MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe**
ID	#4517666
MD5	f0bec0deb10b8bc59a5b2d207b4cdeef
SHA1	452b936847f131abd4b872815ab35c9b9bcd9cbb
SHA256	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83
File Size	183.50 KB
Report Created	2022-06-06 12:43 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (18 rules, 23 matches)

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe tries to delete zone identifier of file "C:\ProgramData\images.exe".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #4) images.exe modifies memory of (process #6) cmd.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #4) images.exe creates thread in (process #6) cmd.exe.			
4/5	Reputation	Resolves known malicious domain	1	-
	• Resolved domain "udooiuyt.dynamic-dns.net" is a known malicious domain.			
3/5	Network Connection	Performs DNS request for known DDNS domain	1	-
	• (Process #4) images.exe resolves host name "udooiuyt.dynamic-dns.net" of dynamic DNS provider "changeip.com".			
2/5	Discovery	Executes WMI query	1	-
	• (Process #4) images.exe executes WMI query: .			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #6) cmd.exe has a thread which sleeps more than 5 minutes. • (Process #4) images.exe has a thread which sleeps more than 5 minutes.			
1/5	System Modification	Modifies application directory	2	-
	• (Process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe modifies "C:\Program Files\Microsoft DN1". • (Process #4) images.exe modifies "C:\Program Files\Microsoft DN1".			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe starts (process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe with a hidden window. • (Process #4) images.exe starts (process #4) images.exe with a hidden window.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe adds "C:\ProgramData\images.exe" to Windows startup via registry.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #4) images.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Reads system data	1	-
	• (Process #4) images.exe reads the cryptographic machine GUID from registry.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #4) images.exe resolves host name "udooiuyt.dynamic-dns.net" to IP "45.137.22.163".			

Score	Category	Operation	Count	Classification
1/5	Network Connection	Connects to remote host	1	-
	• (Process #4) images.exe opens an outgoing TCP connection to host "45.137.22.163:5200".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #4) images.exe tries to connect to TCP port 5200 at 45.137.22.163.			
1/5	Obfuscation	Overwrites code	2	-
	• (Process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe overwrites code to possibly hide behavior. • (Process #4) images.exe overwrites code to possibly hide behavior.			
1/5	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe resolves 312 API functions by name. • (Process #4) images.exe resolves 313 API functions by name.			
1/5	Execution	Executes itself	1	-
	• (Process #1) b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe.			
-	Trusted	Known clean file	1	-
	• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\r1nl1b3y.rqq.psm1" is a known clean file.			

Mitre ATT&CK Matrix

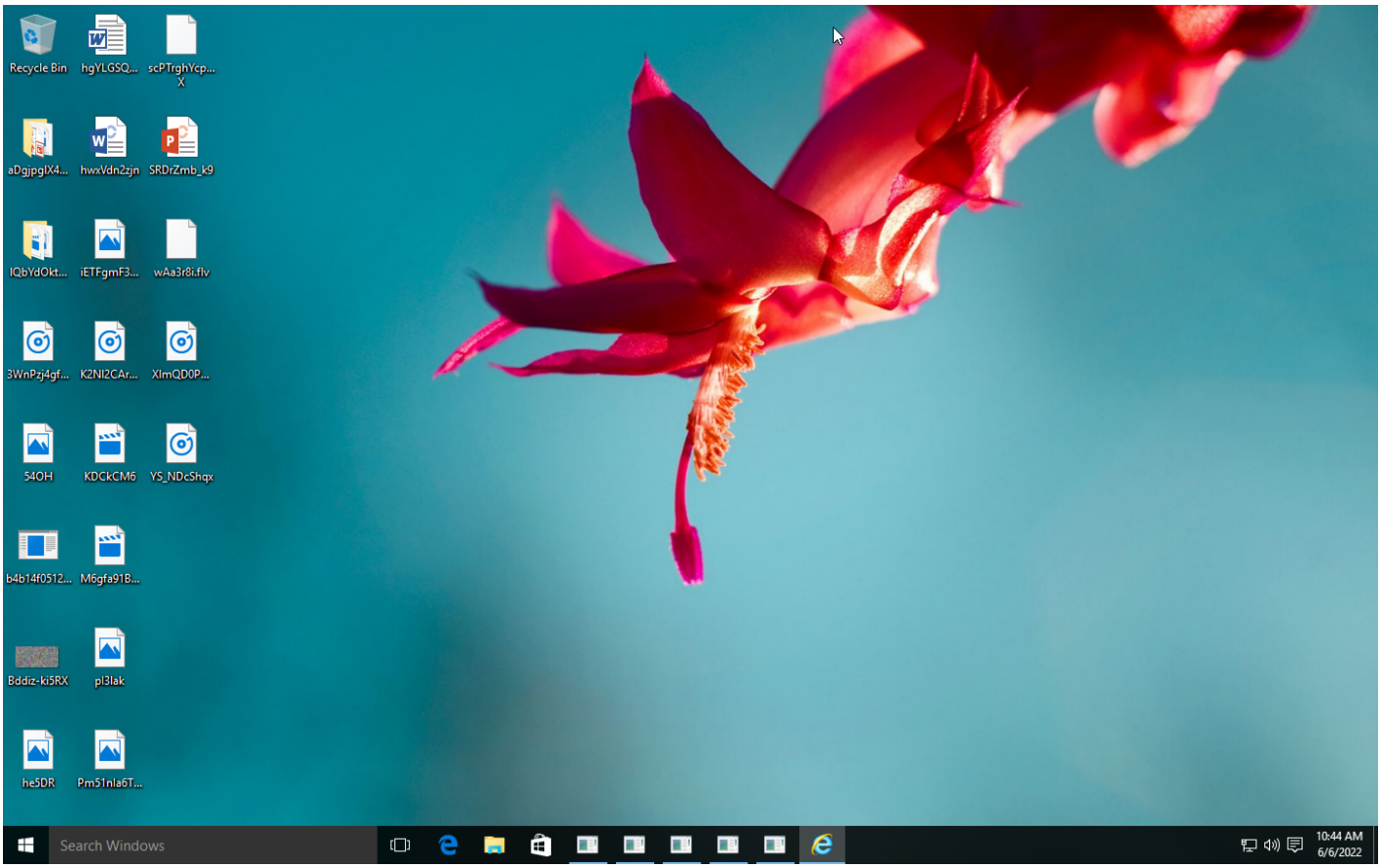
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window		#T1082 System Information Discovery			#T1065 Uncommonly Used Port		
				#T1112 Modify Registry		#T1012 Query Registry					
				#T1096 NTFS File Attributes							
				#T1045 Software Packing							

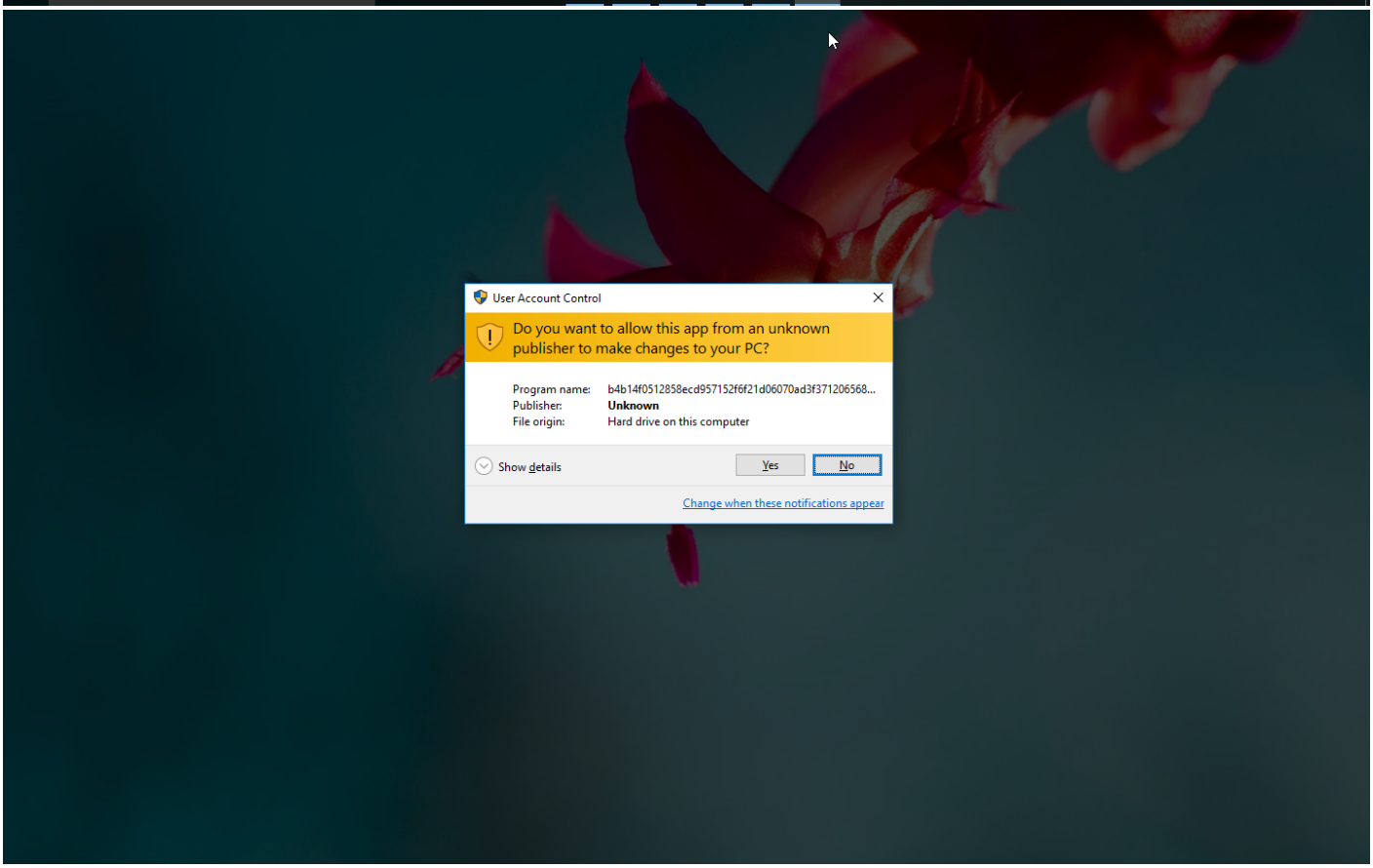
Sample Information

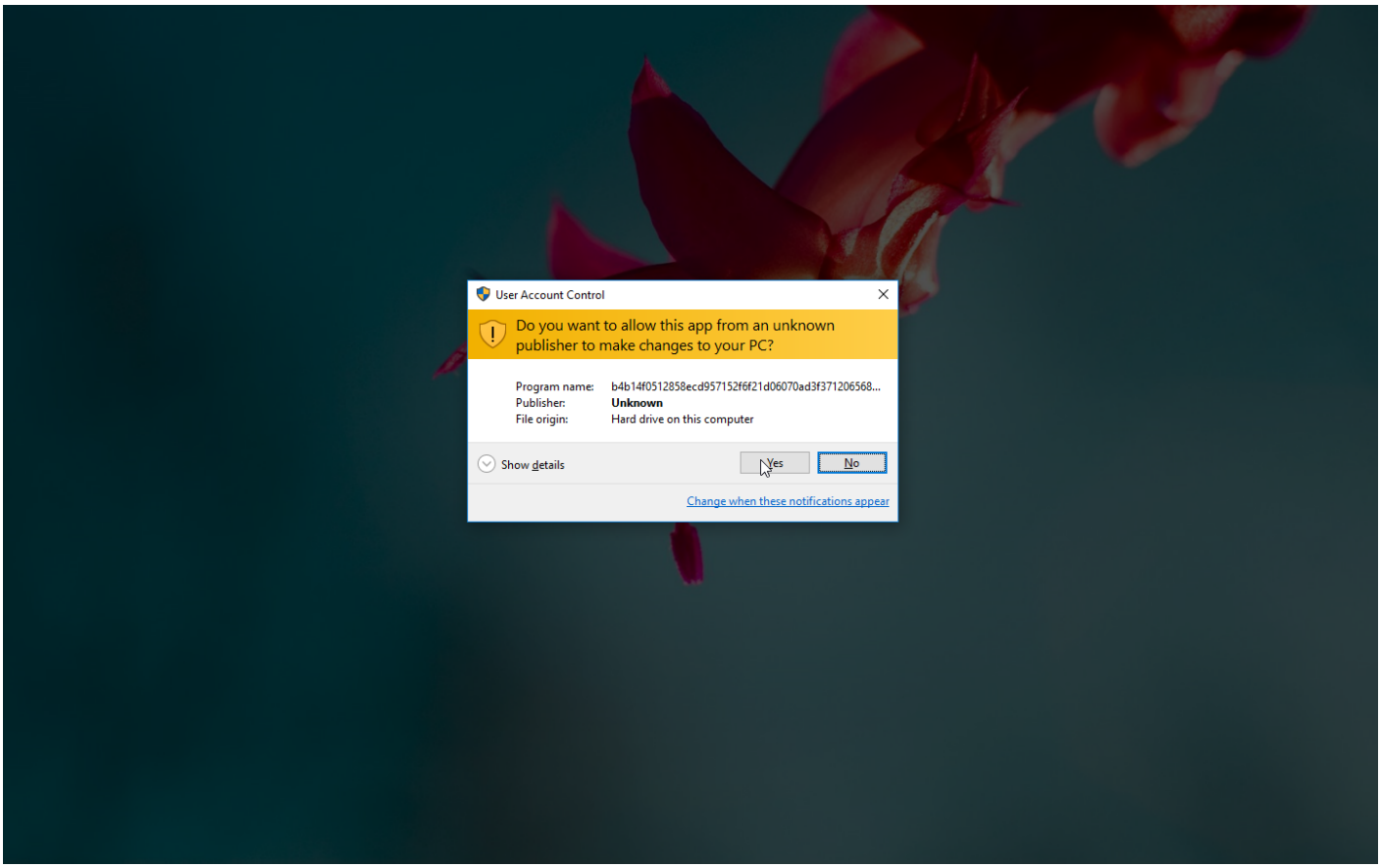
ID	#4517666
MD5	f0bec0deb10b8bc59a5b2d207b4cdeef
SHA1	452b936847f131abd4b872815ab35c9b9bcd9cbb
SHA256	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83
SSDeep	3072:hFZRWMN2EyOdnHN/0f5B2gPcvTt728bZK3LyAw1HG7GMbcDK90XKgwcG2O5NCMLo:aMXHB0zlSTt728N5tuWXKVvPHq7
ImpHash	b89c0acb10e1bafbe56a95fb03ea7ddd
File Name	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe
File Size	183.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

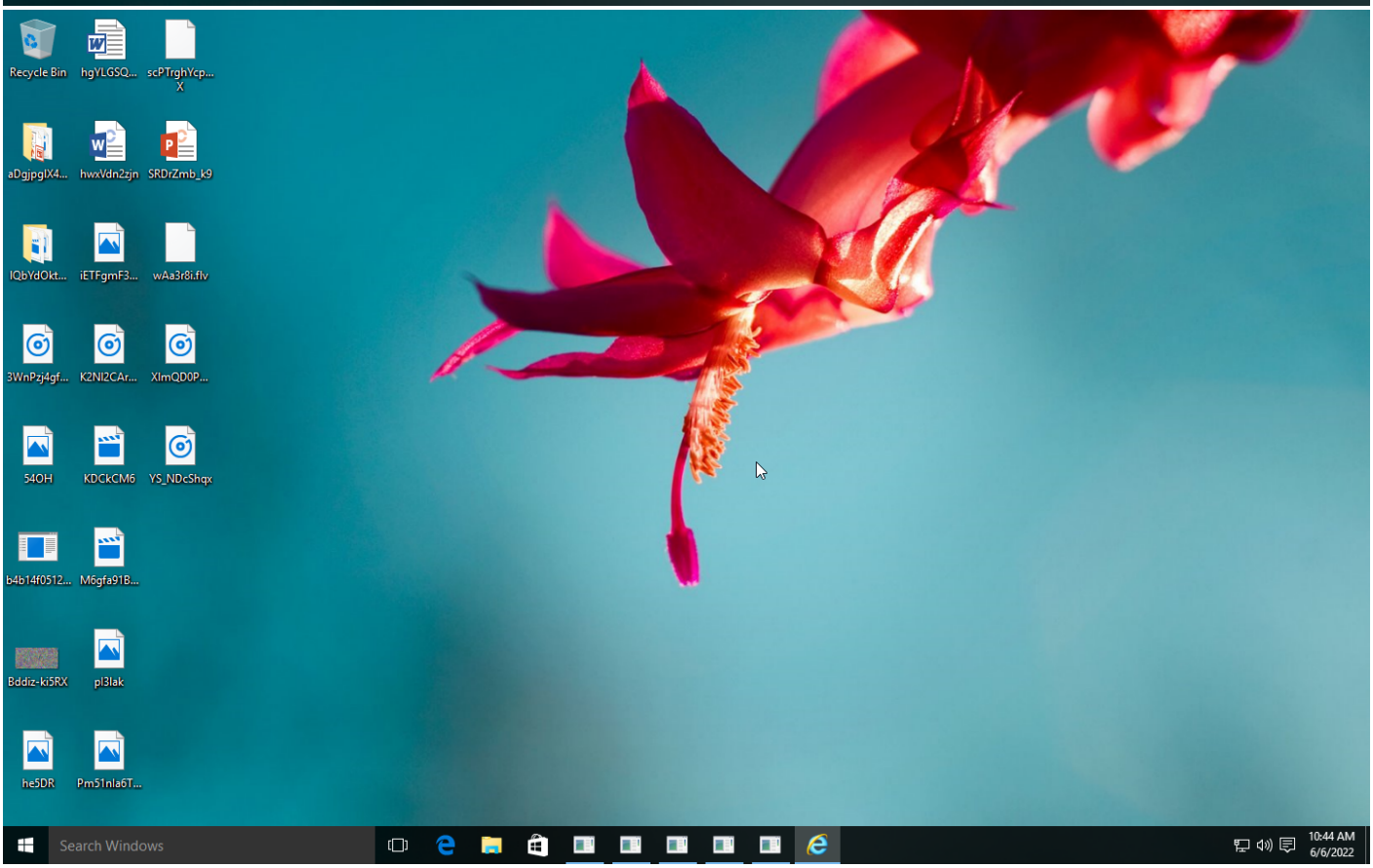
Analysis Information

Creation Time	2022-06-06 12:43 (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	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
hgYLGSQ...
scPTrghYcp...
X
aDgjpgIX4...
hwxVdn2zjn
SRDrZmb_k9
IQbYdOkt...
iETFgmF3...
wAa3r8i.flv
3WnPzj4gf...
K2NI2CAr...
XlmQD0P...
54OH
KDCkCM6
YS_NDcShqx
b4b14f0512...
M6gfa91B...
Bddiz-ki5RX
pl3lak
he5DR
Pm51nla6T...
Search Windows
10:44 AM
6/6/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: b4b14f0512858ecd957152f6f21d06070ad3f371206568...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

1.61 KB total sent

598 bytes total received

2 ports 5200, 53

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	udooiuyt.dynamic-dns.net	NO_ERROR	45.137.22.163		NA

BEHAVIOR

Process Graph

Process #1: b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 66504, Reason: Analysis Target
Unmonitor End Time	End Time: 144362, Reason: Terminated
Monitor duration	77.86s
Return Code	0
PID	2976
Parent PID	1932
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	183.50 KB	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83	✖

Host Behavior

Type	Count
Module	410
Window	249
System	136
File	14
-	7
Mutex	14
Registry	9
Process	2
COM	1
Environment	1

Process #3: powershell.exe

ID	3
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	powershell Add-MpPreference -ExclusionPath C:\
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 141353, Reason: Child Process
Unmonitor End Time	End Time: 308772, Reason: Terminated by timeout
Monitor duration	167.42s
Return Code	Unknown
PID	3456
Parent PID	2976
Bitness	32 Bit

Dropped Files (21)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b7aa28d5-c07d-4fa3-a057-0006651d806f	1.83 KB	859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b58d55c1-44f2-4801-9046-2bf0948be95f	2.25 KB	5f7a04aa9cbe5e26d72b167faad2c030f3aadbd1237dccc5561a699e0b560b6d	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fee7b07-4249-469c-8e77-059b1a0893b8	1016 bytes	2a761c02935a44d0f783cfb34aee5b514864da12336527781fa0b341518a9e07	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_77bee94e-8407-4ba9-a4bc-e727958d71d4	1.27 KB	1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bddcf	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_902b44a1-4761-4de3-bc8e-0cf406e24530	690 bytes	4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7fa0d0e1-fd56-4a34-a123-4fa7b641ee97	4.81 KB	d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_80f8d62d-7a61-4ae5-bee1-b16e091c0604	693 bytes	d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\r1nl1b3y.rqq.psm1	1 bytes	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2fe42bb7-c7e4-460c-aa00-9d49bea128e5	925 bytes	4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b8282425-dfaa-4779-a972-aed090c62b86	1.73 KB	33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_8a12d684-f76a-4c35-b868-3bf9f868835e	794 bytes	4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_54415d7c-53c0-4bb9-b247-295a127dc231	7.79 KB	b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	✖

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7dd5c5-5282-497a-aab7-c42f30b0d596	3.79 KB	34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d402a6eb-5577-4d4f-a9b5-367feb9e2a75	2.42 KB	ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9b145d57-d591-4a56-acd6-a4c89787e7f0	4.91 KB	0323d4614482052e68f19ce6f1f3c415da4d6a6e64facdecc910f1c942179b8c	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d949b570-9ee1-4703-aa20-a8d9d314630f	1.86 KB	6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_62c55fb7-1ea1-4722-95ed-2a854a673897	1.77 KB	760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5e68c54d-fa8b-42b7-b2f2-864d3fdc9ec0	974 bytes	627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6d49f2a0-e6f8-4398-b8a5-0816938bad54	1.94 KB	196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9304cd69-ae0b-4b5d-99b4-eb9f871d477d	1.07 KB	1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3986c98c-c639-4206-bf2a-5a52d6e8dadf	2.89 KB	91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	✖

Host Behavior

Type	Count
File	12165
Registry	731
-	120
Mutex	168
System	360
Environment	208
Module	9
User	2
-	1

Process #4: images.exe

ID	4
File Name	c:\programdata\images.exe
Command Line	"C:\ProgramData\images.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 142821, Reason: Child Process
Unmonitor End Time	End Time: 308772, Reason: Terminated by timeout
Monitor duration	165.95s
Return Code	Unknown
PID	176
Parent PID	2976
Bitness	32 Bit

Host Behavior

Type	Count
System	1053
Window	249
Module	416
-	5
Registry	9
File	14
Process	3
-	7
-	1
Mutex	9
-	1
COM	2
-	1
Environment	1

Network Behavior

Type	Count
DNS	1
TCP	1

Process #5: powershell.exe

ID	5
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	powershell Add-MpPreference -ExclusionPath C:\
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 203423, Reason: Child Process
Unmonitor End Time	End Time: 308772, Reason: Terminated by timeout
Monitor duration	105.35s
Return Code	Unknown
PID	5112
Parent PID	176
Bitness	32 Bit

Dropped Files (6)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5bde1bf8-6441-4991-a87f-23ddbecbbff0	1.83 KB	859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b9bfd780-12a8-412f-88ba-d793b8f7c3b8	2.25 KB	5f7a04aa9cbe5e26d72b167faad2c030f3aadbd1237dccc5561a699e0b560b6d	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\rqrvmrt4.m3y.ps1	1 bytes	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f487eaec-ce45-421c-bf35-c6e543664a4f	794 bytes	4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6ffaac7c-e630-426c-983b-90a7c7bcac99	1.07 KB	1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_047927fe-b20c-406d-a7a1-3a54f40092bf	2.89 KB	91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	✖

Host Behavior

Type	Count
File	6065
Environment	134
Registry	567
System	256
Mutex	100
-	60
Module	9
-	1
User	2

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 203690, Reason: Child Process
Unmonitor End Time	End Time: 308772, Reason: Terminated by timeout
Monitor duration	105.08s
Return Code	Unknown
PID	5076
Parent PID	176
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#4: c:\programdata\images.exe	0x238	0x20000(131072)	0x800	✔	1
Modify Memory	#4: c:\programdata\images.exe	0x238	0x30000(196608)	0x103	✔	1
Create Remote Thread	#4: c:\programdata\images.exe	0x238	0x2010e(131342)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\images.exe	183.50 KB	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83	✖

Host Behavior

Type	Count
System	776
Process	773
Environment	12
Module	11
Registry	17
File	62

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83	C:\Users\RDhJ0CNFevzX\Desktop\b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe, C:\ProgramData\images.exe	Sample File	183.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
859d86cd7b237289c836b9a4d5fcecc4dd12b81e8093b36ddeeafe554c1ea6c2	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5bde1bf8-6441-4991-...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b7aa28d5-c07d-4fa3-a057-0006651d806f	Dropped File	1.83 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
cf0df8e249d263d56f176653c3b2c8c6f82b97d84d7ba6a3b1b59ab269d7bc75	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	2.97 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
5f7a04aa9cbe5e26d72b167faad2c030f3aadbd1237dccc5561a699e0b560b6d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b58d55c1-44f2-4801-...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b9bfd780-12a8-412f-88ba-d793b8f7c3b8	Dropped File	2.25 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
2a761c02935a44d0f783cfb34aee5b514864da12336527781fa0b341518a9e07	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fee7b07-4249-469c-8e77-059b1a0893b8	Dropped File	1016 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
7c2b466fe08e68db82bb85e9ae9c809c9707f2c1fab2d702fd328c971d02b849	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	3.43 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
884e9939683bdeac72709939a6792ebc55ebb33e4533a7e588e3141f99ecb328	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.75 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f0e32b5a1ab685adb7ffe69f81c93ce8ad9478497a1be6dbdf60b54d970bf17e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.04 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a712a428d5a2823618e05ea0dea4f25af44e3ae185962a1b77bb96dbe17db872	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
1c6d2138e5de6c498ce47beaa181f5717420306bfffc174c75d7b2f7d9bdddcf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_77bee94e-8407-4ba9-a4bc-e727958d71d4	Dropped File	1.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
55493109d7e8c8aefd051d3a7745034d6c2b8f9522a5b82f18c5b9e062574244	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	3.21 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
4985daa10ab2e4770670a38d5cd2a15c3fd7cd1c8ed679d202a5e9e09b983fc3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_902b44a1-4761-4de3-bc8e-0cf406e24530	Dropped File	690 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d50565da7a88193302998e0f8f3d72ceaa151dbdeffa2e51d961917e0bc57537	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7fa0d0e1-fd56-4a34-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0cf70ae4-6773-489a-ba97-c66494b427aa	Dropped File	4.81 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
afbc519e06b114d7bda4438df8ae207eee290c450f1647734a9e85271ca43ab7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.98 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
c49a729beae4eb35d972bb07f05d203c295ea158057afb6fe7beed89676fccdc	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.49 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b23e8cff81177d96beab97719c6568d45dcb015fcee6cf6f1af46d61fc9adedf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	4.86 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
54228fb011c17df2ce5c806e51a332d3ea7f841f71551ca3112dfead766ab538	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	5.82 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
94c1827c04dc51b341bfdd0c9830e1e4bace81d4973658177f7a8997651113adb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	7.21 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ab00a0faddb58a36f5e80fe02764241217aa29c8bd30f544bf25dc35fc9c16fd	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	2.42 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d4047357a1edf5d34dafe49e58d3023d40fda12732c9e7e7e65fa6769e7aacf4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_80f8d62d-7a61-4ae5-bee1-b16e091c0604	Dropped File	693 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
b46c2b03a4d3a775a86dcda7f5ba0ac0cdff79a34a8a9834a3c79c9e724a81bc	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	3.91 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\r1nl1b3y.rqq.psm1, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\vnwpgmcr.mmw.ps1, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\rqrvmrt4.m3y.ps1, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\yro3ppfs.tea.psm1	Dropped File	1 bytes	application/octet-stream	Access, Create, Delete, Write	CLEAN
349b1670e62b0b642e7c50f7b5c3479995004c01825e5d73fcdeb344e85afcc5	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.49 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
46ff794f4d025de4275916935df7a09974091b945bb4097029a673f1cff77a7c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.04 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
91ce2d4bade453914ef73b343000699887213b2780b70e610f7c2c5d4e03309c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	4.42 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
5234aacb7bd281b71b4cba2c72113983cc0e3981ff5851f82d7b1094d6949d14	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	5.36 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dd32f818380a8b62a70335030f1a249ebd71a1585e52cb6ef85b86cd5030a415	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	4.64 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
4a2dd2df7152fb43329c7556364a6bc21bff2ecf04b405fe1d92cc5443dd8ab6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_2fe42bb7-c7e4-460c-aa00-9d49bea128e5	Dropped File	925 bytes	application/octet-stream	Access, Create, Write	CLEAN
33c437958cadcc941697cc775c7530d7f3cf2ed35a82980406411ac7f02e7c10	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b8282425-dfaa-4779-a972-aed090c62b86	Dropped File	1.73 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f2ae841c1b370773b377c9390c507fc404455aa9a24dbecdd6325ae1fa2b87eb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	7.21 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
4a2fa6deca0ec447255cbf4e535ee0ea6c3a239fd3d111bf7c0f8f0ab629dd75	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_8a12d684-f76a-4c35-... ...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f487eaec-ce45-421c-bf35-c6e543664a4f	Dropped File	794 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
6b290ad64d61ad3c0bb313df53d4df1cf0faabcb51b810c43595b0543d03f889	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	5.60 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b85946385a713a0b3157830a59d2b29bb2a1fec55ab88e4871360e0b244e7476	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_54415d7c-53c0-4bb9-... ...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b44503bc-656c-473f-b74a-2c1b95cfb155	Dropped File	7.79 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
34ed6390a3bc4bc2e0e7fa5c8e4623e59d88ad14e14b96513d812689493be057	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_be7dd5c5-5282-497a-aab7-c42f30b0d596	Dropped File	3.79 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ee6e3226afd49cda69f95d7fda445afb1e2a68035bdb25fefbfd6c38dbe5ebaf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d402a6eb-5577-4d4f-a9b5-367feb9e2a75	Dropped File	2.42 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
18646bc1ca8d0fcef57ef2ce346f2fb6a1ef3718a3f0f41a05d045c533b59677	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	5.82 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
0323d4614482052e68f19ce6f1f3c415da4d6a6e64facdecc910f1c942179b8c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9b145d57-d591-4a56-acd6-a4c89787e7f0	Dropped File	4.91 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a86dfe1b9b4d780ec065dab9e5da86e280717a1404945ae1849a26a5e3ea740f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.75 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e1b9ac65db1eaf83151c1dba1df338ead4aab065910e9cbf07cb7c707180e82a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	3.67 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d524f49d3105859b2710336ec9503766f5e8b14550762a0aa80b6c4a024f14cf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	6.98 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b47b2f06ee2a47ae1901e9178643a0af3dac30cdb58670b6c0b3cc00bf82ffcc	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	4.14 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
6b6c06abd51531f3f2129e3927074b7df0624435d9fc652883b6e2b57fc6db02	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d949b570-9ee1-4703-aa20-a8d9d314630f	Dropped File	1.86 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
760834a2fc0a34fe77b0f5baf9ce839ba004b7fd73d0c9750476f472a10ad229	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_62c55fb7-1ea1-4722-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_8da28785-77df-4cdd-82ea-56a7c77f9dec	Dropped File	1.77 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
36b2a37b7ac293919b1b73a3d80a69aa979806ddadb13884d73ac268a8f8c476	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	4.86 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
83b5984164cf87daddb7667235d5cf07778c21296704548631b7bcf7520968bb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	5.10 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
de6747fba9c2e9edf879c75115dcdbda7c568fbcafad5f80f943f68a9bab8c9e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	5.60 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
627e6b88e61562ed24ee216f5153264bbd7bb259605f2f9f89beed3c4aefca57	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5e68c54d-fa8b-42b7-b2f2-864d3fdc9ec0	Dropped File	974 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
196decb4f6feb7877e81dd16a579487ac2815ed2c17d6825a283e7e9ed488c40	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6d49f2a0-e6f8-4398-b8a5-0816938bad54	Dropped File	1.94 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
1847a56755536a3dbef979ed8ef80e5b20ed1ffb27895876a9d80b592c278cd7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6ffaac7c-e630-426c-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9304cd69-ae0b-4b5d-99b4-eb9f871d477d	Dropped File	1.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
91963953d5bab4cf5d8b01acaf5f39e809e32567ec8794e810566e8402e220c7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_047927fe-b20c-406d-...\...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_3986c98c-c639-4206-bf2a-5a52d6e8dadf	Dropped File	2.89 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e9371d62ffc8c23da48f777b3f1d9117357bed04e33cb8f073c1b9bba2c0345f	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	2.70 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ceac0873fd572d797a0d9bdf461b67120bdfccb9a2dd8cc5a4b198bdc1ce1fba	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File	2.16 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
C:\ProgramData\images.exe	Sample File, Dropped File, VM File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\Microsoft.Management.Infrastructure.CimCmdlets\Microsoft.Management.Infrastructure.CimCmdlets.psd1	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\International\en\International.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsConfig.Types.ps1xml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b7aa28d5-c07d-4fa3-a057-0006651d806f	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ConsoleHost	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\MSFT_DASiteTableEntry.cdxml	Accessed File	Access, Read	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PrintManagement	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.Format.ps1xml	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\BranchCache\BranchCacheOrchestrator.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\dnslookup.psm1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Storage	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCacheHostedCacheServerSettingData.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\en\Microsoft.WSMan.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\Microsoft.Dtc.PowerShell.psd1	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.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.Types.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Kds\Microsoft.KeyDistributionService.Cmdlets\Microsoft.KeyDistributionService.Cmdlets.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Kds\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCacheClientSettingData.cdxml	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\iSCSI\en\iSCSI.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.InternationalSettings.Commands	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\iSCSI\en-US\iSCSI.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\WSMan.format.ps1xml	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\NetAdapter\MSFT_NetAdapterVmqQueue.cmdletDefinition.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\Microsoft.Dtc.PowerShell\Microsoft.Dtc.PowerShell.dll	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetSecurity	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.cmdletDefinition.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsCmdlets.Format.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.cdxml	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.Dtc.PowerShell\Microsoft.Dtc.PowerShell.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\International\Microsoft.InternationalSettings.Commands\Microsoft.InternationalSettings.Commands.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5e68c54d-fa8b-42b7-b2f2-864d3fdc9ec0	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.cdxml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft_Corporation\DefaultDomain_Path_vts5ulh4lcatsmkjq054m5tgofqeypsd\10.0.10586.0\user.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\r1nl1b3y.rqq.psm1	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Dism\Microsoft.Dism.PowerShell.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\International\Microsoft.InternationalSettings.Commands.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\TestDtc.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\Microsoft.Dtc.PowerShell.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterEncapsulatedPacketTaskOffload.cdxml	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\Microsoft.Dtc.PowerShell	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\en\ISE.psd1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_8a12d684-f76a-4c35-b868-3bf9f868835e	Dropped File, Accessed File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterIPsecOffload.Format.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRss.Format.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\Microsoft.Management.Infrastructure.CimCmdlets	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSIConnection.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterQos.cdxml	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_b9bfd780-12a8-412f-88ba-d793b8f7c3b8	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\en\EventTracingManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.dll	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TLS	Accessed File	Access	CLEAN
C:\ProgramData	Accessed File	Access, Create	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterAdvancedProperty.cmdletDefinition.cdxml	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\Microsoft.BackgroundIntelligentTransfer.Management.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterRsc.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PKI	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx\Microsoft.Windows.Appx.PackageManager.Commands	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Dism\Dism.psm1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.types.ps1xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc38888a-7080-4220-9b7d-de7a9b2167ba	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\1.0.0.1.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\vnwpgmcr.mmw.ps1	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.psm1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9304cd69-ae0b-4b5d-99b4-eb9f871d477d	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\en\AppLocker.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\International\Microsoft.InternationalSettings.Commands\Microsoft.InternationalSettings.Commands.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	Accessed File	Access, Read	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\NetNat\NetNat.psd1	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\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\MSFT_DAClientExperienceConfiguration.format.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\TestDtc	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\MSFT_NetAdapterChecksumOffload.cdxml	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\PS_DnsClientNrptPolicy_v1.0.0.cdxml	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.xaml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetNat	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\Kds\Microsoft.KeyDistributionService.Cmdlets.cdxml	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WindowsPowerShell\profile.ps1	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\NetAdapter\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_0cf70ae4-6773-489a-ba97-c66494b427aa	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsConfig.Format.ps1xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.Formats.ps1xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_54415d7c-53c0-4bb9-b247-295a127dc231	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx\en\Appx.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx\Appx.format.ps1xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d949b570-9ee1-4703-aa20-a8d9d314630f	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.BackgroundIntelligentTransfer.Management\Microsoft.BackgroundIntelligentTransfer.Management.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_80f8d62d-7a61-4ae5-bee1-b16e091c0604	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Diagnostics\Microsoft.PowerShell.Commands.Diagnostics.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx\Microsoft.Windows.Appx.PackageManager.Commands\Microsoft.Windows.Appx.PackageManager.Commands.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Diagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.Dtc.PowerShell\Microsoft.Dtc.PowerShell.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.InternationalSettings.Commands\Microsoft.InternationalSettings.Commands.xaml	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\EventTracingManagement\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	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\AppLocker\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets\Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\PS_DnsClientNRPTGlobal_v1.0.0.cdxml	Accessed File	Access, Read	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Kds	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.InternationalSettings.Commands\Microsoft.InternationalSettings.Commands.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	Accessed File	Access, Read	CLEAN

Reduced dataset

Domain

Domain	IP Address	Country	Protocols	Verdict
udooiuyt.dynamic-dns.net	45.137.22.163	-	DNS, TCP	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
45.137.22.163	udooiuyt.dynamic-dns.net	Netherlands	DNS, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	delete, access	images.exe, b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN
Global\PowerShell_CommandAnalysis_Lock_S-1-5-21-1560258661-3990802383-1811730007-1000	delete, access	powershell.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\Transcription	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPer1_0Server	access, write	images.exe, b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\OAlerts\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\PipelineMaxStackSizeMB	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	access, read	images.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Internet Explorer	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Key Management Service\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Images	access, write	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\OAlerts	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\Transcription	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	images.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\HardwareEvents\PowerShell	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPerServer	access, write	images.exe, b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WSMAN	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WSMAN\ServiceStackVersion	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Windows PowerShell\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	access	b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Key Management Service	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	create, access	images.exe, b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Internet Explorer\PowerShell	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\HardwareEvents	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Environment	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\V7Q5BQYDTT	create, access	images.exe, b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\V7Q5BQYDTT\inst	access, write, read	images.exe, b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment\PSMODULEPATH	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\Environment\PSMODULEPATH	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Windows PowerShell	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds	access	powershell.exe	CLEAN

Process

Process Name	Commandline	Verdict
b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe	"C:\Users\RDhJ0CNFevzX\Desktop\b4b14f0512858ecd957152f6f21d06070ad3f371206568871d0f92d5a41ecd83.exe"	MALICIOUS
images.exe	"C:\ProgramData\images.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe"	SUSPICIOUS
powershell.exe	powershell Add-MpPreference -ExclusionPath C:\	CLEAN
powershell.exe	powershell Add-MpPreference -ExclusionPath C:\	CLEAN

YARA / AV

No YARA or AV matches available.

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	4.5.1
Dynamic Engine Version	4.5.1 / 05/09/2022 04:24
Static Engine Version	4.5.1.0 / 2022-05-09 03:00:28
AV Exceptions Version	4.5.1.25 / 2022-04-28 14:12:58
Link Detonation Heuristics Version	4.5.1.34 / 2022-05-26 20:19:34
Smart Memory Dumping Rules Version	4.5.1.25 / 2022-04-28 14:12:58
Config Extractors Version	4.5.1.34 / 2022-05-26 20:19:34
Signature Trust Store Version	4.5.1.30 / 2022-05-16 06:57:54
VMRay Threat Identifiers Version	4.5.1.34 / 2022-05-26 20:19:34
YARA Built-in Ruleset Version	4.5.1.29

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