ID: 641726
Sample Name: r.exe
Cookbook: default.jbs
Time: 18:54:40
Date: 08/06/2022
Version: 35.0.0 Citrine

Table of Contents

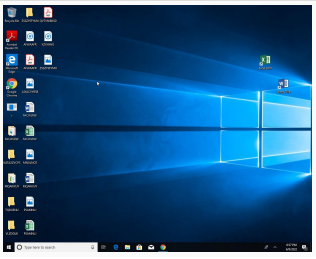
Windows Analysis Report

r.exe

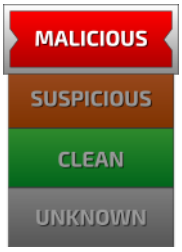
Overview

General Information

Sample Name:	r.exe
Analysis ID:	641726
MD5:	601ccdad5d4329..
SHA1:	d6a142337788d0.
SHA256:	f78aa003a899db..
Tags:	exe
Infos:	



Detection

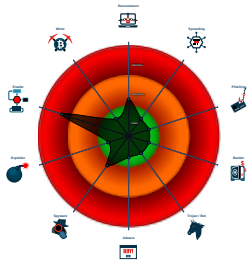


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Queries sensitive video device infor…
- Machine Learning detection for drop…
- Uses schtasks.exe or at.exe to add…
- Disable Windows Defender notificati…
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec

Classification



Process Tree

- **System is w10x64**
- r.exe (PID: 2984 cmdline: "C:\Users\user\Desktop\r.exe" MD5: 601CCDAD5D43290B18CE9C0728E52D38)
  - schtasks.exe (PID: 3396 cmdline: "C:\Windows\System32\schtasks.exe" /create /sc MINUTE /mo 3 /tn "MicrosoftEdgeUpdate" /tr "C:\Users\user\AppData\Roaming\Z\Z.exe" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - conhost.exe (PID: 3968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6476 cmdline: "powershell" Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1 MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Z.exe (PID: 6456 cmdline: C:\Users\user\AppData\Roaming\Z\Z.exe MD5: 601CCDAD5D43290B18CE9C0728E52D38)
  - schtasks.exe (PID: 5096 cmdline: "C:\Windows\System32\schtasks.exe" /create /sc MINUTE /mo 3 /tn "MicrosoftEdgeUpdate" /tr "C:\Users\user\AppData\Roaming\Z\Z.exe" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - conhost.exe (PID: 5168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6372 cmdline: "powershell" Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1 MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Boot Survival

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

Malware Analysis System Evasion

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Lowering of HIPS / PFW / Operating System Security Settings

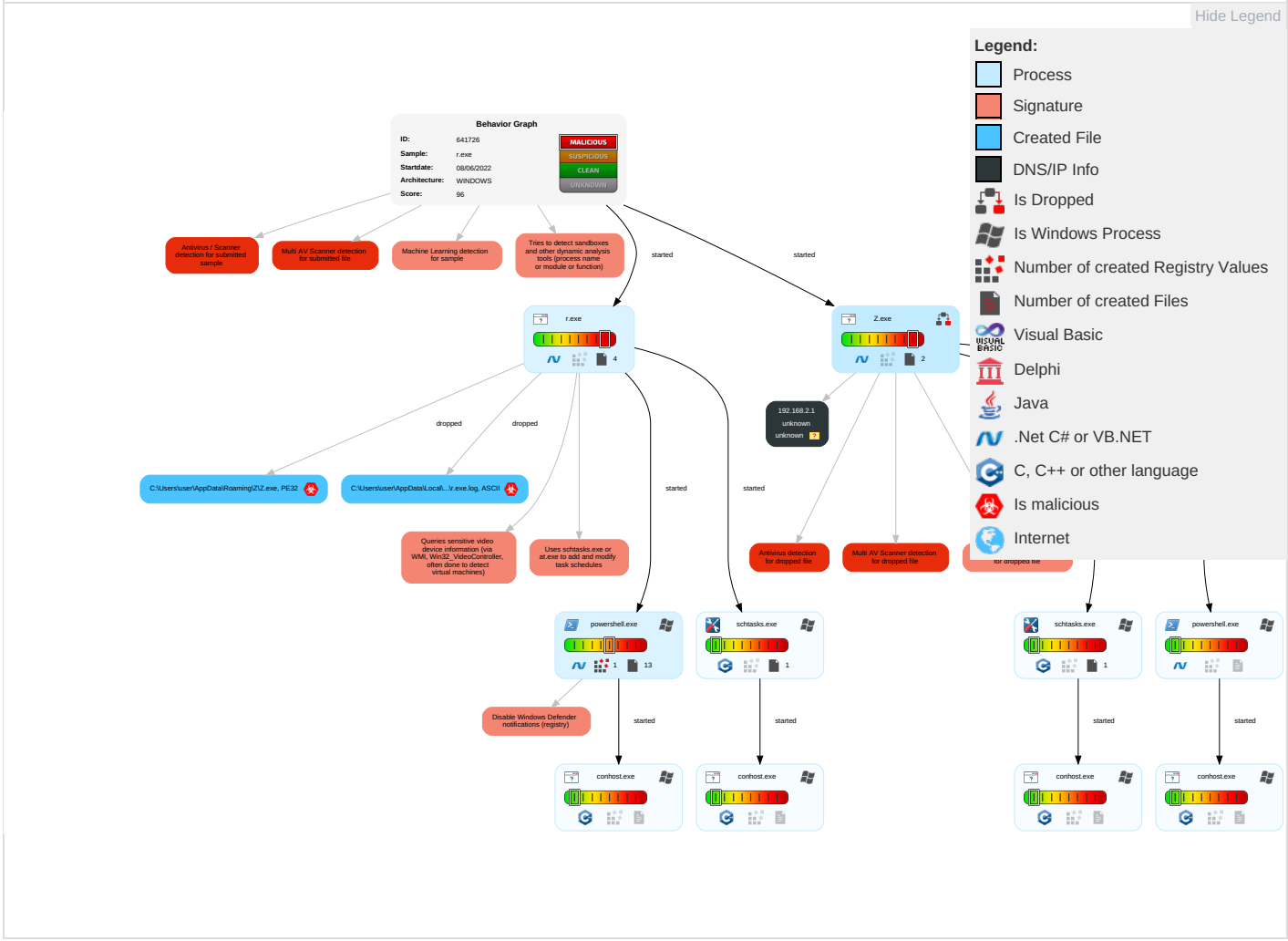
Disable Windows Defender notifications (registry)

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 Scheduled Task/Job	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	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	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	3 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	At (Linux)	Logon Script (Windows)	1 Bypass User Access Control	1 2 1 Virtualization/Sandbox Evasion	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	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 Software Packing	Cached Domain Credentials	1 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	1 Bypass User Access Control	DCSync	1 3 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

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

Source	Detection	Scanner	Label	Link
r.exe	66%	Virustotal		Browse
r.exe	31%	Metadefender		Browse
r.exe	81%	ReversingLabs	Win32.PUA.MiscX	
r.exe	100%	Avira	TR/Dropper.Gen	
r.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Z\Z.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Z\Z.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Z\Z.exe	66%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Z\Z.exe	31%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Z\Z.exe	81%	ReversingLabs	Win32.PUA.MiscX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.Z.exe.7c0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.r.exe.b40000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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/Icon	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

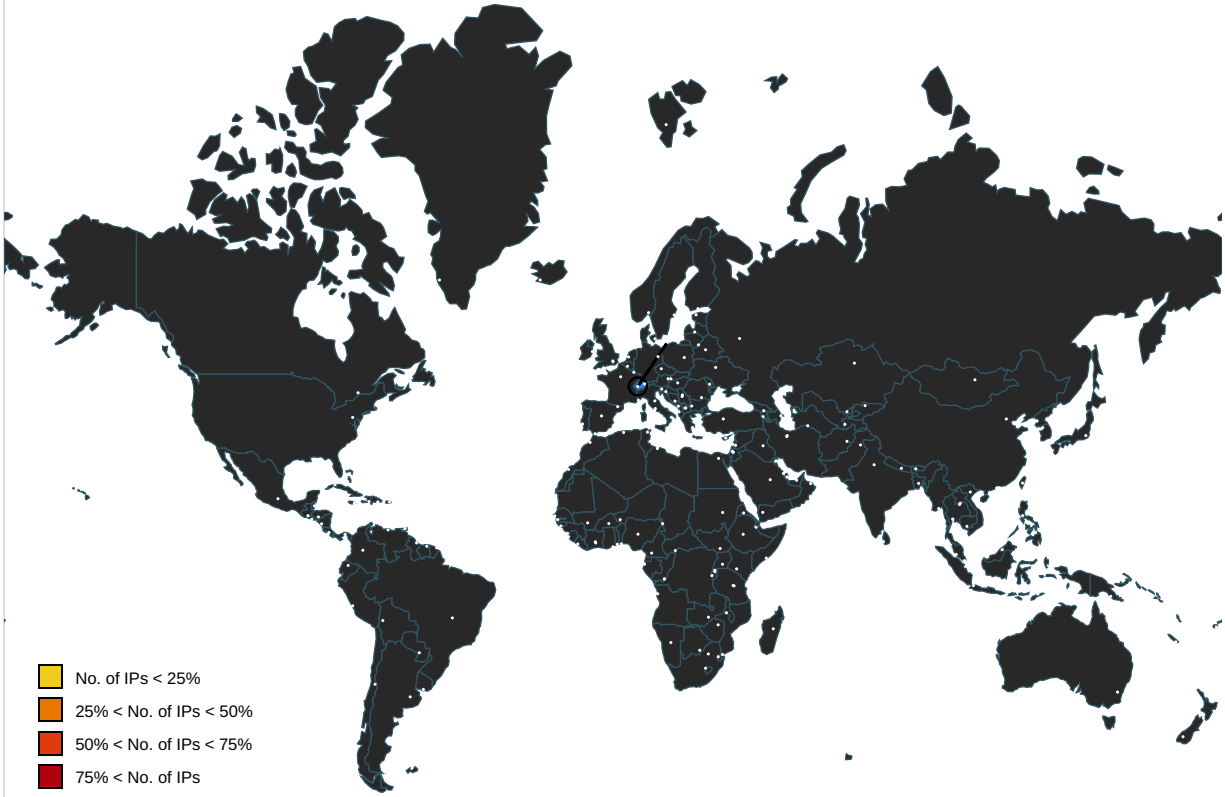
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000006.00000002.474450346.000001F8711B1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000A.00000002.497605055.00000248DA26F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	r.exe, Z.exe.0.dr	false	• URL Reputation: safe	unknown
http://ocsp.sectigo.com0	r.exe, Z.exe.0.dr	false	• URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000A.00000002.489474628.00000248CA412000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000A.00000002.489474628.00000248CA412000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 0000000A.00000002.497605055.00000248DA26F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000006.00000002.474450346.000001F8711B1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000A.00000002.497605055.00000248DA26F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000A.00000002.497605055.00000248DA26F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000A.00000002.497605055.00000248DA26F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	r.exe, Z.exe.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	r.exe, Z.exe.0.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000006.00000002.462161730.000001F861141000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000A.00000002.488556362.00000248CA201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000000A.00000002.489474628.00000248CA412000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	641726
Start date and time: 08/06/202218:54:40	2022-06-08 18:54:40 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	r.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.evad.winEXE@14/10@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, licensing.mp.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target Z.exe, PID 6456 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 6476 because it is empty
- Execution Graph export aborted for target r.exe, PID 2984 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:56:00	Task Scheduler	Run new task: MicrosoftEdgeUpdate path: C:\Users\user\AppData\Roaming\Z\Z.exe
18:56:04	API Interceptor	38x Sleep call for process: powershell.exe modified

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\CLR_v4.0\UsageLogs\Z.exe.log

Process:	C:\Users\user\AppData\Roaming\Z\Z.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1076
Entropy (8bit):	5.359758749701665
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhBsXE4+Y:MxHKn1qHGiD0HKeGiYHKGD8AokH+Y
MD5:	96C02D101311A155C6517E433AED892E
SHA1:	52E393477D5A279909C8FC47A9EFFE9FA8BF964E
SHA-256:	9F20781DB029AA6D5F1F1CCC3EDB3D5D08A5A072AC65D0EFDACF24B9C2F15B28
SHA-512:	361F2E24B3F4BEBB7B5DBE8C61A014EFEEFFA63C8D4F9E2DFC9FD591E9ECAE2FCF089D2C9AD211DA57DCD4D06A91FE232356CD5F532CBBE7D2ACA99C5CA87AD5
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Syst

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\r.exe.log

Process:	C:\Users\user\Desktop\r.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1076
Entropy (8bit):	5.359758749701665
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhBsXE4+Y:MxHKn1qHGiD0HKeGiYHKGD8AokH+Y
MD5:	96C02D101311A155C6517E433AED892E
SHA1:	52E393477D5A279909C8FC47A9EFFE9FA8BF964E
SHA-256:	9F20781DB029AA6D5F1F1CCC3EDB3D5D08A5A072AC65D0EFDACF24B9C2F15B28
SHA-512:	361F2E24B3F4BEBB7B5DBE8C61A014EFEEFFA63C8D4F9E2DFC9FD591E9ECAE2FCF089D2C9AD211DA57DCD4D06A91FE232356CD5F532CBBE7D2ACA99C5CA87AD5
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Syst

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):	1112
Entropy (8bit):	5.261317746785248
Encrypted:	false
SSDEEP:	24:3APpQrLAo4KAxX5qRPD42HOoFe9t4CvKaBPnKyH5X:QPerB4nqRL/HvFe9t4CvpBfnHZ
MD5:	10B3604B711FAAE4E7D98576FF54D22C
SHA1:	FFFE9478665B13C99518C8C5FCC9DF3BC112E507
SHA-256:	283F1509E6EE6F2CBA7EE7B27A6E4D3657E12E025E12DAF8F8EC87DE9A58067B
SHA-512:	10EAC10853F51427C7F79A03FDB09B8330388638AE65753E9790BF3A1B59C49DD185650F9ACB6EA65F66E891D620E2BEC8FA72F45AB3A3BF23DBC97199BDBBA9
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@.....~.....#.Microsoft.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.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ah1ubo23.vbf.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_dmtrlsuy.biy.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_fr1wyhfr.h15.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:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ipc0mrd1.2vr.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:\Users\user\AppData\Roaming\Z\Z.exe

Process:	C:\Users\user\Desktop\r.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4773888
Entropy (8bit):	**7.999198263550714**
Encrypted:	**true**
SSDEEP:	98304:+XjW2zyivc/oHruK4uOQRKRvIgfxgGtaeOwvPDUG2WImwOsxJ:+XjWtivIoHStuOFIIogGc7wvAepwTxJ
MD5:	601CCDAD5D43290B18CE9C0728E52D38
SHA1:	D6A142337788D09E98AF6665EA44899B248E46FD
SHA-256:	F78AA003A899DB2D88065EEFCAD78377325E31BC2F7C4D6CE19E21773CD27D23
SHA-512:	52ACB52A19CF2D74ED7C6FBE8E256E5EEC4856C36B37D4A8025658FDF2F6E4BCFB3CA46BF2DF8761E42A7289DE6E576D8E156B267A493F40E5C20B1FA41C1A22
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 66%, Browse • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[.b.....H.....H.. ....I...@.. .....@I.....@.....<.H.O....I.X..... I..... ....H.....text.....H.. ....H..... ..`.rsrc...X.....I.....H.....@..@.reloc..... I.....H.....@..B.....p.H.....H.....4.H..-.....H;...H.....0.....s&...(%.....&..~....r...p(.....,(.....,..(.....&..~....r...p(.....,(.....,..(.....&..(....-..(....s.....r...po.....o.....o.....r%..p....~.....r...p....~.....r...p...(....o.....(....&..&....(.....&..(.....r...p....~.....r...p....~.....r...p....~.....(.....(....r...pr...po.....(.....r...p....~.....r...p....~.....r...p....~.....

C:\Users\user\Documents\20220608\PowerShell_transcript.932923.1sSVV7rz.20220608185617.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1132
Entropy (8bit):	5.1834370445458635
Encrypted:	false
SSDEEP:	24:BxSApDvBBox2DOXITP+6zoXW1UHjeTKKjX4CIym1ZJXRTP+6zokGnxSAZJi:BZBv/ooOb6zoG1UqDYB1Zy6zokIZZJi
MD5:	27C072763A444EAF1C7DF9052B6EA378
SHA1:	57191F90EA48872BFCE0304C11CDF6DAB721726A
SHA-256:	0F3FC81B21062E48F5D9FC30819869A1D44A7C9B48C5F5E613AEC23816EDAFAC
SHA-512:	CFBE4ACBBC58049AC445BDD42EC2ADC7C2405BAE5DA041964D0AB4C79C0E448448FD2BF90DDBAB88DD0BED02CE4FDEAEB188280086F642D5F1CD3C709D7E3E35
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220608185618..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 932923 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1..Process ID: 6372..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1.. **********..**********..Command start time: 20220608185618..**********..PS>Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1..**********..Command start time: 20220608185717..**********

C:\Users\user\Documents\20220608\PowerShell_transcript.932923.P2yThJ8b.20220608185603.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1132
Entropy (8bit):	5.184362928318124
Encrypted:	false

SSDEEP:	24:BxSARyDvBBox2DOXITP+6zoXW5HjeTKKjX4Clym1ZJXITP+6zooDnxSAZxH:BZUv/ooOb6zoG5qDYB1Zh6zooDZZxH
MD5:	A94CB7CFA9DD7F887D7BF3AB5ECEC8B6
SHA1:	B27EA6935C61E4D9755731417C182E9C4AD63CD5
SHA-256:	FF05687B561107C14453DC6B81F697FF79F2291DBD161C15B21CE3EEA265350D
SHA-512:	3B1FCD7C533FF4625BFB9EBA190A2C04EF9C7394907CFA9B46925DCB6F440389D2DAFD59F255A8AE92062937A42376DEB87BE9CFA10A467A7F3444017C127BD
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220608185604..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 932923 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1..Process ID: 6476..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1.. **********..**********..Command start time: 20220608185604..**********..PS>Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1..**********..Command start time: 20220608185712..**********

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.999198263550714
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.76% • Win32 Executable (generic) a (10002005/4) 49.71% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • UPX compressed Win32 Executable (30571/9) 0.15% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	r.exe
File size:	4773888
MD5:	601ccdad5d43290b18ce9c0728e52d38
SHA1:	d6a142337788d09e98af6665ea44899b248e46fd
SHA256:	f78aa003a899db2d88065eefcad78377325e31bc2f7c4d6ce19e21773cd27d23
SHA512:	52acb52a19cf2d74ed7c6fbe8e256e5eec4856c36b37d4a8025658fdf2f6e4bcfb3ca46bf2df8761e42a7289de6e576d8e156b267a493f40e5c20b1fa41c1a22
SSDEEP:	98304:+XjW2zyivc/oHruK4uOQRKRvlgfxgGtaeOwvPDUG2WImwOsxJ:+XjWtivIoHStuOFIIogGc7wvAepwTxJ
TLSH:	782633E3B48C33ACD4538CB467E5916289B4B089A2E71CFA49C7C13E78E3B578A20D55
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....[.b.....H.....H.. ....I...@.. .....@I.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x88ea8e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x629A5BAC [Fri Jun 3 19:06:20 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x48ea3c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x490000	0x658	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x492000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x48ca94	0x48cc00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x490000	0x658	0x800	False	0.33837890625	data	3.49508042781	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x492000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x4900a0	0x3c4	data		
RT_MANIFEST	0x490468	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

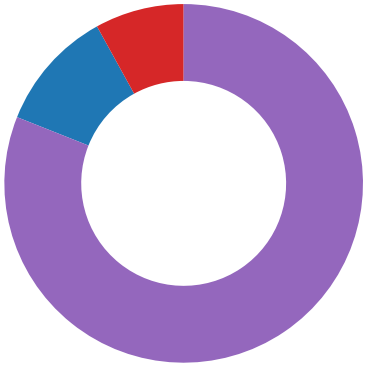
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Microsoft Corporation. All rights reserved.
Assembly Version	0.0.0.0
InternalName	s.exe
FileVersion	0.0.0.0
CompanyName	Microsoft .NET Framework
Comments	Microsoft .NET Services Installation Utility
ProductName	Microsoft Corporation
ProductVersion	0.0.0.0
FileDescription	Installation Utility
OriginalFilename	s.exe

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: r.exe PID: **2984**, Parent PID: **6040**

General

Target ID:	0
Start time:	18:55:52
Start date:	08/06/2022
Path:	C:\Users\user\Desktop\r.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\r.exe"
Imagebase:	0xb40000
File size:	4773888 bytes
MD5 hash:	601CCDAD5D43290B18CE9C0728E52D38
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Analysis Process: schtasks.exe PID: **3396**, Parent PID: **2984**

General

Target ID:	3
Start time:	18:55:58
Start date:	08/06/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\schtasks.exe" /create /sc MINUTE /mo 3 /tn "MicrosoftEdgeUpdate" /tr "C:\Users\user\AppData\Roaming\Z\Z.exe" /f
Imagebase:	0x7ff7cc9d0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
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: 3968, Parent PID: 3396

General

Target ID:	4
Start time:	18:55:59
Start date:	08/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: Z.exe PID: 6456, Parent PID: 1040

General

Target ID:	5
Start time:	18:56:00
Start date:	08/06/2022
Path:	C:\Users\user\AppData\Roaming\Z\Z.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Z\Z.exe
Imagebase:	0x7c0000
File size:	4773888 bytes
MD5 hash:	601CCDAD5D43290B18CE9C0728E52D38
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 66%, Virustotal, Browse • Detection: 31%, Metadefender, Browse • Detection: 81%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Z.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA518886ED	CreateFileW

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:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Z.exe.log	0	1076	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Drawing, Version=4.	success or wait	1	7FFA51888769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA512EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA512EB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA512F2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA513C12E7	ReadFile

Analysis Process: powershell.exe PID: **6476**, Parent PID: **2984**

General

Target ID:	6
Start time:	18:56:01
Start date:	08/06/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"powershell" Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFA5141F1E9	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	7FFA5141F1E9	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	7FFA48ED03FC	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	7FFA48ED03FC	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_dmtrlsuy.biy.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CB06FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ipc0mrd1.2vr.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CB06FDD	CreateFileW
C:\Users\user\Documents\20220608	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4CB0F35D	CreateDirectoryW
C:\Users\user\Documents\20220608\PowerShell_transcript.932923.P2yThJ8b.20220608185603.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CB06FDD	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	7FFA48ED03FC	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	7FFA48ED03FC	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	7FFA48ED03FC	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	7FFA48ED03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_dmtrlsuy.biy.ps1	success or wait	1	7FFA4CB0F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ipc0mrd1.2vr.psm1	success or wait	1	7FFA4CB0F270	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	7FFA48ED9D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dmtrlsuy.biy.ps1	0	1	31	1	success or wait	1	7FFA4CB0B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ipc0mrd1.2vr.psm1	0	1	31	1	success or wait	1	7FFA4CB0B526	WriteFile
C:\Users\user\Documents\20220608\PowerShell_transcript.932923.P2yThJ8b.20220608185603.txt	0	3	ff		success or wait	1	7FFA4CB0B526	WriteFile
C:\Users\user\Documents\20220608\PowerShell_transcript.932923.P2yThJ8b.20220608185603.txt	3	691	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 36 30 38 31 38 35 36 30 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 39 33 32 39 32 33 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77	**********Windows PowerShell transcript startStart time: 20220608185604Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 932923 (Microsoft Windows NT 10.0.17134.0)Host Application: pow	success or wait	11	7FFA4CB0B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9FE5	unknown
unknown	94	138	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFA48ED9FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFA48ED9EED	unknown
unknown	232	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9FE5	unknown
unknown	4446	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFA48ED9FE5	unknown
unknown	177	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9EED	unknown
unknown	7324	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9FE5	unknown
unknown	190	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9EED	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ED9EED	unknown
unknown	216	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA48ECBC97	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 11 00 00 00 09 00 00 00 09 00 09 00 09 00 00 00 00 00 fd 00 05 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFA5183F6E8	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	8'L}	success or wait	15	7FFA5183F6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	7FFA5183F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	9	7FFA5183F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	6c 00 00 03	l	success or wait	1	7FFA5183F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	104	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 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 00 00 24 00 00 00 6a 00 00 00 fd 00 00 00 fd 00 00 00 00 fd 00 00 00 fd 00 00 00 18 00 00 00 57 00 00 00 09 0e fd 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00	"$jW	success or wait	1	7FFA5183F6E8	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	7FFA512EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA512EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA512EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA512EB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA512F2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA512F2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA512F2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA512EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA512EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA512EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA512EB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA512EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA512EB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA513C12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA512D62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFA512D63B9	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA513C12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CB0B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuratio n.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA513C12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4CB0B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4CB0B526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFT WARE\Microsoft\Windows Defender Security Center\Notifications	DisableNotificati ons	dword	1	success or wait	1	7FFA4D1EA911	RegSetValueEx W

Analysis Process: conhost.exe PID: **6460**, Parent PID: **6476**

General

Target ID:	7
Start time:	18:56:02
Start date:	08/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: schtasks.exe PID: **5096**, Parent PID: **6456**

General

Target ID:	8
Start time:	18:56:11
Start date:	08/06/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\schtasks.exe" /create /sc MINUTE /mo 3 /tn "MicrosoftEdgeUpdate" /tr "C:\Users\user\AppData\Roaming\Z\Z.exe" /f
Imagebase:	0x7ff7cc9d0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
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: **5168**, Parent PID: **5096**

General

Target ID:	9
Start time:	18:56:12
Start date:	08/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: powershell.exe PID: **6372**, Parent PID: **6456**

General

Target ID:	10
Start time:	18:56:16
Start date:	08/06/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"powershell" Set-ItemProperty -Path 'HKLM:\\SOFTWARE\\Microsoft\\Windows Defender Security Center\\Notifications' -Name DisableNotifications -Value 1
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **5416**, Parent PID: **6372**

General

Target ID:	12
Start time:	18:56:16
Start date:	08/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly