MALICIOUS

Classifications: Downloader

Threat Names: -

Verdict Reason: -

Sample Type	**Word Document**
File Name	**template[1].doc**
ID	#5143442
MD5	8f21756219d4e736219011174eb0534b
SHA1	4429c35b62d55abe159e130c095fc988e640f3fd
SHA256	394c97cc9d567e556a357f129aea03f737cbd2a1761df32146ef69d93afc73dc
File Size	59.00 KB
Report Created	2022-08-13 22:41 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (12 rules, 16 matches)

Score	Category	Operation	Count	Classification
4/5	Network Connection	Downloads file	2	Downloader
	• (Process #1) winword.exe downloads file via http from http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXllz8vjv1TPmuyrc2ylu.mp3. • (Process #1) winword.exe downloads file via http from http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXllz8vjv1TPmuyrc2ylu.ico.			
4/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
	• (Process #4) rundll32.exe uploads 122.604KB data using HTTP POST.			
4/5	Network Connection	Attempts to connect through HTTP	2	-
	• (Process #1) winword.exe connects to http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXllz8vjv1TPmuyrc2ylu.mp3. • (Process #1) winword.exe connects to http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXllz8vjv1TPmuyrc2ylu.ico.			
4/5	Network Connection	Attempts to connect through HTTPS	2	-
	• (Process #4) rundll32.exe connects to https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel. • (Process #4) rundll32.exe connects to https://www.google.com.			
4/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Windows\system32\rundll32.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.			
3/5	Anti Analysis	Delays execution	1	-
	• (Process #4) rundll32.exe has a thread which sleeps more than 5 minutes.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) winword.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Execution	Executes macro on specific event	1	-
	• Executes macro automatically on target "document" and event "open".			
2/5	Execution	Drops PE file	2	-
	• (Process #1) winword.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll". • (Process #1) winword.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\wnitmpo.dll".			
1/5	Mutex	Creates mutex	1	-
	• (Process #4) rundll32.exe creates mutex with name "MyMutextuin".			
1/5	Heuristics	Contains suspicious meta data	1	-
	• Office document contains below average content data.			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			

Mitre ATT&CK Matrix

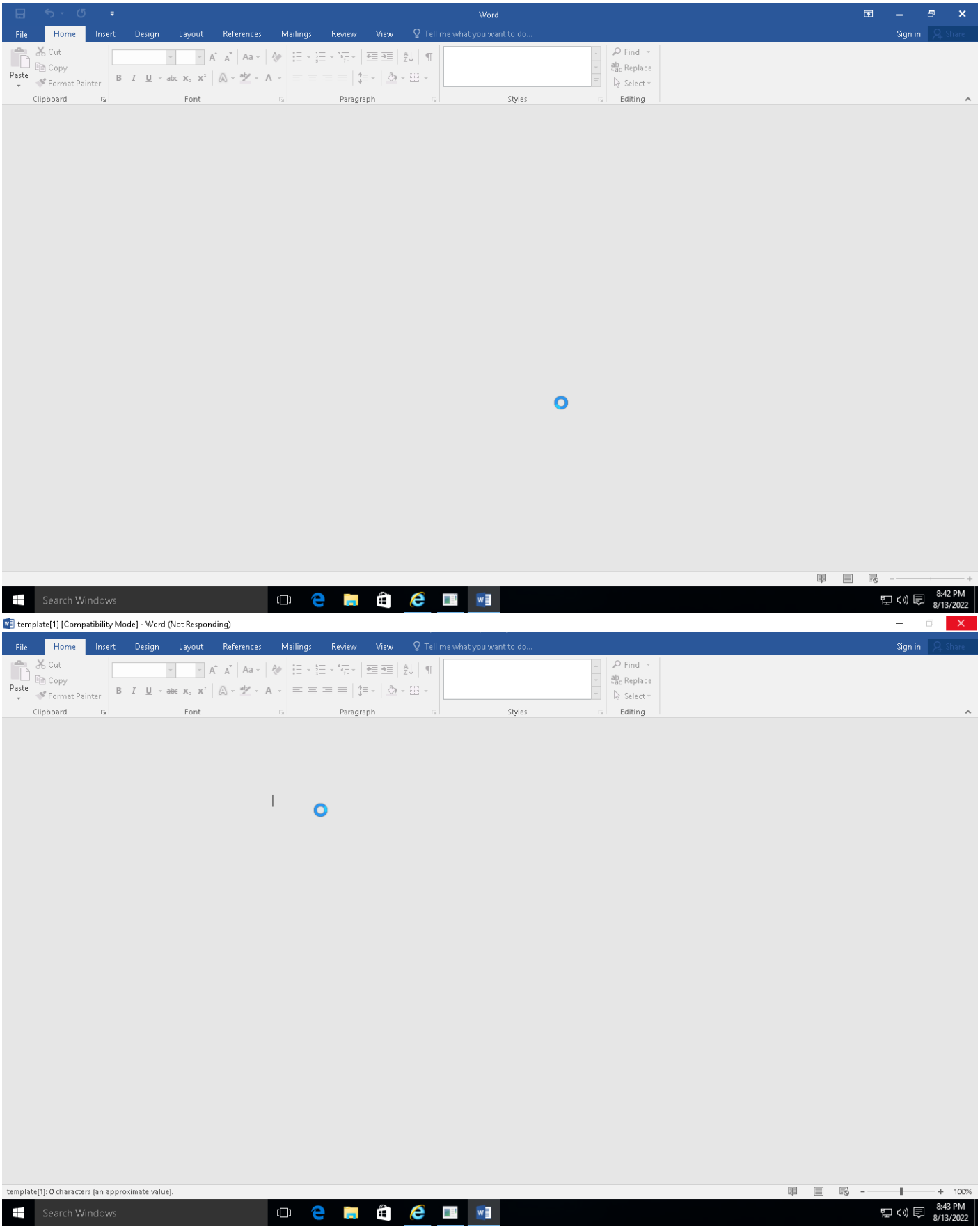
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1064 Scripting	#T1081 Credentials in Files	#T1083 File and Directory Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
	#T1053 Scheduled Task							#T1005 Data from Local System	#T1105 Remote File Copy		
									#T1032 Standard Cryptographic Protocol		

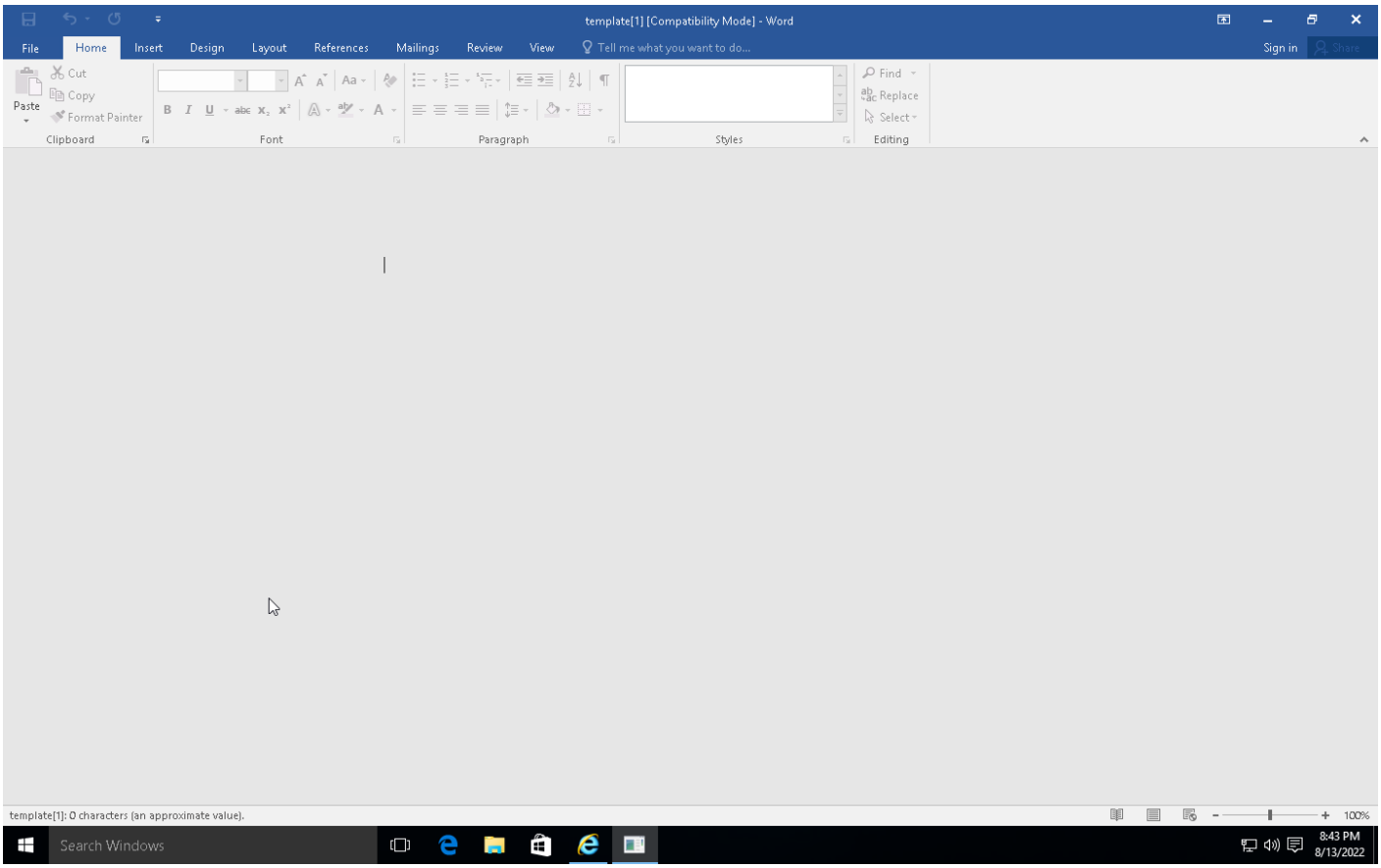
Sample Information

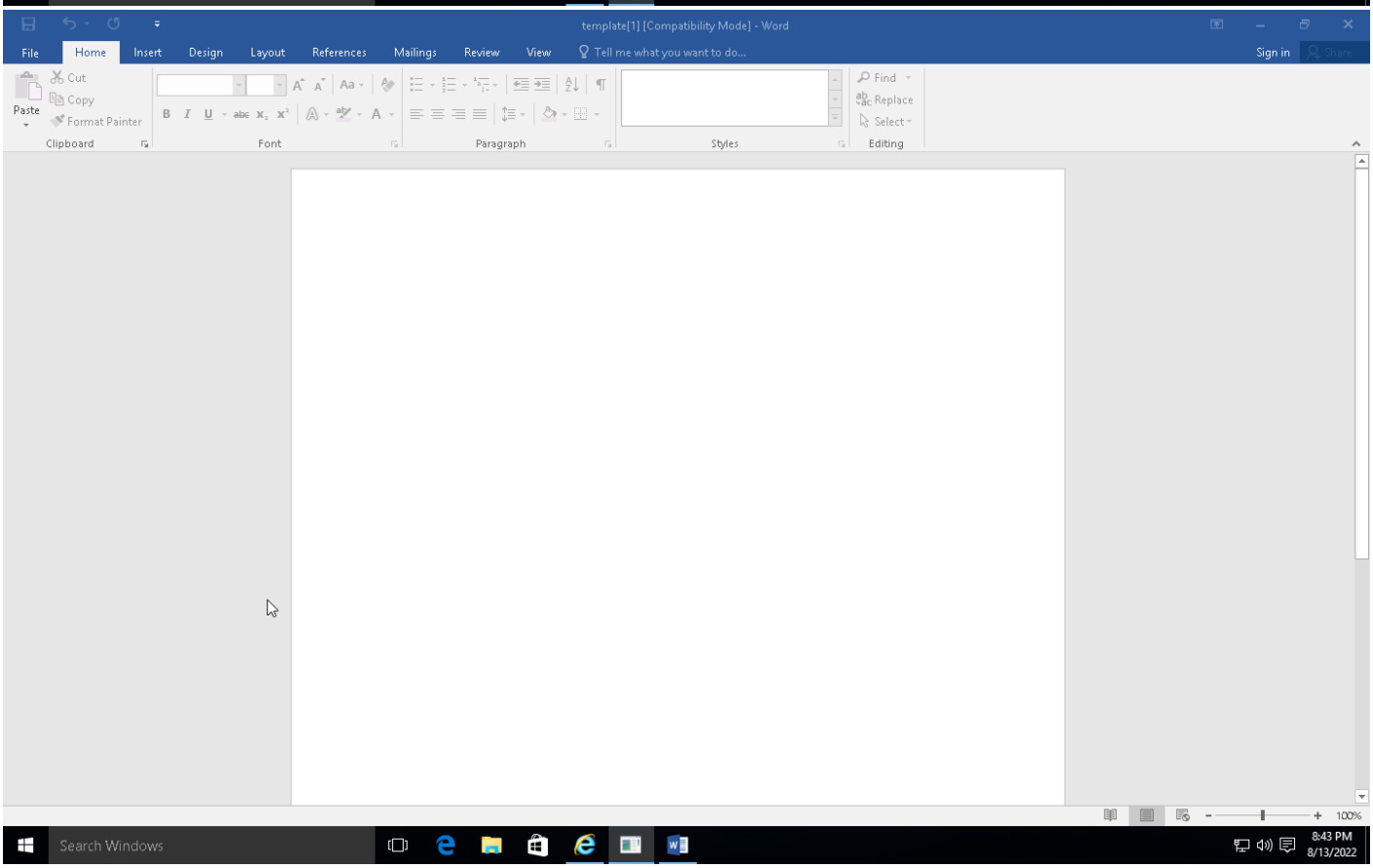
ID	#5143442
MD5	8f21756219d4e736219011174eb0534b
SHA1	4429c35b62d55abe159e130c095fc988e640f3fd
SHA256	394c97cc9d567e556a357f129aea03f737cbd2a1761df32146ef69d93afc73dc
SSDeep	768:urH9EDL1s1p6qCS1ioGwmFRdoUzQLgRlpqVmbTzD1CNJbOz+zaN18OlZ5grp/0GR:ur6Lm1p7QDdoaQLgRYm7pQNOz71lW5R
File Name	template[1].doc
File Size	59.00 KB
Sample Type	Word Document
Has Macros	✔

Analysis Information

Creation Time	2022-08-13 22:41 (UTC+2)
Analysis Duration	00:04:07
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	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


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 Editing
Find Replace Select
Search Windows
8:42 PM 8/13/2022
template[1] [Compatibility Mode] - Word (Not Responding)
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 Editing
Find Replace Select
template[1]: 0 characters (an approximate value).
100%
Search Windows
8:43 PM 8/13/2022





Screenshots truncated

NETWORK

General

249.32 KB total sent

401.76 KB total received

4 ports 80, 443, 53, 445

4 contacted IP addresses

1 URLs extracted

4 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

106 sessions, 252.62 KB sent, 724.95 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.google.com	-	-		0 bytes	NA
GET	http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2ylu.mp3	-	-		0 bytes	NA
GET	http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2ylu.ico	-	-		0 bytes	NA
POST	https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel	-	-		0 bytes	NA
POST	https://www.google.com	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	com.lightbuzear.buzz	NO_ERROR	64.52.80.180		NA
A	www.google.com	NO_ERROR	216.58.212.164		NA
A	worldoptions.buzz	NO_ERROR	64.52.80.45		NA

BEHAVIOR

Process Graph

Process #1: winword.exe

ID	1
File Name	c:\program files (x86)\microsoft office\office16\winword.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 63319, Reason: Analysis Target
Unmonitor End Time	End Time: 311211, Reason: Terminated by timeout
Monitor duration	247.89s
Return Code	Unknown
PID	4808
Parent PID	1972
Bitness	32 Bit

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCache\IE\5RNK44FE\OGHAYZZFhfCtspqorBFNYMrxHN7TXllz8vjv1TPmuyrc2ylu[1].ico	4.04 KB	95db57f061cf2727bed50ec9a5c91fb10d94fc6b49897ea6857f91c7affb4ffe	✖
C:\ProgramData\Windose.txt	88 bytes	460b4e4095c0c983517b80c81ab918a0d24149fa222d2625b9ad78a8e9e0f5bb	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll	310.00 KB	3a11cd850a5c7d077d270f39f68d1f16a174a7d4bfc057dd95fa79b8133a4d6f	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\wnitmpo.dll	310.00 KB	022ee269651686570c983e78450948c8e2dcfda0244d0d7d2aac7f8723507298	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\wnitmpo.dll	310.00 KB	c5480e975998c3556f1c0d70924ce3d9e8b56676fe13639ebf409add3ccf20c3	✖

Host Behavior

Type	Count
Keyboard	61
Module	51
File	180
System	3
Environment	1
COM	1

Network Behavior

Type	Count
HTTP	2

Process #2: svchost.exe

ID	2
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: 119441, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 311211, Reason: Terminated by timeout
Monitor duration	191.77s
Return Code	Unknown
PID	864
Parent PID	4808
Bitness	64 Bit

Process #3: rundll32.exe

ID	3
File Name	c:\windows\system32\rundll32.exe
Command Line	C:\Windows\system32\rundll32.exe "C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll",Rdwmnjioffws
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 130155, Reason: Child Process
Unmonitor End Time	End Time: 311211, Reason: Terminated by timeout
Monitor duration	181.06s
Return Code	Unknown
PID	3188
Parent PID	864
Bitness	64 Bit

Process #4: rundll32.exe

ID	4
File Name	c:\windows\syswow64\rundll32.exe
Command Line	C:\Windows\system32\rundll32.exe "C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll",Rdwmnjioffws
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 139000, Reason: Child Process
Unmonitor End Time	End Time: 311211, Reason: Terminated by timeout
Monitor duration	172.21s
Return Code	Unknown
PID	2748
Parent PID	3188
Bitness	32 Bit

Host Behavior

Type	Count
Module	989
Environment	1
File	8
Mutex	1
System	109
User	2
Registry	380

Network Behavior

Type	Count
HTTPS	105

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
394c97cc9d567e556a357f129aea03f737cbd2a1761df32146ef69d93afc73dc	C:\Users\RDhJ0CNFevzX\Desktop\template[1].doc	Sample File	59.00 KB	application/vnd.ms-word.document.macroEnabled.12	-	MALICIOUS
5bcaa3dc31090a32e9f7813b5583f5df7a8a8d9d65e0f80daa013df5d8ba35c1	-	Web Response	1.55 KB	text/html	-	CLEAN
95db57f061cf2727bed50ec9a5c91fb10d94fc6b49897ea6857f91c7affb4ffe	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCache\IE\5RNK44FE\OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2ylu[1].ico	Downloaded File	4.04 KB	application/octet-stream	Access, Create, Read	CLEAN
460b4e4095c0c983517b80c81ab918a0d24149fa222d2625b9ad78a8e9e0f5bb	C:\ProgramData\Windose.txt	Dropped File	88 bytes	text/plain	Access, Create, Read, Write	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
3a11cd850a5c7d077d270f39f68d1f16a174a7d4bfc057dd95fa79b8133a4d6f	C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll	Dropped File	310.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
b5e0eee6e28efca6d6ad05d7b8a94631576037ec9e5ff6d305fe89faa0e1032e	-	Web Response	5 bytes	text/plain	-	CLEAN
022ee269651686570c983e78450948c8e2dcfda0244d0d7d2aac7f8723507298	C:\Users\RDHJ0C~1\AppData\Local\Temp\wnitmpo.dll	Dropped File	310.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	CLEAN
c5480e975998c3556f1c0d70924ce3d9e8b56676fe13639ebf409add3ccf20c3	C:\Users\RDHJ0C~1\AppData\Local\Temp\wnitmpo.dll	Downloaded File	310.00 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\system32\rundll32.exe	-	-	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\template[1].doc	Sample File, VM File	-	MALICIOUS
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\h8ucitgd\oghayzzfhfctspqorbfnymrxhn7txilz8vjv1tpmuyrc2yiu[1].mp3	Downloaded File, Extracted File	-	CLEAN
C:\windows\system32\drivers\ehdrv.sys	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\windows\system32\drivers\gzflt.sys	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	Accessed File	Access	CLEAN
ThisDocument	-	-	CLEAN
C:\windows\system32\drivers\360AvFlt.sys	Accessed File	Access	CLEAN
C:\windows\system32\drivers\bsfs.sys	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\wnitmpo.dll	Dropped File, Downloaded File, Extracted File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Windows\SysWOW64\rundll32.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\windows\system32\drivers\aswsp.sys	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCache\IE\5RNK44FE\OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2ylu[1].ico	Accessed File, Downloaded File, Extracted File	Access, Create, Read	CLEAN
C:\ProgramData\Windose.txt	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\windows\system32\drivers\klif.sys	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://com.lightbuzear.buzz/Kolpt523ytcserstrew/torel	-	64.52.80.180	-	POST	CLEAN
http://www.google.com	-	216.58.212.164	-	-	CLEAN
http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2ylu.mp3	-	64.52.80.45	-	GET	CLEAN
https://www.google.com	-	216.58.212.164	-	POST	CLEAN
http://worldoptions.buzz/agE7nqQLgssuVeUY/OGHAYZZFhfCtspqorBFNYMrxHN7TXIlz8vjv1TPmuyrc2ylu.ico	-	64.52.80.45	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.google.com	216.58.212.164	-	TCP, DNS, HTTPS	CLEAN
com.lightbuzear.buzz	64.52.80.180	-	TCP, DNS, HTTPS	CLEAN
worldoptions.buzz	64.52.80.45	-	TCP, DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
64.52.80.180	com.lightbuzear.buzz	United States	TCP, DNS, HTTPS	CLEAN
64.52.80.45	worldoptions.buzz	United States	TCP, DNS, HTTP	CLEAN
216.58.212.164	www.google.com	United States	TCP, DNS, HTTPS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
MyMutextuin	access	rundll32.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE40\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001B-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE40\ParentKeyName	read, access	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-040C-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0090-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IEData\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0016-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WIC\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00E2-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayVersion	read, access	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\c1c4f01781cc94c4c8fb1542c0981a2a\ProductIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001A-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WIC\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IEData\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayIcon	read, access	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0044-0409-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-012B-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WIC\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0115-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\6E815EB96CCE9A53884E7857C57002F0	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0409-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0018-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\ParentKeyName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IEData\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\InstallLocation	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-001F-0C0A-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0011-0000-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	rundll32.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\WindowsInstaller	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayIcon	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-002C-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-00BA-0409-0000-0000000FF1CE}	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\UninstallString	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-0015-0409-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-006E-0409-0000-0000000FF1CE}\SystemComponent	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Office16.PROPLUS\ReleaseType	read, access	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\ParentKeyName	read, access	rundll32.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
rundll32.exe	C:\Windows\system32\rundll32.exe "C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll",Rdwmnjioffws	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
rundll32.exe	C:\Windows\system32\rundll32.exe "C:\Users\RDHJ0C~1\AppData\Local\Temp\dnrdfsi11023.dll",Rdwmnjioffws	CLEAN
winword.exe	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n	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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.16 / 2022-08-10 15:34:29
YARA Built-in Ruleset Version	4.6.1.10

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	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