MALICIOUS

Classifications: Ransomware

Threat Names: Mal/Generic-S CatB CatB.Loader

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**bucbja.dll**
ID	#6950503
MD5	a9e08e50aee2180cb8c6c3ee669ba785
SHA1	940be8f144bde7713e592dea4d3f3fda90bd7c37
SHA256	3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642
File Size	118.66 KB
Report Created	2023-02-23 18:59 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 37 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #16) msdtc.exe modifies the content of multiple user files.			
5/5	YARA	Malicious content matched by YARA rules	5	Ransomware
	• Rule "CatB" from ruleset "Ransomware" has matched on a memory dump for (process #1) jhafdvir.exe. • Rule "CatB_Loader" from ruleset "Ransomware" has matched on a memory dump for (process #1) jhafdvir.exe. • Rule "CatB_FunctionStrings" from ruleset "Ransomware" has matched on the function strings for (process #16) msdtc.exe. • Rule "CatB" from ruleset "Ransomware" has matched on the dropped file "C:\windows\system32\oci.dll". • Rule "CatB_FunctionStrings" from ruleset "Ransomware" has matched on the function strings for (process #21) msdtc.exe.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels file "C:\windows\system32\oci.dll" as Mal/Generic-S. • Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Defense Evasion	Accesses physical drive	3	-
	• (Process #1) jhafdvir.exe accesses physical drive "\\.\PhysicalDrive0". • (Process #16) msdtc.exe accesses physical drive "\\.\PhysicalDrive0". • (Process #21) msdtc.exe accesses physical drive "\\.\PhysicalDrive0".			
2/5	Defense Evasion	Sends control codes to connected devices	3	-
	• (Process #1) jhafdvir.exe controls device "\\.\PhysicalDrive0" through API DeviceIOControl. • (Process #16) msdtc.exe controls device "\\.\PhysicalDrive0" through API DeviceIOControl. • (Process #21) msdtc.exe controls device "\\.\PhysicalDrive0" through API DeviceIOControl.			
2/5	Defense Evasion	Loads a dropped DLL	2	-
	• Dropped DLL oci.dll is side-loaded into (Process #16) msdtc.exe. • Dropped DLL oci.dll is side-loaded into (Process #21) msdtc.exe.			
1/5	System Modification	Modifies operating system directory	1	-
	• (Process #1) jhafdvir.exe creates file "C:\windows\system32\oci.dll" in the OS directory.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) jhafdvir.exe enumerates running processes.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) jhafdvir.exe starts (process #17) cmd.exe with a hidden window.			
1/5	Hide Tracks	Changes folder appearance	16	-

Score	Category	Operation	Count	Classification
		• (Process #16) msdtc.exe changes the appearance of folder "C:\Users". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Contacts". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Desktop". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Documents". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Downloads". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Favorites". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Favorites\Links". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Links". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Music". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\OneDrive". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Pictures". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Saved Games". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Searches". • (Process #16) msdtc.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Videos".		
1/5	Execution	Drops PE file	1	-
		• (Process #1) jhafdvir.exe drops file "C:\windows\system32\oci.dll".		
1/5	Obfuscation	Resolves API functions dynamically	1	-
		• (Process #1) jhafdvir.exe resolves 92 API functions by name.		

Mitre ATT&CK Matrix

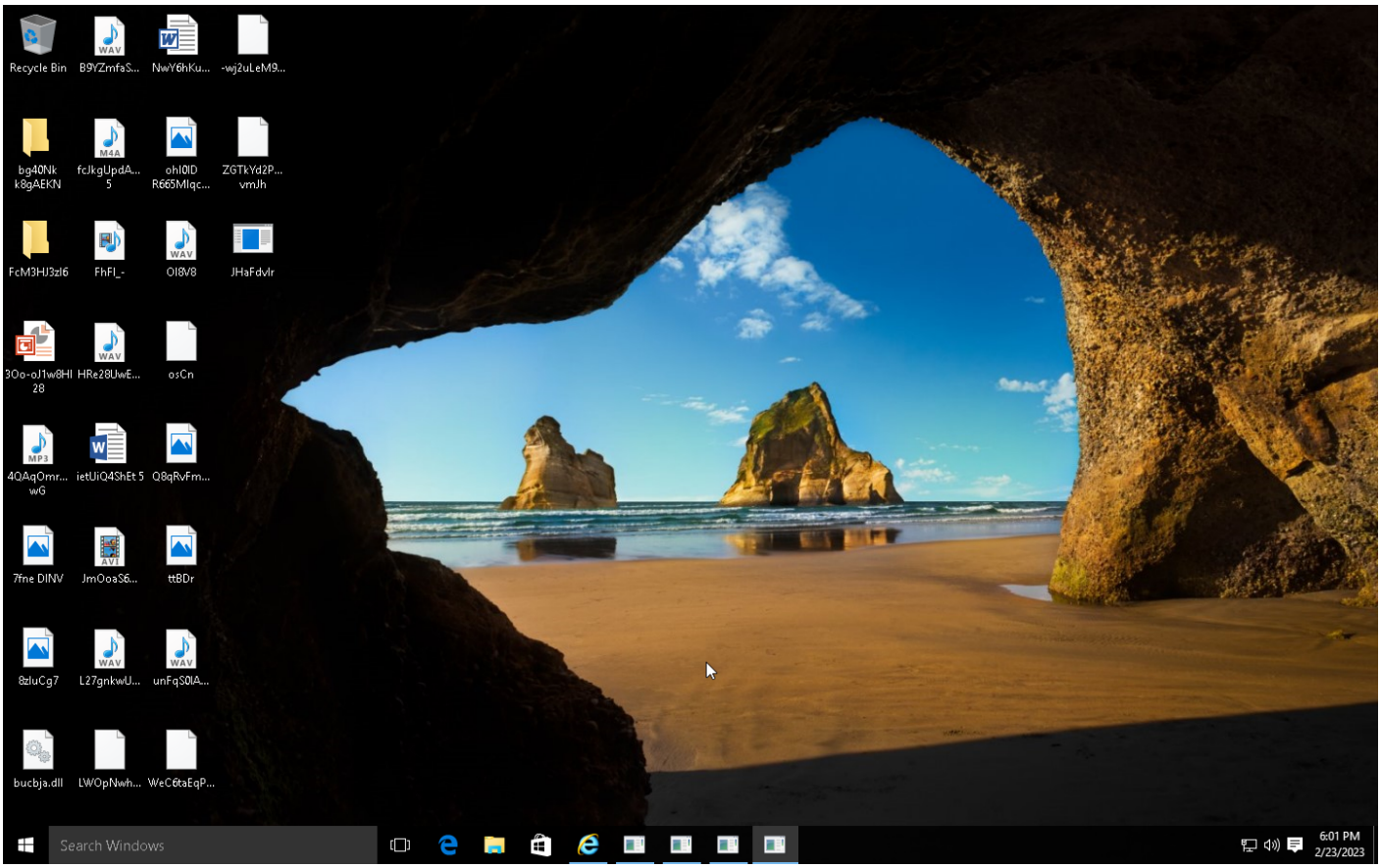
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1006 File System Logical Offsets		#T1057 Process Discovery					#T1486 Data Encrypted for Impact
				#T1143 Hidden Window							
				#T1036 Masquerading							
				#T1073 DLL Side-Loading							
				#T1045 Software Packing							

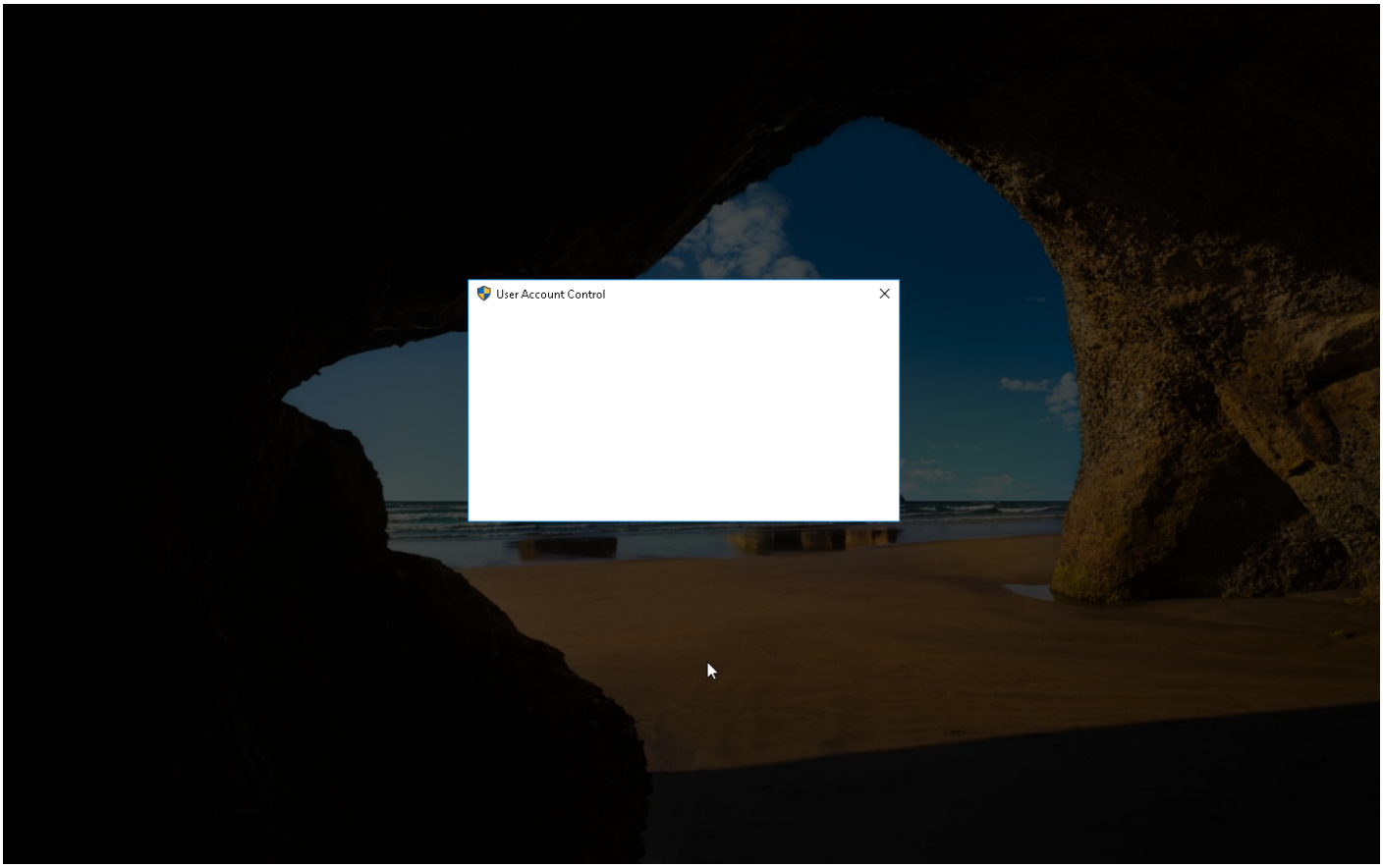
Sample Information

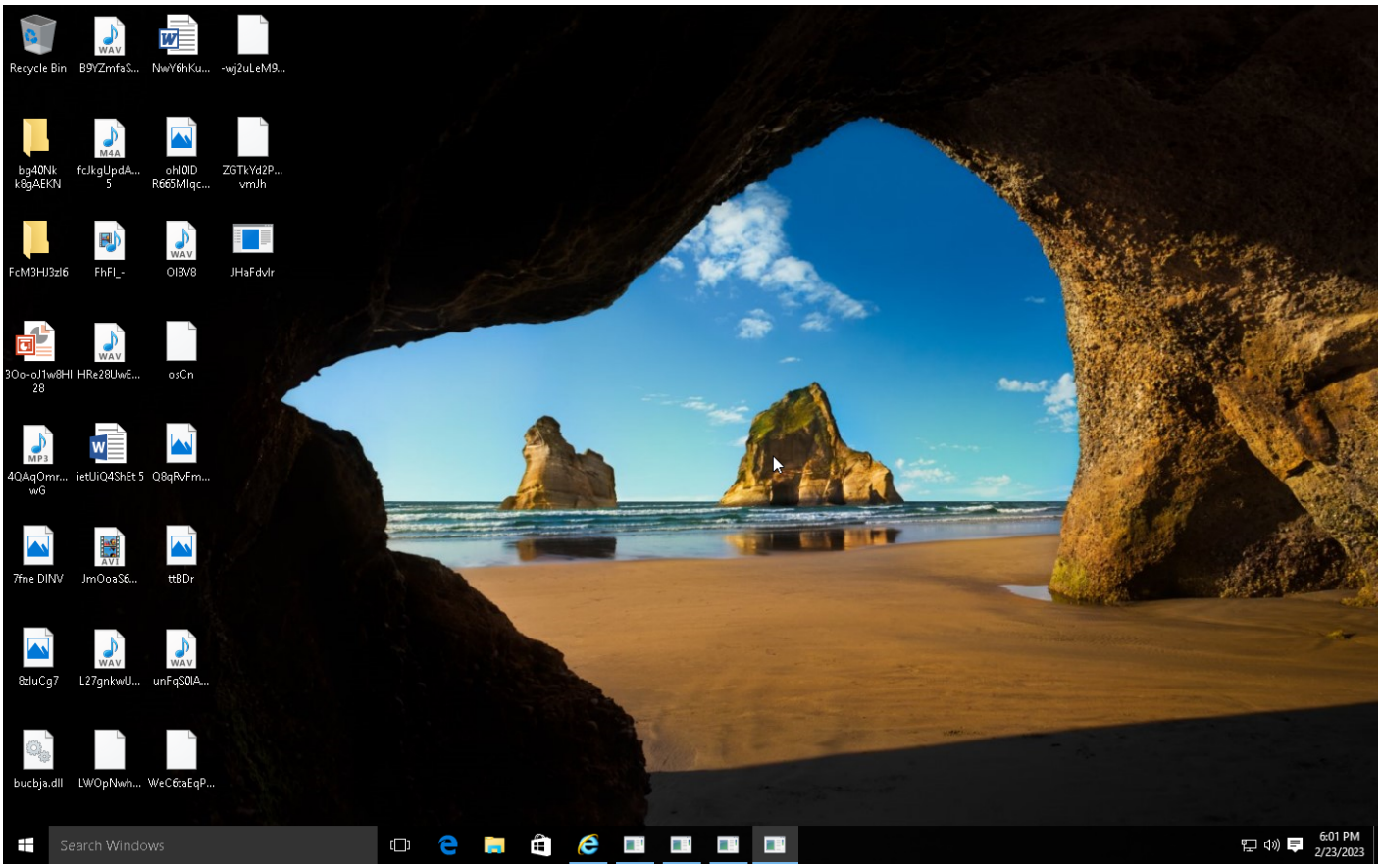
ID	#6950503
MD5	a9e08e50aee2180cb8c6c3ee669ba785
SHA1	940be8f144bde7713e592dea4d3f3fda90bd7c37
SHA256	3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642
SSDeep	3072:xiHTIEAU2M3VtjyEtNdf0NZBQ8PGgqi+kj3pww5:xiHTBAJMFFNyZ5PQkjZww5
ImpHash	71b6fe83cf5e67f60a0052d06ddf05a3
File Name	bucbja.dll
File Size	118.66 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2023-02-23 18:59 (UTC+1)
Analysis Duration	00:02:00
Termination Reason	Timeout
Number of Monitored Processes	22
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	17


Recycle Bin
B9YZmfaS...
NwY6hKu...
-wj2uLeM9...
bg40Nk k8gAEKN
fcJkgUpdA... 5
ohI0ID R665MIqc...
ZGTkYd2P... vmJh
FcM3HJ3zI6
FhFl_-
OI8V8
JHaFdvlr
3Oo-oJ1w8HI 28
HRe28UwE...
osCn
4QAqOmr... wG
ietUiQ4ShEt 5
Q8qRvFm...
7fne DINV
JmOoaS6...
ttBDr
8zluCg7
L27gnkwU...
unFqS0lA...
bucbja.dll
LWOpNwh...
WeC6taEqP...
Search Windows
6:01 PM
2/23/2023


User Account Control


Recycle Bin
B9YZmfaS...
NwY6hKu...
-wj2uLeM9...
bg40Nk
k8gAEKN
fcJkgUpdA...
5
ohI0ID
R665MIqc...
ZGTkYd2P...
vmJh
FcM3HJ3zl6
FhFl_-
OI8V8
JHaFdvlr
3Oo-oJ1w8HI
28
HRe28UwE...
osCn
4QAqOmr...
wG
ietUiQ4ShEt 5
Q8qRvFm...
7fne DINV
JmOoaS6...
ttBDr
8zluCg7
L27gnkwU...
unFqS0lA...
bucbja.dll
LWOpNwh...
WeC6taEqP...
Search Windows
6:01 PM
2/23/2023

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

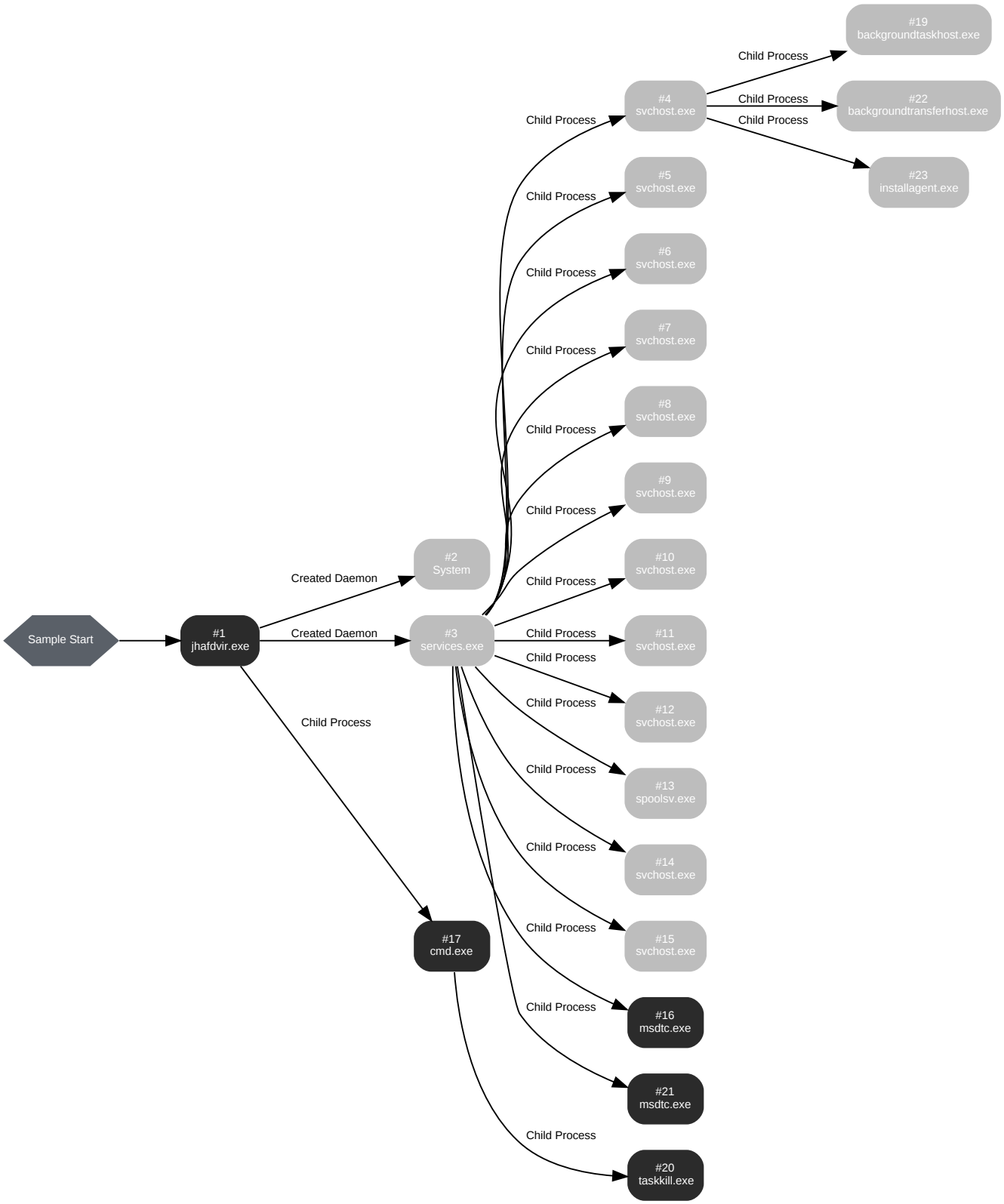
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: jhafdvir.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\jhafdvir.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JHaFdvIr.exe" /dll="C:\Users\RDHJ0C~1\Desktop\bucbja.dll" /fn_id=versions
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 121783, Reason: Analysis Target
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	120.21s
Return Code	Unknown
PID	4892
Parent PID	1912
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\windows\system32\oci.dll	165.66 KB	35a273df61f4506cdb286ecc40415efaa5797379b16d44c240e3ca44714f945b	✔

Host Behavior

Type	Count
Module	120
File	11
Environment	2
System	3
-	1
-	4
Process	108

Process #2: System

ID	2
File Name	System
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 126446, Reason: Created Daemon
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	4
Parent PID	-
Bitness	64 Bit

Process #3: services.exe

ID	3
File Name	c:\windows\system32\services.exe
Command Line	C:\Windows\system32\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126446, Reason: Created Daemon
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	528
Parent PID	4892
Bitness	64 Bit

Process #4: svchost.exe

ID	4
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126446, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	628
Parent PID	528
Bitness	64 Bit

Process #5: svchost.exe

ID	5
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k RPCSS
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126446, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	660
Parent PID	528
Bitness	64 Bit

Process #6: svchost.exe

ID	6
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: 126446, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	856
Parent PID	528
Bitness	64 Bit

Process #7: svchost.exe

ID	7
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126446, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	888
Parent PID	528
Bitness	64 Bit

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	908
Parent PID	528
Bitness	64 Bit

Process #9: svchost.exe

ID	9
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	924
Parent PID	528
Bitness	64 Bit

Process #10: svchost.exe

ID	10
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	1016
Parent PID	528
Bitness	64 Bit

Process #11: svchost.exe

ID	11
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	328
Parent PID	528
Bitness	64 Bit

Process #12: svchost.exe

ID	12
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k NetworkService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	1148
Parent PID	528
Bitness	64 Bit

Process #13: spoolsv.exe

ID	13
File Name	c:\windows\system32\spoolsv.exe
Command Line	C:\Windows\System32\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	1260
Parent PID	528
Bitness	64 Bit

Process #14: svchost.exe

ID	14
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k appmodel
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	1588
Parent PID	528
Bitness	64 Bit

Process #15: svchost.exe

ID	15
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126447, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	115.55s
Return Code	Unknown
PID	2864
Parent PID	528
Bitness	64 Bit

Process #16: msdtc.exe

ID	16
File Name	c:\windows\system32\msdtc.exe
Command Line	C:\Windows\System32\msdtc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 127679, Reason: Child Process
Unmonitor End Time	End Time: 144048, Reason: Terminated
Monitor duration	16.37s
Return Code	1
PID	4904
Parent PID	528
Bitness	64 Bit

Host Behavior

Type	Count
Module	17
File	1282
Environment	2
System	224
-	1

Process #17: cmd.exe

ID	17
File Name	c:\windows\system32\cmd.exe
Command Line	cmd.exe /c taskkill /f /im msdtc.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 129606, Reason: Child Process
Unmonitor End Time	End Time: 144047, Reason: Terminated
Monitor duration	14.44s
Return Code	0
PID	4936
Parent PID	4892
Bitness	64 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	18
Environment	19
System	1
Process	2

Process #19: backgroundtaskhost.exe

ID	19
File Name	c:\windows\system32\backgroundtaskhost.exe
Command Line	"C:\Windows\system32\backgroundTaskHost.exe" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca
Initial Working Directory	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\
Monitor Start Time	Start Time: 137327, Reason: Child Process
Unmonitor End Time	End Time: 139570, Reason: Terminated
Monitor duration	2.24s
Return Code	3221225473
PID	5016
Parent PID	628
Bitness	64 Bit

Process #20: taskkill.exe

ID	20
File Name	c:\windows\system32\taskkill.exe
Command Line	taskkill /f /im msdtc.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 139252, Reason: Child Process
Unmonitor End Time	End Time: 144047, Reason: Terminated
Monitor duration	4.79s
Return Code	0
PID	5024
Parent PID	4936
Bitness	64 Bit

Process #21: msdtc.exe

ID	21
File Name	c:\windows\system32\msdtc.exe
Command Line	C:\Windows\System32\msdtc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 143843, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated by timeout
Monitor duration	98.15s
Return Code	Unknown
PID	5064
Parent PID	528
Bitness	64 Bit

Host Behavior

Type	Count
Module	17
File	690
Environment	2
System	224
-	1

Process #22: backgroundtransferhost.exe

ID	22
File Name	c:\windows\system32\backgroundtransferhost.exe
Command Line	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Initial Working Directory	C:\Windows\SystemApps\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\
Monitor Start Time	Start Time: 179797, Reason: Child Process
Unmonitor End Time	End Time: 189321, Reason: Terminated
Monitor duration	9.52s
Return Code	1
PID	4216
Parent PID	628
Bitness	64 Bit

Process #23: installagent.exe

ID	23
File Name	c:\windows\system32\installagent.exe
Command Line	C:\Windows\System32\InstallAgent.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 231736, Reason: Child Process
Unmonitor End Time	End Time: 241997, Reason: Terminated
Monitor duration	10.26s
Return Code	0
PID	4304
Parent PID	628
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
35a273df61f4506cdb286ecc40415efaa5797379b16d44c240e3ca44714f945b	C:\windows\system32\oci.dll	Dropped File	165.66 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642	C:\Users\RDhJ0CNFevzX\Desktop\bucbja.dll	Sample File	118.66 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
38af0288cd9d262a1c470796d217eb3c5ef3f61a2d9168dd511745cf34028853	C:\Users\RDhJ0CNFevzX\Documents\Uu2MHcR ne4f5 jN\zLTL9eQH4Dtg.xlsx	Modified File	4.19 KB	application/octet-stream	Access, Read, Write	CLEAN
df6b256cb4eb8e0dfb878bd69d7d1cd89aa5b5fed4f3b78e8befd3fc272f0ab1	C:\Users\RDhJ0CNFevzX\Desktop\B9YZmfaSyzYcy.wav	Modified File	102.04 KB	application/octet-stream	Access, Read, Write	CLEAN
b69e5bfd1de411d736b4becd5ac85adafe642aab348fd20769bb78dafefb6fcc	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\GaQ1TU-ns4-u6B3Pj_F.swf	Modified File	23.47 KB	application/octet-stream	Access, Read, Write	CLEAN
d53a1aa649f3f6c2630a7317bf1cf325a404debfe1bed513d171bc0dfc813c1c	C:\Users\RDhJ0CNFevzX\Videos\cFQCAjt-9.avi	Modified File	54.49 KB	application/octet-stream	Access, Read, Write	CLEAN
975416bf7bdb455de79236fee2424a5acccce20241ad4611e7be5eb3d3d387148	C:\Users\RDhJ0CNFevzX\Desktop\osCn.swf	Modified File	67.38 KB	application/octet-stream	Access, Read, Write	CLEAN
09136343ac62446d660393b4bf78a436fdc6a8352999979bc8120e66adfd2c4c	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\Xk6OsGw80BZF.wav	Modified File	103.77 KB	application/octet-stream	Access, Read, Write	CLEAN
2b3b2a232e1369bbe69f751e19dc916483a9023752d12c0b1dad220383cad39d	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\60hPj\0i-BfxeBoDoclU3m-.bmp	Modified File	50.29 KB	application/octet-stream	Access, Read, Write	CLEAN
8795efc7c78f39cae32232af2429edeac86a5869e22ae2aff578971179f95794	C:\Users\RDhJ0CNFevzX\Music\u7iCIl5l.m4a	Modified File	22.89 KB	application/octet-stream	Access, Read, Write	CLEAN
a3c6e007db3fbc9597799d897dd9bdbc37e435aa8a05bfb3f52b76876dc6d341	C:\Users\RDhJ0CNFevzX\Videos\i3QToQLiB.mkv	Modified File	44.83 KB	application/octet-stream	Access, Read, Write	CLEAN
5428bfccb73a9b35543a831818c94e4c0051c3a7db54493f85edc469ab4484ea	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\7qhpz8_JHXZdpvy.jpg	Modified File	85.98 KB	application/octet-stream	Access, Read, Write	CLEAN
eace93e7d747b5791149f5db6a536acf15e0f4d5c9ee58ba8235ba7d2f28f188	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\gfULfaB3zo.wav	Modified File	55.08 KB	application/octet-stream	Access, Read, Write	CLEAN
0ef342ad71fbf9eba4d841e51fce7daee360aad30e6930d54b4cc5fa8274ec1b	C:\Users\RDhJ0CNFevzX\Desktop\FhFl_-.mkv	Modified File	81.56 KB	application/octet-stream	Access, Read, Write	CLEAN
e3598548b4d3a401c41280518807760fa3341e00a4604cb211b2e4b43c449ec9c	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\iYt4Sr4pkbCs4T.m4a	Modified File	50.50 KB	application/octet-stream	Access, Read, Write	CLEAN
30d21d3b39909dc661e011fe75e275109b49c410d357a1185680d3eeeb898a72	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\kQdD.rtf	Modified File	105.06 KB	application/octet-stream	Access, Read, Write	CLEAN
040fac9dc16da77bb61b777150cca1c1429dc9f17a410b4b9c02006434dbfeaf	C:\Users\RDhJ0CNFevzX\Documents\2hljBgD1 RG.docx	Modified File	69.73 KB	application/octet-stream	Access, Read, Write	CLEAN
38a7722de9bf6bec84200b0a56e145a06eef85b88082ecd08cdd67930ef78f83	C:\Users\RDhJ0CNFevzX\Desktop\8zluCg7.png	Modified File	114.95 KB	application/octet-stream	Access, Read, Write	CLEAN
43b51b2edfaf5eea99cbac1deacf742e229b95019306af572ae6c651bf062165	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeYJKK9\fagweFCcJWoKDe1Q\fn-0d2Jap.xls	Modified File	43.22 KB	application/octet-stream	Access, Read, Write	CLEAN
7a85e6eb0fddb3307d5d8e894bfe2657bc38015ec3b3cfc09ac0e180601c741b	C:\Users\RDhJ0CNFevzX\Desktop\ohl0ID R665MIqcWPnkd.jpg	Modified File	49.58 KB	application/octet-stream	Access, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dcdf906e76cb9f7562fd0624c09808f8f809086a756b5be1200e3c250bd58ffe	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\60hPj\XpUr.gif	Modified File	65.49 KB	application/octet-stream	Access, Read, Write	CLEAN
faf1025292eff61143b74b36581704430dc116aefcec7260714ae3008dd4de49	C:\Users\RDhJ0CNFevzX\Videos\m6XkSaeR.avi	Modified File	27.33 KB	application/octet-stream	Access, Read, Write	CLEAN
3d594a0d89d6f1ec38c7ebea83b5a7f629272ea97dc5c8f8e8f0fc41dfa2047e	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\lxjKufO2Ryx0y\JGs8\Pc158sefqrED.bmp	Modified File	33.58 KB	application/octet-stream	Access, Read, Write	CLEAN
91764ba24590b836cd1e2584c8676c113d892bd04fcf7eb22ecb188753e5fcc5	C:\Users\RDhJ0CNFevzX\Videos\RtNwIB-43m.swf	Modified File	24.22 KB	application/octet-stream	Access, Read, Write	CLEAN
7188bc57060480bfcb083a2ad1ad2db44de6fbea8eb63cf4eb6c394521492622	C:\Users\RDhJ0CNFevzX\Music\xD9qeXinUK4Z9ql4.mp3	Modified File	81.02 KB	application/octet-stream	Access, Read, Write	CLEAN
aa196b9cab0dd0d7d9b62421e8fd6eb6364186f3e7e2c7c1407cfcad182ac4cb	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\NMRVXijqDWuZSGmsqvb.png	Modified File	64.65 KB	application/octet-stream	Access, Read, Write	CLEAN
95b12d48160e58bdea128fae58f4b01c137336bc162a6a20f1202c6880af5b96	C:\Users\RDhJ0CNFevzX\Documents\3Ozrn-C\CdvPrp3Nu1pnlZzw.pps	Modified File	115.40 KB	application/octet-stream	Access, Read, Write	CLEAN
838d89b0bde4de99f061406b391ab39b569f6e9cff11afe5fd1fe4d7f1d6d004	C:\Users\RDhJ0CNFevzX\Desktop\ZGTkYd2PTX5 vmJh.swf	Modified File	119.43 KB	application/octet-stream	Access, Read, Write	CLEAN
573c8d871cedb7d6a1f484b0ada25a7b2e9fe4386830c55d8b6f321d3b56c8ee	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeY JKK9\W5M-\RkyCu.xls	Modified File	9.12 KB	application/octet-stream	Access, Read, Write	CLEAN
65d2feb455b3e79ea01a424aeef823889ac521bd8ab2b849376b40c63c11b364	C:\Users\RDhJ0CNFevzX\Videos\Nfz8xn.flv	Modified File	94.40 KB	application/octet-stream	Access, Read, Write	CLEAN
1a7a56c4916d2f8e2010df37499c0c8d4be0b3ba0f168ab29f642e8d1241521c	C:\Users\RDhJ0CNFevzX\Documents\5oXD JYe1.xlsx	Modified File	74.81 KB	application/octet-stream	Access, Read, Write	CLEAN
3f9ee339bab7637d4c68aacfcb5081d72556f8ef9d00dd2b7fc3846e1aee8f97	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeY JKK9\Vh2glqLH1V.xls	Modified File	37.47 KB	application/octet-stream	Access, Read, Write	CLEAN
987542ab81711eb40a32f3e97836026cafb6b80f19c3f9b858ea113dad843d5a	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\8B8Hy6zF_MS.m4a	Modified File	95.38 KB	application/octet-stream	Access, Read, Write	CLEAN
3f0a8711a1176f1f9d3a712f39df061a23ee78e844e6bdf9380cde89c54b019d	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\lxjKufO2Ryx0y\Eupj8q.png	Modified File	99.72 KB	application/octet-stream	Access, Read, Write	CLEAN
430b59a00382ae6e926202b7a8300b125cab1c43a39afe7fe7ec9901c6aa375c	C:\Users\RDhJ0CNFevzX\Favorites\desktop.ini	Modified File	20.66 KB	application/octet-stream	Access, Read, Write	CLEAN
5812ef5ccb83b4e91525f6d973c4f4cc52bcf9573ffb332917de5e4890fac276	C:\Users\RDhJ0CNFevzX\Pictures\ikvCOG.jpg	Modified File	114.61 KB	application/octet-stream	Access, Read, Write	CLEAN
08f544081462b770b7a31e598c2e791b72a9b4b38d494e0595db32a4204df556	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\S2eTpaTNodEH.png	Modified File	74.23 KB	application/octet-stream	Access, Read, Write	CLEAN
f3a7320cfb675d134454286c28f1fd1f2812e25faac4fea218b4940b2870293d	C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Modified File	20.66 KB	application/octet-stream	Access, Read, Write	CLEAN
a8b2b4c9e1b0f64dfc091314a3e5a550cd86da206387dcdb1346c96568eae87b	C:\Users\RDhJ0CNFevzX\Videos\CXrX4S7HWEbBL.swf	Modified File	69.92 KB	application/octet-stream	Access, Read, Write	CLEAN
93924f303523d82ab1f19c2931d3d73effee1dcee7f78d9dfb90d20ec2988a9f	C:\Users\RDhJ0CNFevzX\Desktop\bg40Nk k8gAEKN\O9JzJbgS7Mb5w.csv	Modified File	66.89 KB	application/octet-stream	Access, Read, Write	CLEAN
1e4aa7f61b85c4814e1a6fa6d823bc225defb781b37ad919e9aa45cb262dfa32	C:\Users\desktop.ini	Modified File	20.42 KB	application/octet-stream	Access, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fe89ebb57fc6e10f6f53604b5dc0cc04c7db3ce37ed5f99d6a20ea099ec1b125	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\4wJ3vQA\FaNivGNUHSksG.gif	Modified File	93.60 KB	application/octet-stream	Access, Read, Write	CLEAN
b0bd8ae3facbe6669ad6406f78b90cc1aa7bc061406149151234c29271d32aae	C:\Users\RDhJ0CNFevzX\Desktop\LWOpNwhoWf-tD6cICMOy.flv	Modified File	119.92 KB	application/octet-stream	Access, Read, Write	CLEAN
b45e10460a6af768e56a0b20cbfaad1605a8ccb0d5e74818b6a6df829033076f	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\60hPj\zEVmASXzrNvdV1gT-HkQ.gif	Modified File	102.48 KB	application/octet-stream	Access, Read, Write	CLEAN
752b526497ac81f65fbf4ddfb6f09491612e25d8c61c0371f578014d8693c437	C:\Users\RDhJ0CNFevzX\Videos\CLdzw536TG.mp4	Modified File	62.27 KB	application/octet-stream	Access, Read, Write	CLEAN
92c516d478eb4b2c1b7325a06c7a3c1bf48e3765663a0ff7d68700c1484eea4e	C:\Users\RDhJ0CNFevzX\Documents\6PDiYDbFPa.pptx	Modified File	6.51 KB	application/octet-stream	Access, Read, Write	CLEAN
e1139530e006f72ee1b741fadba55abef255f03b0edd919b60ca2e2bec524ea0	C:\Users\RDhJ0CNFevzX\Music\XaYVlV-JmayNd53_Mt.wav	Modified File	88.85 KB	application/octet-stream	Access, Read, Write	CLEAN
5110cc5832662e4946e06326cb7da5d2d39eab2cc757fecef1a20a8e2094e75e	C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Modified File	20.53 KB	application/octet-stream	Access, Read, Write	CLEAN
062eac9734baf8c3171d8c176060bf34ee66c1c3adc7985bd5254de9c851b75f	C:\Users\RDhJ0CNFevzX\Videos\6h1ZcPvX-.avi	Modified File	75.61 KB	application/octet-stream	Access, Read, Write	CLEAN
bcab4395509da561254ad08bfa21ef224e26c0b15e383335b9bf3f422b1fa4d6	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeYJKK9\3vwP7Ny7F0uOf\2ejGWQ2Q1PK.csv	Modified File	20.72 KB	application/octet-stream	Access, Read, Write	CLEAN
8cb22bfbdc0fce13531d9529515a1ae5f389c5d050bf14590c616ee650a45760	C:\Users\RDhJ0CNFevzX\Documents\SCTYy9mjk3.docx	Modified File	59.97 KB	application/octet-stream	Access, Read, Write	CLEAN
3c261aa25365b7b58f803ddf731c6e221b664a534ff0ab97e0d1e8175df973eb	C:\Users\RDhJ0CNFevzX\Music\LoNNdvzwPSF50eP.wav	Modified File	28.45 KB	application/octet-stream	Access, Read, Write	CLEAN
3edb954018dfdcc7d85f0c1e2f92a47c2151d9d37572cd86fb09af0080d95dd7	C:\Users\RDhJ0CNFevzX\Videos\Wax7.mp4	Modified File	38.17 KB	application/octet-stream	Access, Read, Write	CLEAN
a04f371a7416f2acc6ed265b4cd48f5b058abe34dceef72523b1c20162066c60	C:\Users\RDhJ0CNFevzX\Desktop\3Oo-oJ1w8HI 28.ppt	Modified File	100.42 KB	application/octet-stream	Access, Read, Write	CLEAN
f0766f9efceac047493c3e8d2988f5c8ff28c88a8afe52be7356b06801b76225	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\iOvCnRfLTkM9.wav	Modified File	90.07 KB	application/octet-stream	Access, Read, Write	CLEAN
0be4d63d532e81242b26eeeff96ab0a875d9d6f0c617a090232a03b0b247d28f	C:\Users\RDhJ0CNFevzX\Videos\auWbn4Aenq.mp4	Modified File	117.13 KB	application/octet-stream	Access, Read, Write	CLEAN
9b21a9914dba3cf16943e162cdf660bbd2cf30e1235258a892de5276e8c7f231	C:\Users\RDhJ0CNFevzX\Music\M3D2dAGIAkc0.wav	Modified File	91.31 KB	application/octet-stream	Access, Read, Write	CLEAN
c7899147dfde5d9a18d2ce47c98e4706c7c678ef09e329792c09b511d7e7cdea	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\4wJ3vQA\M70zS.png	Modified File	94.49 KB	application/octet-stream	Access, Read, Write	CLEAN
9fcadada66a62dce62661a277f5d1f20393b73f154761545d97daef57a36149a	C:\Users\RDhJ0CNFevzX\Links\desktop.ini	Modified File	20.75 KB	application/octet-stream	Access, Read, Write	CLEAN
194f8c5624249a573ef072f4b60dec0bf50e573dda92b05305ed0c8bd6368162	C:\Users\RDhJ0CNFevzX\Videos\sb8Hk69e2bii.mkv	Modified File	90.08 KB	application/octet-stream	Access, Read, Write	CLEAN
f23d42e2afa6e340b37dba48a3ec639219e9a4c6d825dfa33719043230937ccb	C:\Users\RDhJ0CNFevzX\Contacts\desktop.ini	Modified File	20.66 KB	application/octet-stream	Access, Read, Write	CLEAN
55f0b2b8f9704a899b870c808cd2537b0a79bec56123f7ee1ece775235e91997	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\60hPj\G1KIWWVdxjOl4J I-dX.jpg	Modified File	37.20 KB	application/octet-stream	Access, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
36127b99c9c910f660313a531f1275d03f5fac101cdc9a09f45de4f531f9c9b6	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\nq8ktm1kT2WY3NIUwi.jpg	Modified File	24.77 KB	application/octet-stream	Access, Read, Write	CLEAN
d48c773a56d94b746e9b9511b82f96030a3beef8f0c1a8aff09d48ad0d42bae2	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeY JKK9\W5M-\MxzwvznxGUpfEWUPt7.odt	Modified File	101.83 KB	application/octet-stream	Access, Read, Write	CLEAN
1816d164a87b28b3883534196d9a4d50c0337cfa689e9359571e3b91597ef61b	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\9vXU0CCZC77b8.m4a	Modified File	73.57 KB	application/octet-stream	Access, Read, Write	CLEAN
6dd730bc4a2ab45628e23fcca41a7cd9b255fd61db9b9f7aaecab7d93dd8430e	C:\Users\RDhJ0CNFevzX\Desktop\bg40Nk k8gAEKN\N QZTMIXjBIoZTX.png	Modified File	116.61 KB	application/octet-stream	Access, Read, Write	CLEAN
e2169772eaec68c8c2bc976d4a039f6134da1cb3fd275e750822d967306cff0b	C:\Users\RDhJ0CNFevzX\Documents\3Ozrn-C\h38g6jq9H1qf ZYhaRF.docx	Modified File	16.69 KB	application/octet-stream	Access, Read, Write	CLEAN
c776b624293f51cbf9e5bf840775799170ab6ac00bad3f4820c906bd5cc10891	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\xKw XH2hna1hjh-.bmp	Modified File	57.35 KB	application/octet-stream	Access, Read, Write	CLEAN
b63f06882ba2cc151c51d67810db885b050ca95d85c1fd927fe56c2edf6e8326	C:\Users\RDhJ0CNFevzX\Desktop\unFqS0IAA-HHEp.wav	Modified File	91.30 KB	application/octet-stream	Access, Read, Write	CLEAN
faa5edcc238c7b287b2eabee098b87d835f0b00e09e5cd513f3fc0ef7556511f	C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk	Modified File	21.22 KB	application/octet-stream	Access, Read, Write	CLEAN
c53ca070bd63d499338b0ef5027ad008d10c92f502a27024ff1cd56f00023720	C:\Users\RDhJ0CNFevzX\Videos\D_kC7XGuuJT.mp4	Modified File	90.75 KB	application/octet-stream	Access, Read, Write	CLEAN
ee2b8b2fe130a97187c69624fc9cb4742d4104414353ade7fb6ff87eecd07a57	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\4wJ3vQA\bQzgCK.jpg	Modified File	100.95 KB	application/octet-stream	Access, Read, Write	CLEAN
3245522941a4797f0d1fe361da0a62f411c8ce35efe715f604022ee0b7730987	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\lxjKufO2Ryx0y\JGs8\1_ul7.png	Modified File	84.90 KB	application/octet-stream	Access, Read, Write	CLEAN
6ea9ab1e736e40169c18667c97e3e2ad0f09c5a8c250c9e441d1e908c1975256	C:\Users\RDhJ0CNFevzX\Music\rPff8m_vb3qiWXJ Wg0b.m4a	Modified File	106.63 KB	application/octet-stream	Access, Read, Write	CLEAN
2704039c68ba3966e87062fa93c7ebfb2d3d98b6af9e6fa019f98f7aae598151	C:\Users\RDhJ0CNFevzX\Documents\9adZsO.xlsx	Modified File	62.01 KB	application/octet-stream	Access, Read, Write	CLEAN
055c467047bd9f92c3d507fb86998f2c142238a48c794fcaba36201a6489fe1f	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\lxjKufO2Ryx0y\JGs8\too6KBp5Juglc.jpg	Modified File	54.12 KB	application/octet-stream	Access, Read, Write	CLEAN
16e027357ef3595497b61160b66b3f3fde0c83072b4b6840f7ef30ce6020d0b7	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\oZwW.m4a	Modified File	64.47 KB	application/octet-stream	Access, Read, Write	CLEAN
7295bde8e5f06a04d8f7cd8d7522c18a399c9ffb464f3574a4ae8869bc199939	C:\Users\RDhJ0CNFevzX\ntuser.ini	Modified File	20.28 KB	application/octet-stream	Access, Read, Write	CLEAN
5ebaef503a10ddfae317ed398554befbf1ee3d5df968e78d82c7fbbcd7edaa13	C:\Users\RDhJ0CNFevzX\Desktop\bg40Nk k8gAEKN\MEbNa.png	Modified File	112.89 KB	application/octet-stream	Access, Read, Write	CLEAN
1e2e53eba1ad4a717b0c64bf17a37acd9799c84501f8f99c30698b2641ebf523	C:\Users\RDhJ0CNFevzX\Documents\lxly.ots	Modified File	62.92 KB	application/octet-stream	Access, Read, Write	CLEAN
bbc51ede3bec935b6b45840973efe57661db57043558a11b9c33f1e18044a888	C:\Users\RDhJ0CNFevzX\Desktop\bg40Nk k8gAEKN\Tkmuw2oxS7Skgbs.avi	Modified File	51.37 KB	application/octet-stream	Access, Read, Write	CLEAN
450ffad2fc93da1d7888bcbf221206ff7d560a22fd4c6bd28c4e8456572aa57f	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\x5oeGxuFd3ZTD.jpg	Modified File	33.33 KB	application/octet-stream	Access, Read, Write	CLEAN
ed4cad38df0304231a8e66bb7b82fda4b08ce751fb6b6ecc65bfaadda967e752	C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Modified File	20.75 KB	application/octet-stream	Access, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4a81d07d19d00b95304532abd7bbe60d28e35d92dce4fbdcb36669aab166cbcd	C:\Users\RDhJ0CNFevzX\Desktop\ttBDr.gif	Modified File	84.94 KB	application/octet-stream	Access, Read, Write	CLEAN
c5935db7d1d138c0b4fa291f57e0504d35248036c624dd3e1a0b09e8d357d36d	C:\Users\RDhJ0CNFevzX\Desktop\Q8qRvFmm3lQe7eqKqz.bmp	Modified File	80.39 KB	application/octet-stream	Access, Read, Write	CLEAN
f85d434626355e1715f395193a0cf11f2af44c6d252157d4d355c151c674a913	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\Lw9 ysK.mp3	Modified File	82.32 KB	application/octet-stream	Access, Read, Write	CLEAN
2a570580c682b3278bb213c217ef3e3e346eb1ae98fe8d7aff6580c20c118590	C:\Users\RDhJ0CNFevzX\Pictures\pkqOdeK\LoRrpbPb3hyX.bmp	Modified File	88.65 KB	application/octet-stream	Access, Read, Write	CLEAN
36a380f85d0b0a234fd3f118ed9139ee34147597f9e5ee1c9bfb443f8c4e3c19	C:\Users\RDhJ0CNFevzX\Desktop\L27gnkwUaPU.wav	Modified File	29.11 KB	application/octet-stream	Access, Read, Write	CLEAN
569ea68f42d8d2742ff70f682ed78248acae420469fe1ea5c1014b866baa0393	C:\Users\RDhJ0CNFevzX\Documents\Uu2MHcR ne4f5jN\NGki7l1lYyPGQLmPou.ots	Modified File	103.33 KB	application/octet-stream	Access, Read, Write	CLEAN
59e188da50f0ace8c3a3d0fb30d7a6049665e8040558ebf2bb0a274d014e6366	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\gHqlr7ucmVxDpvt.m4a	Modified File	65.84 KB	application/octet-stream	Access, Read, Write	CLEAN
ce535feb92e32429df78b16276822220df79b959f829b9560d254b4ac63686ca	C:\Users\RDhJ0CNFevzX\Pictures\pkqOdeK\SBhHtZEuj_zd1mmTI__S3.gif	Modified File	70.17 KB	application/octet-stream	Access, Read, Write	CLEAN
131fde57f4e0fdf57f369751d05eee30aa3dcae172c7b2617e36a7b56ee054a4	C:\Users\RDhJ0CNFevzX\Desktop\bg40Nk k8gAEKN\MQux2 vq81yYA.jpg	Modified File	28.38 KB	application/octet-stream	Access, Read, Write	CLEAN
fb6e3595da7e69cd391998d4ab4f4f9c13434652aab5f7b2378bda066f549f22	C:\Users\RDhJ0CNFevzX\Videos\20JqECm5e6wvbNcfi.flv	Modified File	50.11 KB	application/octet-stream	Access, Read, Write	CLEAN
f9f21b1b0bf5b1f4ff6fd14f8de837f2fee313be0069ee3d1b3046bfa0fd6ad0	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\QQPwJf44SZ2yym1FzZ6q.gif	Modified File	44.04 KB	application/octet-stream	Access, Read, Write	CLEAN
da0fa56bd59096dca8dd790beeae7421f27dcc30a2a23ba916b795cd94a42dd3	C:\Users\RDhJ0CNFevzX\Desktop\7fneDINV.bmp	Modified File	49.94 KB	application/octet-stream	Access, Read, Write	CLEAN
712c8bdf11ba00acc30f1fcfdd5fa57bbc4101f4e3b9cebdfa27fb9d2bffd94e	C:\Users\RDhJ0CNFevzX\Desktop\HRe28UwE020sVBMZQXSM.wav	Modified File	76.07 KB	application/octet-stream	Access, Read, Write	CLEAN
a4253096f9af775c7235c9c4ee512a8fea3192e02e7c69a3eaa7dc679f8e3fe0	C:\Users\RDhJ0CNFevzX\Desktop\WeC6taEqPlgqc7c.swf	Modified File	87.06 KB	application/octet-stream	Access, Read, Write	CLEAN
c832cfb30c8e1c77fdd118b589870fda9151b433eeca7958bfa0e9fe6ce5d82e	C:\Users\RDhJ0CNFevzX\Music\desktop.ini	Modified File	20.75 KB	application/octet-stream	Access, Read, Write	CLEAN
0424e04637cbbdb0151c258d3d2af697efa37841535c1c3203d89a11a906da44	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\-4kdm22YV4v.wav	Modified File	34.22 KB	application/octet-stream	Access, Read, Write	CLEAN
2a8a7ec20a2335bb7414f37dc16cee4aa1b9d1608f68027df69612aedea7d982	C:\Users\RDhJ0CNFevzX\Desktop\bg40Nk k8gAEKN\cWfz.ods	Modified File	25.03 KB	application/octet-stream	Access, Read, Write	CLEAN
97cdfc3a6085efd485e0c00509f53873a41381ce9ae0019fa21ac200e79c038b	C:\Users\RDhJ0CNFevzX\Desktop\-wj2uLeM9ZxLBKGeYYU.ots	Modified File	30.03 KB	application/octet-stream	Access, Read, Write	CLEAN
5b482885cb1530ec1d72156aecb83c2d99fae3cfef653b4de036d16e44474418	C:\Users\RDhJ0CNFevzX\Documents\aJADt6bVVwkuva.pptx	Modified File	77.29 KB	application/octet-stream	Access, Read, Write	CLEAN
7f98ac2c01397e8d5c0d1f2ba6cb3374ef9e7085d1bf4591df69ddfe6ae116c5	C:\Users\RDhJ0CNFevzX\Documents\xmqtd.rtf	Modified File	21.61 KB	application/octet-stream	Access, Read, Write	CLEAN
3b5d61d0d03f9b6434a2892599bfed3393089a28cf268e5a13b63c7ac888a8df	C:\Users\RDhJ0CNFevzX\Videos\selU_Klo.avi	Modified File	94.65 KB	application/octet-stream	Access, Read, Write	CLEAN
5eda0221cc43cb431baefed87df44acb2df0c753aadf771c53569c2677143792	C:\Users\RDhJ0CNFevzX\Documents\glrC80297sFhHoMM1Ql3.pps	Modified File	70.59 KB	application/octet-stream	Access, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
eff8c7ddd139d5b62921b2f5456cdadd74fa27d0c05e8023847450880ca5f59e	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\5iJsNnxngia9PWK-bt_D.bmp	Modified File	40.09 KB	application/octet-stream	Access, Read, Write	CLEAN
a4420ec5a521f0430c9269eb7820d0fbedcb5b38281158f2875761f20f4aeb35	C:\Users\RDhJ0CNFevzX\Desktop\fcJkgUpdA60JQ 5.m4a	Modified File	30.17 KB	application/octet-stream	Access, Read, Write	CLEAN
b88a05b6dd45b086abff1b429071f9c65d83067ee640031b5c57143ea3657a94	C:\Users\RDhJ0CNFevzX\Searches\desktop.ini	Modified File	20.77 KB	application/octet-stream	Access, Read, Write	CLEAN
4245389a5b32bdb24514f4667d3b8066139b0071db3a8fb3043e43c4434c88c2	C:\Users\RDhJ0CNFevzX\Documents\XWr5dH0lj.pptx	Modified File	90.67 KB	application/octet-stream	Access, Read, Write	CLEAN
3c2612ea71777b069d6d6c08aa2a1c5f8eb7e358fbcd6eb9fc8210ec7caaacda	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\Eis9xSD3cZ.swf	Modified File	75.33 KB	application/octet-stream	Access, Read, Write	CLEAN
99bbf5f5570cfc483d7dee58dbc6322e21a1aa376ed6dd585b09a83789ca416b	C:\Users\RDhJ0CNFevzX\Pictures\H9kLrv3 mNT.png	Modified File	51.14 KB	application/octet-stream	Access, Read, Write	CLEAN
74cbeca5b5efbdda9a0674854a6a3dec222e294d2af8d69feaae3640d4c7ec03	C:\Users\RDhJ0CNFevzX\Music\H0Bu7WE L.mp3	Modified File	49.27 KB	application/octet-stream	Access, Read, Write	CLEAN
0da7a23c6ff08d0d89c04dfb572eddee097a8ef31b1d66eaead45050a4ea890d	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeY JKK9\W5M-\gMxI3jBTRFbiX9pWbXu.docx	Modified File	91.23 KB	application/octet-stream	Access, Read, Write	CLEAN
71807ae661c8bb754fd52277c2724c3572335086db4d0902c3e7fa37770cdf28	C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Modified File	20.44 KB	application/octet-stream	Access, Read, Write	CLEAN
21136e68ca703622be08bd4c64a3f30cdc5c0432f8303071faf2f789b813d7fd	C:\Users\RDhJ0CNFevzX\Videos\aoyCAw5Qajftw0RqZ.mkv	Modified File	67.50 KB	application/octet-stream	Access, Read, Write	CLEAN
a70ba20cb3946dd2d6c18520bdfc018be20df4c8cacd9397b05ecc5420c98a49	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeY JKK9\fagweFCcJWoKDe1Q\F4SU660iGO.pps	Modified File	63.97 KB	application/octet-stream	Access, Read, Write	CLEAN
e0b620911d9e103fe9eee1064a664d27fadd94684ed715cb5f350288c6d71042	C:\Users\RDhJ0CNFevzX\Documents\8KT1V6XMJnk5nR_vJ-\QH2yTaFyQ15m.ots	Modified File	44.46 KB	application/octet-stream	Access, Read, Write	CLEAN
0b4f7ff2446d5fd43f5cd7708efb99a0392a2b6a938208dc7dd2a5f4e43a47e3	C:\Users\RDhJ0CNFevzX\Videos\rx_L5.mkv	Modified File	114.78 KB	application/octet-stream	Access, Read, Write	CLEAN
5f5a06acff66a6f724dcf40289d27ab1afacc0c54dd110f7eaf4fbd104a0475b	C:\Users\RDhJ0CNFevzX\Videos\w1eNTJHkZu7fh3.flv	Modified File	79.43 KB	application/octet-stream	Access, Read, Write	CLEAN
509323d7e7a3f8ed0820ad2c78d9ea9552c7d724a4529d797d5ba197e5b3b41c	C:\Users\RDhJ0CNFevzX\Favorites\Links\desktop.ini	Modified File	20.34 KB	application/octet-stream	Access, Read, Write	CLEAN
3b65a50418a766fa15912ef1826bc7e73838ad13efd378983b6cb5dcb49794a5	C:\Users\RDhJ0CNFevzX\Videos\desktop.ini	Modified File	20.75 KB	application/octet-stream	Access, Read, Write	CLEAN
358ccf6cf4aaca1a9cd9637412d9863877703ef1fc644e514da37921c61fa262	C:\Users\RDhJ0CNFevzX\Videos\qv8vJ_2.flv	Modified File	57.45 KB	application/octet-stream	Access, Read, Write	CLEAN
a192cd31e1d82219781f0d9b16f78e1898581c8cbfa6dee7c0b3ef04c039dc72	C:\Users\RDhJ0CNFevzX\Videos\6xGdnFO5Q_.mp4	Modified File	40.47 KB	application/octet-stream	Access, Read, Write	CLEAN
956056ac50e51fd4d320cd32fa08922320d39e81617e875d99e64d200d52adcf	C:\Users\RDhJ0CNFevzX\Saved Games\desktop.ini	Modified File	20.53 KB	application/octet-stream	Access, Read, Write	CLEAN
bf3f4486ecbaa0f74cf83bdb8891bc6c5cec53a50975af090eca89431e122914	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6_g9Eb.mp3	Modified File	28.95 KB	application/octet-stream	Access, Read, Write	CLEAN
5d1b39b6c6ccc0e7ad82c8fbc3b5eee9cdeb67721fc1f856b417e4647e69dc32	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\lxjKufO2Ryx0y\JGs8\M3 f2oSr-.jpg	Modified File	114.54 KB	application/octet-stream	Access, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8625034d31bcfd3349f384548c69ac2bc10fa098169478646d69e79f8f38705c	C:\Users\RDhJ0CNFevzX\Videos\zUyYqWvMI4.flv	Modified File	93.01 KB	application/octet-stream	Access, Read, Write	CLEAN
4cfd34558f631dbb003eb5f310e9f95d3b9413d69d4077179 38781910d270a48	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\aWf4X0dmD13O.jpg	Modified File	24.91 KB	application/octet-stream	Access, Read, Write	CLEAN
87e3fa192b07eb37ba781767c0c46d82fb1f906a7864bb1bfe0dbb73e37456aa	C:\Users\RDhJ0CNFevzX\Documents\i-aInfNn8gwF6sT2ZSD.docx	Modified File	33.36 KB	application/octet-stream	Access, Read, Write	CLEAN
b8e6d97b79ceecc706d325a95d28b8524c6843ae0f5184607e6b0ded2aaa6502	C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Modified File	20.44 KB	application/octet-stream	Access, Read, Write	CLEAN
5c5ef3986e7e2a0aab20b9354cf56445c6575a6ba464e4fec12b4d2cebaa94be	C:\Users\RDhJ0CNFevzX\Documents\i1cfxv.pptx	Modified File	3.59 KB	application/octet-stream	Access, Read, Write	CLEAN
3ff196c0f59c67504ca2a0e378d60793212a2ff6fe79c58db5bc5505f57b2719	C:\Users\RDhJ0CNFevzX\Videos\DXvT6A.swf	Modified File	93.29 KB	application/octet-stream	Access, Read, Write	CLEAN
854581f916fde5e7ca3434360af45ff3d71e95829457b7b55fd3a58d8caac9ff	C:\Users\RDhJ0CNFevzX\Videos_93Ekpde.swf	Modified File	32.91 KB	application/octet-stream	Access, Read, Write	CLEAN
4de36c35b8c9aa9887df5e70d13906bd85906f68c619f23c16814b454625f2ae	C:\Users\RDhJ0CNFevzX\Music\R4zOe8GwtZ1.wav	Modified File	58.85 KB	application/octet-stream	Access, Read, Write	CLEAN
b6ae05fefdc67f4774aa0417e94779fcf73453c6e76d7d9184daaf00957de4b5	C:\Users\RDhJ0CNFevzX\Pictures\pkqOdeK\Ogc4R89imU.gif	Modified File	86.53 KB	application/octet-stream	Access, Read, Write	CLEAN
a1e63d0b8e5e788e85120da1e0652b9953bc19b91a45248bf5ed2662b90d245b	C:\Users\RDhJ0CNFevzX\Desktop\FcM3HJ3zl6\-LrxdLy.mkv	Modified File	57.98 KB	application/octet-stream	Access, Read, Write	CLEAN
49c5ae46c0a379824be3ac24819d0b0b36e1634e6950f9117a7db62c3d34a551	C:\Users\RDhJ0CNFevzX\Pictures\EhhsBihcckCr8lG\lxjKufO2Ryx0y\JGs8\7UDTxkOjDUVVzv7hqCX.jpg	Modified File	33.25 KB	application/octet-stream	Access, Read, Write	CLEAN
83741860d25fa0e750fd1762319e8cf26603d9383d5d5698198ed5e4149fd5c4	C:\Users\RDhJ0CNFevzX\Videos\L8br.swf	Modified File	84.14 KB	application/octet-stream	Access, Read, Write	CLEAN
2b59292eb893ca15879ef76b689034ca8f8b3cb4f259f9329d74c8762d405a93	C:\Users\RDhJ0CNFevzX\Music\FXGh0g6\uFwI7-queadFi7ry6ZM5.mp3	Modified File	72.60 KB	application/octet-stream	Access, Read, Write	CLEAN
53ac3b57787cc14ad5d906defac361da905de319e453ddc70d447d3c0aded2f1	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\-WjqwOI4uBb8V.jpg	Modified File	77.82 KB	application/octet-stream	Access, Read, Write	CLEAN
d8762f1e5449c280095792aecc4ec3b8b3eb9e6756fd7672e1ada78ff46140d7	C:\Users\RDhJ0CNFevzX\Pictures\s3tdcFngvww9ooYMn\60hPj\OQZhyhRrm5gu.gif	Modified File	51.28 KB	application/octet-stream	Access, Read, Write	CLEAN
1337ddbdd8d286dbc58ba8cf60e04c2f96edaf2ce68447dafbe810194703f5a9	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeY JKK9\W5M-\xsz6r2s1m.pdf	Modified File	70.01 KB	application/octet-stream	Access, Read, Write	CLEAN
205f406ccba63b975c34b07225481bb40214395a3681cf7cd20bf3f486943847	C:\Users\RDhJ0CNFevzX\Desktop\bg40Nk k8gAEKN\ESCJ7tJ.pps	Modified File	106.87 KB	application/octet-stream	Access, Read, Write	CLEAN
2559c91b0fbc8a8446fc98e7791b4c4af8f0e46c568087d9969b64c626eb6d73	C:\Users\RDhJ0CNFevzX\Desktop\ietUiQ4ShEt 5.docx	Modified File	88.70 KB	application/octet-stream	Access, Read, Write	CLEAN
985ebba06f916795c3206a9605a2f5005da9f3d924d97d92d8f630b84cc641ab	C:\Users\RDhJ0CNFevzX\Documents\3Ozrn-C\Vrr3e.ppt	Modified File	81.79 KB	application/octet-stream	Access, Read, Write	CLEAN
21a5dd1303724188f3672d987f51d2f01bcc50fa30fd7dfd09e9614368312f51	C:\Users\RDhJ0CNFevzX\Documents\3MLRCwi-_Xdb6cchu_-.xlsx	Modified File	58.58 KB	application/octet-stream	Access, Read, Write	CLEAN
1abf14eac005e94026a0ed548377ee3fb14371c02db8e15ef91cbda0ae807106	C:\Users\RDhJ0CNFevzX\Desktop\4QAqOmrwkjZgC0q wG.mp3	Modified File	37.16 KB	application/octet-stream	Access, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f7a4a84244f9ffa5d0a5a8f7d19366bdda63f1a2f637ba7fa88ee6cf6b2491ba	C:\Users\RDhJ0CNFevzX\Documents\-1C3jY4VI.xlsx	Modified File	83.94 KB	application/octet-stream	Access, Read, Write	CLEAN
1733eb31a2e82d6684f87d4a6283a26784da6777e329e07b2ac138440bbd90a1	C:\Users\RDhJ0CNFevzX\Documents\Uu2MHcR ne4f5 jN\ejbo2.odt	Modified File	100.80 KB	application/octet-stream	Access, Read, Write	CLEAN
620706ed25318cd30b4a8e3b01925df645267fdddbb7481b012e0d3b783ae433	C:\Users\RDhJ0CNFevzX\Documents\JMnxWVH_VkEeY JKK9\fagweFCcJWoKDe1Q\9k0JJ5Y1erJl.csv	Modified File	45.15 KB	application/octet-stream	Access, Read, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\bucbja.dll	Sample File	-	MALICIOUS
C:\Users\RDhJ0CNFevzX\Downloads\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\ntuser.dat.LOG2	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Links\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Saved Games\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Searches\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Favorites\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\JHaFdvIr.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Searches\Indexed Locations.search-ms	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Contacts\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\OneDrive\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\ntuser.dat.LOG1	Accessed File	Access	CLEAN
\\.\PhysicalDrive0	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Videos\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Favorites\Links\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Windows\SYSTEM32\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Searches\Everywhere.search-ms	Accessed File	Access	CLEAN
C:\Windows\System32\msdtc.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN

File Name	Category	Operations	Verdict
C:\windows\system32\oci.dll	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Favorites\Bing.url	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Links\Desktop.lnk	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\ntuser.ini	Accessed File, Modified File	Access, Read, Write	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
jhafdvir.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JHaFdvIr.exe" /dll="C:\Users\RDHJ0C~1\Desktop\bucbja.dll" /fn_id=versions	SUSPICIOUS
msdtc.exe	C:\Windows\System32\msdtc.exe	SUSPICIOUS
msdtc.exe	C:\Windows\System32\msdtc.exe	SUSPICIOUS
System	-	CLEAN
services.exe	C:\Windows\system32\services.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	CLEAN

Process Name	Commandline	Verdict
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService	CLEAN
spoolsv.exe	C:\Windows\System32\spoolsv.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k appmodel	CLEAN
cmd.exe	cmd.exe /c taskkill /f /im msdtc.exe	CLEAN
backgroundtaskhost.exe	"C:\Windows\system32\backgroundTaskHost.exe" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca	CLEAN
taskkill.exe	taskkill /f /im msdtc.exe	CLEAN
backgroundtransferhost.exe	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	CLEAN
installagent.exe	C:\Windows\System32\InstallAgent.exe -Embedding	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	CLEAN

YARA / AV

YARA (17)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	CatB	CatB Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_Loader	CatB Ransomware Loader	Memory Dump	-	Ransomware	5/5
Ransomware	CatB	CatB Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_Loader	CatB Ransomware Loader	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_FunctionStrings	CatB Ransomware	Function Strings	-	Ransomware	5/5
Ransomware	CatB	CatB Ransomware	Dropped File	C:\windows\system32\oci.dll	Ransomware	5/5
Ransomware	CatB	CatB Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_Loader	CatB Ransomware Loader	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_Loader	CatB Ransomware Loader	Memory Dump	-	Ransomware	5/5
Ransomware	CatB	CatB Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CatB	CatB Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_Loader	CatB Ransomware Loader	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_Loader	CatB Ransomware Loader	Memory Dump	-	Ransomware	5/5
Ransomware	CatB	CatB Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CatB_FunctionStrings	CatB Ransomware	Function Strings	-	Ransomware	5/5
Ransomware	CatB_Loader	CatB Ransomware Loader	Memory Dump	-	Ransomware	5/5
Ransomware	CatB	CatB Ransomware	Memory Dump	-	Ransomware	5/5

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	2023.1.0
Dynamic Engine Version	2023.1.0 / 01/31/2023 04:27
Static Engine Version	2023.1.0.0 / 2023-01-31 03:00:19
AV Exceptions Version	2023.1.1.6 / 2023-02-03 15:34:21
Link Detonation Heuristics Version	2023.1.1.12 / 2023-02-20 08:47:29
Smart Memory Dumping Rules Version	2023.1.1.6 / 2023-02-03 15:34:21
Config Extractors Version	2023.1.1.12 / 2023-02-20 08:47:29
Signature Trust Store Version	2023.1.1.7 / 2023-02-06 18:37:42
VMRay Threat Identifiers Version	2023.1.1.12 / 2023-02-20 08:47:29
YARA Built-in Ruleset Version	2023.1.1.12

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	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