Malware Being Distributed by Disguising Itself as Icon of V3 Lite

asec.ahnlab.com/en/36629/

July 21, 2022

The ASEC analysis team has discovered the distribution of malware disguised as a V3 Lite icon and packed with the .NET packer. The attacker likely created an icon that is almost identical to that of V3 Lite to trick the user, and AveMaria RAT and AgentTesla were discovered during the last month using this method.

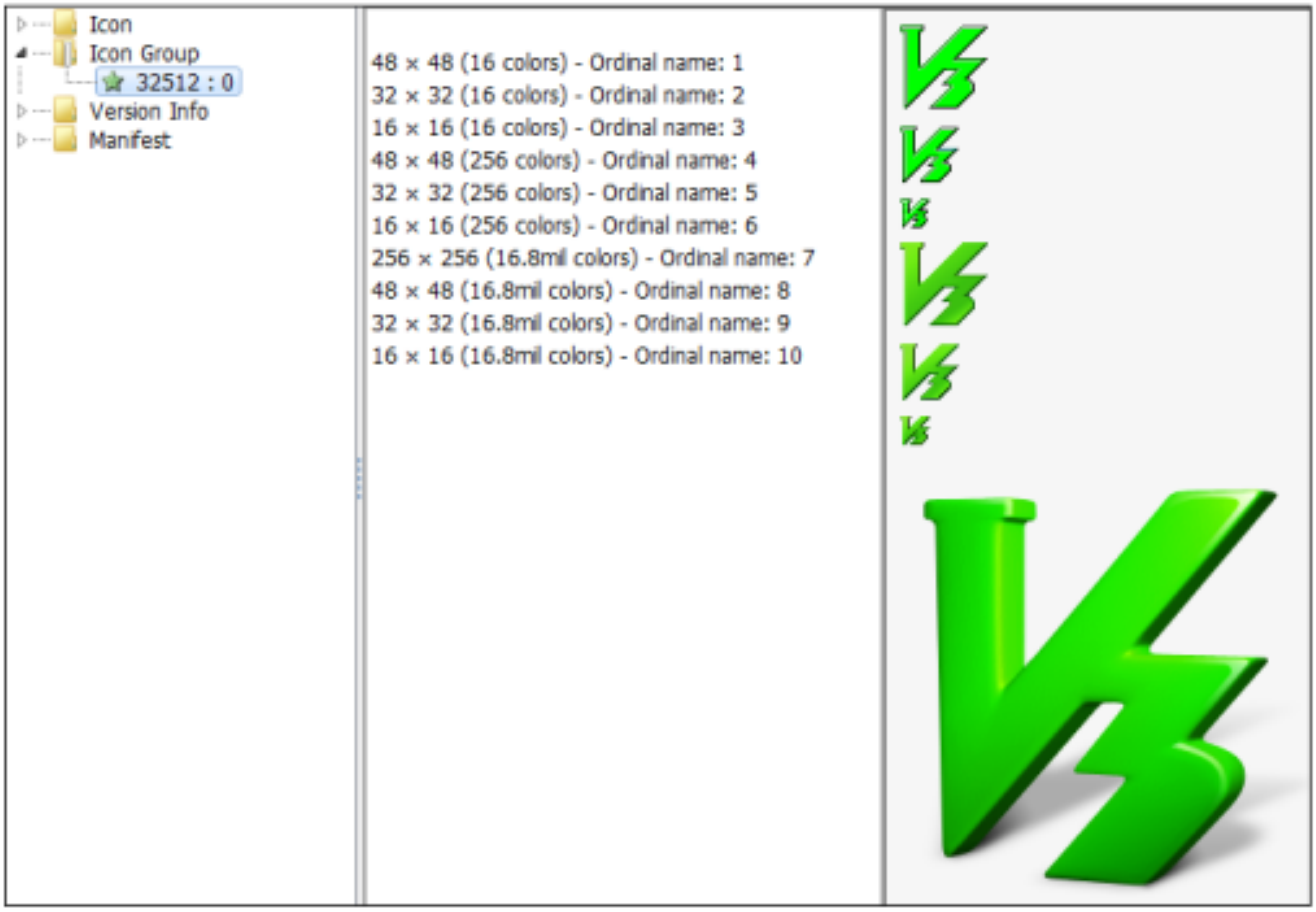

Figure 1. Malware using icon identical to that of V3 Lite executable
As shown in Figure 1, the icon looks almost identical to the actual V3 Lite icon.

AveMaria is a RAT (Remote Administration Tool) malware with remote control features that receives commands from the C&C server and performs a variety of malicious behaviors. It is usually distributed in the .NET packer form like AgentTesla, Lokibot, and Formbook to bypass anti-malware detection.

Although the original name of AveMaria is WARZONE RAT, it sends the “AVE_MARIA” string for authentication when performing a proxy connection with the C2 server, thereyby also known as AveMaria.

Additional features of the malware and the analysis information of its binary can be found in the AhnLab TIP Portal’s detailed analysis report and ASEC blog post.

> AveMaria malware being distributed as spam mail

While the malware is operating, winSAT.exe (Windows System Assessment Tool) and a command for UAC privilege escalation using the winmm.dll file were found, which were explained in the previous blog.

> Distribution of Remcos RAT Disguised as Tax Invoice

```
0x419d48 (184): Ave_Maria Stealer OpenSource github Link: https://github.com/syohex/java-simple-mine-sweeper
0x419e08 (128): C:\Users\Vitali Kremez\Documents\MidgetPorn\workspace\MsgBox.exe
0x419e90 (102): Software\Microsoft\Windows\CurrentVersion\Explorer\
0x419ef8 (8): inst
0x419f04 (22): InitWindows
0x419f20 (104): Software\Microsoft\Windows NT\CurrentVersion\Windows
0x419f8c (26): \programs.bat
0x419fa8 (72): for /F "usebackq tokens=*" %%A in ("
0x419ff4 (12): :start
0x41a004 (18): ") do %%A
0x41a018 (32): :ApplicationData
0x41a03c (54): wmic process call create '"
0x41a080 (104): cmd.exe /c REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /f /v Load /t REG_SZ /d "
0x41a0f0 (32): :Zone.Identifier
0x41a114 (8): Load
0x41a120 (55): cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q
0x41a158 (22): \winSAT.exe
0x41a170 (20): \winmm.dll
0x41a188 (32): \\?\C:\Windows \
0x41a1ac (48): \\?\C:\Windows \System32
0x41a1e0 (70): \\?\C:\Windows \System32\winSAT.exe
0x41a228 (70): \\?\C:\Windows \System32\winmmd.dll
0x41a270 (66): SOFTWARE\Microsoft\Control Panel\
0x41a2b4 (48): Virtual Machine Platform
0x41a2e8 (68): \\?\C:\Windows \System32\WINMM.dll
0x41a330 (62): C:\Windows \System32\winSAT.exe
```

Figure 2. UAC Bypass behavior found in the memory when AveMaria is executed

When the malware is run, it deliberately causes a delay with timeout.exe. It then performs additional malicious behaviors by injecting a malicious binary into a normal Windows process named RegAsm.exe. Figure 4 shows the malicious binary inside the process.

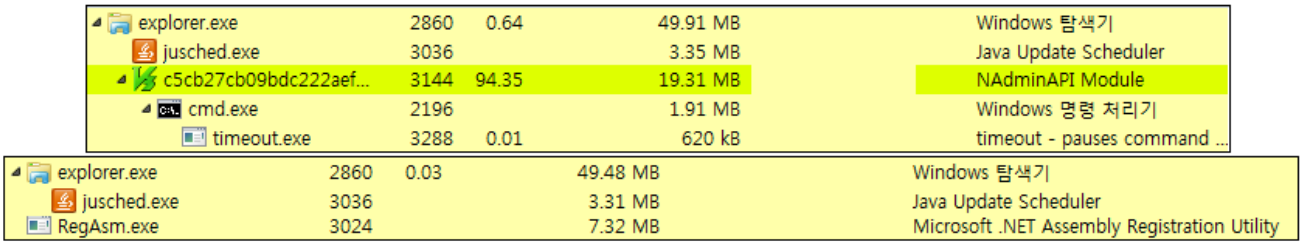

Figure 3. Process tree (injected into a normal process RegAsm.exe)

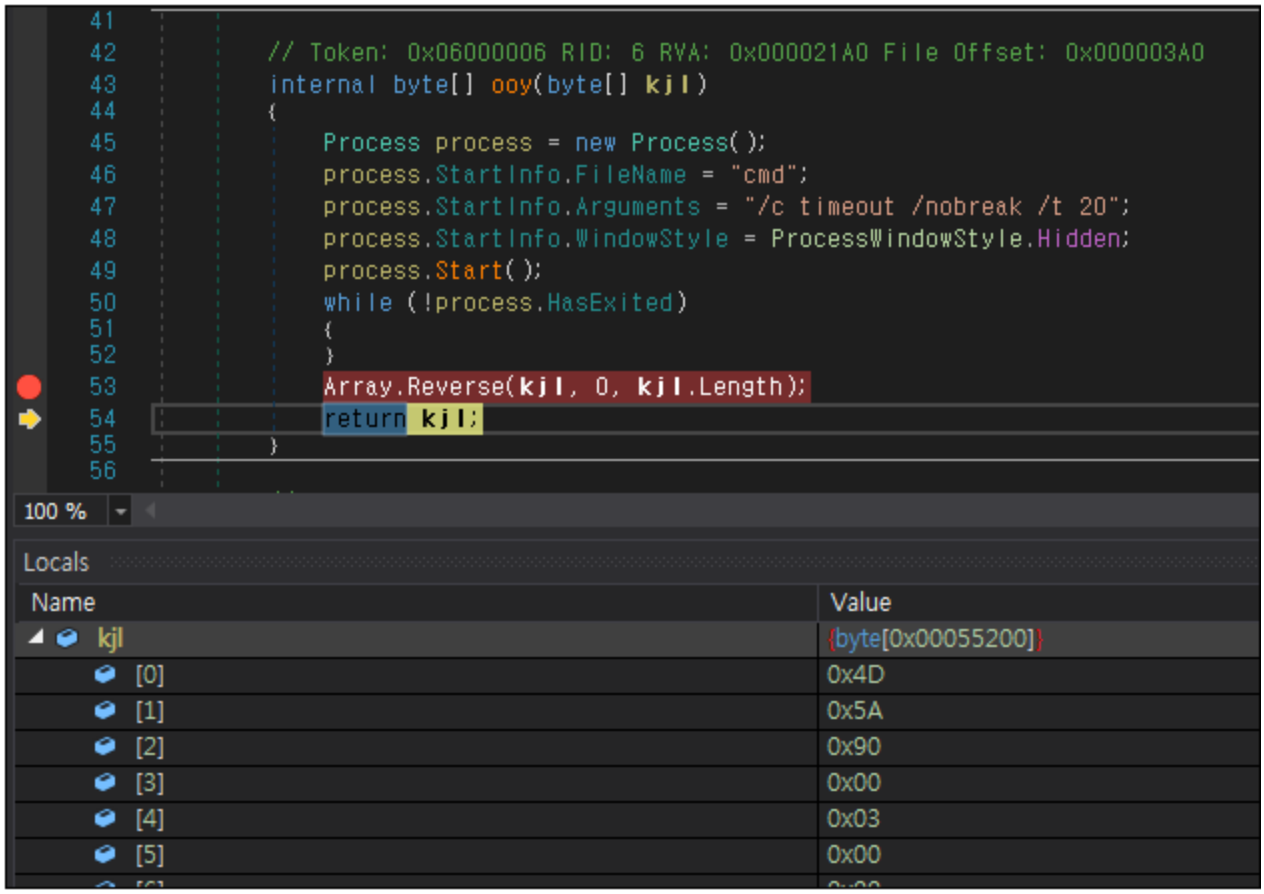

Figure 4. Malicious internal DLL binary found during the debugging process

Besides AveMaria, the distribution of AgentTesla was also found. AgentTesla is an info-stealer that leaks user information saved in web browsers, emails, and FTP clients. It is one of the most prolific malware in terms of distribution, being constantly ranked high in the ASEC Weekly Malware Statistics.

> How AgentTesla Malware is Being Distributed in Korea

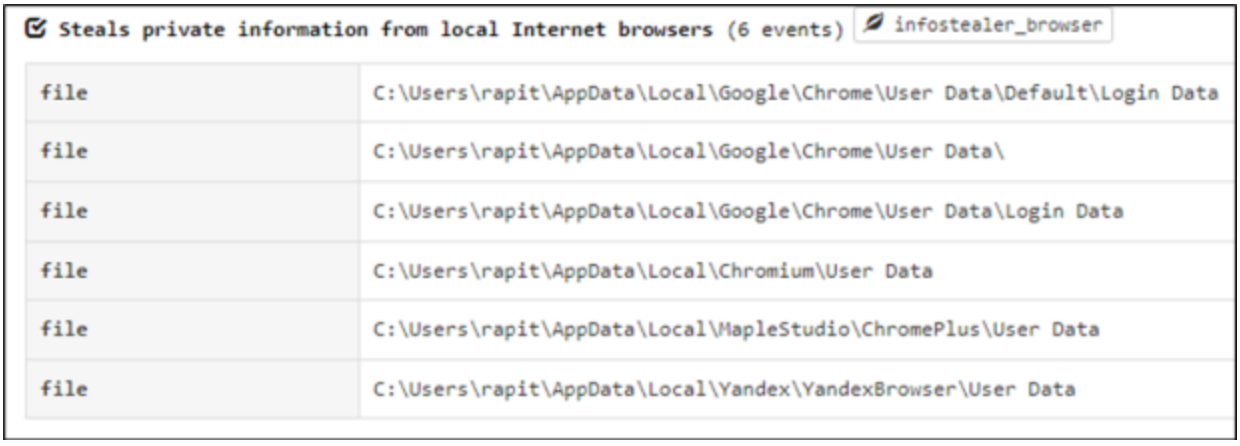

Figure 5. RAPIT log – Snatching web browser data

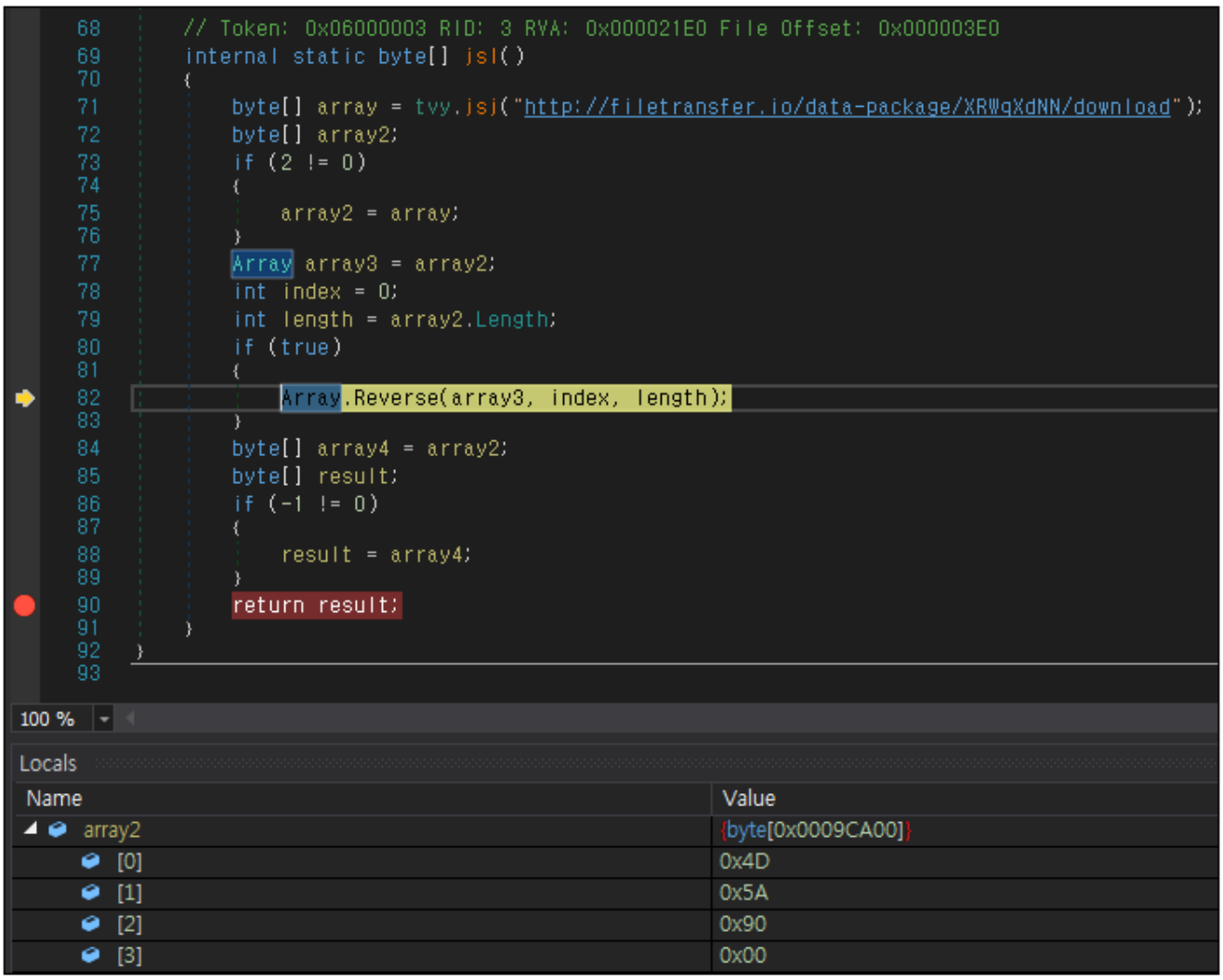

Figure 6. Malicious binary downloaded from an external URL

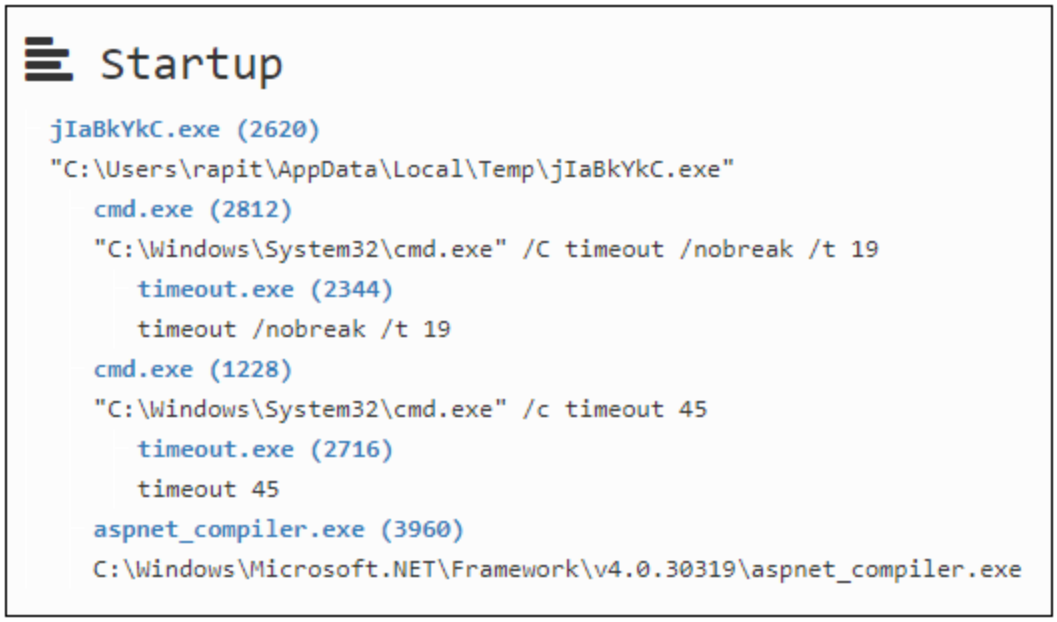

Figure 7. RAPIT process tree

Upon using AhnLab's infrastructure to check the related malicious files that use V3 Lite icon, it was found that the distribution is done actively. Most of such malicious files are distributed through attachments of phishing emails.

At the basic level, users should refrain from opening attachments in emails from unknown sources and update the anti-malware program 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.MSILKrypt.R495355
Trojan/Win.MSILKrypt.R498085
Trojan/Win.MSIL.C5152589
Trojan/Win.MSIL.R500015
Trojan/Win.MSIL.C515258
Trojan/Win.AveMaria.R498632
Trojan/Win.Tnega.C5059801
Downloader/Win.MSIL.R498629

[Memory Detection]
Trojan/Win.AgentTesla.XM95

[Behavior Detection]
Persistence/MDP.AutoRun.M224

[IOC]
c5cb27cb09bdc222aeffaf0cccb96bad
ccb55c0200203e7fb4748d28c30ba2f9
45.162.228[.]171:26112
3280690e018ceb2112ee695933f65742
hxxp://ppz.devel.gns.com[.]br/temps/donexx.exe
hxxp://filetransfer[.]io/data-package/XRWqXdNN/download

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

Categories:Malware Information

Tagged as:AGENTTESLA, Avemaria, InfoStealer, malware, Phishing email