Posted on June 2, 2022

NSIS Installer Malware Included with Various Malicious Files

The ASEC analysis team recently discovered attackers distributing multiple malicious files with NSIS installers.

NSIS (Nullsoft Scriptable Install System) is normally used to create installers for certain programs. It can be also used for creating malware strains as it is script-based and thus makes nearly identical forms for NSIS installers.

NSIS installer-type malware strains have been used a lot by attackers. The type introduced in this post includes multiple malicious files in a single installer: running one file will infect the system with various malware strains.

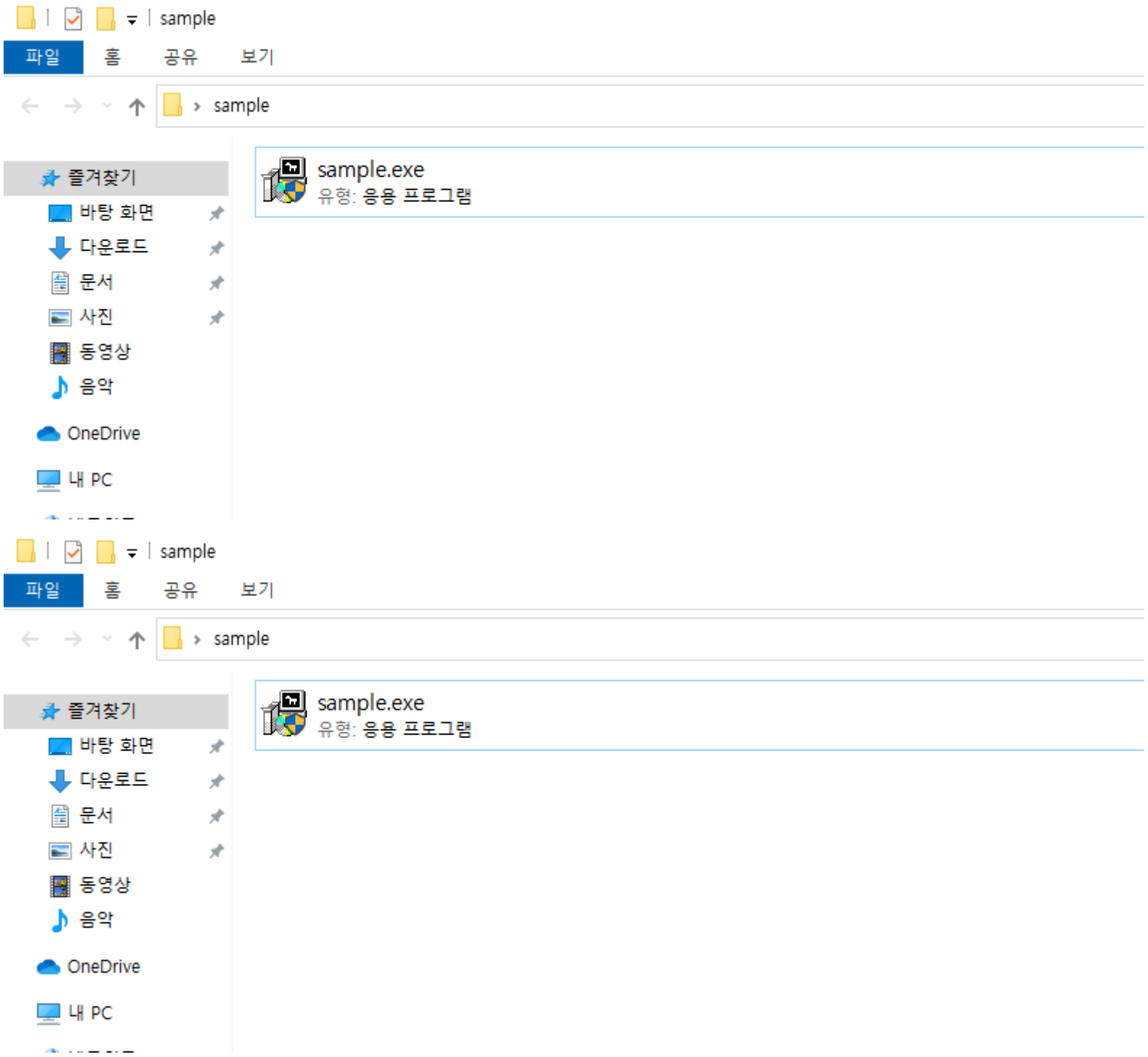

Figure 1. Malware icon

Inside the NSIS installer is a file named setup_installer.exe and the NSI script as shown below.

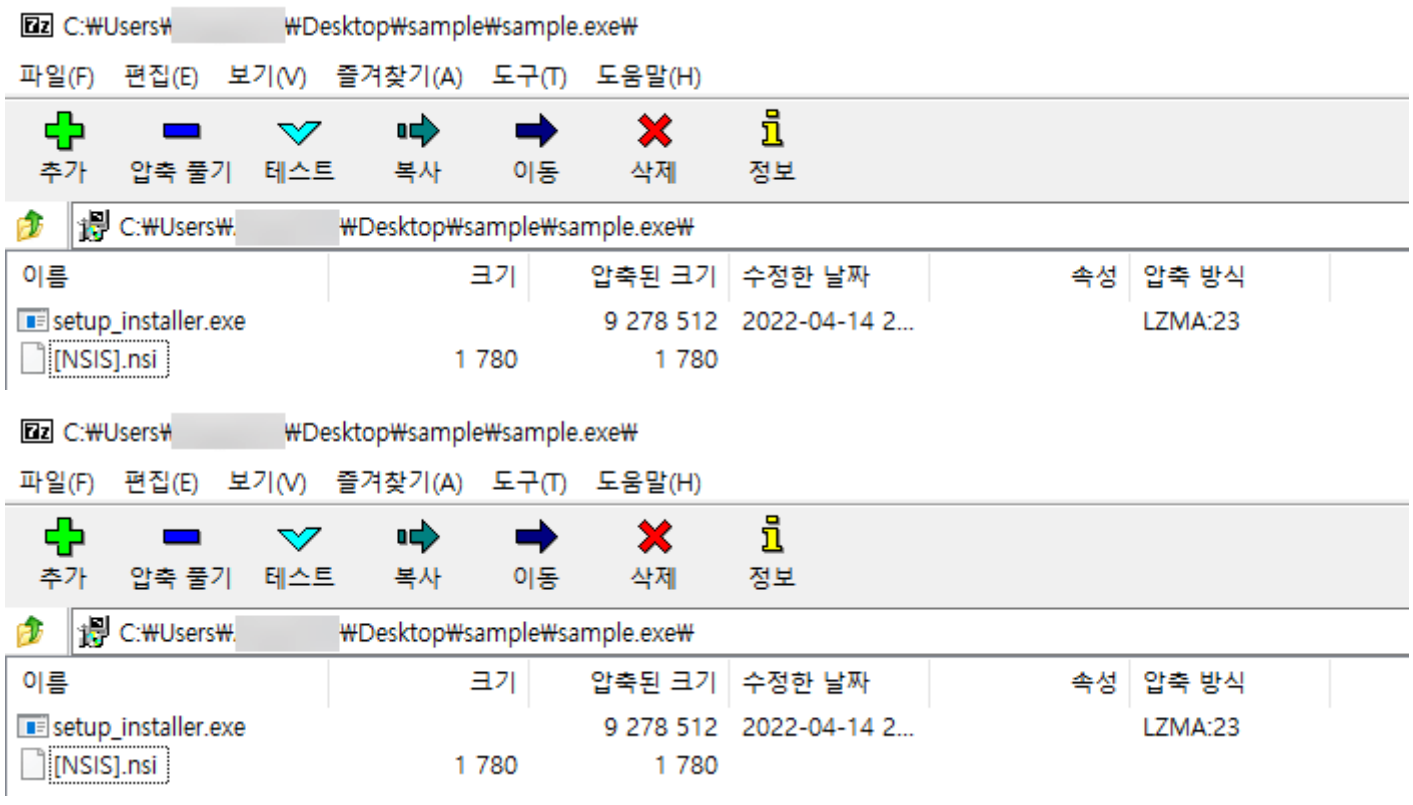

Figure 2. Files inside the malware

The script simply has a routine for running setup_installer.exe. It does not have anti-sandbox techniques such as obfuscation or time delay.

```
Section setup ; Section_0
  ; AddSize 9008
  SetOutPath $INSTDIR
  File setup_installer.exe
SectionEnd


Section runit ; Section_1
  ExecShell runas $INSTDIR\setup_installer.exe    ; "runas $INSTDIR\setup_installer.exe"
SectionEnd
```


```
Section setup ; Section_0
  ; AddSize 9008
  SetOutPath $INSTDIR
  File setup_installer.exe
SectionEnd


Section runit ; Section_1
  ExecShell runas $INSTDIR\setup_installer.exe    ; "runas $INSTDIR\setup_installer.exe"
SectionEnd
```


Figure 3. Part of NSI script file

setup_installer.exe consists of 7Zip SFX (Self-extracting archive) that can extract internally compressed files to a certain folder and run certain programs.

The setup_installer.exe file contains malicious files, library files, and setup_install.exe (15 in total). When the installer is run, it is automatically decompressed in the %TEMP% (temporary folder) \7zS[random 8 characters] folder and runs setup_install.exe when the process is complete.

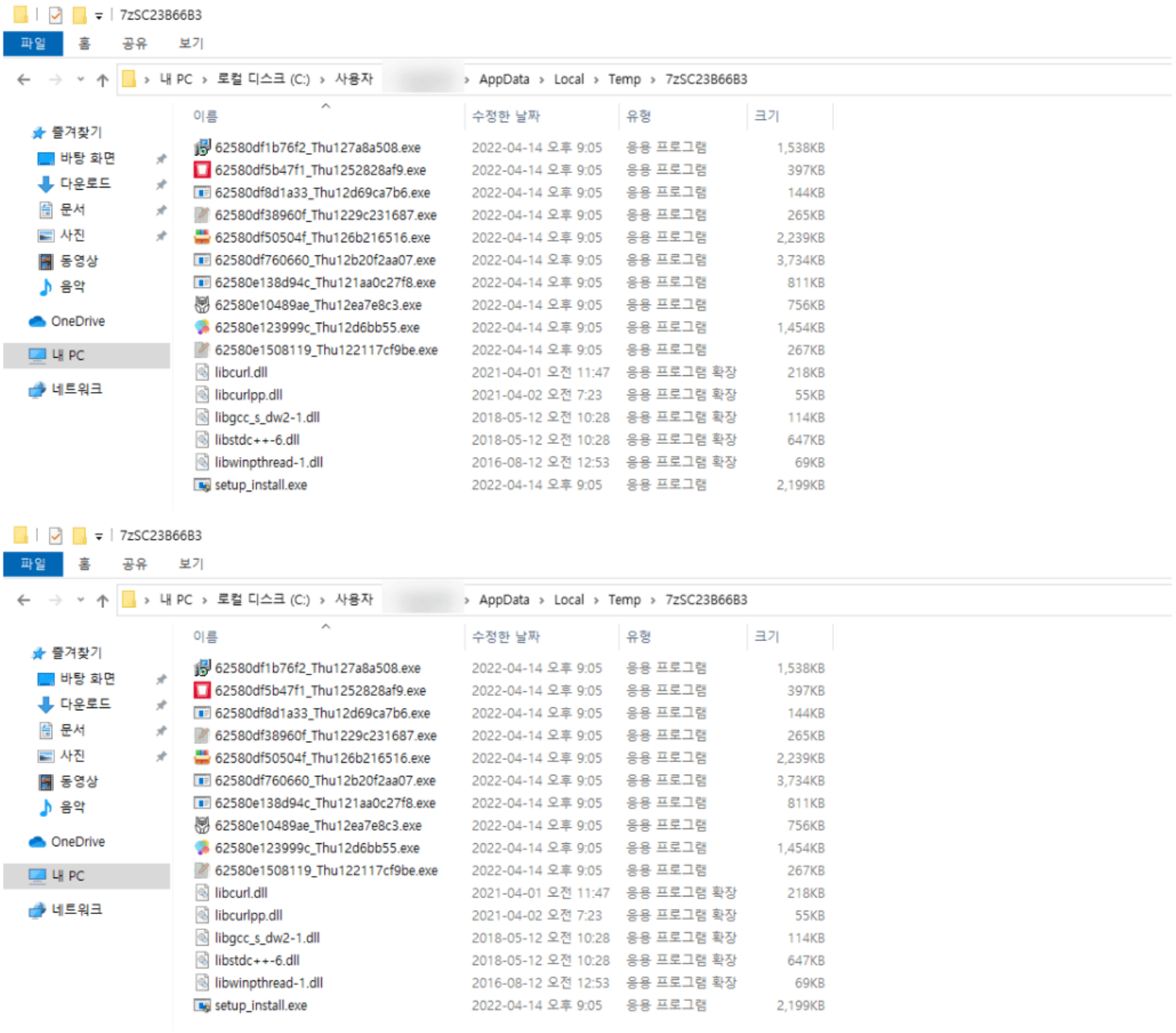

Figure 4. Decompressing setup_installer.exe

The file uses Powershell to set an exclusion for MS Defender on the %TEMP% folder and runs 15 malicious files in order.

```
167  std::operator+<char>(
168    v71,
169    "powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath  \"",
170    tempPath);
171  std::operator+<char>(v70, v71, "\"");
172  std::string::~string(v71);
173  std::string::~string(tempPath);
174  std::allocator<char>::~allocator(&v73);
175  powerShellCode = (const char *)std::string::c_str(v70);
176  v155 = __popen(powerShellCode, "r");
```


```
167  std::operator+<char>(
168    v71,
169    "powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath  \"",
170    tempPath);
171  std::operator+<char>(v70, v71, "\"");
172  std::string::~string(v71);
173  std::string::~string(tempPath);
174  std::allocator<char>::~allocator(&v73);
175  powerShellCode = (const char *)std::string::c_str(v70);
176  v155 = __popen(powerShellCode, "r");
```


Figure 5. Powershell used to set an exclusion for MS Defender

The figure below shows the process explained above.

Figure 6. Process tree

The file distributes various malware types in a package form including info-leaking malware such as AgentTesla, RedLine, and SmokeLoader, downloaders such as BeamWinHTTP, STOP ransomware, etc.

As the malicious files mentioned above are often disguised as installers, users should take caution when downloading files from unknown sources. They should also refrain from downloading illegal software as installing it can infect the system with malware strains.

Users should also update the anti-malware software they are using to the latest version. As for V3 products, you can set the compressed file option to detect the malware type more effectively.

Figure 7. Option for detecting compressed files

AhnLab V3 detects and blocks the malware using the aliases below.

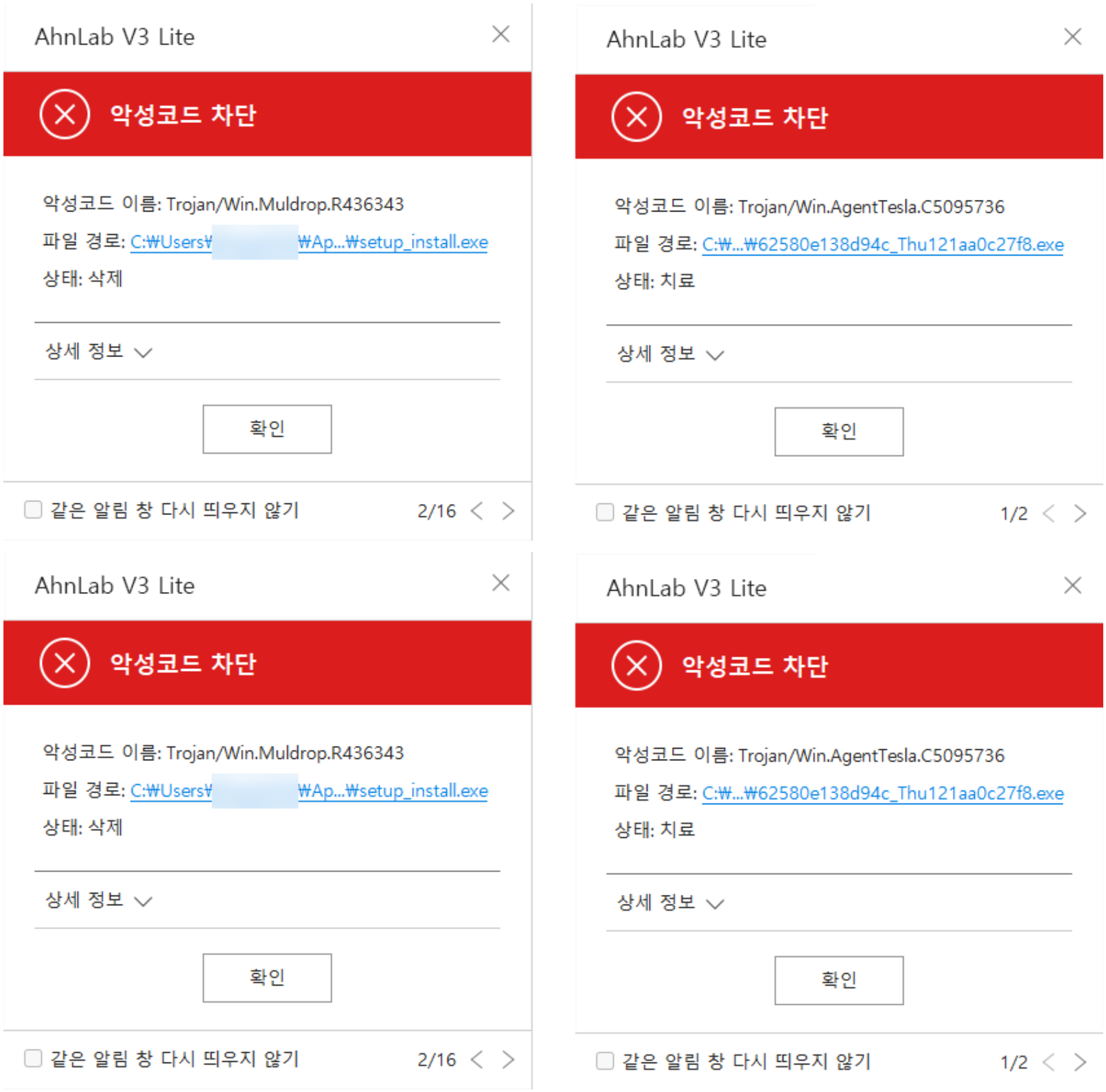

Figure 8. V3 detection information

[File Detection] Trojan/Win.Muldrop.R436343 Trojan/Win.AgentTesla.C5095736 Infostealer/Win.ColdStealer.C5082387 Infostealer/Win.RedLine.C4628732 Ransomware/Win.Stop.R484442

[IOC Info] 1f63405b97e1472330b563644c3e863e 1940b45ad2b6368f3b2a8c53c6bde8c9 f01d8c7ecb9e450748ca65931d9dc7a7 74df6867e4cdecfcaa15349a63b648ac e043798557dc106b7fdd4d0974768edc

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

Categories:Malware Information

Tagged as:ASEC, Installation, malware