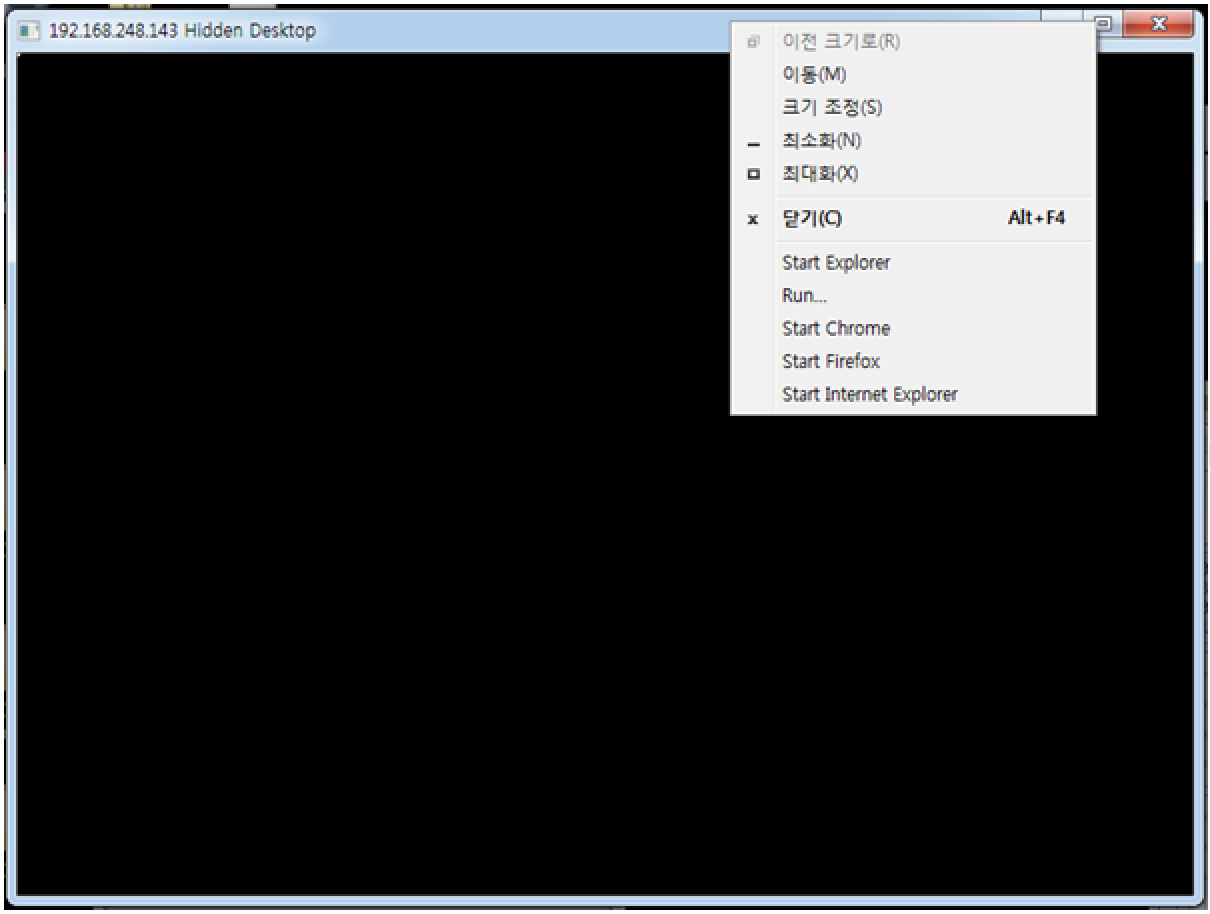
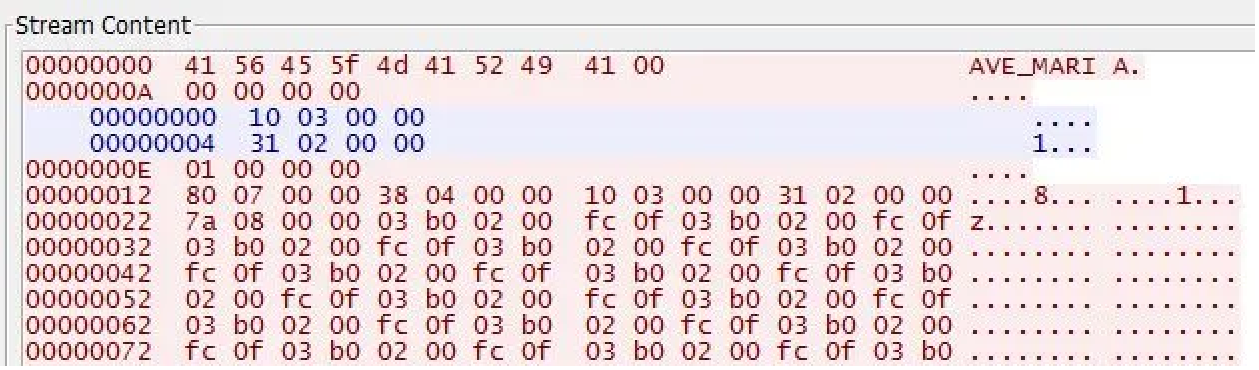


Figure 2. Attacker’s HVNC screen

Note that TinyNuke uses “AVE_MARIA” string for verification when establishing HVNC communication between the server and the client. This means that when “AVE_MARIA” string is sent from the HVNC client to the server, the server verifies the name, and HVNC communication can be enabled if “AVE_MARIA” is correct.

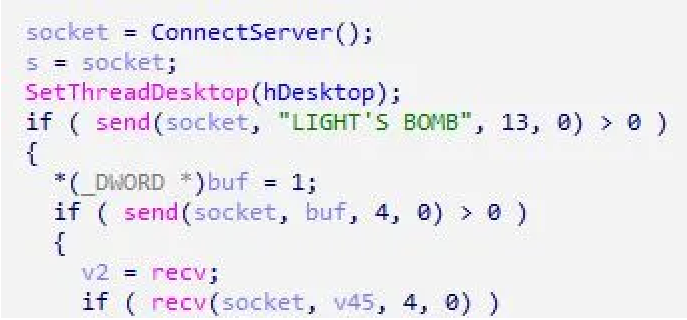


Stream Content

```
00000000  41 56 45 5f 4d 41 52 49  41 00                     AVE_MARI A.
0000000A  00 00 00 00                                        ....
    00000000  10 03 00 00                                        ....
    00000004  31 02 00 00                                        1...
0000000E  01 00 00 00                                        ....
00000012  80 07 00 00 38 04 00 00  10 03 00 00 31 02 00 00 ....8... ....1...
00000022  7a 08 00 00 03 b0 02 00  fc 0f 03 b0 02 00 fc 0f z....... ........
00000032  03 b0 02 00 fc 0f 03 b0  02 00 fc 0f 03 b0 02 00 ........ ........
00000042  fc 0f 03 b0 02 00 fc 0f  03 b0 02 00 fc 0f 03 b0 ........ ........
00000052  02 00 fc 0f 03 b0 02 00  fc 0f 03 b0 02 00 fc 0f ........ ........
00000062  03 b0 02 00 fc 0f 03 b0  02 00 fc 0f 03 b0 02 00 ........ ........
00000072  fc 0f 03 b0 02 00 fc 0f  03 b0 02 00 fc 0f 03 b0 ........ ........
```

Figure 3. AVE_MARIA string used in HVNC

This is identical to that of HVNC used by Kimsuky group, however, recently there have been HVNCs using “LIGHT’s BOMB” string.



```
socket = ConnectServer();
s = socket;
SetThreadDesktop(hDesktop);
if ( send(socket, "LIGHT'S BOMB", 13, 0) > 0 )
{
  *(_DWORD *)buf = 1;
  if ( send(socket, buf, 4, 0) > 0 )
  {
    v2 = recv;
    if ( recv(socket, v45, 4, 0) )
```

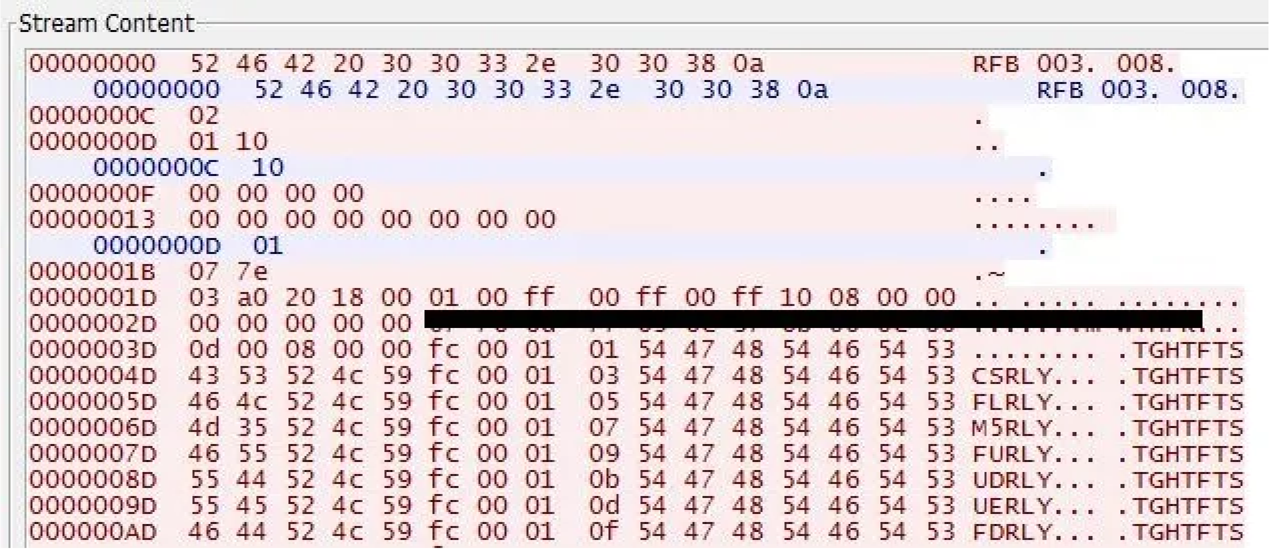
Figure 4. “LIGHT’S BOMB” string used in place of AVE_MARIA

2. TightVNC (VNC)

Another VNC malware distributed via AppleSeed backdoor is TightVNC. TightVNC is an open-source VNC utility, and the attacker customizes it to use it. TightVNC can be regarded as a normal VNC utility, but it is different in that it supports the reverse VNC feature discussed earlier.

TightVNC consists of tvnserver.exe, the server module, and tvnviewer.exe, the client module. In a normal environment, it installs tvnserver on the remote control target and accesses the target using tvnviewer in the user environment. In order to use the reverse VNC feature, it runs tvnviewer as a listening mode on the client, then uses tvnserver that is installed as a service on the access target system to set the client address using controlservice and connect commands for access gain.

Kimsuky group distributes tvnserver, and it is customized so that the reverse VNC feature can be used in the infected environment without installing a service. Simply running tvnserver will allow the attacker to access tvnviewer that operates on the C&C server and gain control of the screen of the infected system.



```
00000000  52 46 42 20 30 30 33 2e  30 30 38 0a              RFB 003. 008.
    00000000  52 46 42 20 30 30 33 2e  30 30 38 0a              RFB 003. 008.
0000000C  02                                                .
0000000D  01 10                                             ..
    0000000C  10                                                .
0000000F  00 00 00 00                                       ....
00000013  00 00 00 00 00 00 00 00                           ........
    0000000D  01                                                .
0000001B  07 7e                                             .~
0000001D  03 a0 20 18 00 01 00 ff  00 ff 00 ff 10 08 00 00 .. ..... ........
0000002D  00 00 00 00 00 [redacted] ..
0000003D  0d 00 08 00 00 fc 00 01  01 54 47 48 54 46 54 53 ........ .TGHTFTS
0000004D  43 53 52 4c 59 fc 00 01  03 54 47 48 54 46 54 53 CSRLY... .TGHTFTS
0000005D  46 4c 52 4c 59 fc 00 01  05 54 47 48 54 46 54 53 FLRLY... .TGHTFTS
0000006D  4d 35 52 4c 59 fc 00 01  07 54 47 48 54 46 54 53 M5RLY... .TGHTFTS
0000007D  46 55 52 4c 59 fc 00 01  09 54 47 48 54 46 54 53 FURLY... .TGHTFTS
0000008D  55 44 52 4c 59 fc 00 01  0b 54 47 48 54 46 54 53 UDRLY... .TGHTFTS
0000009D  55 45 52 4c 59 fc 00 01  0d 54 47 48 54 46 54 53 UERLY... .TGHTFTS
000000AD  46 44 52 4c 59 fc 00 01  0f 54 47 48 54 46 54 53 FDRLY... .TGHTFTS
```

Figure 5. Reverse VNC communication using tvnviewer

3. Conclusion

As introduced in the *previous blog post*, Kimsuky group uses AppleSeed to install Meterpreter, a different backdoor malware, and uses TinyNuke, TightVNC and RDP Wrapper for screen control. There is also evidence of the use of Mimikatz for account info-stealing.

Feature	Tool Name
Remote Control	AppleSeed, Meterpreter
Screen Control	TinyNuke, TightVNC, RDP Wrapper
Account Info-stealing	Powerkatz

Table 1. Recently-found attack tools used by Kimsuky group
Kimsuky group's malware trend is being monitored constantly, and users need to take extra caution when opening attachments in emails from unknown sources and refrain from visiting untrusted websites.

Alias Information

Trojan/Win.VNC (2021.09.16.00)
Trojan/Win.TinyNuke (2021.09.16.03)
Trojan/Win.HVNC (2021.09.18.01)

IOC

[TinyNuke]

[MD5]
00ced88950283d32300eb32a5018dada
535827d41b144614e582167813fbbc4c
67aa7ddecc758dddfa8afc9d4c208af1
93efab6654a67af99bbc7f0e8fcf970f
f7839eeb778ff17cf3c3518089f9bbec
dd90cb5dcd7bd748baa54da870df606c
5bd6cb6747f782c0a712b8e1b1f0c735
16c0e70e63fcb6e60d6595eacbd8eeba

[C&C]
27.102.102.70:33890
27.102.112.58:33890
31.172.80.104:3030
27.255.81.109:33890
27.255.81.71:33890
79.133.41.237:3030

[TightVNC]

[MD5]

26eaff22da15256f210762a817e6dec9
088cb0d0628a82e896857de9013075f3
9a71e7e57213290a372dd5277106b65a
db4ff347151c7aa1400a6b239f336375
4301a75d1fcd9752bd3006e6520f7e73
a07ddce072d7df55abdc3d05ad05fde1
5b6da21f7feb7e44d1f06fbd957fd4e7
be14ced87e2203ad5896754273511a14
4fdba5a94e52191ce9152a0fe1a16099
bb761c2ac19a15db657005e7bc01b822

[C&C]

27.102.114.79:5500
27.102.127.240:5500
31.172.80.104:5500
27.102.114.89:5500
27.102.128.169:5500
27.255.81.109:5500
31.172.80.104:5500
61.14.211.175:5500
27.255.81.71:5500

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

Categories:Malware Information

Tagged as:HVNC, Kimsuky, TightVNC, TinyNuke, VNC