MALICIOUS

Classifications: Backdoor

Threat Names: NanoCore, Mal/Generic-S, Trojan.GenericKD.37642032, Gen:Variant.Cerbu.11615

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe**
ID	#967561
MD5	b462382cb954466386f9334247e0a34c
SHA1	0ac9e261eafc36f2d8a7bda5755b44c9d8c883e9
SHA256	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b
File Size	30.50 KB
Report Created	2021-09-27 22:30 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (26 rules, 36 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Backdoor
	• Rule "NanoCoreRAT" from ruleset "RATs" has matched on a memory dump for (process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe".			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.37642032". • Built-in AV detected a memory dump of (process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe as "Gen:Variant.Cerbu.11615".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
3/5	Defense Evasion	Modifies Windows Defender configuration	1	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe adds exclusion for Windows Defender.			
3/5	Anti Analysis	Tries to evade debugger	1	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe hides thread via API "NtSetInformationThread".			
3/5	Defense Evasion	Tries to detect the presence of anti-spyware software	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe tries to detect anti-spyware software via WMI query: "SELECT DisplayName FROM AntiSpywareProduct".			
3/5	Defense Evasion	Tries to detect the presence of firewall software	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe tries to detect firewall via WMI query: "SELECT DisplayName FROM FirewallProduct".			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe tries to detect antivirus software via WMI query: "SELECT DisplayName FROM AntiVirusProduct".			
3/5	Network Connection	Performs DNS request for known DDNS domain	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe resolves host name "friomo.duckdns.org" of dynamic DNS provider "duckdns.org".			
2/5	Discovery	Executes WMI query	3	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe executes WMI query: SELECT DisplayName FROM AntiSpywareProduct. • (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe executes WMI query: SELECT DisplayName FROM FirewallProduct. • (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe executes WMI query: SELECT DisplayName FROM AntiVirusProduct.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe modifies memory of (process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe alters context of (process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe.			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe starts (process #4) powershell.exe with a hidden window. • (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe starts (process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe with a hidden window.		
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe enables process privilege "SeDebugPrivilege". • (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe enables process privilege "SeDebugPrivilege".		
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe reads from (process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Enumerates running processes	2	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe enumerates running processes. • (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe enumerates running processes.			
1/5	Mutex	Creates mutex	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe creates mutex with name "Global\{5fb3fc63-476b-43ac-865e-d84d77cfacac}".			
1/5	Discovery	Reads system data	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe reads the cryptographic machine GUID from registry.			
1/5	Execution	Executes itself	1	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe resolves host name "cdn.discordapp.com" to IP "162.159.130.233". • (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe resolves host name "friomo.duckdns.org" to IP "194.147.140.25".			
1/5	Network Connection	Connects to remote host	3	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe accepts an incoming TCP connection from host "194.147.140.25:6746". • (Process #1) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe opens an outgoing TCP connection to host "162.159.130.233:443". • (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe opens an outgoing TCP connection to host "194.147.140.25:6746".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe tries to connect to TCP port 6746 at 194.147.140.25.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #8) 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe resolves 57 API functions by name.			

Score	Category	Operation	Count	Classification
1/5	System Modification	Creates an unusually large number of files	1	-

• (Process #2) powershell.exe creates an above average number of files.

Mitre ATT&CK Matrix

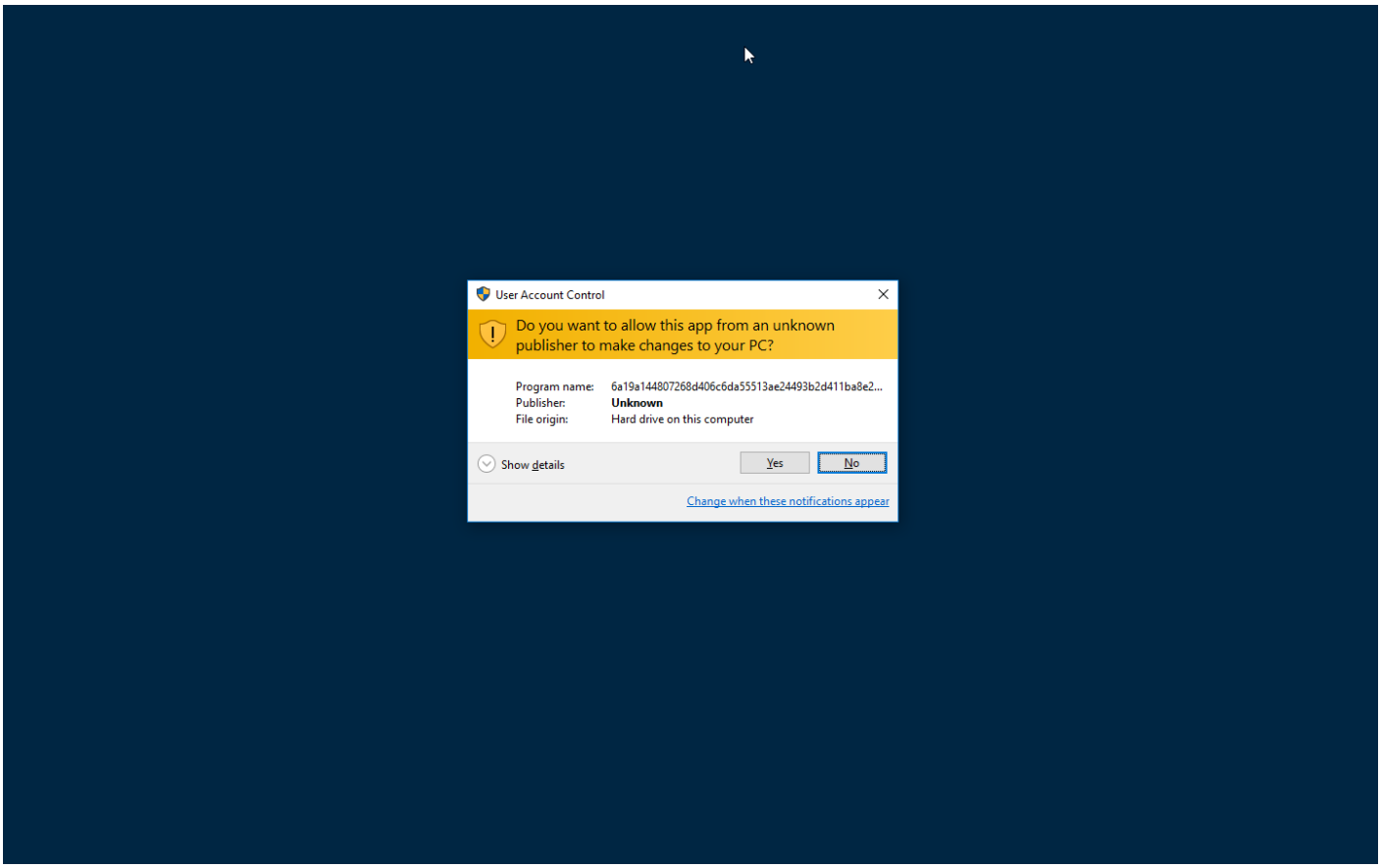
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1089 Disabling Security Tools		#T1057 Process Discovery			#T1065 Uncommonly Used Port		
				#T1112 Modify Registry		#T1082 System Information Discovery					
				#T1143 Hidden Window		#T1012 Query Registry					
				#T1045 Software Packing		#T1063 Security Software Discovery					
				#T1096 NTFS File Attributes							

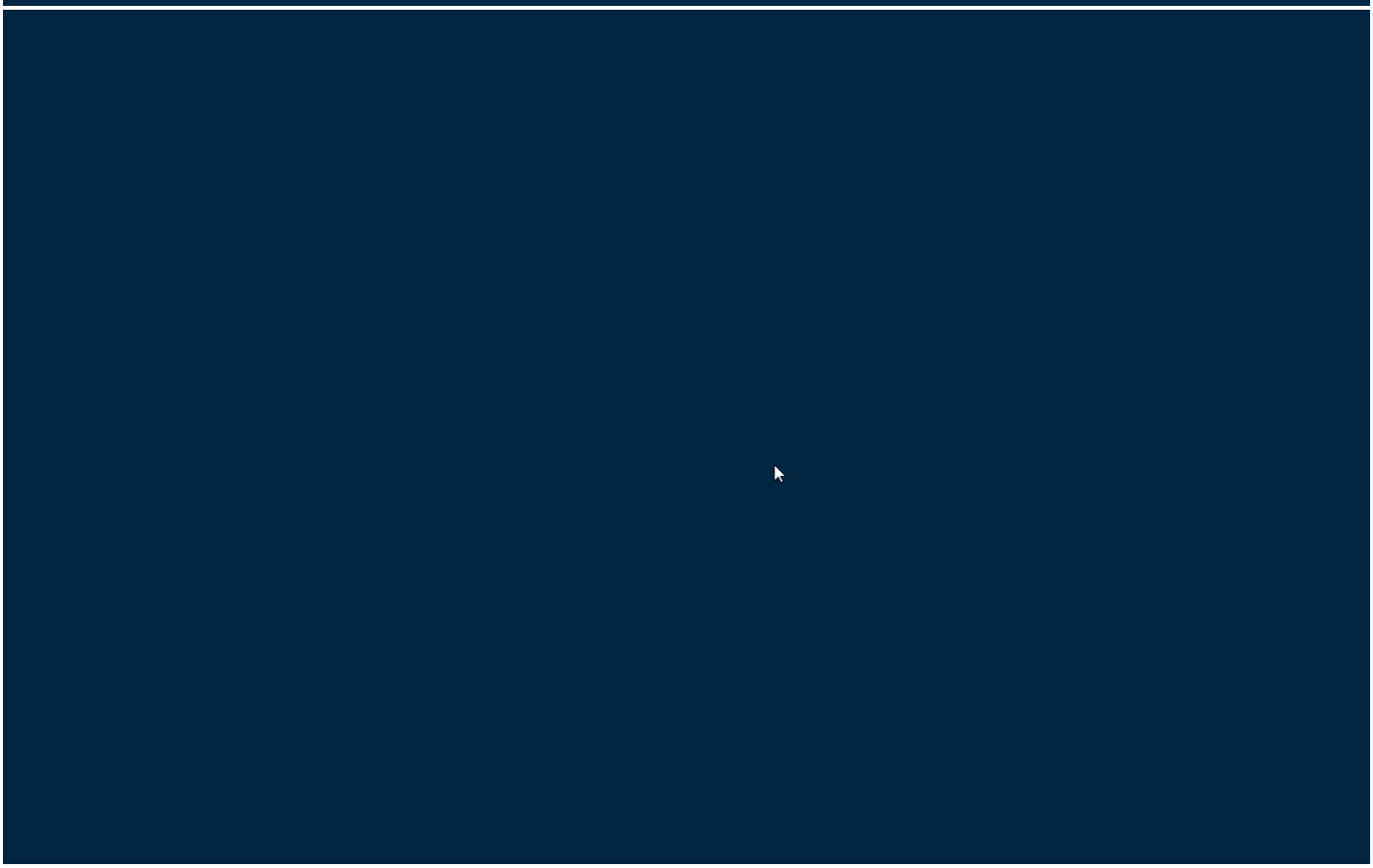
Sample Information

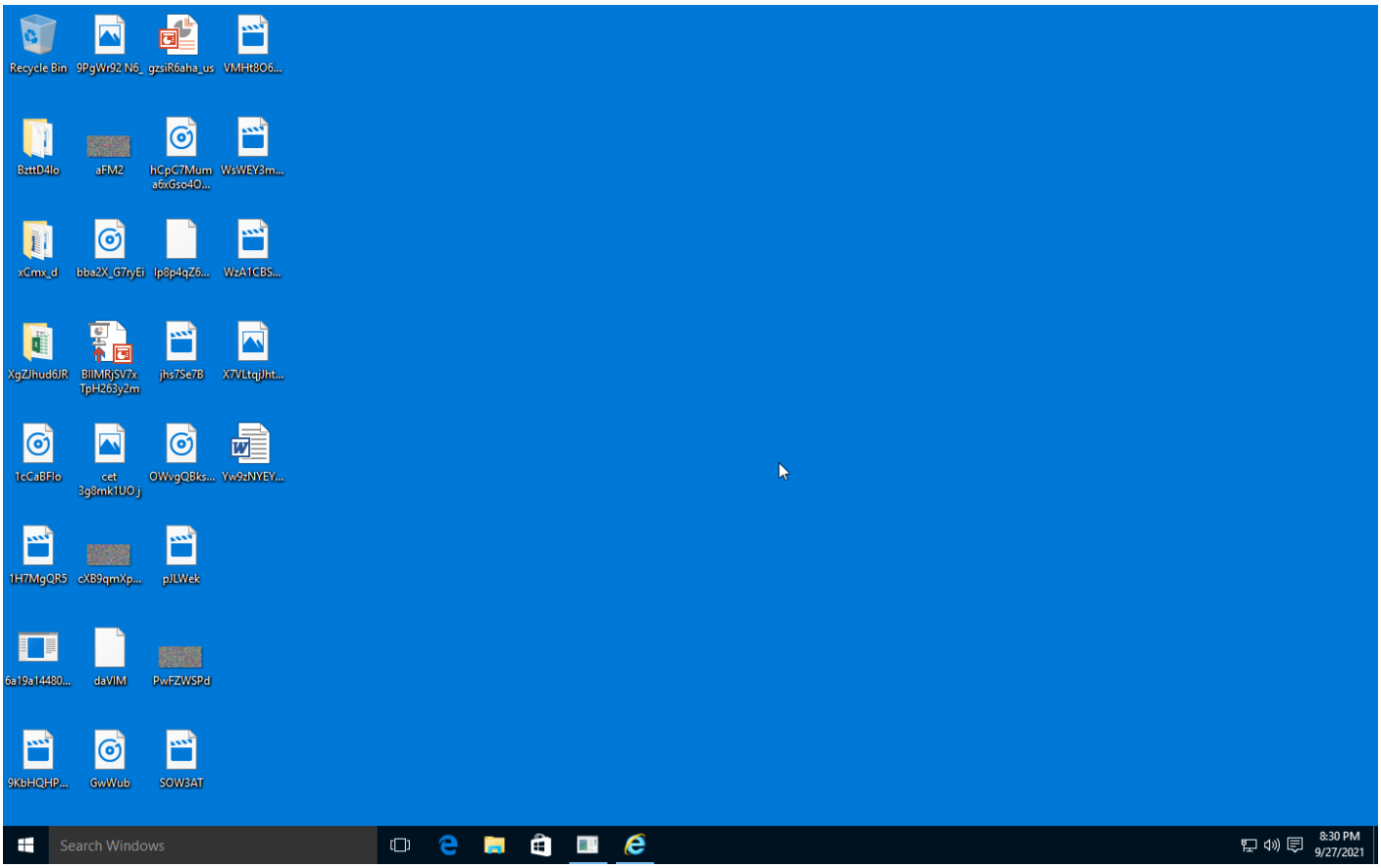
ID	#967561
MD5	b462382cb954466386f9334247e0a34c
SHA1	0ac9e261eafc36f2d8a7bda5755b44c9d8c883e9
SHA256	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b
SSDeep	768:X1S7dO4lGn8pAw5sY0ElWCqgFDlZ8Lq7d:X1YbEnDwOEnCqMZF7d
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe
File Size	30.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 22:30 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	5
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	2
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 6a19a144807268d406c6da55513ae24493b2d411ba8e2...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear




Recycle Bin
9PgWr92 N6_
gzsiR6aha_us
VMHt8O6...
BzttD4lo
aFM2
hCpC7Mum a6xGso4O...
WsWEY3m...
xCmx_d
bba2X_G7ryEi
lp8p4qZ6...
WzA1CBS...
XgZJhud6JR
BIIMRjsV7x TpH263y2m
jhs7Se7B
X7VLtqjJht...
1cCaBFlo
cet 3g8mk1UO j
OWvgQBks...
Yw9zNYEY...
1H7MgQR5
cXB9qmXp...
pJLWek
6a19a14480...
daVIM
PwFZWSPd
9KbHQHP...
GwWub
SOW3AT
Search Windows
8:30 PM
9/27/2021

NETWORK

General

15.94 KB total sent

7164.87 KB total received

2 ports 6746, 443

4 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

2 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 7.97 KB sent, 2683.50 KB received

HTTP Requests

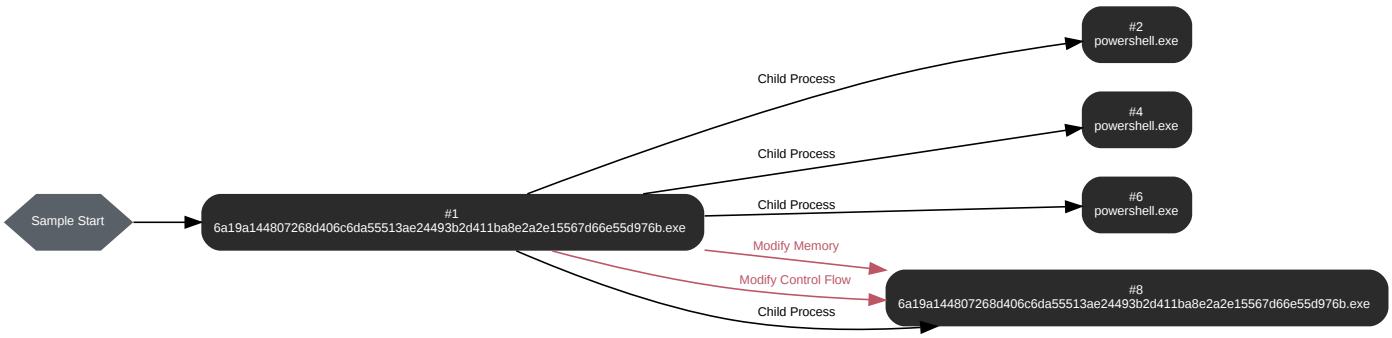
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://cdn.discordapp.com/attachments/886962207051640872/890689205934620692/4102A6C4.jpg	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	cdn.discordapp.com	NoError	162.159.130.233, 162.159.135.233, 162.159.133.233, 162.159.129.233, 162.159.134.233		NA
A	friomo.duckdns.org	NoError	194.147.140.25		NA

BEHAVIOR

Process Graph



Process #1: 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 42140, Reason: Analysis Target
Unmonitor End Time	End Time: 98981, Reason: Terminated
Monitor duration	56.84s
Return Code	1
PID	4976
Parent PID	1636
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\Public\Documents\[redacted]\svchost.exe	30.50 KB	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b	✗

Host Behavior

Type	Count
System	5
Process	6
File	25
-	10
Registry	40
Environment	8
Module	38
Window	4
User	1
-	13
-	3
-	7

Network Behavior

Type	Count
HTTPS	1
DNS	1
TCP	1

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\Public\Documents\[redacted]\svchost.exe" -Force
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 79250, Reason: Child Process
Unmonitor End Time	End Time: 216208, Reason: Terminated
Monitor duration	136.96s
Return Code	1
PID	2104
Parent PID	4976
Bitness	32 Bit

Dropped Files (42)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0e4ec6a4-ddbd-4b05-bf53-d0cd196fcc10	690 bytes	4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ff6b0af3-d9d6-448b-82a7-1b5351dfd1be	974 bytes	627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_8f921901-ecf0-4e9c-a117-4dfaa27bfe4c	693 bytes	d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_556426f6-aecc-4bb8-8f4f-d46b696907e9	1.86 KB	6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ce402089-b365-4e0b-927f-1fde169227f3	1.27 KB	1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bddcf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_368098d7-a75d-4662-99aa-fddd436c3339	3.79 KB	34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fba3eb17-6f3b-40cc-a0c1-947cd8b4b5b0	2.89 KB	91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_eddf4502-371c-4620-9242-dd0b48c521f7	1.73 KB	33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_22d99bb5-463e-4ef4-a0ee-1079b8c3de12	925 bytes	4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e90615c2-182d-44b3-9293-d5b19dece4ec	2.25 KB	5f7a04aa9cbe5e26d72b167faad2c030f3aadbd1237dccc5561a699e0b560b6d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f2674441-2965-43fa-bff4-5779811b3e64	1.94 KB	196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73bf0bc1-f5da-4824-9c66-c5a40c862bff	2.42 KB	ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_de0996c6-5e79-4c81-a72c-850a4ec7e6f8	1.83 KB	859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f6c943b7-2da3-4095-90d9-d1639d451bd3	794 bytes	4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_624b8724-08c3-4af2-9f97-1e915473ee11	1.07 KB	1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6e7e7eb7-c82e-4aa1-a321-88b7dae67d85	1.77 KB	760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_041d0332-fa3c-4f5c-964e-fa665ce46a38	4.81 KB	d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73ee3bb6-aaa8-4628-900e-a2fbb3de2ae5	7.79 KB	b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1afa74a9-01b2-4b56-ad76-867dd642d6be	711 bytes	3efc14d5f3f284d8b564fcc9a6df06e6e911365ac56ce54266e5631a4d33c301	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5fde1883-2b9b-422c-8f4e-fbd41463d12a	3.42 KB	9e09fa3e6c0cf5f5dcd00d2db5327c914e167430ed811638330098a42a9d7abb	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_df188c9f-7615-4def-8309-c0925a415cff	1.81 KB	000e5c18df1ae71ac0b4402c8aa8a34da881f559bc8b7edccf05ce1ff0686067	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_79f8bc92-df4d-4aff-96bd-f447ed3da7e4	1.81 KB	2c6c6e562e6336e90daed97a6ec6fc2e36c439a4e45f76f587bc895d0805c995	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fe81037d-2bcd-45da-8eac-26c2cc5cf4e7	902 bytes	28de346b7d29d63eb092ccdcd69df55ba4592e5782be73d48bf50e8e217a77c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_633bd5d6-e5fc-4045-8b1a-15ec0acad86b	9.67 KB	a9b5795280d1048e0daa6e27e869492db115cf92a57a9817e6d894b0bec31b1b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b22fbde2-a75a-4d02-b37a-9af65ed29e41	1.21 KB	d6914a2a649b85a5dfd8fd00cfb466a3b43f3663f53a017e826eef5dc6235e8e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c767758a-3533-461b-becf-c9cbd699ccdd	4.10 KB	be0522e891f07b196eb4cdd8761c7f53caf642c16ad5d691c7d32c327f26d075	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1f6d357a-d20b-4443-8730-5e258e1fa24f	940 bytes	ff157433bdd0e5a4a61f27172591a53d88d2e2ccfe9a5b16bf33c250cab869e8	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1101bf46-9afd-439d-94ba-3f764ed35d6c	4.30 KB	2410c4686683f3a71dceae28781a8ca886360d84213c426b64d40bb751329f6c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6a124592-2bb4-4c6e-a547-f6d8846f0c8a	2.31 KB	bbb309c7c6bb3927cbe380a7ce2743ec5b80e4aee32f4f640049e39ddca3ef8c	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_62a821dc-55dd-4743-bd16-b75374284bb8	902 bytes	ab8f309bf9116247713e709cb680ca550b2e557ccc06a4e9e7957a35bff55bc5	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4295b2ed-5018-4e04-8efb-491b5932b3e4	2.67 KB	1a17618fb70e56a97d01e2a76d7a18471fb05d3f102db3fa9419ba1eccc09eda	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5827393e-0047-47ff-9960-004c5fbe5885	3.11 KB	0f051424fac4f2a24698fbb339c96372385eb29556e2cf43d9eed1bbdc2b6957	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_917d511e-ca61-4d47-8831-f3b55eb99131	1.49 KB	1823874d8b80e06660a68b79930710e65c04b1d70d8967554b54eb83ab7ff36d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fe51fd64-42bd-482f-80c7-1b158004b548	2.50 KB	d4a59c4162645b2dc38ea8ac7c8795b05bcd3783abf33c881fefe85fb0e19ced	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4289b915-7b00-4da8-b59c-d89fa11b2bf9	708 bytes	0ee5fbe0c1899975f01475b9c8b36035c4cc631ad987599692b46e164c3350b6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4718c3e0-c931-47ee-ba57-141bdf05f605	2.61 KB	d43d0455455af25b42c3466d3cd3f4041cf22a64aab99addf82ae0c55c3ec08c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9428f661-f4e6-43d4-81bb-34d70c8be0c0	1.68 KB	ae6e63ef96530ae69b12ece4dc45ec8b0a1424d6735a70707f55f77f807abbe0	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_698c6765-d53e-4ace-9ecc-8e97a8d66cd5	850 bytes	1a437083770bc56268a6d97b6c0bacb02b306d85b22eb780c5d39bca8b00994f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2da3ccc9-70bc-4781-a552-914007ce7bc7	597 bytes	703b4ac87dc31b323f8942d2960695cb6a6ca34e15855e63b30ab0007a802318	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f74bf451-48a0-410b-91de-ad8fb1cfd6b5	1.77 KB	9299f52332d53dff0cd6c724cb734c2571c5528aec9bcca70f3c5af7fda3ae74	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07f04788-2e3f-4d57-b6fe-dbc80a39e7ed	675 bytes	4bba0e3f5d5dd5c6c0aacdc45a2c80daea65d2795eecf0076ab38093fcd35c11	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9609b496-b281-41b0-ba44-620e217b2664	598 bytes	4d87ced394269fa7c324f7a3411c8a9c020cb7f33888112e8289117979eed0d9	✗

Host Behavior

Type	Count
Module	6
File	11261
Environment	396
Registry	1512
Mutex	392
-	256
System	932

Process #4: powershell.exe

ID	4
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe" -Force
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 79704, Reason: Child Process
Unmonitor End Time	End Time: 216588, Reason: Terminated
Monitor duration	136.88s
Return Code	1
PID	3160
Parent PID	4976
Bitness	32 Bit

Dropped Files (181)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6f27244a-c514-41dc-baa8-9344f2d82db6	690 bytes	4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_15cf0bc9-a103-4b1d-88e4-59b36d95aeaa	974 bytes	627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_709de7b1-7c38-4d41-880a-2aca2510b268	693 bytes	d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_98469bea-9168-4cdf-ade5-7044e7be7857	1016 bytes	2a761c02935a44d0f783cfb34aee5b514864da12336527781fa0b341518a9e07	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_daac0758-fe61-4c95-a884-d6481030734c	1.86 KB	6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_226b8498-3f59-4b9d-af62-126d30031620	1.27 KB	1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bdddcf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ab56b518-df80-48fc-a40a-ce7b4eb4ec18	3.79 KB	34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_8870225c-8e1e-45ff-a867-459e6cac650f	2.89 KB	91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_79f7f1f4-7db1-4081-b729-9e7dbfbefe01	1.73 KB	33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_347c2958-578c-4312-9e7f-b9e3267da351	925 bytes	4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_de6e6c80-fa07-48b6-b475-b42293516a68	2.25 KB	5f7a04aa9cbe5e26d72b167faad2c030f3aadbd1237dccc5561a699e0b560b6d	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3b298130-65e9-4f8f-8609-9f275d753d63	1.94 KB	196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_85e440a5-b476-479d-a26c-2c25d2bbadbe	2.42 KB	ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95f69f37-3d72-4379-9722-7dfe56023e93	1.83 KB	859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b3cb74a7-8b4e-4590-ac5e-62066f383617	794 bytes	4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7c969125-2514-4e55-9a5d-1956bd655c6a	1.07 KB	1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cca87233-b034-4c65-a14d-e7af944547a7	1.77 KB	760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ab56670-54e2-48fc-bdd3-df3385d49fb0	4.81 KB	d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_429c54ad-b288-4ea7-8d6c-e894568299b9	7.79 KB	b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_deea50a1-52d7-478a-9000-61c95d05f51f	711 bytes	3efc14d5f3f284d8b564fcc9a6df06e6e911365ac56ce54266e5631a4d33c301	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9fe3dd1f-b99c-432f-b812-904a309b05ec	3.42 KB	9e09fa3e6c0cf5f5dcd00d2db5327c914e167430ed811638330098a42a9d7abb	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5fd0ec6a-d5ac-456a-ad5c-89b003dbb698	1.81 KB	000e5c18df1ae71ac0b4402c8aa8a34da881f559bc8b7edccf05ce1ff0686067	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9c5fa5f0-5a7a-476c-bc83-528303797146	1.81 KB	2c6c6e562e6336e90daed97a6ec6fc2e36c439a4e45f76f587bc895d0805c995	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2d26d6eb-22af-4a07-8b8c-0d98b8ff4a32	902 bytes	28de346b7d29d63eb092ccdcd69df55ba4592e5782be73d48bf50e8e217a77c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_499fc8f5-be57-4e70-b801-9d62c1f39bec	9.67 KB	a9b5795280d1048e0daa6e27e869492db115cf92a57a9817e6d894b0bec31b1b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4b99ea6a-e714-4d9c-980e-f3b06d9ae3b0	1.21 KB	d6914a2a649b85a5dfd8fd00cfb466a3b43f3663f53a017e826eef5dc6235e8e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4ba00582-a2d0-48c9-ba5b-ebe39d5888a3	4.10 KB	be0522e891f07b196eb4cdd8761c7f53caf642c16ad5d691c7d32c327f26d075	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_052c9a54-7507-47c8-bc69-7a64a17bb0ca	940 bytes	ff157433bdd0e5a4a61f27172591a53d88d2e2ccfe9a5b16bf33c250cab869e8	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7dd186ff-55a9-4243-8153-ef089dcc0ead	4.30 KB	2410c4686683f3a71dceae28781a8ca886360d84213c426b64d40bb751329f6c	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_90139960-e14d-4af4-b940-922da330ebe9	902 bytes	ab8f309bf9116247713e709cb680ca550b2e557ccc06a4e9e7957a35bff55bc5	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f42dfa61-c1b7-4d72-b4d8-2f4ae9134f67	2.67 KB	1a17618fb70e56a97d01e2a76d7a18471fb05d3f102db3fa9419ba1eccc09eda	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_05921866-d46d-4c03-8c0a-741936c96791	2.07 KB	4efc10918360ff44d6aeefcc47750f6cb4d4c2d90d8def2f7fb50dc90f7e781f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e6419846-85ea-4b32-899e-8f6ee569215d	2.50 KB	d4a59c4162645b2dc38ea8ac7c8795b05bcd3783abf33c881fefe85fb0e19ced	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9d9a204c-57df-4ac2-b025-23619953d462	1010 bytes	ded817ecb8d9b2aa750e54a746cf63d87725719f36a5d97550d8351d46b5e944	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_46f1bb0e-4a51-48a8-b31b-5f80905fe0bd	16.04 KB	f3a85f8f484f9f5ebf08e1238fc2a9332e3ee3759f2b49e5b2743864d7aa6678	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_de4adc50-1ed6-4915-b54b-093812d7617f	1.21 KB	4c2d15172dbd86e5fb80af1b664940c5bab98b9e3a27c34f5987248fcf040ec7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7287a41d-5a63-40b8-9ab3-113a5b356f07	708 bytes	0ee5fbe0c1899975f01475b9c8b36035c4cc631ad987599692b46e164c3350b6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_19a97c7d-e131-4d9e-a282-097e854a3af3	1.58 KB	606c56344741860222a4171e069398c49e0331fbfb04c0fc37fd69629d24bfdf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7c3a3a31-aa6d-4e4f-8244-8f8f63011957	2.61 KB	d43d0455455af25b42c3466d3cd3f4041cf22a64aab99addf82ae0c55c3ec08c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_677427e0-1b94-4db9-a683-8a621d928cc3	1.68 KB	ae6e63ef96530ae69b12ece4dc45ec8b0a1424d6735a70707f55f77f807abbe0	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a89ea3ad-87df-4a35-a89f-45f3488ec350	850 bytes	1a437083770bc56268a6d97b6c0bacb02b306d85b22eb780c5d39bca8b00994f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_971a2c52-c834-445a-a6e1-9ed00f014434	491 bytes	e4295924ee4a4087eae831962333d3227bf1cd4dd951f096c65934a98e9a10b3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b83b146a-7d6e-439e-af7d-ea7ac093eda3	825 bytes	d137168421e27f18381d9ea441abd1d8c45a5281dad9d1237887889ef42087b6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8253c19-33ab-4b5e-a485-d9a145f9a371	597 bytes	703b4ac87dc31b323f8942d2960695cb6a6ca34e15855e63b30ab0007a802318	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cbabd4f4-e21d-4f77-b7fa-df378ca0e656	1.77 KB	9299f52332d53dff0cd6c724cb734c2571c5528aec9bcca70f3c5af7fda3ae74	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b501c8b5-b507-4c7d-87de-c573b6111c75	675 bytes	4bba0e3f5d5dd5c6c0aacdc45a2c80daea65d2795eecf0076ab38093fcd35c11	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7db70c6b-b783-4a8b-a7b3-951946679d17	3.11 KB	b667afe32d773d431b76965b361f1dbcce60d4627b4ca0a85e905cf4d98d634a	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fdb68e5a-8f37-4dfc-be47-b1579962e4a3	1.11 KB	063261bb48211cca71e8f2d8ed48972fca8c12f1f11a87267e75ba50c5f1449f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.42 KB	2ea0849530c7fdf3ec26662722ce2136dcf7a588029cf3dfd3b92081f9ac7b20	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.42 KB	fa08cb9e98f7e4277058db5d9d33ba60327584a42eb30a3b3d52238dcdbda473	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.42 KB	23719a572b0ac4930cea0a112250db9d722174618afae19237d8469682c410cf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.70 KB	744c815e44dcff0cb645c39ae4e2faa9a1bd4b1d4c087834f8a4729de9371f45	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.70 KB	9253d3186cf602edd06f8a1803442a9868d7fe5850bf497c7d69bf76973fd1d8	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.70 KB	d6816f607601bef3787d27718cea995052a74809d1efd1f486e3cbd61cc5a025	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.97 KB	abeb1c36498f0d04c6e81170d84b6f6e38423dd92588e5b6f8cce58c853411a0	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.97 KB	8ee0a5021684ebfbc04165209192d2fb8af52b10a24b6f666a3177be09c39fc3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.21 KB	78aa67e9880202c432b43a7bab70e008f422508f4e1fa63a065adb05a60c94d6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.21 KB	95094fe9e49a2205afc8edd054e1b8bf1656582fc72c5e213136abc5bb805178	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.21 KB	142567e96d2baf6814275863da0e9fd023a269e947715b5378e3d51eebbd47c0	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.43 KB	7f0186ba2f401d8023deb2f13de52dc0026ff64757873e5137fed9609fc45efe	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.43 KB	ce78c67e751f0ccd977a855e03d1ea6fe0afd70d76e39282a702716f6efe33c4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.43 KB	840a573a2aa889e87f1099b2d70f13ac903f58310e69abf55d80e8aea1fa9331	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.67 KB	c2e57ca30987df4cb4ac7238a33fe378b8419edba1cba88cbab337f151a9809d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.67 KB	9cb0d6e88401c33f20a3178d67523a42e9606304aaea9539e614ab6683028cd9	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.67 KB	86a23616e1dcd86948171ab993b0dbbe5515cdacbb941ad16a2e79a2704256b5	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.91 KB	e9084e5ffe2b2af21e89b506cdabc5f077ac25ed9d0bd12b6dfb8da5f13d8cc9	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.91 KB	b4b72ac508ec1f58c272880874e792dd18fefacdd71dc77cfbe3d2fa877a3a81	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	3.91 KB	67b9841ec2ecf9ace1eae4bb8d4a90a974ed01ec5f7e97012e71ee53fc224ca3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.14 KB	22ed04090abbf5dacf94d529b7c02b8c9548f55032172fc41448d5c031ba1645	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.14 KB	149b3f59efd723763be5949b3861631965a5e5affbf6aacbd518adbbb64a875b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.14 KB	ed859c3212910a62139a3217619184d545c17fd5f217b681168afbae2a840978	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.42 KB	cb671c785af92dac17e505e8ddf42a58b8126d3d544f9f2d1e4bc58dc36e58ad	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.42 KB	87ca26f05404ab41f669daf94121a91fdb1546b9b0b1a8a420dc3701d0231a4c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.42 KB	ebc78e70a5c862bbde6dcf30d24f3dec31ade0f55cae0361e5862fc2efb4ad5e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.64 KB	b1da3341de9b93722ad72ef0b01e5a15b3ff7e1d028fa98f71693394339d5eb4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.86 KB	0462ee3b26c390a9d04e7eca73cc7a3c51c8f079fe4c6197b6b345d75ed8f4b3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.86 KB	3152cedcae0854a82cb310adb9899fe0d33eb16e421f0333ffd4bd0a5528b28d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	4.86 KB	b4ed46a1d8af04791401e97dc49bd4a27a204468fc47081247b9e9ce25de48b0	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.10 KB	da8291539528349889971caabf3a42587cda90f3855de3b319fb6bf624ce7097	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.10 KB	06c4d9f581b752363439efd73b894e4317bb59729157de2f7f93d0e1d1153c4d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.10 KB	af66ff69abb3fd6b21933e0c139b297c2bfec9d331f92aad8d74c92298d32d22	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.36 KB	93598b20f7b97121d498287803573df395a1a75fa1da9ad36aa3ac0790836b1e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.36 KB	8eccfb5e416fa023901a485cb447647a62f56adc907abb90104fe2fb167e5f62	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.36 KB	a5f1bf2ab97ee0fe00b7be402a148b1d2ba508f4ddf6056d79ba7c888fccedae	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.60 KB	f2de7d1a4fe4b515a9206c0a8ac03abc5ab31ab0c6228948fa8d074dbe3de598	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.60 KB	7b0cb62173cec725eba7246da19148b696162895ce13d11ea7da7422bf7b6582	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.60 KB	1f1e3f25f8958dc59014616dbb26ef430e41068961682c8c768ecca9b8e3213a	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.82 KB	0576a8469d79928c10a3d8e6d7ee8ab0aad169c8820a51736c794bb9bc0bd6f9	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.82 KB	20f1e9803f99ffd68f0a068e69cb1fa604ab5668cf548b2d5e2b79ba00e50a6f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	5.82 KB	96562525690484ed9f425d34dd664bcb3d1ec7f56fee0806f0f38b8c42c85e09	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.04 KB	5a6437588e6ae8cb9ddd544716999df02ada275077c80ab4347fafefb066aeaf	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.04 KB	fdfd9652007e0f1d859a09c562024b2962b30b45b9d63e7853119248b521b434	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.27 KB	7d89fc4a55f47186cf3dcb5c3d55df743920965a4761a5abe9caa50ee876f30b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.27 KB	c8defa8bf055ef93ecd685b4947dad69cfddb4dca7258419cb12ead74ec15120	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.49 KB	84e08d6badb0ffb926e49dc0e0c970004e1c8a1c35cd1c4bc8d49fd315342e0c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.49 KB	05eba04070a7eb2fd13050c1c44f6421db0745d4fee0f18013a18df5dd0cd258	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.49 KB	961156aa031bf52742623bf1f2fc21a96da1e8bcf1ab43a7f771d6cea573bee1	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.75 KB	4af1955c6b6a9d41a801a448d9e4be9af5cd4e1c3235eb0c03ac3f68cdd8baff	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.75 KB	7dd89677c2a8fa99af9a8c116cf58924ac4b9826c2756fc7f9c132ea6c4318d4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.98 KB	4f5b2354db1b4c641a2cb2a11da058271dfd247f7ff888a988f4620281c4bc04	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.98 KB	81979f49a9760265a8f3def1470ec57779536722c2043fba6b9f8ec0a5df9ad9	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	6.98 KB	adf9d919b721c0df57c95fb04fce3fb8489059139af70912e3dee45d760b0fe6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.21 KB	c9a7517f02e4b4ee7c9cb6f6dacb8231a682888795158405c71ff36c8e0767a1	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.21 KB	cc898842dc27fd22dcdc8877345cb1c187c3a13573b423f1d960e0c2d9882edd	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.21 KB	1ad8bf559a3f83a10ccf08c40e39047cb7ccf18a7ef195162400a28daf0bbc08	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.46 KB	65f081797e12c3f4065d2f9f8ae29d0d30d1a65d8cbc22353e3a34ad1fd8677c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.71 KB	a4af910e0fcc6b0807ed7d3a63d7c634f2a3d52a562330b6d55fd61c2410d931	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.71 KB	944b622c134e62dbf7dba847fdb181201fcc56388ec04c9f458b9fc5db22f562	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.71 KB	efc94ddd8b824066cebf1d6bf3efbbedbf76f83db02404462f247f1eb64575df	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.94 KB	9bda1e604eccf98cb1b5d9e9b0bbceb0673ea86167475f82793174d207b45f9e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	7.94 KB	72d0b6dd0ccd0394139c29ce4972946db1fee9f01b0aef793cc8259499737a91	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.17 KB	be0bb5ba01ec1fd5fb1fd28741e548dba5efc04dd4aa62c9d19037b682814ccc	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.17 KB	431c1251d35f0afb4ebe1721daf0474afb6c1fe4b7ef6aac6ab6721498ab2d6c	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.17 KB	3ac1ecda72ab210e44b2f086498916c40756d26d121ddeafab63ed21fe64a02c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.40 KB	8fd905e7a8a32a12ec970f87659b9c30a73a6674a7e8ca078fb7cb75adcc1052	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.40 KB	8609a78c302255e196e8db52d7fb440d564a19a3a9b261ae210755700585fc1f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.64 KB	f5ebfb6564cb6c0afe9ccf169e2e9b78b6e75f73a6210ddb4b54b18d21557571	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.64 KB	0ed7b5171adc4e5893b13f4e59a8aa821573f3721393fc0842e6557624dd8730	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.64 KB	c20c7a51a499c585199d03fa8664c1529fecd27433870cbafbd8330b36c73638	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.88 KB	8bb478852eeefdba36bb665f91337f7324c41385bfdde6edc3541a8c1d08e593	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.88 KB	e6df868b087b0ef380a7b11ccd903d6236dce2a7987a55459b56045d46a3a070	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	8.88 KB	aeefb1b9d55be54fb21128bc1ab6e80174f27b2d77b324b98851cbe866479120	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.11 KB	02504b1a898e5a8b8b40ed00bb338ba7e1f215ddad718b67ec141f50e027d739	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.11 KB	c867d6233d7cf8f6f9ff9e5ccd63ef8c71618f524900fcf42ac8b33387a47580	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.11 KB	9299b6383523adf197cef678e132ee5cd2c8330b45f222ce836cf906a13b515c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.37 KB	6d80ebbdaa159f225ee1522bd62ab25cec73f46e55d01b192a0fa370b43dea58	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.37 KB	4224d3485353b0c163e8d27e93131c10c1cb5a3fb5e82a88000f034ec844759a	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.37 KB	29ba0d13272526708713226241 2eceb6f2e738a75da2a44780d4d4e7f758f618	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.62 KB	d9370379d1a7036387fee9de3d7c89981a97d4677587f3fd5aaeab970024a1d1	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.62 KB	f6b636342a2acf6aa0fad2fa790eaf2214dafd8243defe332efa9598b9db2880	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.62 KB	743f64587ca9e2dc642bd7930a2e18b9ee14772f455270c81bdad65f25271da2	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	9.85 KB	e55ef91aa6033f2c002e8ac6fcdc27278e6faba1b9a1d92786134397a2b496fe	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.08 KB	93aaea229ca26ac445df42cfc80fc6358d09df1a3b7374efe2cc9968c4e2423b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.08 KB	c8406c2cccc5faadcead43862329d1deba8d38241713f38b7249f4e88b2571bc	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.08 KB	c88b864ff46839799b77362b58bc9393bfabd3ada0bd2c7afabb31f10c5e110a	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.33 KB	ef95c373f76432be97cc439ae4787e378a07475c632421b5bb4b5d5b3c371bc5	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.33 KB	7d18ef0c28eef793e77adca2e38178826e8cdcd8c2ee75003e04d51c804fe82b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.33 KB	60a9a3ef0e8ab0ab15c166b997b34eb928d1b52adc442bfafa21aff1d2de7d5a	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.59 KB	31baa5964086edbf99d42fe4f2240c5c689b950da7906e52f34c79a3a657d416	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	10.59 KB	ba7af1e9dac57cd6b9afa70ce1075cdb038816da71317e1eb62d267e00dbb5f3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.08 KB	c8068e04109a39594d84a472cdbfeae2d4adf5ea9793cb9362dac3830c1596ad	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.32 KB	02dc3ba8710d7f97ee6c9202160c6b3963f3228f7bd756dd5cc235afac6689a4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.32 KB	7c2ff4848697eb35a372ce1af1c4a2b5f8d0059020e95cba26e12e0d4ba76bd1	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.56 KB	4cac4dee3d50d08b1451ee088f0ea7cb668b81cc6fa10722468ab0e90afd4e3b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.56 KB	bdf03ea6e020afac38bd61eaba8a191c19479d198cc02701eacc80d2dce50d82	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.56 KB	c398700260796da0cb2dbfa4f3ab0418a763801993526d8fb1bac2f404b1e076	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.80 KB	f4a3e753a9c7926dd2bc55803c0d188b89c82137da9a05f7e5a8f0a5c55d7e9d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	11.80 KB	669df3be46d49da2cb7c570632d31e6d0488604dd20e75b843681b3566d0a56c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	12.03 KB	2d2dfab38310330a2745013a21fcce16afd0d1392a1e043566a754152dd7a41f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	12.03 KB	5d140d82c9038304798bc72f87d0d665d52b128527601d701d65df52a51fd2b7	✗

Reduced dataset

Host Behavior

Type	Count
Module	6
File	10606
Environment	410
Registry	1520
Mutex	407
-	260
System	940

Process #6: powershell.exe

ID	6
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\Public\Documents\[redacted]\svchost.exe" -Force
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 79911, Reason: Child Process
Unmonitor End Time	End Time: 216590, Reason: Terminated
Monitor duration	136.68s
Return Code	1
PID	1964
Parent PID	4976
Bitness	32 Bit

Dropped Files (52)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_dcbe30aa-e1ef-49d7-bee9-bdcb330c041b	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_676eea4e-e15a-48bd-bdec-027e6ab2e677	690 bytes	4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b3bbad2a-3aa7-4078-9cad-3cfc7ac2712b	974 bytes	627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9b115b6a-c32b-474c-8511-480dc5edb845	693 bytes	d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b0f8684b-4a15-4c4e-a98c-f720c0bd4371	1016 bytes	2a761c02935a44d0f783cfb34aee5b514864da12336527781fa0b341518a9e07	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0c5d7aa3-fb8d-4fbf-b2fc-77878f076297	1.86 KB	6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7747426a-3553-4c0b-80cb-4196926e21d4	1.27 KB	1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bddddcf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5a3dbc4-c7d8-4c5b-851e-555ecd1bfe70	3.79 KB	34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bce0f13e-cb33-464d-8684-a1a039d2aa50	2.89 KB	91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5084c725-0e9b-4a18-828e-65955e30dd4a	1.73 KB	33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_315322d0-a280-4570-bfff-b0bca00e113b	925 bytes	4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e9b688a1-74fb-424b-a4c4-40918f2f21c0	4.91 KB	0323d4614482052e68f19ce6f1f3c415da4d6a6e64facdecc910f1c942179b8c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_638e120f-a3fa-44e9-9a82-7d2cea876423	2.25 KB	5f7a04aa9cbe5e26d72b167faad2c030f3aadbd1237dccc5561a699e0b560b6d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_858fb4c5-ebfb-4229-a1d0-bc2a0b3927d0	1.94 KB	196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e140f113-2755-404c-a2c1-e40979ef69d4	2.42 KB	ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e21d1972-3ab8-44cf-9342-1873d6122e13	1.83 KB	859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c71d6604-8079-4d04-8703-f954eefa6c82	794 bytes	4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1552d438-f2c8-4a68-aace-230298bf39d3	1.07 KB	1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_04ad4a0d-b809-494b-8d8e-5b1ef6523103	1.77 KB	760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7b1ddfb4-8ea4-42d1-b49a-46641942d536	4.81 KB	d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fd8d38a7-01c8-4367-bf62-3ace12724d86	7.79 KB	b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_83b4d489-f3ca-41ae-8ac4-20172e04abc4	711 bytes	3efc14d5f3f284d8b564fcc9a6df06e6e911365ac56ce54266e5631a4d33c301	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9ca330bc-a578-4701-b15b-5f55ea71e3d6	3.42 KB	9e09fa3e6c0cf5f5dcd00d2db5327c914e167430ed811638330098a42a9d7abb	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3306a657-eca8-4cd1-ab29-af8aafe97080	1.81 KB	000e5c18df1ae71ac0b4402c8aa8a34da881f559bc8b7edccf05ce1ff0686067	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a58c4493-9c43-4e40-9f84-f6399859fd58	1.81 KB	2c6c6e562e6336e90daed97a6ec6fc2e36c439a4e45f76f587bc895d0805c995	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_485d7c88-22e5-47bc-afa8-76e9cccb2945	902 bytes	28de346b7d29d63eb092ccdcd69df55ba4592e5782be73d48bf50e8e217a77c7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_54d8e2e2-38e8-45c2-92c2-fb0ebeac7d50	9.67 KB	a9b5795280d1048e0daa6e27e869492db115cf92a57a9817e6d894b0bec31b1b	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f58b1d8-acd2-498a-bbc4-1fd7ad4d0c27	1.21 KB	d6914a2a649b85a5dfd8fd00cfb466a3b43f3663f53a017e826eef5dc6235e8e	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7570fff1-6751-4484-8ab6-8d7bfe6826b4	4.10 KB	be0522e891f07b196eb4cdd8761c7f53caf642c16ad5d691c7d32c327f26d075	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_88260f84-df03-4959-a4b1-73229c081688	940 bytes	ff157433bdd0e5a4a61f27172591a53d88d2e2ccfe9a5b16bf33c250cab869e8	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_37f5caad-1373-4d2b-8754-87eecfd97bc8	4.30 KB	2410c4686683f3a71dceae28781a8ca886360d84213c426b64d40bb751329f6c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a4061659-dfec-4ef0-bf1c-5ce027b250a5	902 bytes	ab8f309bf9116247713e709cb680ca550b2e557ccc06a4e9e7957a35bff55bc5	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_421f845c-a18d-48a4-bcf3-182040408529	2.67 KB	1a17618fb70e56a97d01e2a76d7a18471fb05d3f102db3fa9419ba1eccc09eda	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e00f2fd0-0a58-4890-acb6-5bc5c6f51acf	3.11 KB	0f051424fac4f2a24698fbb339c96372385eb29556e2cf43d9eed1bbdc2b6957	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1b26cbb5-c091-4bcc-a9e2-086e7ea4241e	1.49 KB	182dd6206f187dc34372ef0e3f6a9b9bd7e7f2e2623e7445613a58380bc34a49	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bed6e759-72eb-4e45-9c6a-3a413411352c	2.07 KB	4efc10918360ff44d6aeefcc47750f6cb4d4c2d90d8def2f7fb50dc90f7e781f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2f628527-07de-4880-b4ad-98cf4948bf9d	2.50 KB	d4a59c4162645b2dc38ea8ac7c8795b05bcd3783abf33c881fefe85fb0e19ced	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_df1afb55-c8fe-47a2-8d7d-9a47855372d2	1010 bytes	ded817ecb8d9b2aa750e54a746cf63d87725719f36a5d97550d8351d46b5e944	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2d78c31a-58ae-427d-8966-db1254811974	16.04 KB	f3a85f8f484f9f5ebf08e1238fc2a9332e3ee3759f2b49e5b2743864d7aa6678	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c74e182f-0dc5-46d7-8b59-bffbb42190c0	1.21 KB	4c2d15172dbd86e5fb80af1b664940c5bab98b9e3a27c34f5987248fcf040ec7	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0e3406bc-b9a2-48c9-98e5-b9a282cad3e5	708 bytes	0ee5fbe0c1899975f01475b9c8b36035c4cc631ad987599692b46e164c3350b6	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c77ca345-1239-4809-a09f-baa07da634bb	1.58 KB	606c56344741860222a4171e069398c49e0331fbfb04c0fc37fd69629d24bfdf	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ea7e6e2-3404-42d1-b7c5-627164f837ab	2.61 KB	d43d0455455af25b42c3466d3cd3f4041cf22a64aab99addf82ae0c55c3ec08c	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_25604da3-ce65-4a60-8d5c-b7833bdebe0e	1.68 KB	ae6e63ef96530ae69b12ece4dc45ec8b0a1424d6735a70707f55f77f807abbe0	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ec6327af-e9a6-464e-a751-7559b7967727	850 bytes	1a437083770bc56268a6d97b6c0bacb02b306d85b22eb780c5d39bca8b00994f	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c829fd-352e-4623-bd1a-c7a3beecd461	491 bytes	e4295924ee4a4087eae831962333d3227bf1cd4dd951f096c65934a98e9a10b3	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_803db84d-db07-43ad-b6ff-4130e2ccc80d	825 bytes	d137168421e27f18381d9ea441abd1d8c45a5281dad9d1237887889ef42087b6	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f1a3c97-81e8-48ae-9425-f898713a4491	597 bytes	703b4ac87dc31b323f8942d2960695cb6a6ca34e15855e63b30ab0007a802318	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a1a35388-1e8d-4737-a453-2717b584320c	1.77 KB	9299f52332d53dff0cd6c724cb734c2571c5528aec9bcca70f3c5af7fda3ae74	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5710ec06-c2ff-44b4-a98c-73271ac4fcb2	2.38 KB	097db09147298db5dc60f22f82e4680a99a726426b358f5e23b8cc97d3b6feb9	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d8fc70ef-a4d5-4bea-8ad6-02cb9717c6d7	2.38 KB	93c13fbb909520e9d32af069ecb7c9b90530cb672e393889edda5a4b6f2ffe83	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4e893a07-5349-4d99-bba1-f3bb467f8311	675 bytes	4bba0e3f5d5dd5c6c0aacdc45a2c80daea65d2795eecf0076ab38093fcd35c11	✗

Host Behavior

Type	Count
Module	6
File	11351
Environment	409
Registry	1520
Mutex	411
-	256
System	940

Process #8: 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94874, Reason: Child Process
Unmonitor End Time	End Time: 282311, Reason: Terminated by Timeout
Monitor duration	187.44s
Return Code	Unknown
PID	4680
Parent PID	4976
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	0x1368	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	0x1368	0x402000(4202496)	0x1c800	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	0x1368	0x420000(4325376)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	0x1368	0x422000(4333568)	0x16200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	0x1368	0x354008(3489800)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	0x1368 / 0x124c		-	✓	1

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\run.dat	8 bytes	e78d8f4b2f5c98803fd8c0a63e9285e86222f839ed283e0b64539661373b36e4	✗
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\catalog.dat	232 bytes	aafc7b40c5fe680a2bb549c3b90aabaac63163f74fffc0b00277c6bbff88b757	✗
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\storage.dat	320.09 KB	2f7479aa2661bd259747bc89106031c11b3a3f79f12190e7f19f5df65b7c15c8	✗
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\settings.bin	24 bytes	dc3ae604991c9bb8ff8bc4502ae3d0db8a3317512c0f432490b103b89c1a4368	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\settings.bin	40 bytes	f8098a6290118f2944b9e7c842bd014377d45844379f863b00d54515a8a64b48	✗

Host Behavior

Type	Count
Module	82
System	8619
Window	17
Registry	22
Mutex	1
Process	896
File	63
User	3
Keyboard	896
Environment	2
-	4
COM	9
-	3

Network Behavior

Type	Count
DNS	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b	C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe, C:\Users\Public\Documents\[redacted]\svchost.exe	Sample File	30.50 KB	application/vnd.microsoft.portable-executable	Create, Access, Write	MALICIOUS
210ba79b18d7df0f2e08c4e1c236247a4936ef573aa224f1db1d7d9b70b07814	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	2.16 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
e78d8f4b2f5c98803fd8c0a63e9285e86222f839ed283e0b64539661373b36e4	C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\run.dat	Dropped File	8 bytes	text/plain	Create, Access, Write	CLEAN
aafc7b40c5fe680a2bb549c3b90aabaac63163f74fffc0b00277c6bbff88b757	C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\catalog.dat	Dropped File	232 bytes	application/octet-stream	Create, Access, Write	CLEAN
2f7479aa2661bd259747bc89106031c11b3a3f79f12190e7f19f5df65b7c15c8	C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\storage.dat	Dropped File	320.09 KB	application/octet-stream	Create, Access, Write	CLEAN
dc3ae604991c9bb8ff8bc4502ae3d0db8a3317512c0f432490b103b89c1a4368	C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\settings.bin, C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\settings.bak	Dropped File	24 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_676eea4e-e15a-48bd-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0e4ec6a4-ddbd-4b05-bf53-d0cd196fcc10	Dropped File	690 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b3bbad2a-3aa7-4078-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ff6b0af3-d9d6-448b-82a7-1b5351dfd1be	Dropped File	974 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_8f921901-ecf0-4e9c-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_709de7b1-7c38-4d41-880a-2aca2510b268	Dropped File	693 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
2a761c02935a44d0f783cfb34aee5b514864da12336527781fa0b341518a9e07	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b0f8684b-4a15-4c4e-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_98469bea-9168-4cdf-ade5-7044e7be7857	Dropped File	1016 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0c5d7aa3-fb8d-4fbf-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_556426f6-aecc-4bb8-8f4f-d46b696907e9	Dropped File	1.86 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bdddcf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7747426a-3553-4c0b-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_226b8498-3f59-4b9d-af62-126d30031620	Dropped File	1.27 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e5a3dbc4-c7d8-4c5b-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ab56b518-df80-48fc-a40a-ce7b4eb4ec18	Dropped File	3.79 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fba3eb17-6f3b-40cc-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bce0f13e-cb33-464d-8684-a1a039d2aa50	Dropped File	2.89 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_79f7f1f4-7db1-4081-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5084c725-0e9b-4a18-828e-65955e30dd4a	Dropped File	1.73 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_347c2958-578c-4312-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_315322d0-a280-4570-bfff-b0bca00e113b	Dropped File	925 bytes	application/octet-stream	Create, Access, Write	CLEAN
0323d4614482052e68f19ce6f1f3c415da4d6a6e64facdecc910f1c942179b8c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e9b688a1-74fb-424b-a4c4-40918f2f21c0	Dropped File	4.91 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
5f7a04aa9cbe5e26d72b167faad2c030f3aadbd1237dccc5561a699e0b560b6d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e90615c2-182d-44b3-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_de6e6c80-fa07-48b6-b475-b42293516a68	Dropped File	2.25 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_858fb4c5-ebfb-4229-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f2674441-2965-43fa-bff4-5779811b3e64	Dropped File	1.94 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73bf0bc1-f5da-4824-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_85e440a5-b476-479d-a26c-2c25d2bbadbe	Dropped File	2.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_de0996c6-5e79-4c81-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95f69f37-3d72-4379-9722-7dfe56023e93	Dropped File	1.83 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b3cb74a7-8b4e-4590-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c71d6604-8079-4d04-8703-f954eefa6c82	Dropped File	794 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1552d438-f2c8-4a68-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7c969125-2514-4e55-9a5d-1956bd655c6a	Dropped File	1.07 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6e7e7eb7-c82e-4aa1-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_04ad4a0d-b809-494b-8d8e-5b1ef6523103	Dropped File	1.77 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ab56670-54e2-48fc-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7b1ddfb4-8ea4-42d1-b49a-46641942d536	Dropped File	4.81 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73ee3bb6-aaa8-4628-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_429c54ad-b288-4ea7-8d6c-e894568299b9	Dropped File	7.79 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
3efc14d5f3f284d8b564fcc9a6df06e6e911365ac56ce54266e5631a4d33c301	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1afa74a9-01b2-4b56-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_83b4d489-f3ca-41ae-8ac4-20172e04abc4	Dropped File	711 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
9e09fa3e6c0cf5f5dcd00d2db5327c914e167430ed811638330098a42a9d7abb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9ca330bc-a578-4701-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5fde1883-2b9b-422c-8f4e-fbd41463d12a	Dropped File	3.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
000e5c18df1ae71ac0b4402c8aa8a34da881f559bc8b7edccf05ce1ff0686067	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_df188c9f-7615-4def-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3306a657-eca8-4cd1-ab29-af8aafe97080	Dropped File	1.81 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2c6c6e562e6336e90daed97a6ec6fc2e36c439a4e45f76f587bc895d0805c995	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a58c4493-9c43-4e40-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_79f8bc92-df4d-4aff-96bd-f447ed3da7e4	Dropped File	1.81 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
28de346b7d29d63eb092ccdcd69df55ba4592e5782be73d48bf50e8e217a77c7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2d26d6eb-22af-4a07-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fe81037d-2bcd-45da-8eac-26c2cc5cf4e7	Dropped File	902 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
a9b5795280d1048e0daa6e27e869492db115cf92a57a9817e6d894b0bec31b1b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_499fc8f5-be57-4e70-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_54d8e2e2-38e8-45c2-92c2-fb0ebeac7d50	Dropped File	9.67 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
d6914a2a649b85a5dfd8fd00cfb466a3b43f3663f53a017e826eef5dc6235e8e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7f58b1d8-acd2-498a-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4b99ea6a-e714-4d9c-980e-f3b06d9ae3b0	Dropped File	1.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
be0522e891f07b196eb4cdd8761c7f53caf642c16ad5d691c7d32c327f26d075	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7570fff1-6751-4484-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4ba00582-a2d0-48c9-ba5b-ebe39d5888a3	Dropped File	4.10 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ff157433bdd0e5a4a61f27172591a53d88d2e2ccfe9a5b16bf33c250cab869e8	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_88260f84-df03-4959-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_052c9a54-7507-47c8-bc69-7a64a17bb0ca	Dropped File	940 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
2410c4686683f3a71dceae28781a8ca886360d84213c426b64d40bb751329f6c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7dd186ff-55a9-4243-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_37f5caad-1373-4d2b-8754-87eecfd97bc8	Dropped File	4.30 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
bbb309c7c6bb3927cbe380a7ce2743ec5b80e4aee32f4f640049e39ddca3ef8c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6a124592-2bb4-4c6e-a547-f6d8846f0c8a	Dropped File	2.31 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ab8f309bf9116247713e709cb680ca550b2e557ccc06a4e9e7957a35bff55bc5	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_62a821dc-55dd-4743-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a4061659-dfec-4ef0-bf1c-5ce027b250a5	Dropped File	902 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1a17618fb70e56a97d01e2a76d7a18471fb05d3f102db3fa9419ba1eccc09eda	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_421f845c-a18d-48a4-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4295b2ed-5018-4e04-8efb-491b5932b3e4	Dropped File	2.67 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
0f051424fac4f2a24698fbb339c96372385eb29556e2cf43d9eed1bbdc2b6957	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e00f2fd0-0a58-4890-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5827393e-0047-47ff-9960-004c5fbe5885	Dropped File	3.11 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
182dd6206f187dc34372ef0e3f6a9b9bd7e7f2e2623e7445613a58380bc34a49	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1b26cbb5-c091-4bcc-a9e2-086e7ea4241e	Dropped File	1.49 KB	application/octet-stream	Read, Create, Access	CLEAN
1823874d8b80e06660a68b79930710e65c04b1d70d8967554b54eb83ab7ff36d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_917d511e-ca61-4d47-8831-f3b55eb99131	Dropped File	1.49 KB	application/octet-stream	Create, Access, Write	CLEAN
4efc10918360ff44d6aeefcc47750f6cb4d4c2d90d8def2f7fb50dc90f7e781f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_bed6e759-72eb-4e45-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_05921866-d46d-4c03-8c0a-741936c96791	Dropped File	2.07 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
d4a59c4162645b2dc38ea8ac7c8795b05bcd3783abf33c881fefe85fb0e19ced	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2f628527-07de-4880-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fe51fd64-42bd-482f-80c7-1b158004b548	Dropped File	2.50 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ded817ecb8d9b2aa750e54a746cf63d87725719f36a5d97550d8351d46b5e944	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_df1afb55-c8fe-47a2-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9d9a204c-57df-4ac2-b025-23619953d462	Dropped File	1010 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
f3a85f8f484f9f5ebf08e1238fc2a9332e3ee3759f2b49e5b2743864d7aa6678	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_46f1bb0e-4a51-48a8-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2d78c31a-58ae-427d-8966-db1254811974	Dropped File	16.04 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
4c2d15172dbd86e5fb80af1b664940c5bab98b9e3a27c34f5987248fcf040ec7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c74e182f-0dc5-46d7-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_de4adc50-1ed6-4915-b54b-093812d7617f	Dropped File	1.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
0ee5fbe0c1899975f01475b9c8b36035c4cc631ad987599692b46e164c3350b6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0e3406bc-b9a2-48c9-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4289b915-7b00-4da8-b59c-d89fa11b2bf9	Dropped File	708 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
606c56344741860222a4171e069398c49e0331fbfb04c0fc37fd69629d24bfdf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_19a97c7d-e131-4d9e-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c77ca345-1239-4809-a09f-baa07da634bb	Dropped File	1.58 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
d43d0455455af25b42c3466d3cd3f4041cf22a64aab99addf82ae0c55c3ec08c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4718c3e0-c931-47ee-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3ea7e6e2-3404-42d1-b7c5-627164f837ab	Dropped File	2.61 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ae6e63ef96530ae69b12ece4dc45ec8b0a1424d6735a70707f55f77f807abbe0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_677427e0-1b94-4db9-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9428f661-f4e6-43d4-81bb-34d70c8be0c0	Dropped File	1.68 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
1a437083770bc56268a6d97b6c0bacb02b306d85b22eb780c5d39bca8b00994f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a89ea3ad-87df-4a35-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_698c6765-d53e-4ace-9ecc-8e97a8d66cd5	Dropped File	850 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
e4295924ee4a4087eae831962333d3227bf1cd4dd951f096c65934a98e9a10b3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_971a2c52-c834-445a-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_73c829fd-352e-4623-bd1a-c7a3beecd461	Dropped File	491 bytes	application/octet-stream	Create, Access, Write	CLEAN
d137168421e27f18381d9ea441abd1d8c45a5281dad9d1237887889ef42087b6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b83b146a-7d6e-439e-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_803db84d-db07-43ad-b6ff-4130e2ccc80d	Dropped File	825 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
703b4ac87dc31b323f8942d2960695cb6a6ca34e15855e63b30ab0007a802318	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2da3ccc9-70bc-4781-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e8253c19-33ab-4b5e-a485-d9a145f9a371	Dropped File	597 bytes	application/octet-stream	Read, Create, Access, Write	CLEAN
9299f52332d53dff0cd6c724cb734c2571c5528aec9bcca70f3c5af7fda3ae74	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a1a35388-1e8d-4737-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f74bf451-48a0-410b-91de-ad8fb1cfd6b5	Dropped File	1.77 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
097db09147298db5dc60f22f82e4680a99a726426b358f5e23b8cc97d3b6feb9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5710ec06-c2ff-44b4-a98c-73271ac4fcb2	Dropped File	2.38 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
93c13fbb909520e9d32af069ecb7c9b90530cb672e393889edda5a4b6f2ffe83	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d8fc70ef-a4d5-4bea-8ad6-02cb9717c6d7	Dropped File	2.38 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4bba0e3f5d5dd5c6c0aacdc45a2c80daea65d2795eecf0076ab38093fcd35c11	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b501c8b5-b507-4c7d-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_07f04788-2e3f-4d57-b6fe-dbc80a39e7ed	Dropped File	675 bytes	application/octet-stream	Create, Access, Write	CLEAN
b667afe32d773d431b76965b361f1dbcce60d4627b4ca0a85e905cf4d98d634a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7db70c6b-b783-4a8b-a7b3-951946679d17	Dropped File	3.11 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
063261bb48211cca71e8f2d8ed48972fca8c12f1f11a87267e75ba50c5f1449f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_fdb68e5a-8f37-4dfc-be47-b1579962e4a3	Dropped File	1.11 KB	application/octet-stream	Read, Create, Access	CLEAN
4d87ced394269fa7c324f7a3411c8a9c020cb7f33888112e8289117979eed0d9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9609b496-b281-41b0-ba44-620e217b2664	Dropped File	598 bytes	application/octet-stream	Create, Access, Write	CLEAN
f8098a6290118f2944b9e7c842bd014377d45844379f863b00d54515a8a64b48	C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\settings.bin	Dropped File	40 bytes	application/octet-stream	Create, Access, Write	CLEAN
2ea0849530c7fdf3ec26662722ce2136dcf7a588029cf3dfd3b92081f9ac7b20	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
fa08cb9e98f7e4277058db5d9d33ba60327584a42eb30a3b3d52238dcdbda473	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
23719a572b0ac4930cea0a112250db9d722174618afae19237d8469682c410cf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
744c815e44dcff0cb645c39ae4e2faa9a1bd4b1d4c087834f8a4729de9371f45	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.70 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
9253d3186cf602edd06f8a1803442a9868d7fe5850bf497c7d69bf76973fd1d8	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.70 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
d6816f607601bef3787d27718cea995052a74809d1efd1f486e3cbd61cc5a025	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.70 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
abeb1c36498f0d04c6e81170d84b6f6e38423dd92588e5b6f8cce58c853411a0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.97 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
8ee0a5021684ebfbc04165209192d2fb8af52b10a24b6f666a3177be09c39fc3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.97 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
78aa67e9880202c432b43a7bab70e008f422508f4e1fa63a065adb05a60c94d6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
95094fe9e49a2205afc8edd054e1b8bf1656582fc72c5e213136abc5bb805178	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
142567e96d2baf6814275863da0e9fd023a269e947715b5378e3d51eebbd47c0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
7f0186ba2f401d8023deb2f13de52dc0026ff64757873e5137fed9609fc45efe	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.43 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ce78c67e751f0ccd977a855e03d1ea6fe0afd70d76e39282a702716f6efe33c4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.43 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
840a573a2aa889e87f1099b2d70f13ac903f58310e69abf55d80e8aea1fa9331	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.43 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
c2e57ca30987df4cb4ac7238a33fe378b8419edba1cba88cbab337f151a9809d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.67 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
9cb0d6e88401c33f20a3178d67523a42e9606304aaea9539e614ab6683028cd9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.67 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
86a23616e1dcd86948171ab993b0dbbe5515cdacbb941ad16a2e79a2704256b5	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.67 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
e9084e5ffe2b2af21e89b506cdabc5f077ac25ed9d0bd12b6dfb8da5f13d8cc9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.91 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
b4b72ac508ec1f58c272880874e792dd18fefacdd71dc77cfbe3d2fa877a3a81	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.91 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
67b9841ec2ecf9ace1eae4bb8d4a90a974ed01ec5f7e97012e71ee53fc224ca3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	3.91 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
22ed04090abbf5dacf94d529b7c02b8c9548f55032172fc41448d5c031ba1645	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.14 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
149b3f59efd723763be5949b3861631965a5e5affbf6aacbd518adbbb64a875b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.14 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ed859c3212910a62139a3217619184d545c17fd5f217b681168afbae2a840978	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.14 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
cb671c785af92dac17e505e8ddf42a58b8126d3d544f9f2d1e4bc58dc36e58ad	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
87ca26f05404ab41f669daf94121a91fdb1546b9b0b1a8a420dc3701d0231a4c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
ebc78e70a5c862bbde6dcf30d24f3dec31ade0f55cae0361e5862fc2efb4ad5e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.42 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
b1da3341de9b93722ad72ef0b01e5a15b3ff7e1d028fa98f71693394339d5eb4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.64 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
0462ee3b26c390a9d04e7eca73cc7a3c51c8f079fe4c6197b6b345d75ed8f4b3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.86 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
3152cedcae0854a82cb310adb9899fe0d33eb16e421f0333ffd4bd0a5528b28d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.86 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
b4ed46a1d8af04791401e97dc49bd4a27a204468fc47081247b9e9ce25de48b0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	4.86 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
da82915395283498899 71caabf3a42587cda90f3855de3b319fb6bf624ce7097	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.10 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
06c4d9f581b752363439efd73b894e4317bb59729157de2f7f93d0e1d1153c4d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.10 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
af66ff69abb3fd6b21933e0c139b297c2bfec9d331f92aad8d74c92298d32d22	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.10 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
93598b20f7b97121d4982878 03573df395a1a75fa1da9ad36aa3ac0790836b1e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.36 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
8eccfb5e416fa023901a485cb447647a62f56adc907abb90104fe2fb167e5f62	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.36 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
a5f1bf2ab97ee0fe00b7be402a148b1d2ba508f4ddf6056d79ba7c888fccedae	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.36 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
f2de7d1a4fe4b515a9206c0a8ac03abc5ab31ab0c6228948fa8d074dbe3de598	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.60 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
7b0cb62173cec725eba7246da19148b696162895ce13d11ea7da7422bf7b6582	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.60 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
1f1e3f25f8958dc59014616dbb26ef430e41068961682c8c768ecca9b8e3213a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.60 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0576a8469d79928c10a3d8e6d7ee8ab0aad169c8820a51736c794bb9bc0bd6f9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.82 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
20f1e9803f99ffd68f0a068e69cb1fa604ab5668cf548b2d5e2b79ba00e50a6f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.82 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
96562525690484ed9f425d34dd664bcb3d1ec7f56fee0806f0f38b8c42c85e09	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	5.82 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
5a6437588e6ae8cb9ddd544716999df02ada275077c80ab4347fafefb066aeaf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.04 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
fdfd9652007e0f1d859a09c562024b2962b30b45b9d63e7853119248b521b434	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.04 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
7d89fc4a55f47186cf3dcb5c3d55df743920965a4761a5abe9caa50ee876f30b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.27 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
c8defa8bf055ef93ecd685b4947dad69cfddb4dca7258419cb12ead74ec15120	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.27 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
84e08d6badb0ffb926e49dc0e0c970004e1c8a1c35cd1c4bc8d49fd315342e0c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.49 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
05eba04070a7eb2fd13050c1c44f6421db0745d4fee0f18013a18df5dd0cd258	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.49 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
961156aa031bf52742623bf1f2fc21a96da1e8bcf1ab43a7f771d6cea573bee1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.49 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
4af1955c6b6a9d41a801a448d9e4be9af5cd4e1c3235eb0c03ac3f68cdd8baff	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.75 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
7dd89677c2a8fa99af9a8c116cf58924ac4b9826c2756fc7f9c132ea6c4318d4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.75 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
4f5b2354db1b4c641a2cb2a11da058271dfd247f7ff888a988f4620281c4bc04	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.98 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
81979f49a9760265a8f3def1470ec57779536722c2043fba6b9f8ec0a5df9ad9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.98 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
adf9d919b721c0df57c95fb04fce3fb8489059139af70912e3dee45d760b0fe6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	6.98 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c9a7517f02e4b4ee7c9cb6f6dacb8231a68288879515840 5c71ff36c8e0767a1	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
cc898842dc27fd22dcdc8877345cb1c187c3a13573b423f1d960e0c2d9882edd	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
1ad8bf559a3f83a10ccf08c40e39047cb7ccf18a7ef195162400a28daf0bbc08	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.21 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
65f081797e12c3f4065d2f9f8ae29d0d30d1a65d8cbc22353e3a34ad1fd8677c	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.46 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
a4af910e0fcc6b0807ed7d3a63d7c634f2a3d52a562330b6d55fd61c2410d931	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.71 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
944b622c134e62dbf7dba847fdb181201fcc56388ec04c9f458b9fc5db22f562	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.71 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
efc94ddd8b824066cebf1d6bf3efbbedbf76f83db02404462f247f1eb64575df	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.71 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
9bda1e604eccf98cb1b5d9e9b0bbceb0673ea86167475f82793174d207b45f9e	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.94 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
72d0b6dd0ccd0394139c29ce4972946db1fee9f01b0aef793cc8259499737a91	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	7.94 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
be0bb5ba01ec1fd5fb1fd28741e548dba5efc04dd4aa62c9d19037b682814ccc	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.17 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
431c1251d35f0afb4ebe1721daf0474afb6c1fe4b7ef6aac6ab6721498ab2d6c	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.17 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
3ac1ecda72ab210e44b2f086498916c40756d26d121ddeafab63ed21fe64a02c	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.17 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
8fd905e7a8a32a12ec970f87659b9c30a73a6674a7e8ca078fb7cb75adcc1052	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.40 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
8609a78c302255e196e8db52d7fb440d564a19a3a9b261ae210755700585fc1f	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.40 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
f5ebfb6564cb6c0afe9ccf169e2e9b78b6e75f73a6210ddb4b54b18d21557571	C: \Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.64 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0ed7b5171adc4e5893b13f4e59a8aa821573f3721393fc0842e6557624dd8730	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.64 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
c20c7a51a499c585199d03fa8664c1529fecd27433870cbafbd8330b36c73638	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.64 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
8bb478852eeefdba36bb665f91337f7324c41385bfdde6edc3541a8c1d08e593	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.88 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
e6df868b087b0ef380a7b11ccd903d6236dce2a7987a55459b56045d46a3a070	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.88 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
aeefb1b9d55be54fb21128bc1ab6e80174f27b2d77b324b98851cbe866479120	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	8.88 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
02504b1a898e5a8b8b40ed00bb338ba7e1f215ddad718b67ec141f50e027d739	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.11 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
c867d6233d7cf8f6f9ff9e5ccd63ef8c71618f524900fcf42ac8b33387a47580	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.11 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
9299b6383523adf197cef678e132ee5cd2c8330b45f222ce836cf906a13b515c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.11 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
6d80ebbdaa159f225ee1522bd62ab25cec73f46e55d01b192a0fa370b43dea58	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.37 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
4224d3485353b0c163e8d27e93131c10c1cb5a3fb5e82a88000f034ec844759a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.37 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
29ba0d13272526708713226 2412eceb6f2e738a75da2a44780d4d4e7f758f618	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.37 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
d9370379d1a7036387fee9de3d7c89981a97d4677587f3fd5aaeab970024a1d1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.62 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
f6b636342a2acf6aa0fad2fa790eaf2214dafd8243defe332efa9598b9db2880	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.62 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
743f64587ca9e2dc642bd7930a2e18b9ee14772f455270c81bdad65f25271da2	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.62 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
e55ef91aa6033f2c002e8ac6fcdc27278e6faba1b9a1d92786134397a2b496fe	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	9.85 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
93aaea229ca26ac445df42cfc80fc6358d09df1a3b7374efe2cc9968c4e2423b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	10.08 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
c8406c2cccc5faadcead43862329d1deba8d38241713f38b7249f4e88b2571bc	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	10.08 KB	application/octet-stream	Read, Create, Access, Write	CLEAN
c88b864ff46839799b77362b58bc9393bfabd3ada0bd2c7afabb31f10c5e110a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	10.08 KB	application/octet-stream	Read, Create, Access, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe.config	Accessed File	Access	CLEAN
C:\Users\Public\Documents\[redacted]	Accessed File	Create, Access	CLEAN
C:\Users\Public\Documents	Accessed File	Access	CLEAN
C:\Users\Public\Documents\[redacted]\svchost.exe	Sample File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	Sample File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\run.dat	Dropped File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\Exceptions\1.2.2.0	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe:Zone.Identifier	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\catalog.dat	Dropped File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\storage.dat	Dropped File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\settings.bin	Dropped File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\settings.bak	Dropped File	Create, Delete, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\Logs\RDhJ0CNFevzX	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\03845CB8-7441-4A2F-8C0F-C90408AF5778\Logs	Accessed File	Create, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrcompression.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SysWOW64\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:\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\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\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\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

File Name	Category	Operations	Verdict
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
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

File Name	Category	Operations	Verdict
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
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\Microsoft.WSMan.Management	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.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

File Name	Category	Operations	Verdict
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\PSScheduledJob\PSScheduledJob.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\ScheduledTasks	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SecureBoot	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\SecureBoot\SecureBoot.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Storage	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Storage\Storage.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\TLS	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\TLS\TLS.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\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\PKI	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PKI\PKI.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\TroubleshootingPack	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\TrustedPlatformModule\TrustedPlatformModule.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\VpnClient	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\VpnClient\VpnClient.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\Wdac	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Wdac\Wdac.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\WindowsDeveloperLicense\WindowsDeveloperLicense.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\WindowsUpdate	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Modules.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Modules.psm1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Modules.cdxml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Modules.xaml	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Modules.dll	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PnpDevice	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PnpDevice\PnpDevice.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PrintManagement	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PrintManagement\PrintManagement.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PSDiagnostics	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PSScheduledJob	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\1.0.0.1.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\1.0.0.1.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\1.0.0.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\1.0.0.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\1.0.0.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://cdn.discordapp.com/attachments/886962207051640872/890689205934620692/4102A6C4.jpg	-	162.159.130.233	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
friomo.duckdns.org	194.147.140.25	-	DNS	SUSPICIOUS
cdn.discordapp.com	162.159.133.233, 162.159.130.233, 162.159.129.233, 162.159.135.233, 162.159.134.233	-	DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	DNS, UDP	CLEAN
162.159.130.233	cdn.discordapp.com	-	DNS, HTTPS, TCP	CLEAN
8.8.8.8	-	-	DNS, UDP	CLEAN
194.147.140.25	friomo.duckdns.org	Mongolia	DNS, TCP	CLEAN
162.159.135.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.133.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.129.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.134.233	cdn.discordapp.com	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\{5fb3fc63-476b-43ac-865e-d84d77cfacac}	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
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_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\Users\Public\Documents\[redacted]\svchost.exe	read, access, write	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	SUSPICIOUS
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_CURRENT_USER	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	create, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	read, access, write	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	powershell.exe, 6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.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\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\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\Microsoft\NET Framework Setup\NDP\v4\Client	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Client\Install	read, access	powershell.exe	CLEAN

Process

Process Name	Commandline	Verdict
6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe"	MALICIOUS
6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe"	MALICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\Public\Documents\[redacted]\svchost.exe" -Force	CLEAN
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe" -Force	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	NanoCoreRAT	NanoCore RAT	Memory Dump	-	Backdoor	5/5

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.37642032	C:\Users\RDhJ0CNFevzX\Desktop\6a19a144807268d406c6da55513ae24493b2d411ba8e2a2e15567d66e55d976b.exe	MALICIOUS
Memory Dump	Gen:Variant.Cerbu.11615	-	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	2021-09-27 16:34:30+00:00
Built-in AV Database Records	10473840

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