ID: 1443953
Sample Name:
FGGx944Qu7.exe
Cookbook: default.jbs
Time: 08:04:06
Date: 19/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

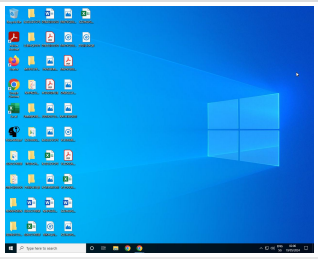
Windows Analysis Report

FGGx944Qu7.exe

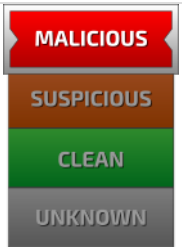
Overview

General Information

Sample name:	FGGx944Qu7.exerena med because original name is a hash value
Original sample name:	21d18e20b8b0…
Analysis ID:	1443953
MD5:	21d18e20b8b0…
SHA1:	bad65794a2bc…
SHA256:	b600c43e2980…
Tags:	32 exe trojan
Infos:	



Detection



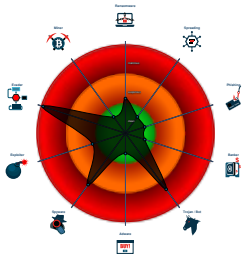
FormBook

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp fil…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains method …
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…

Classification



Process Tree

- **System is w10x64**
- FGGx944Qu7.exe (PID: 7252 cmdline: "C:\Users\user\Desktop\FGGx944Qu7.exe" MD5: 21D18E20B8B0E17E0B554B5940A7AAED)
  - powershell.exe (PID: 7344 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\FGGx944Qu7.exe" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 7352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - powershell.exe (PID: 7400 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 7416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - WmiPrvSE.exe (PID: 7716 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: 60FF40CFD7FB8FE41EE4FE9AE5FE1C51)
  - schtasks.exe (PID: 7424 cmdline: "C:\Windows\System32\schtasks.exe" /Create /TN "Updates\TBsjWljiCpR" /XML "C:\Users\user\AppData\Local\Temp\tmp1454.tmp" MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 7480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - FGGx944Qu7.exe (PID: 7604 cmdline: "C:\Users\user\Desktop\FGGx944Qu7.exe" MD5: 21D18E20B8B0E17E0B554B5940A7AAED)
  - FGGx944Qu7.exe (PID: 7620 cmdline: "C:\Users\user\Desktop\FGGx944Qu7.exe" MD5: 21D18E20B8B0E17E0B554B5940A7AAED)
    - usFxdnRPYjnb.exe (PID: 4460 cmdline: "C:\Program Files (x86)\ATqfrwJeiSEkHpSwLmQcLcKjltaMjYnOwempnyfloVJBHkJly\usFxdnRPYjnb.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
      - SearchProtocolHost.exe (PID: 8040 cmdline: "C:\Windows\SysWOW64\SearchProtocolHost.exe" MD5: 727FE964E574EEAF8917308FFF0880DE)
        - usFxdnRPYjnb.exe (PID: 2492 cmdline: "C:\Program Files (x86)\ATqfrwJeiSEkHpSwLmQcLcKjltaMjYnOwempnyfloVJBHkJly\usFxdnRPYjnb.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
        - firefox.exe (PID: 7468 cmdline: "C:\Program Files\Mozilla Firefox\Firefox.exe" MD5: C86B1BE9ED6496FE0E0CBE73F81D8045)
- TBsjWljiCpR.exe (PID: 7680 cmdline: C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe MD5: 21D18E20B8B0E17E0B554B5940A7AAED)
  - schtasks.exe (PID: 7864 cmdline: "C:\Windows\System32\schtasks.exe" /Create /TN "Updates\TBsjWljiCpR" /XML "C:\Users\user\AppData\Local\Temp\tmp350B.tmp" MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 7872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - TBsjWljiCpR.exe (PID: 7908 cmdline: "C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe" MD5: 21D18E20B8B0E17E0B554B5940A7AAED)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://any.run/cybersecurity-blog/xloader-formbook-encryption-analysis-and-malware-decryption/https://asec.ahnlab.com/en/32149/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.2863758312.0000000003070000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000010.00000002.2863758312.0000000003070000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x2a530:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x13b6f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01
00000010.00000002.2861231272.0000000002A20000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000010.00000002.2861231272.0000000002A20000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x2a530:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x13b6f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01
00000008.00000002.1946159228.0000000001510000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	

Click to see the 12 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.FGGx944Qu7.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
8.2.FGGx944Qu7.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x2da33:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x17072:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01
8.2.FGGx944Qu7.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
8.2.FGGx944Qu7.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x2cc33:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x16272:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01

Sigma Signatures

System Summary

Sigma detected: Powershell Base64 Encoded MpPreference Cmdlet

Sigma detected: Powershell Defender Exclusion

Sigma detected: Suspicious Add Scheduled Task Parent

Sigma detected: Suspicious Schtasks From Env Var Folder

Sigma detected: Non Interactive PowerShell Process Spawned

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Loading BitLocker PowerShell Module

Malware Analysis System Evasion

Yara detected AntiVM3

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Found direct / indirect Syscall (likely to bypass EDR)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file / registry access)

Remote Access Functionality

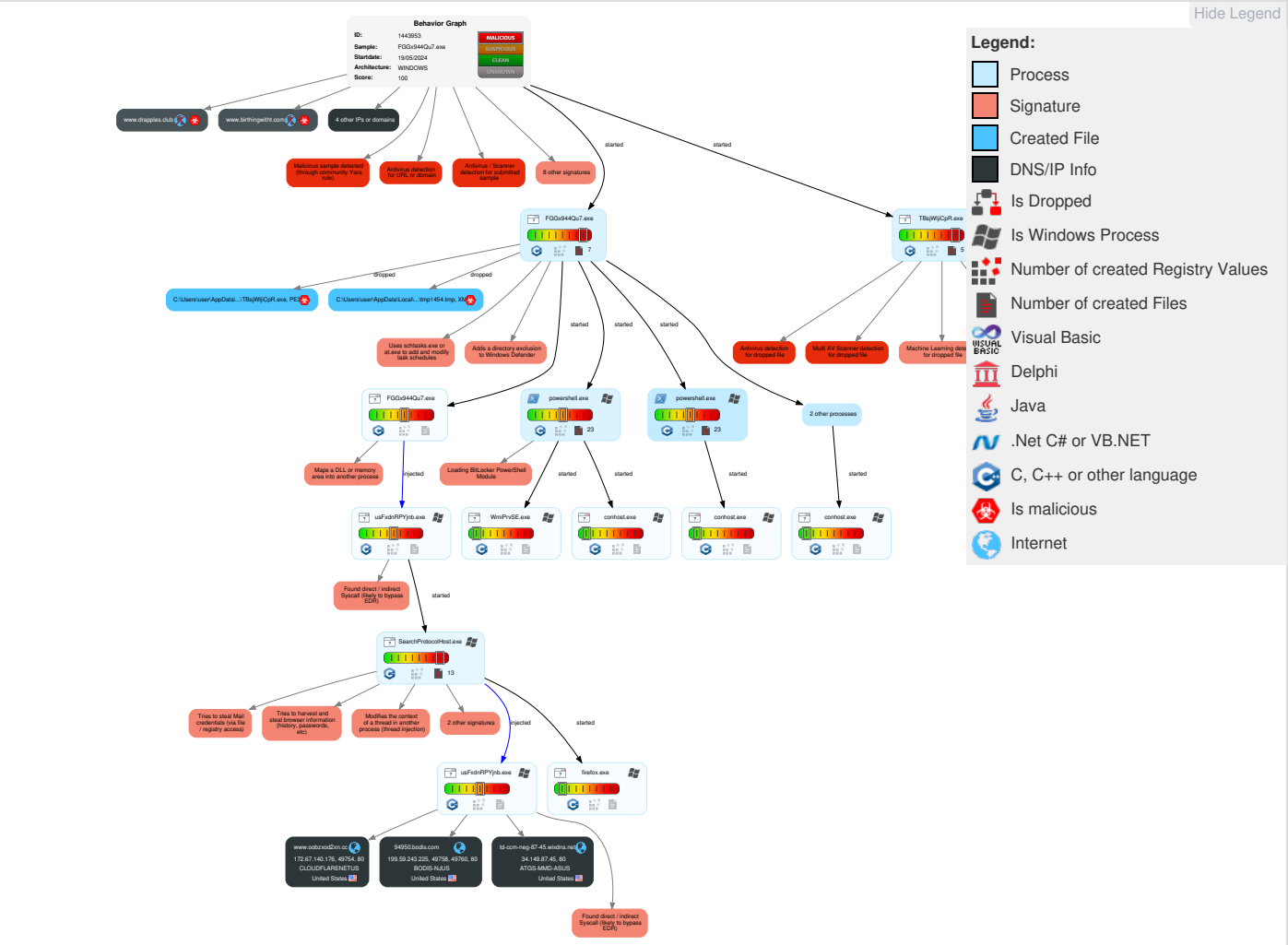
Yara detected FormBook

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	4 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Scheduled Task/Job	1 Modify Registry	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	1 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 Abuse Elevation Control Mechanism	1 1 1 Disable or Modify Tools	Security Account Manager	4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	1 DLL Side-Loading	4 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	3 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	4 1 2 Process Injection	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 Abuse Elevation Control Mechanism	DCSync	Remote System Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	4 Obfuscated Files or Information	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	2 2 Software Packing	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	1 DLL Side-Loading	Network Sniffing	Network Service Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

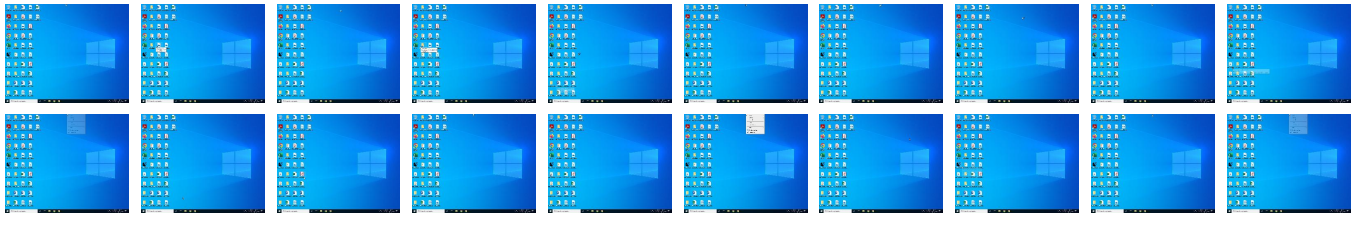
Behavior Graph



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
FGGx944Qu7.exe	62%	ReversingLabs	Win32.Trojan.Nekark	
FGGx944Qu7.exe	67%	Virustotal		Browse
FGGx944Qu7.exe	100%	Avira	HEUR/AGEN.1304432	
FGGx944Qu7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\TBsjWIjiCpR.exe	100%	Avira	HEUR/AGEN.1304432	
C:\Users\user\AppData\Roaming\TBsjWIjiCpR.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\TBsjWIjiCpR.exe	62%	ReversingLabs	Win32.Trojan.Nekark	
C:\Users\user\AppData\Roaming\TBsjWIjiCpR.exe	67%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.oobzxod2xn.cc	2%	Virustotal		Browse
td-ccm-neg-87-45.wixdns.net	0%	Virustotal		Browse
www.drapples.club	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0%	URL Reputation	safe	
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	0%	URL Reputation	safe	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	URL Reputation	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://www.drapples.club/q0r6/	100%	Avira URL Cloud	phishing	
http://https://duckduckgo.com/ac/?q=	0%	Virustotal		Browse
http://www.oobzxod2xn.cc/q0r6/?uZgP=5pyvScKx6ZbOO2uX774/2f03V4PpvoLdLg/OCd1FMvXsxJY7YeHi6SxOzHnr25kvmJZHa8XXHydHc3e54xwdxF+eQrhYMnjeuarocBe7v18XiUqzaWXVlPw=&a6m=8Rw4HDhPzbgPS	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Virustotal		Browse
http://www.drapples.club/q0r6/	0%	Virustotal		Browse
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://www.drapples.club	100%	Avira URL Cloud	phishing	
http://https://duckduckgo.com/chrome_newtab	0%	Virustotal		Browse
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Virustotal		Browse
http://www.drapples.club	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.oobzxod2xn.cc	172.67.140.176	true	false	• 2%, Virustotal, Browse	unknown
94950.bodis.com	199.59.243.225	true	false		unknown
td-ccm-neg-87-45.wixdns.net	34.149.87.45	true	false	• 0%, Virustotal, Browse	unknown
www.birthingwitht.com	unknown	unknown	true		unknown
www.drapples.club	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

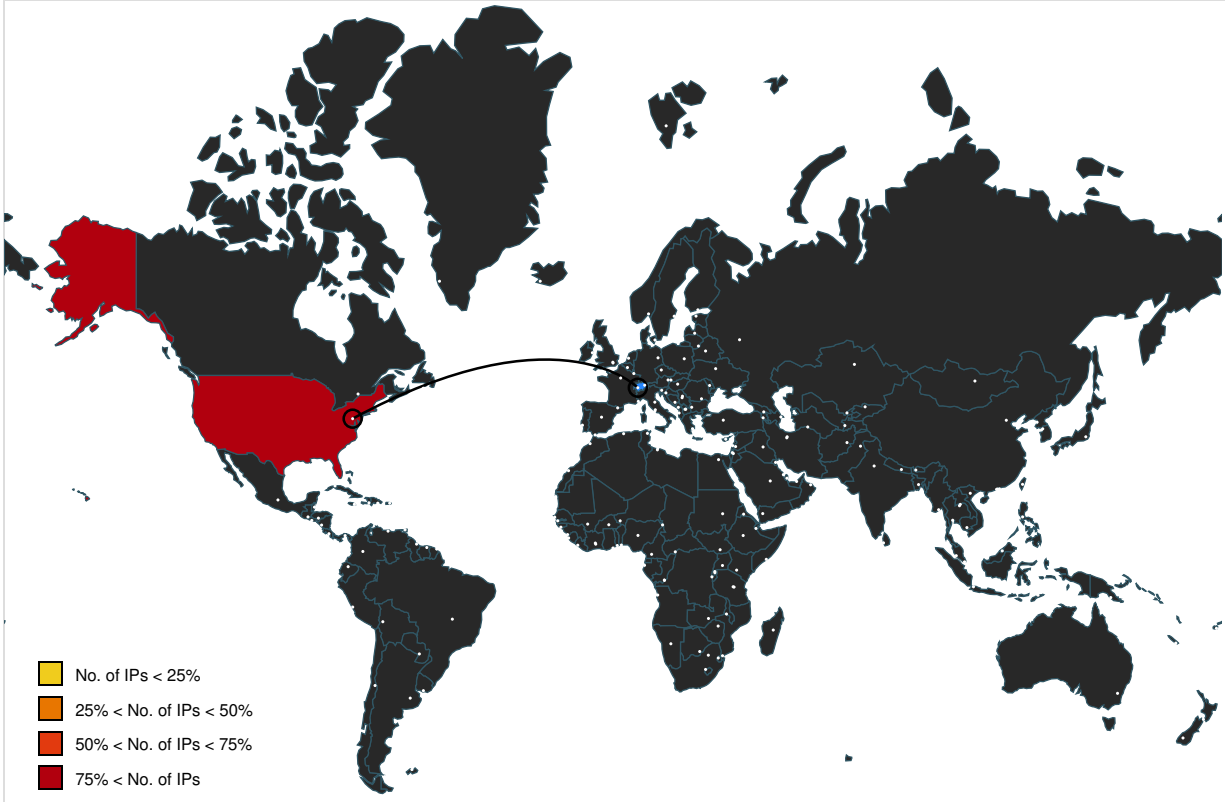
Name	Malicious	Antivirus Detection	Reputation
http://www.oobzxod2xn.cc/q0r6/?uZgP=5pyvScKx6ZbOO2uX774/2f03V4PpvoLdLg/OCd1FMvXsxJY7YeHi6SxOzHnr25kvmJZHa8XXHydHc3e54xwdxF+eQrhYMnjeuarocBe7v18XiUqzaWXVlPw=&a6m=8Rw4HDhPzbgPS	false	• Avira URL Cloud: safe	unknown
http://www.drapples.club/q0r6/	false	• 0%, Virustotal, Browse • Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/chrome_newtab	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.drapples.club	usFxdnRPYjnb.exe, 00000013.00000002.2865 529929.0000000005731000.00000040.8000000 0.00040000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
http://https://www.ecosia.org/newtab/	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	FGGx944Qu7.exe, 00000000.00000002.168885 9188.000000000326F000.00000004.00000800. 00020000.00000000.sdmp, TBsjWljiCpR.exe, 00000009.00000002.1885020055.0000000003 091000.00000004.00000800.00020000.000000 00.sdmp	false	• URL Reputation: safe	unknown
http://https://www.chiark.greenend.org.uk/~sgtatham/putty/0	FGGx944Qu7.exe, TBsjWljiCpR.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	SearchProtocolHost.exe, 00000010.0000000 3.2412246200.0000000007A18000.00000004.0 0000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.140.176	www.oobzxod2xn.cc	United States		13335	CLOUDFLARENETUS	false
34.149.87.45	td-ccm-neg-87-45.wixdns.net	United States		2686	ATGS-MMD-ASUS	false
199.59.243.225	94950.bodis.com	United States		395082	BODIS-NJUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1443953
Start date and time:	2024-05-19 08:04:06 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	FGGx944Qu7.exerenamed because original name is a hash value
Original Sample Name:	21d18e20b8b0e17e0b554b5940a7aaed.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@25/16@6/3
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe
- Excluded IPs from analysis (whitelisted): 20.223.36.55
- Excluded domains from analysis (whitelisted): ocsp.usertrust.com, ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, crl.usertrust.com, arc.trafficmanager.net, iris-de-prod-azsc-v2-neu-b.northeurope.cloudapp.azure.com, arc.msn.com, ocsp.comodoca.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where 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 NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateKey calls found.
- 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
02:04:52	API Interceptor	1x Sleep call for process: FGGx944Qu7.exe modified
02:04:55	API Interceptor	42x Sleep call for process: powershell.exe modified
02:05:00	API Interceptor	1x Sleep call for process: TBsjWljiCpR.exe modified
02:06:05	API Interceptor	1274978x Sleep call for process: SearchProtocolHost.exe modified

Time	Type	Description
07:04:57	Task Scheduler	Run new task: TBsjWljiCpR path: C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe

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_32\UsageLogs\FGGx944Qu7.exe.log

Process:	C:\Users\user\Desktop\FGGx944Qu7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.34331486778365
Encrypted:	false
SSDEEP:	24:MLUE4K5E4KH1qE4qXKDE4KhKiKhPKIE4oKNzKoZAE4Kze0E4x84j:MIHK5HKH1qHiYHKh3oPtHo6hAHKze0HJ
MD5:	1330C80CAAC9A0FB172F202485E9B1E8
SHA1:	86BAFDA4E4AE68C7C3012714A33D85D2B6E1A492
SHA-256:	B6C63ECE799A8F7E497C2A158B1FFC2F5CB4F745A2F8E585F794572B7CF03560
SHA-512:	75A17AB129FE97BBAB36AA2BD66D59F41DB5AFF44A705EF3E4D094EC5FCD056A3ED59992A0AC96C9D0D40E490F8596B07DCA9B60E606B67223867B061D9D0E B2
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df07665 68\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3 ,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Conf iguration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c56193 4e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TBsjWljiCpR.exe.log

Process:	C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.34331486778365
Encrypted:	false
SSDEEP:	24:MLUE4K5E4KH1qE4qXKDE4KhKiKhPKIE4oKNzKoZAE4Kze0E4x84j:MIHK5HKH1qHiYHKh3oPtHo6hAHKze0HJ

MD5:	1330C80CAAC9A0FB172F202485E9B1E8
SHA1:	86BAFDA4E4AE68C7C3012714A33D85D2B6E1A492
SHA-256:	B6C63ECE799A8F7E497C2A158B1FFC2F5CB4F745A2F8E585F794572B7CF03560
SHA-512:	75A17AB129FE97BBAB36AA2BD66D59F41DB5AFF44A705EF3E4D094EC5FCD056A3ED59992A0AC96C9D0D40E490F8596B07DCA9B60E606B67223867B061D9D0E B2
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	2232
Entropy (8bit):	5.380285623575084
Encrypted:	false
SSDEEP:	48:+WSU4xympjgs4Rc9tEoUl8NPZHUl7u1iMugeoM0Uyus:+LHxvCsIcnSKRHmOugU1s
MD5:	EFC6A63D5F23F5AC7FECDFF451741D55
SHA1:	E5D4F71EDFE006A4625D308446757E6F3E218895
SHA-256:	539B0A534102AC5E5F0292C7129D93F1F081ED0D65F40BAC9C6C7E67F1F94983
SHA-512:	13E8224D796FECCC95513E054AD23907138F8C28ABFA6611F534AC1BB7FA1BFCABB452E2EA8EA10B2D311912BEDF3690B2C6304B77D1F669B9438831C99787A 0
Malicious:	false
Preview:	@...e.....@.....P.....1]...E.....j.....(.Microsoft.PowerShell.Commands.ManagementH.....o..b~.D.poM..... .Microsoft.PowerShell.ConsoleHost0.....C.l]..7.s.....System..4.....D...{..|f.....System.Core.D.....4..7..D.#V.....System.Management.Automation<.....i..VdqF...|.....System.Configuration4.....%...K... .....System.Xml..4.....@.[8]'.\.....System.Data.<.....t.,.IG....M.....System.Management...@.....z.U..G...5.f.1.....System.DirectoryServicesH.....WY..2.M.&..g*(g.....Microsoft.PowerShell.Security...L.....*gQ?O.....x5.....#.Microsoft.Management.Infrastructure.<.....V.}...@...i.....System.Transactions.8.....1...L..U;V.<}.....System.Numerics.P.....8..{...@.e..."4.....%.Microsoft.PowerShell.Com

C:\Users\user\AppData\Local\Temp\20291vC

Process:	C:\Windows\SysWOW64\SearchProtocolHost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1k4wtsks.qys.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D

SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1rfx4p55.jzt.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2odq22e3.wb2.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uya4cokv.3zx.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wftn1kob.rrm.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX

MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wms5kunf.vwh.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ys2tmhij.gni.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zuw0b1st.zey.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\tmp1454.tmp

Process:	C:\Users\user\Desktop\FGGx944Qu7.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1577
Entropy (8bit):	5.1110539282546625

Encrypted:	false
SSDEEP:	24:2di4+S2qh11hXy1mvWUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaIGLxvn:cge1wYrFdOFzOzN33ODOiDdKrsuTev
MD5:	F5A32EE27570DB7ED724677268C9778B
SHA1:	55270ECB864E0F02B8258C440A06DF27ECC02C6F
SHA-256:	62FE36F805962CBB20FFA8616A8B37F2FF5628B6B64F65523EA4753B13D76FB6
SHA-512:	C4A42E20B48849299807A98728C0CB3DC1286223F4C3BF0D430DCDA25F1E28BC7CC8273B0524FCC61613A138D0155D5917DE335601D649DB4893B448B9B8045
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Local\Temp\tmp350B.tmp

Process:	C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1577
Entropy (8bit):	5.1110539282546625
Encrypted:	false
SSDEEP:	24:2di4+S2qh11hXy1mvWUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaIGLxvn:cge1wYrFdOFzOzN33ODOiDdKrsuTev
MD5:	F5A32EE27570DB7ED724677268C9778B
SHA1:	55270ECB864E0F02B8258C440A06DF27ECC02C6F
SHA-256:	62FE36F805962CBB20FFA8616A8B37F2FF5628B6B64F65523EA4753B13D76FB6
SHA-512:	C4A42E20B48849299807A98728C0CB3DC1286223F4C3BF0D430DCDA25F1E28BC7CC8273B0524FCC61613A138D0155D5917DE335601D649DB4893B448B9B8045
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe

Process:	C:\Users\user\Desktop\FGGx944Qu7.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	758280
Entropy (8bit):	7.978851063770012
Encrypted:	false
SSDEEP:	12288:CdrLbDZaNRp7+ur4n+Hriagc4UHQlb/xk/ouztXHUT5izyRnA37CB9CdkR:cLDZMRpQnari1c4NR/Wouzt3AkMnA+sA
MD5:	21D18E20B8B0E17E0B554B5940A7AAED
SHA1:	BAD65794A2BC8C23D373F82E11978F11AF1AF57D
SHA-256:	B600C43E2980691952532A79E7A0AEF2351AEEF6F740FD2F56647509C93B6DA0
SHA-512:	D08D0F4D86EABB1C1EC5CDA10675794C0A82E8574E2F5DCB5B56330FF6AFC5AAB94FFBE328B316038ADC5F810DF429D6B6A1DC7842280D3B6072C0F24FBCFCB1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 62% • Antivirus: Virustotal, Detection: 67%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ff.....0..8..."......W... ...`....@.. ..@.....V..O....`.....\...6..... ....H.....text....7... ...8..... ..`.rsrc.....`.... ...:.....@..@.rel oc.....Z.....@..B.....V.....H.....t?..X;.....(....z.....{....*"..}....*....0.....(2...o.....+..*....0..... @B...(2...o.....(....[.+..*....0..v... .....s.....{....o....o.....+4.o....t.....o.....(....(.....,...t....o!.....o"...-....u.....,...o#.....+...*.....@Y.....0.....(@...ol....+..*.0.....($....+..*.0.....{....o%....+..*....0.... .....(@...oA....+..*.0..... ....(&....+..*..0.."...

C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\FGGx944Qu7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.978851063770012
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	FGGx944Qu7.exe
File size:	758'280 bytes
MD5:	21d18e20b8b0e17e0b554b5940a7aaed
SHA1:	bad65794a2bc8c23d373f82e11978f11af1af57d
SHA256:	b600c43e2980691952532a79e7a0aef2351aeef6f740fd2f56647509c93b6da0
SHA512:	d08d0f4d86eabb1c1ec5cda10675794c0a82e8574e2f5dcb5b56330ff6afc5aab94ffbe328b316038adc5f810df429d6b6a1dc7842280d3b6072c0f24fbcfcb1
SSDEEP:	12288:CdrLbDZaNRp7+ur4n+Hriagc4UHQlb/xk/ouztXHUT5izyRnA37CB9CdkR:cLDZMRpQnari1c4NR/Wouzt3AkMnA+sA
TLSH:	B4F423DBAB74E121DA310F35E4F0AB0563724C948A5ED359A9F050D98E97FE0A7118CF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ff.....0..8..."".....W... ...`....@.. .....@.....

File Icon

Icon Hash:	1fb3b1a50d818f8c

Static PE Info

General

Entrypoint:	0x4b570e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6646D806 [Fri May 17 04:07:34 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=COMODO RSA Code Signing CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 12/11/2018 19:00:00 08/11/2021 18:59:59
Subject Chain	• CN=Simon Tatham, O=Simon Tatham, L=Cambridge, S=Cambridgeshire, C=GB
Version:	3
Thumbprint MD5:	DABD77E44EF6B3BB91740FA46696B779
Thumbprint SHA-1:	5B9E273CF11941FD8C6BE3F038C4797BBE884268
Thumbprint SHA-256:	4CD3325617EBB63319BA6E8F2A74B0B8CCA58920B48D8026EBCA2C756630D570
Serial:	7C1118CBBADC95DA3752C46E47A27438

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

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
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	0xb56bc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x1ecc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0xb5c00	0x3608	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb3714	0xb3800	7aeb3253edbbbe13f9349ed13a4771f0	False	0.9753587983112814	SysEx File -	7.9850458366692925	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x1ecc	0x2000	fbd839ddcd3fbbcfef5b4728eca5bd52	False	0.7943115234375	data	7.26218700052124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	db433f0180eff3050b24cbe2b1f454f3	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

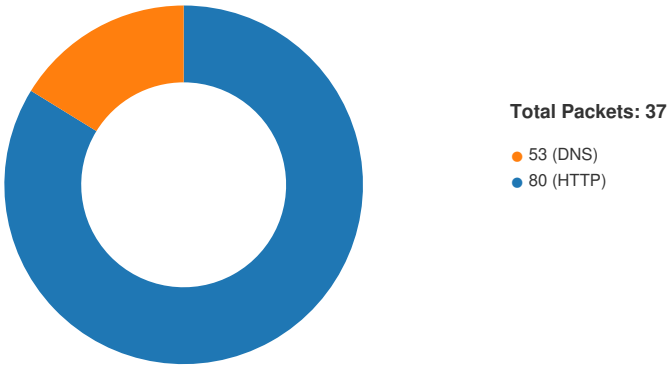
Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0xb6100	0x1725	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced			0.939915611814346
RT_GROUP_ICON	0xb7838	0x14	data			1.05
RT_VERSION	0xb785c	0x470	data			0.4234154929577465
RT_MANIFEST	0xb7cdc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5489795918367347

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 08:05:40.644273996 CEST	49745	80	192.168.2.4	34.149.87.45
May 19, 2024 08:05:41.632376909 CEST	49745	80	192.168.2.4	34.149.87.45
May 19, 2024 08:05:43.632159948 CEST	49745	80	192.168.2.4	34.149.87.45
May 19, 2024 08:05:47.632127047 CEST	49745	80	192.168.2.4	34.149.87.45
May 19, 2024 08:05:55.647808075 CEST	49745	80	192.168.2.4	34.149.87.45
May 19, 2024 08:06:06.686194897 CEST	49754	80	192.168.2.4	172.67.140.176
May 19, 2024 08:06:06.697779894 CEST	80	49754	172.67.140.176	192.168.2.4
May 19, 2024 08:06:06.698401928 CEST	49754	80	192.168.2.4	172.67.140.176
May 19, 2024 08:06:06.700943947 CEST	49754	80	192.168.2.4	172.67.140.176
May 19, 2024 08:06:06.712096930 CEST	80	49754	172.67.140.176	192.168.2.4
May 19, 2024 08:06:06.712138891 CEST	80	49754	172.67.140.176	192.168.2.4
May 19, 2024 08:06:06.713218927 CEST	49754	80	192.168.2.4	172.67.140.176
May 19, 2024 08:06:06.714392900 CEST	49754	80	192.168.2.4	172.67.140.176
May 19, 2024 08:06:06.726528883 CEST	80	49754	172.67.140.176	192.168.2.4
May 19, 2024 08:06:06.726536036 CEST	80	49754	172.67.140.176	192.168.2.4
May 19, 2024 08:06:21.783179045 CEST	49758	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:22.788397074 CEST	49758	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:24.788537979 CEST	49758	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:28.788404942 CEST	49758	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:28.843334913 CEST	80	49758	199.59.243.225	192.168.2.4
May 19, 2024 08:06:28.843456030 CEST	49758	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:28.845993042 CEST	49758	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:28.898433924 CEST	80	49758	199.59.243.225	192.168.2.4
May 19, 2024 08:06:28.898443937 CEST	80	49758	199.59.243.225	192.168.2.4
May 19, 2024 08:06:28.898515940 CEST	49758	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:28.910650015 CEST	80	49758	199.59.243.225	192.168.2.4
May 19, 2024 08:06:31.369384050 CEST	49760	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:32.382164001 CEST	49760	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:34.397778988 CEST	49760	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:34.410768032 CEST	80	49760	199.59.243.225	192.168.2.4
May 19, 2024 08:06:34.410866022 CEST	49760	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:34.412725925 CEST	49760	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:34.420372009 CEST	80	49760	199.59.243.225	192.168.2.4
May 19, 2024 08:06:34.420394897 CEST	80	49760	199.59.243.225	192.168.2.4
May 19, 2024 08:06:36.948486090 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:37.960351944 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:39.960347891 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:43.991570950 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:51.991668940 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:06:59.010922909 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:07:00.023277998 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:07:02.038575888 CEST	49761	80	192.168.2.4	199.59.243.225
May 19, 2024 08:07:06.038486958 CEST	49761	80	192.168.2.4	199.59.243.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 08:05:39.581056118 CEST	64510	53	192.168.2.4	1.1.1.1
May 19, 2024 08:05:40.585340977 CEST	64510	53	192.168.2.4	1.1.1.1
May 19, 2024 08:05:40.638453960 CEST	53	64510	1.1.1.1	192.168.2.4
May 19, 2024 08:05:59.992341995 CEST	49195	53	192.168.2.4	1.1.1.1
May 19, 2024 08:06:00.992129087 CEST	49195	53	192.168.2.4	1.1.1.1
May 19, 2024 08:06:01.158293962 CEST	53	49195	1.1.1.1	192.168.2.4
May 19, 2024 08:06:06.668118000 CEST	62821	53	192.168.2.4	1.1.1.1
May 19, 2024 08:06:06.683228970 CEST	53	62821	1.1.1.1	192.168.2.4
May 19, 2024 08:06:21.760849953 CEST	63578	53	192.168.2.4	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2024 08:06:21.780852079 CEST	53	63578	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 19, 2024 08:05:39.581056118 CEST	192.168.2.4	1.1.1.1	0x3fa2	Standard query (0)	www.birthingwitht.com	A (IP address)	IN (0x0001)	false
May 19, 2024 08:05:40.585340977 CEST	192.168.2.4	1.1.1.1	0x3fa2	Standard query (0)	www.birthingwitht.com	A (IP address)	IN (0x0001)	false
May 19, 2024 08:05:59.992341995 CEST	192.168.2.4	1.1.1.1	0x64dd	Standard query (0)	www.birthingwitht.com	A (IP address)	IN (0x0001)	false
May 19, 2024 08:06:00.992129087 CEST	192.168.2.4	1.1.1.1	0x64dd	Standard query (0)	www.birthingwitht.com	A (IP address)	IN (0x0001)	false
May 19, 2024 08:06:06.668118000 CEST	192.168.2.4	1.1.1.1	0x1301	Standard query (0)	www.oobzxod2xn.cc	A (IP address)	IN (0x0001)	false
May 19, 2024 08:06:21.760849953 CEST	192.168.2.4	1.1.1.1	0xbad3	Standard query (0)	www.drapples.club	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 19, 2024 08:05:40.638453960 CEST	1.1.1.1	192.168.2.4	0x3fa2	No error (0)	www.birthingwitht.com	cdn1.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
May 19, 2024 08:05:40.638453960 CEST	1.1.1.1	192.168.2.4	0x3fa2	No error (0)	cdn1.wixdns.net	td-ccm-neg-87-45.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
May 19, 2024 08:05:40.638453960 CEST	1.1.1.1	192.168.2.4	0x3fa2	No error (0)	td-ccm-neg-87-45.wixdns.net		34.149.87.45	A (IP address)	IN (0x0001)	false
May 19, 2024 08:06:01.158293962 CEST	1.1.1.1	192.168.2.4	0x64dd	No error (0)	www.birthingwitht.com	cdn1.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
May 19, 2024 08:06:01.158293962 CEST	1.1.1.1	192.168.2.4	0x64dd	No error (0)	cdn1.wixdns.net	td-ccm-neg-87-45.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
May 19, 2024 08:06:01.158293962 CEST	1.1.1.1	192.168.2.4	0x64dd	No error (0)	td-ccm-neg-87-45.wixdns.net		34.149.87.45	A (IP address)	IN (0x0001)	false
May 19, 2024 08:06:06.683228970 CEST	1.1.1.1	192.168.2.4	0x1301	No error (0)	www.oobzxod2xn.cc		172.67.140.176	A (IP address)	IN (0x0001)	false
May 19, 2024 08:06:06.683228970 CEST	1.1.1.1	192.168.2.4	0x1301	No error (0)	www.oobzxod2xn.cc		104.21.54.171	A (IP address)	IN (0x0001)	false
May 19, 2024 08:06:21.780852079 CEST	1.1.1.1	192.168.2.4	0xbad3	No error (0)	www.drapples.club	94950.bodis.com		CNAME (Canonical name)	IN (0x0001)	false
May 19, 2024 08:06:21.780852079 CEST	1.1.1.1	192.168.2.4	0xbad3	No error (0)	94950.bodis.com		199.59.243.225	A (IP address)	IN (0x0001)	false

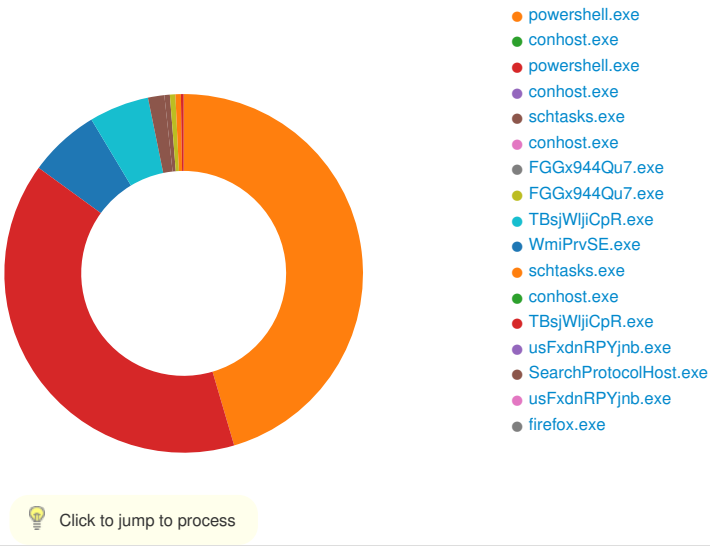
HTTP Request Dependency Graph

- www.oobzxod2xn.cc
- www.drapples.club

Statistics

Behavior

- FGGx944Qu7.exe



System Behavior

Analysis Process: FGGx944Qu7.exe PID: **7252**, Parent PID: **2580**

General

Target ID:	0
Start time:	02:04:51
Start date:	19/05/2024
Path:	C:\Users\user\Desktop\FGGx944Qu7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FGGx944Qu7.exe"
Imagebase:	0xba0000
File size:	758'280 bytes
MD5 hash:	21D18E20B8B0E17E0B554B5940A7AAED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: powershell.exe PID: **7344**, Parent PID: **7252**

General

Target ID:	1
Start time:	02:04:54
Start date:	19/05/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\FGGx944Qu7.exe"
Imagebase:	0xf90000
File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zuw0b1st.zey.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	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	1	6BC78290	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	6BC78290	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ys2tmhij.gni.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW
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	72BBF4C3	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	72BBF4C3	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	5	6BC78290	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	5	6BC78290	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wms5kunf.vwh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1rfx4p55.jzt.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	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	1	6BC78290	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	6BC78290	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	6BC78290	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	8	6BC78290	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	8	6BC78290	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zuw0b1st.zey.ps1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ys2tmhij.gni.psm1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wms5kunf.vwh.ps1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1rfx4p55.jzt.psm1	success or wait	1	71A8E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zuw0b1st.zey.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ys2tmhij.gni.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wms5kunf.vwh.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1rfx4p55.jzt.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 00 00 00 14 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 01 09 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	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	50 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 7f 31 5d 13 fd fd 45 fd 31 a4 86 08 6a 00 00 00 0e 00 28 00	P1]Ej(	success or wait	17	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	40	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6d 6d 61 6e 64 73 2e 4d 61 6e 61 67 65 6d 65 6e 74	Microsoft.PowerShell.Commands.Management	success or wait	17	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	262	2	00 00		success or wait	11	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	28 04 00 03	(	success or wait	1	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	1060	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 0c fd 00 08 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 00 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 19 02 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 07 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 0a 40 00 fd 0a 40 00 fd 01 40 00 0d 02 40 00 10 0d fd 00 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 21 01 40 10 3c 01 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40	@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@!@<@@@@@@@@@@@	success or wait	1	72F876C2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403 a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BD738A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BD738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BD738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb3 78ec07#\bc6fa6cbc82ba7e8e7f31ce87cd85b5f\Microsoft.PowerShel l.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d 1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8 b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa5 7fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.A utomation.ni.dll.aux	0	2764	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	0	64	success or wait	1	72BCB174	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	0	1300	success or wait	1	72BCB27D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuratio n.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\20 62ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\1 b8c564fd69668e6e62d136259980d9e\System.Data.ni.dll.aux	0	1540	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manage ment\96012833bebd5f21714fc508603cda97\System.Management.ni.d ll.aux	0	764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired1 3b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectorySer vices.ni.dll.aux	0	752	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Managemen t.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numeri cs\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f 792626#\fa050a0a5a69ea7573ca6cbffc254e14\Microsoft.PowerShel l.Security.ni.dll.aux	0	1268	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transa ctions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions. ni.dll.aux	0	924	success or wait	1	72B60842	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	0	492	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	0	4096	end of file	1	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	4	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.A9acaf597#\28d73b1a02dd10f20826df677fab36e2\Microsoft.AppV.AppvClientComConsumer.ni.dll.aux	0	712	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\ee7238e0e97151da928155502d6b496b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\48ee4ec9441351bbe4d9095c96b8ea01\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	73	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	444	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	160	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	417	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	4096	success or wait	16	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	950	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	success or wait	12	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	488	end of file	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	end of file	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	113	end of file	1	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	114	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	191	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	0	4096	end of file	1	71A89B71	ReadFile

Registry Activities

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

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

Analysis Process: conhost.exe PID: **7352**, Parent PID: **7344**

General

Target ID:	2
Start time:	02:04:54
Start date:	19/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **7400**, Parent PID: **7252**

General

Target ID:	3
Start time:	02:04:54
Start date:	19/05/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\TBsjWIjiCpR.exe"
Imagebase:	0xf90000
File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wftn1kob.rrm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2odq22e3.wb2.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	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	1	6BC78290	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	6BC78290	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	72BBF4C3	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	72BBF4C3	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	5	6BC78290	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	5	6BC78290	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1k4wtsks.qys.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uya4cokv.3zx.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71A88792	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	1	6BC78290	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	6BC78290	unknown

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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	6BC78290	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	8	6BC78290	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	8	6BC78290	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wftn1kob.rrm.ps1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2odq22e3.wb2.psm1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1k4wtsks.qys.ps1	success or wait	1	71A8E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uya4cokv.3zx.psm1	success or wait	1	71A8E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wftn1kob.rrm.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2odq22e3.wb2.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1k4wtsks.qys.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uya4cokv.3zx.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	71A89B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 00 00 00 14 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 01 09 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	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	50 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 7f 31 5d 13 fd fd 45 fd 31 a4 86 08 6a 00 00 00 0e 00 28 00	P1]Ej(	success or wait	17	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	40	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6d 6d 61 6e 64 73 2e 4d 61 6e 61 67 65 6d 65 6e 74	Microsoft.PowerShell.Commands.Management	success or wait	17	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	262	2	00 00		success or wait	11	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	28 04 00 03	(	success or wait	1	72F876C2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	1060	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 0c fd 00 08 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 00 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 19 02 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 07 0e fd 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 01 40 00 fd 0a 40 00 fd 0a 40 00 fd 01 40 00 0d 02 40 00 10 0d fd 00 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 21 01 40 10 3c 01 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40 10 fd 00 40	@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@!@<@@@@@@@@@@@	success or wait	1	72F876C2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BD738A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BD738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BD738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BD738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb378ec07#\bc6fa6cbc82ba7e8e7f31ce87cd85b5f\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	72BCB174	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	1300	success or wait	1	72BCB27D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\1b8c564fd69668e6e62d136259980d9e\System.Data.ni.dll.aux	0	1540	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f792626#\fa050a0a5a69ea7573ca6cbffc254e14\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	72B60842	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	5	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	4	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	5	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	3	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	149	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	2	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	0	990	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	2	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.A9acaf597#\28d73b1a02dd10f20826df677fab36e2\Microsoft.AppV.AppvClientComConsumer.ni.dll.aux	0	712	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	success or wait	2	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	641	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	0	4096	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	success or wait	6	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	0	4096	end of file	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\ee7238e0e97151da928155502d6b496b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\48ee4ec9441351bbe4d9095c96b8ea01\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	72B60842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	72BBCBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	278	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	success or wait	3	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	768	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	success or wait	73	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	104	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	444	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	success or wait	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	309	end of file	2	71A89B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	0	4096	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	767	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	success or wait	20	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	417	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	0	4096	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	488	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	success or wait	4	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	986	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	success or wait	8	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	994	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	0	4096	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	success or wait	8	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	113	end of file	2	71A89B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	0	4096	end of file	2	71A89B71	ReadFile

Analysis Process: conhost.exe PID: **7416**, Parent PID: **7400**

General

Target ID:	4
Start time:	02:04:54
Start date:	19/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: **7424**, Parent PID: **7252**

General	
Target ID:	5
Start time:	02:04:55
Start date:	19/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\TBsjWljiCpR" /XML "C:\Users\user\AppData\Local\Temp\tmp1454.tmp"
Imagebase:	0x4b0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1454.tmp	0	2	success or wait	1	4BB43E	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1454.tmp	0	1578	success or wait	1	4BB4E3	ReadFile

Analysis Process: conhost.exe PID: **7480**, Parent PID: **7424**

General	
Target ID:	6
Start time:	02:04:55
Start date:	19/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: FGGx944Qu7.exe PID: **7604**, Parent PID: **7252**

General	
Target ID:	7
Start time:	02:04:55
Start date:	19/05/2024
Path:	C:\Users\user\Desktop\FGGx944Qu7.exe

Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\FGGx944Qu7.exe"
Imagebase:	0x370000
File size:	758'280 bytes
MD5 hash:	21D18E20B8B0E17E0B554B5940A7AAED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Analysis Process: FGGx944Qu7.exe PID: **7620**, Parent PID: **7252**

General

Target ID:	8
Start time:	02:04:55
Start date:	19/05/2024
Path:	C:\Users\user\Desktop\FGGx944Qu7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FGGx944Qu7.exe"
Imagebase:	0xb30000
File size:	758'280 bytes
MD5 hash:	21D18E20B8B0E17E0B554B5940A7AAED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.1946159228.0000000001510000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.1946159228.0000000001510000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.1945331228.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.1945331228.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.1948193173.0000000003810000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.1948193173.0000000003810000.00000040.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low
Has exited:	true

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1699896	success or wait	1	40A5D3	NtReadFile
C:\Windows\SysWOW64\SearchProtocolHost.exe	0	340992	success or wait	1	40A5D3	NtReadFile

Analysis Process: TBsjWljiCpR.exe PID: **7680**, Parent PID: **1044**

General

Target ID:	9
Start time:	02:04:57
Start date:	19/05/2024
Path:	C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe
Imagebase:	0xc30000
File size:	758'280 bytes
MD5 hash:	21D18E20B8B0E17E0B554B5940A7AAED
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 62%, ReversingLabs • Detection: 67%, Virustotal, Browse
Reputation:	low
Has exited:	true

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	72BBF4C3	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	72BBF4C3	unknown
C:\Users\user\AppData\Local\Temp\tmp350B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	720B246F	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TBsjWljiCpR.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7303A0B7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp350B.tmp	success or wait	1	71A8E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp350B.tmp	0	1577	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 4a 4f 4e 45 53 2d 50 43 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 3c 54 72 69 67 67	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>user-PC\user</Author> </RegistrationInfo> <Trigg	success or wait	1	71A89B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TBsjWIjiCpR.exe.log	0	1216	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7303A147	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B60842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BD738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BD738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A89B71	ReadFile

Analysis Process: WmiPrvSE.exe PID: **7716**, Parent PID: **752**

General

Target ID:	10
Start time:	02:04:58
Start date:	19/05/2024
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff693ab0000
File size:	496'640 bytes
MD5 hash:	60FF40CFD7FB8FE41EE4FE9AE5FE1C51
Has elevated privileges:	true

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: schtasks.exe PID: **7864**, Parent PID: **7680**

General

Target ID:	11
Start time:	02:05:03
Start date:	19/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\TBsjWljiCpR" /XML "C:\Users\user\AppData\Local\Temp\tmp350B.tmp"
Imagebase:	0x4b0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp350B.tmp	0	2	success or wait	1	4BB43E	ReadFile
C:\Users\user\AppData\Local\Temp\tmp350B.tmp	0	1578	success or wait	1	4BB4E3	ReadFile

Analysis Process: conhost.exe PID: **7872**, Parent PID: **7864**

General

Target ID:	12
Start time:	02:05:03
Start date:	19/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: TBsjWljiCpR.exe PID: **7908**, Parent PID: **7680**

General	
Target ID:	13
Start time:	02:05:04
Start date:	19/05/2024
Path:	C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\TBsjWljiCpR.exe"
Imagebase:	0x570000
File size:	758'280 bytes
MD5 hash:	21D18E20B8B0E17E0B554B5940A7AAED
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.2030469230.0000000000417000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Has exited:	true

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1699896	success or wait	1	40A5D3	NtReadFile

Analysis Process: usFxdnRPYjnb.exe PID: **4460**, Parent PID: **7620**

General	
Target ID:	15
Start time:	02:05:17
Start date:	19/05/2024
Path:	C:\Program Files (x86)\ATqfrwJeiSEkHpSwLmQcLcKjItaMjYnOwempnyfloVJBHkJly\usFxdnRPYjnb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\ATqfrwJeiSEkHpSwLmQcLcKjItaMjYnOwempnyfloVJBHkJly\usFxdnRPYjnb.exe"
Imagebase:	0xfa0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000F.00000002.2863047851.0000000004760000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.2863047851.0000000004760000.00000040.00000001.00040000.00000000.sdmp, Author: unknown
Has exited:	false

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: SearchProtocolHost.exe PID: **8040**, Parent PID: **4460**

General	
Target ID:	16
Start time:	02:05:18
Start date:	19/05/2024
Path:	C:\Windows\SysWOW64\SearchProtocolHost.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\SearchProtocolHost.exe"
Imagebase:	0x230000
File size:	340'992 bytes
MD5 hash:	727FE964E574EEAF8917308FFF0880DE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000010.00000002.2863758312.0000000003070000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000002.2863758312.0000000003070000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000010.00000002.2861231272.0000000002A20000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000002.2861231272.0000000002A20000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000010.00000002.2863668034.0000000003030000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000002.2863668034.0000000003030000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\FGGx944Qu7.exe	cannot delete	1	2A479E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\20291vC	object name not found	1	2A479E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\20291vC	sharing violation	1	2A479E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\20291vC	sharing violation	1	2A479E7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\20291vC	sharing violation	1	2A479E7	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1699896	success or wait	1	2A47957	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: usFxdnRPYjnb.exe PID: **2492**, Parent PID: **8040**

General

Target ID:	19
Start time:	02:05:33
Start date:	19/05/2024
Path:	C:\Program Files (x86)\ATqfrwJeiSEkHpSwLmQcLcKjItaMjYnOwempnyfloVJBHkJly\usFxdnRPYjnb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\ATqfrwJeiSEkHpSwLmQcLcKjItaMjYnOwempnyfloVJBHkJly\usFxdnRPYjnb.exe"
Imagebase:	0xfa0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: firefox.exe PID: **7468**, Parent PID: **8040**

General	
Target ID:	20
Start time:	02:06:11
Start date:	19/05/2024
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Mozilla Firefox\Firefox.exe"
Imagebase:	0x7ff6bf500000
File size:	676'768 bytes
MD5 hash:	C86B1BE9ED6496FE0E0CBE73F81D8045
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Disassembly

No disassembly