MALICIOUS

Classifications: Ransomware | Spyware | Wiper

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe**
ID	#3837111
MD5	0e48b42a225458315816541dd874e97d
SHA1	6c63f2db6be74b6a7261fab44c0afdd03615effe
SHA256	b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965
File Size	3196.00 KB
Report Created	2022-03-18 10:23 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 52 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe modifies the content of multiple user files.			
5/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe deletes multiple user files.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Total Commander, AbleFTP, git, Internet Explorer / Edge.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe possibly drops ransom note files (creates 41 instances of the file "README.html" in different locations).			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Data Collection	Reads sensitive ftp data	2	-
	• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe tries to read sensitive data of ftp application "AbleFTP" by file. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Creates an unusually large number of processes	1	-
	• Above average number of processes were monitored.			
1/5	Hide Tracks	Creates process with hidden window	39	-

Score	Category	Operation	Count	Classification
		• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #3) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #7) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #9) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #11) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #13) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #15) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #17) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #19) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #21) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #23) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #25) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #27) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #29) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #31) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #33) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #35) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #37) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #39) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #41) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #43) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #45) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #47) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #49) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #51) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #53) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #55) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #57) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #59) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #61) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #63) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #65) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #67) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #69) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #71) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #73) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #75) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #77) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #79) cmd.exe with a hidden window. • (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe starts (process #81) cmd.exe with a hidden window.		
1/5	Obfuscation	Resolves API functions dynamically	1	-
		• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe resolves 38 API functions by name.		
1/5	System Modification	Creates an unusually large number of files	1	-
		• (Process #1) b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe creates an above average number of files.		

Mitre ATT&CK Matrix

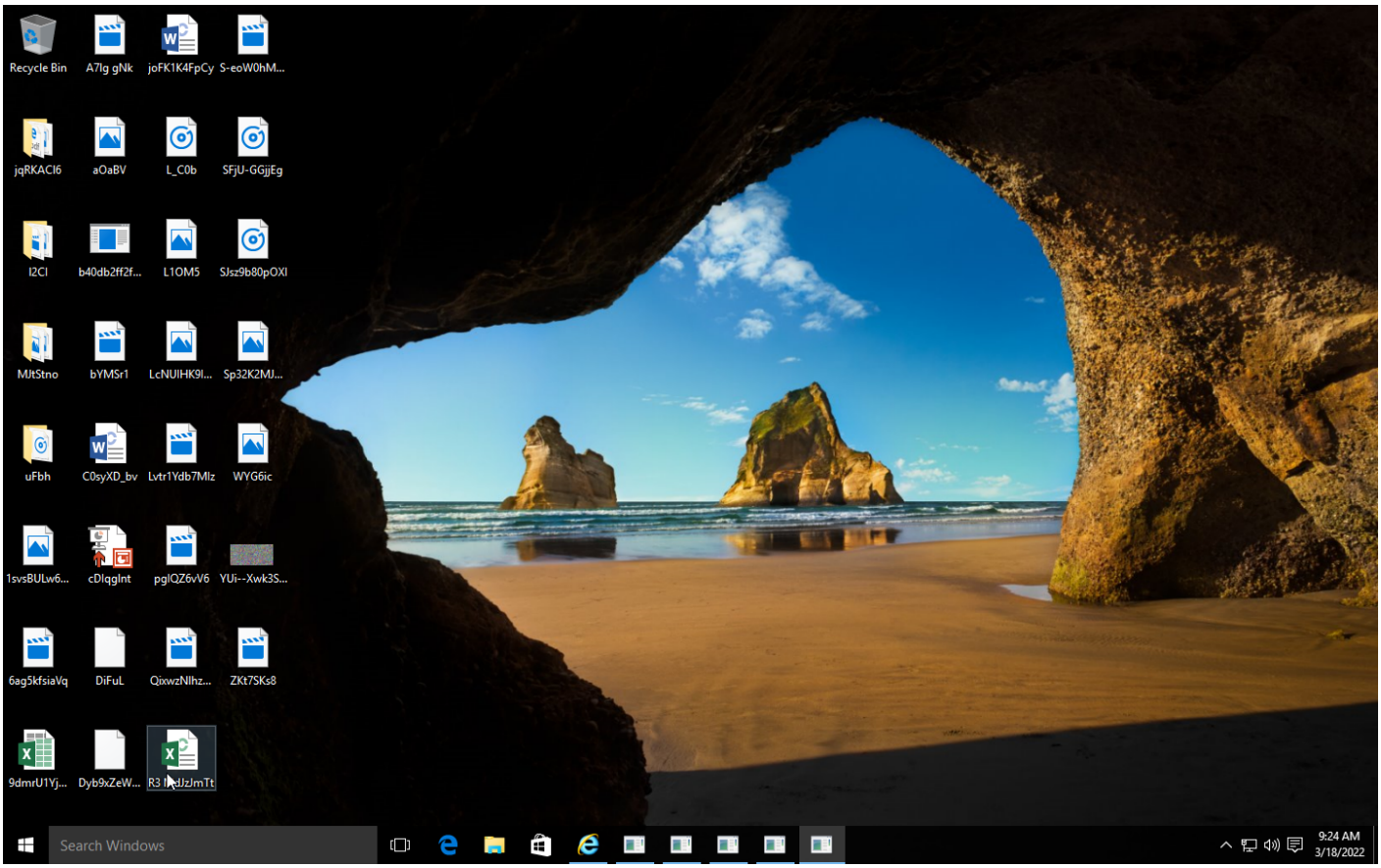
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
				#T1143 Hidden Window		#T1083 File and Directory Discovery		#T1005 Data from Local System			#T1485 Data Destruction
				#T1045 Software Packing							

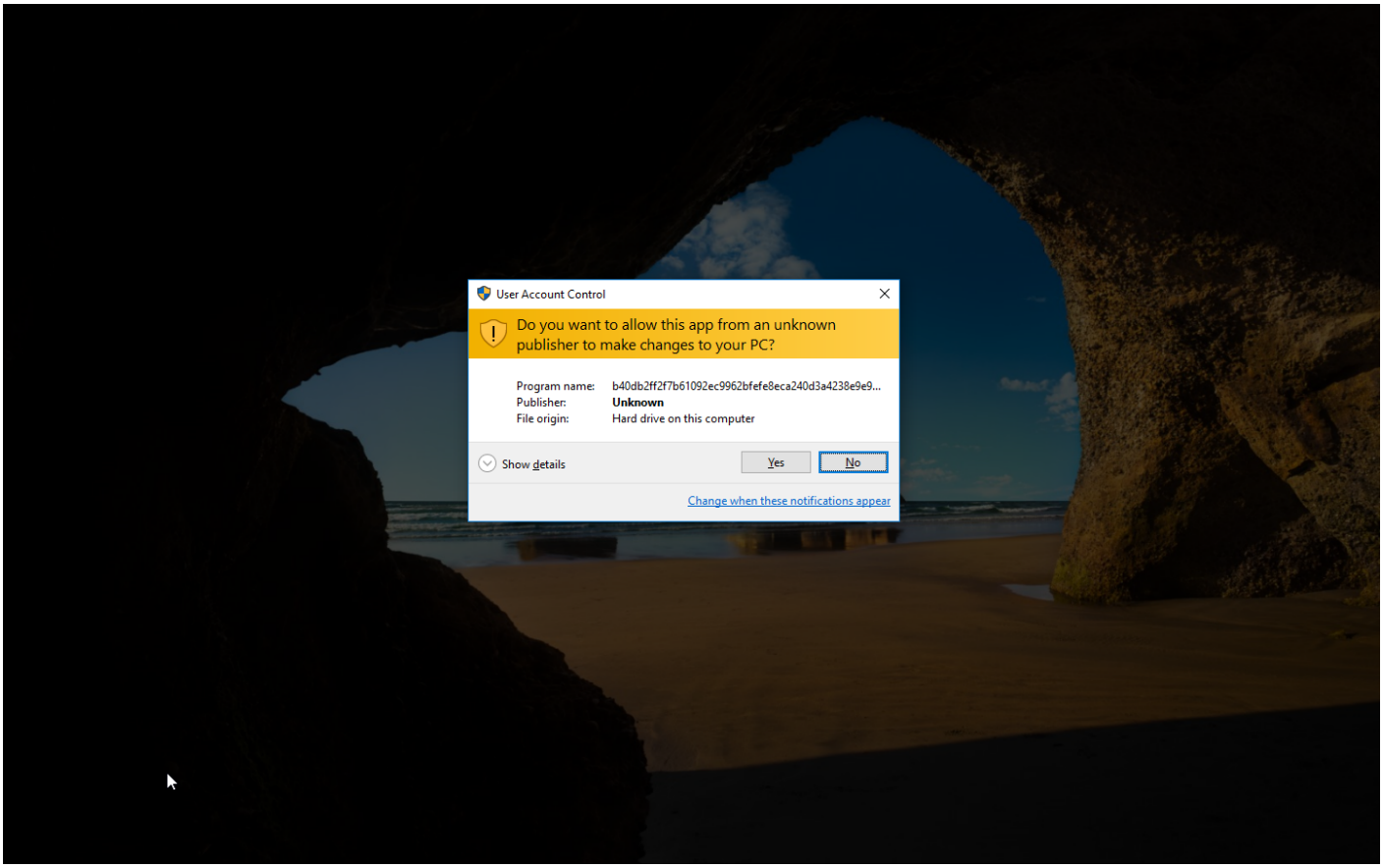
Sample Information

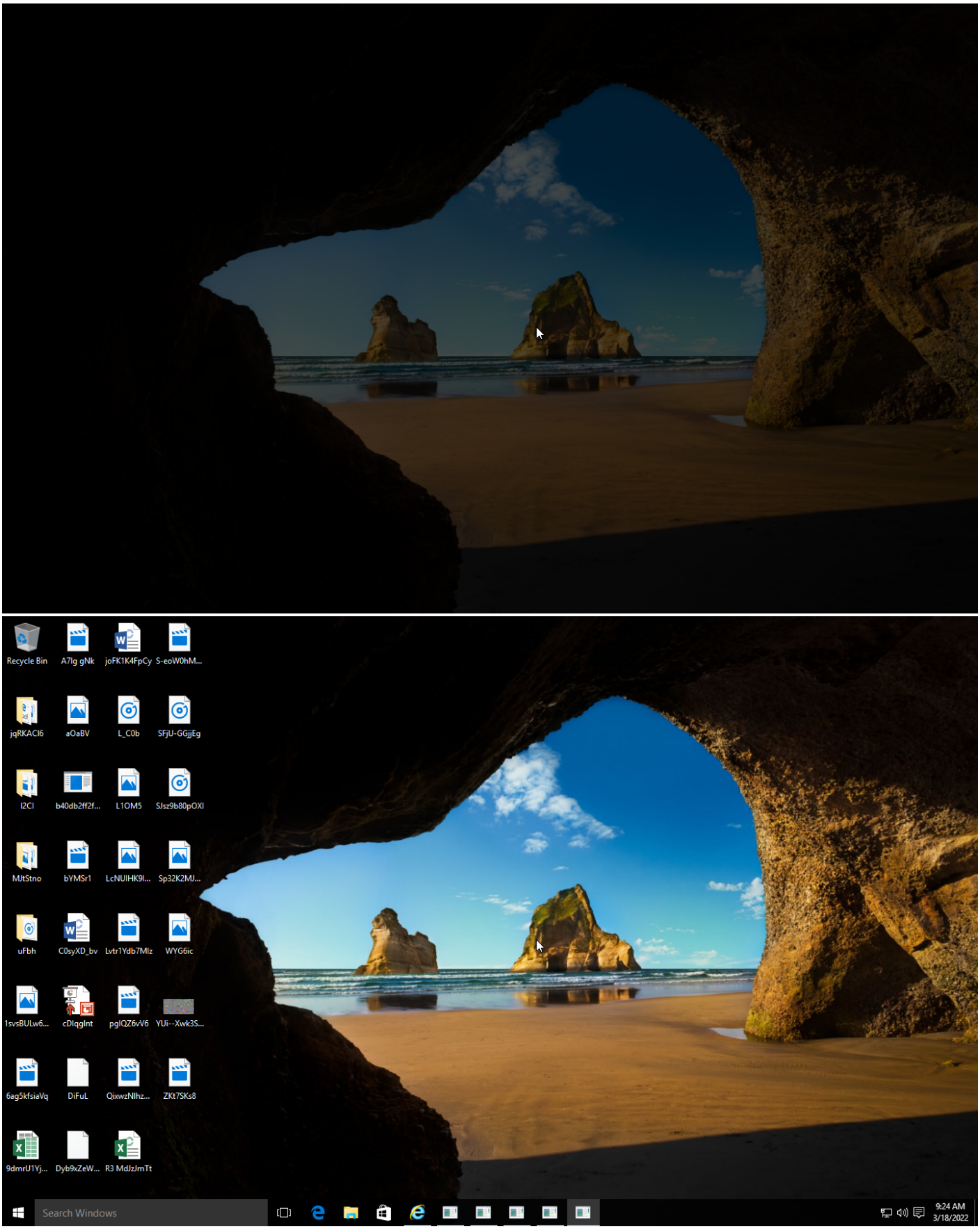
ID	#3837111
MD5	0e48b42a225458315816541dd874e97d
SHA1	6c63f2db6be74b6a7261fab44c0afdd03615effe
SHA256	b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965
SSDeep	24576:6y3ZdgKc1tBErXnOV5EwblcCOOBacp4lWv42JZCWXoBsccaUyz3OL3w00WnzZ9Lb:3ZdghtYOvHbHCstWWBK02Ul8t/f
ImpHash	96c44fa1eee2c4e9b9e77d7bf42d59e6
File Name	b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe
File Size	3196.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-03-18 10:23 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	79
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
A7lg gNk
joFK1K4FpCy
S-eoW0hM...
jqRKACl6
aOaBV
L_C0b
SFjU-GGjjEg
l2Cl
b40db2ff2f...
L1OM5
SJsz9b80pOXl
MJtStno
bYMSr1
LcNUlHK9l...
Sp32K2MJ...
uFbh
C0syXD_bv
Lvtr1Ydb7Mlz
WYG6ic
1svsBULw6...
cDlqgInt
pglQZ6vV6
YUi--Xwk3S...
6ag5kfsiaVq
DiFuL
QixwzNlhz...
ZKt7SKs8
9dmrU1Yj...
Dyb9xZeW...
Search Windows
9:24 AM
3/18/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e9...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

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

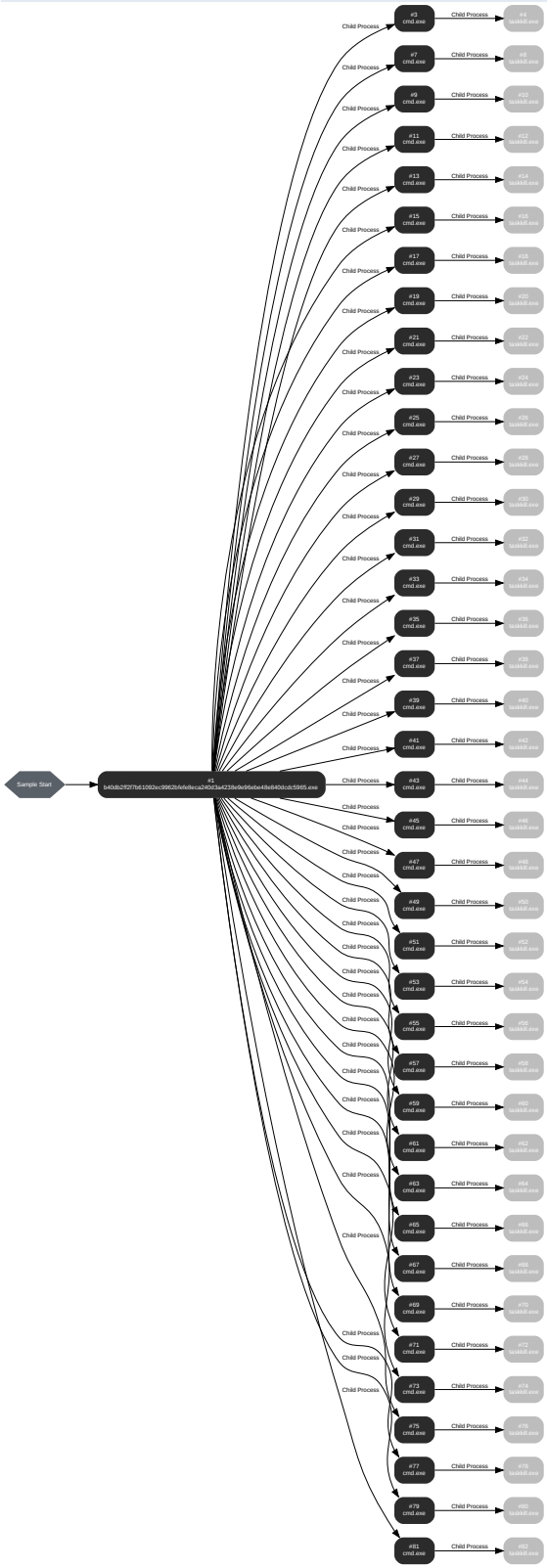
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 76549, Reason: Analysis Target
Unmonitor End Time	End Time: 318053, Reason: Terminated by Timeout
Monitor duration	241.50s
Return Code	Unknown
PID	1556
Parent PID	1184
Bitness	32 Bit

Dropped Files (199)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\windows	1.67 KB	f17946a4b13a3880ab0380888d05c17ee0c6adfc5879e5016774d80e155709c1	✗
C:\README.html	3.13 KB	f4dc1835c4945dd1a3b1d990ded128984218c279a67219110d60f77121727c00	✗
C:\Users\RDhJ0CNFevzX\Desktop\1svsBULw6E2suU5FLV.gif	1000.00 KB	56c956eadd553541e64b28a0ff8014b1717c60bf1ccc528d48c714f850e818e0	✗
C:\Users\RDhJ0CNFevzX\Desktop\1svsBULw6E2suU5FLV.gif.locked	3.14 KB	46c89b4be487ac2d3bf6e18da7eaf442c3db13b50b18b292d721f7f3badc5fa6	✗
C:\Users\RDhJ0CNFevzX\Desktop\6ag5kfsiaVq.mp4	1000.00 KB	d2a2357e75768a4dcc255f9f25e6c613f2b1b7ddc73bc30172bad6948e998ed7	✗
C:\Users\RDhJ0CNFevzX\Desktop\6ag5kfsiaVq.mp4.locked	9.53 KB	ee207e016b7634c79fbdb6a3472d827aecb842bb51b445cf6f8f60c4f302a7b5	✗
C:\Users\RDhJ0CNFevzX\Desktop\9dmrU1YjBAS.xlsx	1000.00 KB	b06004f30d1e202f660abe6e594687f21aec1c80c626a09bf34f782523ea35f6	✗
C:\Users\RDhJ0CNFevzX\Desktop\9dmrU1YjBAS.xlsx.locked	72.26 KB	aa4ecaf31d7e8301c3778e97d78b5f141cff2d4af3cb18e6704754e18da104de	✗
C:\Users\RDhJ0CNFevzX\Desktop\A7lg gNk.mkv	1000.00 KB	a9d2b2e983afe860bc4e5cfeb24f99a6f0e402fa31afae49884cf4a3ddf55f85	✗
C:\Users\RDhJ0CNFevzX\Desktop\A7lg gNk.mkv.locked	22.95 KB	e0acb1199d8a6510da90a8ca084145d5579a434f1c76d7ec17566e11f180c665	✗
C:\Users\RDhJ0CNFevzX\Desktop\C0syXD_bv.odt	1000.00 KB	e44b49b444030e3ce8363c5a423662779fe1b8ee8db70e8ff5a102b465958052	✗
C:\Users\RDhJ0CNFevzX\Desktop\C0syXD_bv.odt.locked	63.93 KB	a94129ce33a3346692f7c6b4f6568cad3a342402160f042d2801557d24174d58	✗
C:\Users\RDhJ0CNFevzX\Desktop\DiFuL.swf	1000.00 KB	510d9e524395f851fcd15c5bba0903697e82ca57c89bff9cfbc859bbb563244f5	✗
C:\Users\RDhJ0CNFevzX\Desktop\DiFuL.swf.locked	94.81 KB	06639bec533d6c37714a2bafe6db0304f2e58ee8a6f40e7370e97f0662ed5ffa	✗
C:\Users\RDhJ0CNFevzX\Desktop\Dyb9xZeWpRv.swf	1000.00 KB	3e3d3d5f575681b7bb94187fd68d1a87a5f159c74b7b9de09f73181da60b3a7e	✗
C:\Users\RDhJ0CNFevzX\Desktop\Dyb9xZeWpRv.swf.locked	15.80 KB	dbf50a3fd46136fa860e0d8722cbfad5a4e72f78bb0d87e29f0b9fc99bc1a7cf	✗
C:\Users\RDhJ0CNFevzX\Desktop\L1OM5.png	1000.00 KB	7a2208c31f931382e0f1b5ce320d8e63f2962452c69cf42e3d6f967431bb3575	✗
C:\Users\RDhJ0CNFevzX\Desktop\L1OM5.png.locked	22.28 KB	86f5e85ededd0c0f357cad2cc95aca2e6f401e3df6ceb35c7f1c45e19950cbbd	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\LcNUIHK9IEvgMQ7.jpg	1000.00 KB	52420db4ef48203a00eac41c6943085e5bea1d66cd69f5dbb7addea14fd5d18e	✗
C:\Users\RDhJ0CNFevzX\Desktop\LcNUIHK9IEvgMQ7.jpg.locked	14.42 KB	a71b6be246997c7bea957839eb1ea553ed0aaa109a5aba89e99884de1463b85c	✗
C:\Users\RDhJ0CNFevzX\Desktop\Lvtr1Ydb7MIz.mkv	1000.00 KB	e2514b14d479909bd67bc999c087670059a57032ae854d2a670a46163539d071	✗
C:\Users\RDhJ0CNFevzX\Desktop\Lvtr1Ydb7MIz.mkv.locked	24.14 KB	46afb2a9171bb6c606f33d51d1d3273046d0e9242e85d44acb1e4e1a64a7ee62	✗
C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\0RzD7W9keho8x2.gif	1000.00 KB	3b73846292ca5cb5f8cf76afd888165c9a118f5c37d2d3825b76d0c51c9c9791	✗
C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\0RzD7W9keho8x2.gif.locked	48.37 KB	8d2b115d97bec1cafcd3f526eb3913f1f97757033db99e06abf5d4165a5f82cb	✗
C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\UQjVL.png	1000.00 KB	dd470399e663d825f486ec8eb377ebba60add29b533bfd7748b93851ed5b90d7	✗
C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\UQjVL.png.locked	42.42 KB	8dd90f0ceedd1ae25106e9968df0f9a9d6f4c10305f84ee084c57ae62900ab04	✗
C:\Users\RDhJ0CNFevzX\Desktop\QixwzNIhzqpngSpTJiG.avi	1000.00 KB	a50a9834abc2bee1dbb6db615052c9d4fdfd0232b9dd29386731f441cd888e0a	✗
C:\Users\RDhJ0CNFevzX\Desktop\QixwzNIhzqpngSpTJiG.avi.locked	57.63 KB	dbb045a2e4b33d514c2a38754b5c4b08a8d78697555f8e4078e84e7d8c578b92	✗
C:\Users\RDhJ0CNFevzX\Desktop\R3 MdJzJmTt.ods	1000.00 KB	b900b2c5b44764fdf3a9c54c3e4e1c214508c5a4d248a73ca3412347b1f6f05c	✗
C:\Users\RDhJ0CNFevzX\Desktop\R3 MdJzJmTt.ods.locked	93.49 KB	267841eaac9aea99758d3a8067c8cb579665f6f07f04ab07a6273f24aed97cdc	✗
C:\Users\RDhJ0CNFevzX\Desktop\S-eoW0hMerDLmPid.mp4	1000.00 KB	0b6a70e93ea97fba2b3c0d01902133cd22e6a44851c426a008fadd2422456ebd	✗
C:\Users\RDhJ0CNFevzX\Desktop\S-eoW0hMerDLmPid.mp4.locked	17.25 KB	2ee99dffdf472a2450dd370794c506404b18580ad97beed53c21887cbf448f69	✗
C:\Users\RDhJ0CNFevzX\Desktop\SFjU-GGjjEg.wav	1000.00 KB	62827cb044d0b66e2e7d6f4ee7e8e718268e48fd8cede1fae47c06751c070757	✗
C:\Users\RDhJ0CNFevzX\Desktop\SFjU-GGjjEg.wav.locked	66.74 KB	15d927151aae287a94e8a5ae7352d97ddbdde7c4b87ea5a81aa0fd016db74781	✗
C:\Users\RDhJ0CNFevzX\Desktop\SJsz9b80pOXI.wav	1000.00 KB	afc263cbcd82e7359589c54466f1bbce56bad04462e1ffee5d00de035e24791b	✗
C:\Users\RDhJ0CNFevzX\Desktop\SJsz9b80pOXI.wav.locked	82.29 KB	59c8c9e2f4c8c909f43ece3618fdd60fe85b40905851392093e3a272aa801a1a	✗
C:\Users\RDhJ0CNFevzX\Desktop\Sp32K2MJT8oGwSN.gif	1000.00 KB	028b2a1f8f6512da8ac142c9a1449a92d8601390c2f2026556adc378959e50b5	✗
C:\Users\RDhJ0CNFevzX\Desktop\Sp32K2MJT8oGwSN.gif.locked	58.36 KB	f742dcc0ba7f4988f315de3a7619fe7b2381ea07e05e681838ef92866ab322fe	✗
C:\Users\RDhJ0CNFevzX\Desktop\WYG6ic.jpg	1000.00 KB	cae22c82669b96970efb8fd945d2844730f08943b23248cbceb07d4f9b73847b	✗
C:\Users\RDhJ0CNFevzX\Desktop\WYG6ic.jpg.locked	13.81 KB	f060645abcf83af491125e739e4a2f2cf366a58758a53f1e677034cdad066e02	✗
C:\Users\RDhJ0CNFevzX\Desktop\YUi--Xwk3SNHRau.bmp	1000.00 KB	04de5f09381081b6b47a9ff6c44527f372569edaeae21f42fb9ef22130b2e9ec	✗
C:\Users\RDhJ0CNFevzX\Desktop\YUi--Xwk3SNHRau.bmp.locked	85.70 KB	7e821cf2a4abb0f7da10f5b7de46bce13ae90c370f160eb339e4231c20c3c340	✗
C:\Users\RDhJ0CNFevzX\Desktop\ZKt7SKs8.mp4	1000.00 KB	b5d738b4493475a857a64ceab256ba3e5830f5e642d4fc113085626c1a19f343	✗
C:\Users\RDhJ0CNFevzX\Desktop\ZKt7SKs8.mp4.locked	10.31 KB	b10533907df5ab74a3d40b1870d0f85a23ba11d18e21039da72878ab7be40909	✗
C:\Users\RDhJ0CNFevzX\Desktop\aOaBV.bmp	1000.00 KB	465fda221fca6e17fd78af63687d2b2bc23e1fc0e23154e4b38305c95ae7e1e1	✗
C:\Users\RDhJ0CNFevzX\Desktop\aOaBV.bmp.locked	16.41 KB	cc9a2823bcd64c901f17ca211e56565d1e82e7c40f25707b7a50edc2a1550c98	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\bYMSr1.mkv	1000.00 KB	a49dc0f910f841ee85d698edac02198ac5decfc2d769fa09e8d3bd446f5bc307	✗
C:\Users\RDhJ0CNFevzX\Desktop\bYMSr1.mkv.locked	24.80 KB	5bb2de92da9cbd4397151a95b6ab2cc144b696cdb57c37c21ab0f32b6539676e	✗
C:\Users\RDhJ0CNFevzX\Desktop\cDIqgInt.pps	1000.00 KB	43f182df9ecf7825a6bccc09588a83e99d20ac78e3f85ffcdcdc5806a72f3554	✗
C:\Users\RDhJ0CNFevzX\Desktop\cDIqgInt.pps.locked	37.33 KB	d53e4d280f815de87c7132a3d8278c61a9822cc21ed5362871b01e6104d216d8	✗
C:\Users\RDhJ0CNFevzX\Desktop\joFK1K4FpCy.odt	1000.00 KB	982c580a49fa03a6bf058ef0e3b79d081fddbc955ba7beb5a35f7f9be4b21db9	✗
C:\Users\RDhJ0CNFevzX\Desktop\joFK1K4FpCy.odt.locked	27.26 KB	d60162c1f31f979c18686bc6406bf099c22025160a63fd4d3647c57f43717dc9	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\27JfCEVulMHbbO.mp3	1000.00 KB	76b71ef39217c8995eb651fa6cbd303bf05b4bbdb5abb56e8203551fe5f69117	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\27JfCEVulMHbbO.mp3.locked	16.62 KB	e0b55af099041861a20e4c70778df0e817f9f3628795213308c5f6f1468bec53	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\9Vntf.mkv	1000.00 KB	d2bf2a730dd8478649f55a39229e394a4f8cdfa336cd77e4adc19b0d625de800	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\9Vntf.mkv.locked	53.05 KB	1435cd76bac95d35a9f0e8aad7011f51f4b2c6e64473b64f9592930fafe33611	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\kfCcoa0Kn4e.mp3	1000.00 KB	78f673b8564763f614b2ecdccf2d65d8d01f1e8d9b8e3e5711b6482c5b0614a9	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\kfCcoa0Kn4e.mp3.locked	47.60 KB	31cfa5bf2a594423f3c0f4d955349824a04cb60ef577c6479cb92d9a8e10c2cd	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\lkG90.jpg	1000.00 KB	19271e7ef63c5163e92c0ef85f58c12ada8561b7732769f242bed082eeafdddd	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\lkG90.jpg.locked	8.40 KB	2fc7888b36c372d90b70da48ce2ccd5c24640b7ea190691c02789629b52863df	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\w8O0bav5Ww_S.pdf	1000.00 KB	d6603040b9e7f4f181826890b901b1082669239a09ff85fc780c4d4b4befc843	✗
C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\w8O0bav5Ww_S.pdf.locked	95.34 KB	b2be9af5b09740471120e08be793ddc8eb9bf56b505f802f174309af509fb77c	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\D-Cg-mvfsgn.flv	1000.00 KB	b7b67aabbfb47069e1840d2b274aee7593939a901934610e9fee7575bf9b0459	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\D-Cg-mvfsgn.flv.locked	4.89 KB	5d81d02d86323e15210db22af3d351015c8e2d83edcba9441baadf53b9d07aa3	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\KBe56raX.jpg	1000.00 KB	29b4805b8be70bff0b471adc691a3c21ea1f49cd5d76362c40d8d4080ed9515f	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\KBe56raX.jpg.locked	14.57 KB	247d7337165b2a27a5c1c568c8b09f5be1dbae1364d48bc7ddcdc22631da9676	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\UyGAh1goU67sQ4n_bFy.mp3	1000.00 KB	5677e2cb5d666bfa137af30e7346b80c4b8969e9f4094240f935c0a2c5225704	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\UyGAh1goU67sQ4n_bFy.mp3.locked	18.08 KB	fada929b7f22f74292efe12b33fcb74de92031ab1270aa28ca9d06d40ed741fd	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\pmRHoZn51.avi	1000.00 KB	a09c6d65c28f1a3302a9dd7f8a5f59be3d91a1af4f3324312754394 61fcd035a	✗
C:\Users\RDhJ0CNFevzX\Desktop\l2CI\pmRHoZn51.avi.locked	82.28 KB	bd3c4aa89e01b886f5faee099ad8aa0ba515dd5e4782bbb1ab33835feb62cfa1	✗
C:\Users\RDhJ0CNFevzX\Desktop\pgIQZ6vV6.mkv	1000.00 KB	73e798c0ea206fe9e841a0e5105bae7caf25a1e21adc0387fb9bcbddc59dd4bd	✗
C:\Users\RDhJ0CNFevzX\Desktop\pgIQZ6vV6.mkv.locked	65.81 KB	f376ae9e7de1343e9a91ef1112b2f51f9adb246d4dae53e307065d7c04fb1304	✗
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\4m1VwisQwNYyO.mp3	1000.00 KB	ece913d714c2b991a89975162850de8a1af1efd06bc3692af0f5a20372f4d41d	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\4m1VwisQwNYyO.mp3.locked	95.92 KB	b85f34a1791299ace654022b289c159d6645dbce4010ef39dc009d3d76f6463f	✗
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drIHYf6Q54DMKd0A\3_vtHE.pptx	1000.00 KB	bdaafdeaee19cb204b67b0e26cb72a4995ed461e0669424c3ef5f086192560de	✗
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drIHYf6Q54DMKd0A\3_vtHE.pptx.locked	68.36 KB	f3f53a25134df8e3cc5dcee88b7da6200b2cc303c39554ef3f1d0b0a38915026	✗
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drIHYf6Q54DMKd0A\664ei1-x8f0_Yk6d9oEE.png	1000.00 KB	797d35946436b04c072eeb7a27994ae601afaddd11692bdb30f8e2a2972df8ac	✗
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drIHYf6Q54DMKd0A\664ei1-x8f0_Yk6d9oEE.png.locked	11.64 KB	4ff9a5b1bf27f87e63e12f6f7a0ebeda24e6e70d386e67b59e474b38b7032364	✗
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drIHYf6Q54DMKd0A\zeUh4blJhKCdE8.swf	1000.00 KB	d29dbd8bd703a6ad3fa28c3e1267b74d2c03a416434769dd35a1293c93c2bcc4	✗
C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drIHYf6Q54DMKd0A\zeUh4blJhKCdE8.swf.locked	78.86 KB	4b5d7e57499730e02e4dde9af5b9a9bb54a07ed83be6c68a8fdff1e7f513e71b	✗
C:\Users\RDhJ0CNFevzX\Documents\2kmOhs9S25.xlsx	1000.00 KB	a3dcc595dafb405dc807798bc1bbfb2b563724b751509ec86567c107c9f0eada	✗
C:\Users\RDhJ0CNFevzX\Documents\2kmOhs9S25.xlsx.locked	47.22 KB	b24f5a9dd65ebe862239800b5f387df564d423a7ea2b0a73a39842c3f6b98ec6	✗
C:\Users\RDhJ0CNFevzX\Documents\5pf90.rtf	1000.00 KB	4880804cdb76879c7be131ba6fe69756977ab7661b7c77a7f6ff9d4d0b1b1a8c	✗
C:\Users\RDhJ0CNFevzX\Documents\5pf90.rtf.locked	47.76 KB	849abb3aa62738cdb26883a6b5f1f0e4bc3b32961aec9d0dab68f60da51c59c4	✗
C:\Users\RDhJ0CNFevzX\Documents\6gmL5X_4slK-0_B6U.xlsx	1000.00 KB	3ad7fe5f7689c4ec5ef202aa26940ce05f99f19b00f9bcf05f20f05e0c388ae2	✗
C:\Users\RDhJ0CNFevzX\Documents\6gmL5X_4slK-0_B6U.xlsx.locked	9.10 KB	3e9d4e0016cac6ca52563e303851f873a3f937366fd5db728f348ca7bd0a20ab	✗
C:\Users\RDhJ0CNFevzX\Documents\7GBj_BHQB3gjCk60.docx	1000.00 KB	5a376e46b2d3e3b77ecffdff0e7d5297f3806d6e095e54b0ef77f1388d8698d3	✗
C:\Users\RDhJ0CNFevzX\Documents\7GBj_BHQB3gjCk60.docx.locked	34.16 KB	6ed16a005ee52e80a37efaf7cee90062d2bd74fe342760dbe3f41aa487d43f78	✗
C:\Users\RDhJ0CNFevzX\Documents\8Y_umCxII.xlsx	1000.00 KB	1bb4151798964ae3ff3a5b6a6f610b6d7d215a76ad5b73fac23e3a5da0ba5b12	✗
C:\Users\RDhJ0CNFevzX\Documents\8Y_umCxII.xlsx.locked	28.94 KB	5ff5c5641c6326d8edb27023683ed4164a6bdf7a93ea60002eb1cb63809e6d98	✗
C:\Users\RDhJ0CNFevzX\Documents\GAL0vICrqtbz5.ots	1000.00 KB	2735dd0f63b377a05100da8a15c92cfa6ccddda9875b4ba939960bed025b4160	✗
C:\Users\RDhJ0CNFevzX\Documents\GAL0vICrqtbz5.ots.locked	30.66 KB	534257e4fbb8f9f6efd600a79131052255a22bef4872d22101488dc005c567ce	✗
C:\Users\RDhJ0CNFevzX\Documents\Nv-fQq_ b.pptx	1000.00 KB	b6bd6ce1de92f12456f0e7d82a30594a0e72e5fc960086fd92032bda815c819f	✗
C:\Users\RDhJ0CNFevzX\Documents\Nv-fQq_ b.pptx.locked	7.08 KB	88d7cc8586c30b451c0525072c35ec7b0ede3f24cb4f1bf64ddb242cc6902ae0	✗
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	1000.00 KB	47dbe12984799f370541228799a9f975f1a696487030a74e149966825a6ee2ef	✗
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.locked	265.12 KB	8308f09745acd3f8933592e4d2b6675cd3c18feeb7922e063f0b5bbb0507bff6	✗
C:\Users\RDhJ0CNFevzX\Documents\SfN_7SLvBv6HWGGZ.docx	1000.00 KB	eb9429e6db28689a46665dbd9d69d2a36915463e9abd1665bee52e0e8b242262	✗
C:\Users\RDhJ0CNFevzX\Documents\SfN_7SLvBv6HWGGZ.docx.locked	38.48 KB	1f979f7805b29aff4f275089ad3eccc14a140e4fb7e5a13860a61f1f2df9dfab	✗
C:\Users\RDhJ0CNFevzX\Documents\TaxhME.pptx	1000.00 KB	2ea233be47c3b6986054a87ba6a28831390013cda71592268b94da583c661979	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\TaxhME.pptx.locked	12.01 KB	87feade60556f8542817febcf84ed6e514e59d8bb98e6f689b557c67673a9347	✗
C:\Users\RDhJ0CNFevzX\Documents\XlenjhZeamfDvL.odt	1000.00 KB	82aa1bfe55d7d1020288ff1ca22c9efbacf6c7d3e82262fdb5d3cf2b5cb4de0a	✗
C:\Users\RDhJ0CNFevzX\Documents\XlenjhZeamfDvL.odt.locked	15.57 KB	5024b442f395b3a7e89d7ec9ba8489fb9c32f6a5238214becc661d4eccc35a2b	✗
C:\Users\RDhJ0CNFevzX\Documents\YKkR7 10Jqcina5HGOD.pptx	1000.00 KB	2d0eac453dd131013110f1d992e6ba5d88c9a09ce6f7c74031cfdd3c5d595658	✗
C:\Users\RDhJ0CNFevzX\Documents\YKkR7 10Jqcina5HGOD.pptx.locked	93.35 KB	9ffa51149977e9e9d42043ae2e3b7f4242005eb42c7f355c1f189a6beadb549c	✗
C:\Users\RDhJ0CNFevzX\Documents\Zx_PeYMMp5W-Vj0.xlsx	1000.00 KB	2d4612a496f218629dd27a97f8c01313bbd17eeb996f3c0dd266d00552702b9b	✗
C:\Users\RDhJ0CNFevzX\Documents\Zx_PeYMMp5W-Vj0.xlsx.locked	76.77 KB	fb6094bb0161408125411f5b113f475190cb8482d2b78832837ec2a486946a7e	✗
C:\Users\RDhJ0CNFevzX\Documents\eBPMR.pptx	1000.00 KB	20fb11714d984a7a76c1bcf2ff271d2337d2648937ba590826162f7bef997da3	✗
C:\Users\RDhJ0CNFevzX\Documents\eBPMR.pptx.locked	35.70 KB	f0ebc663a443ca21e7f83e2010b20f845688aa453db0875111942cce16f35318	✗
C:\Users\RDhJ0CNFevzX\Documents\eau-Oo1pPUvz4w8PX.ppt	1000.00 KB	99592d59d4cb2717c295becc70277a66a5bc95f0fd1e0a321a33ea84e2919f6d	✗
C:\Users\RDhJ0CNFevzX\Documents\eau-Oo1pPUvz4w8PX.ppt.locked	45.76 KB	a0d78e1c293d592fcd5ad4b9e063cbdec23ff321e27071d2c63c874dcd1a8cb6	✗
C:\Users\RDhJ0CNFevzX\Documents\gRpk8Z1c.docx	1000.00 KB	4ee26b626744940ed70bf735521cf2ef7faa107ff738c50ce4d73f82ae486469	✗
C:\Users\RDhJ0CNFevzX\Documents\gRpk8Z1c.docx.locked	76.90 KB	79c8d752d8b033d0347330a0874c82ecb0a8b75f852404ef3f42b195aa4733bb	✗
C:\Users\RDhJ0CNFevzX\Documents\jaCxkmZM5HvA.docx	1000.00 KB	8918f31f3b0ffb1b052bde1b73e77903e64bff55fc7078e39b72af0acd63c8cd	✗
C:\Users\RDhJ0CNFevzX\Documents\jaCxkmZM5HvA.docx.locked	75.31 KB	0b7bace5157a8a2dce4b3de0e08c2e705e8859eba96bd2fca1ffd695d76c4295	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\6ah1b.odp	1000.00 KB	c25cbeedff6478885c9643c862fc8a0719fe7d8c02abcec0051a8c0a26be7405	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\6ah1b.odp.locked	89.17 KB	9d261d21fa605d42e626a9e47d93ed3afe5764d726bb6bb4513b8a8ad6b31f33	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\uMlP.pps	1000.00 KB	7840e46c2638e72710e3964e3413b63e7215fd9de854fe4558d793684d0395f8	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\uMlP.pps.locked	86.34 KB	9439ea10d700ce1df3bd9659c1be74faba963b48bdb1e801283170df291e0dd7	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\3Zq4EcajslY7PFQKVsvW.pdf	1000.00 KB	f425751cdb3f2df2b98df4a3c3ec7736a12534cf2329d746a95f8ad1fd316f12	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\3Zq4EcajslY7PFQKVsvW.pdf.locked	26.55 KB	9735d3500549a4959b0d83d10d71e4e0a4c64ff7fd61c251b45e6174cf45d689	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\9RRM_.csv	1000.00 KB	6a8c3457b179fe43d2a90e6ccb95d09f3386c3a2d4e4a03dc8576b5f17894ff1	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\9RRM_.csv.locked	12.82 KB	cf1c225e48bb705080c2c8e28c998fd6e9f73bf346ce31bc30126bb59f421824	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\H9ZYmL.pptx	1000.00 KB	4e86d73318b19034615d4be799a0ee95c162b8ec3264f5c3321e30422cd8b85f	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\H9ZYmL.pptx.locked	97.12 KB	eeee5b74068de51b045e97b25c9bb117a769ed8c693b5a4fb13494161ec0fa99	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\-iqW_.pptx	1000.00 KB	a388ea78fa468bc98e4f964078f520c4f0aeb1672dc67ac9a5838b4086d4f72f	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\-iqW_.pptx.locked	55.33 KB	9bc7e4d177c69e6a0a480ac68696b55f16c7b4af4dc8ed88e38c2d66006a9a6b	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\Q8qlBA 30gG.ods	1000.00 KB	e530aed9411237e1821616c47917228748ac5f9f8ad44d8bce76ad7678110f5d	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\Q8qlBA 30gG.ods.locked	42.00 KB	52644d8bc87964ba8d8e72166f6093369a45a3e8872f7361f397f082f4a91ca2	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\VNJUeKMIKE5Ysn n.rtf	1000.00 KB	957cbcbd059f6c760407d7e4807c4ee2e8a1c2859ca1b1222facd7747acd3446	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\VNJUeKMIKE5Ysn n.rtf.locked	54.14 KB	befb361243ef7090fc7c5d46c80ac13ce59fa53b9bb38c3d543c03320a694df2	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\xgy7j.pptx	1000.00 KB	315b901ec3e5b8df0bbae4f9b7a53e5809f1efdc8d7c319e9d4370aab475f1af	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\xgy7j.pptx.locked	33.77 KB	4561956a65afec745c32adabd2c0dcda586184497a64d8ebfbf22ef82b1e9fa5	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\zIPqwuKy.rtf	1000.00 KB	29fe4695ed925cd18b9819c7525d00e7e3e4d2235da016ea2e359038ab58d273	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\5A5KELPEB3fxvrO\zIPqwuKy.rtf.locked	72.29 KB	c613ade9d3bcf87a0e86dca7ade78827091c9072db6f1484055ca41f821afe1d	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\LtbtPfDoTJ77Qjxw.odt	1000.00 KB	50b7de5ce870c22203c9ce0ae3066cb8ab6d938f913cdfe77c28e7f96dcb0572	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\LtbtPfDoTJ77Qjxw.odt.locked	65.91 KB	15e2e76b4bb35c643dbd9598c2b4a9527fda055f0653cf794435571ee15e28d1	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\Mh6oNy9bLKM5.pps	1000.00 KB	f22fc6f6ea74e52bf7e0fa6e9197f1c60507520c1182d20254c25c468f64677e	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\Mh6oNy9bLKM5.pps.locked	22.21 KB	167f60a902860fcecc06e5a5b35023c3e0f966cf185db220746f385858b3a96e	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\ZjvJmA1w8wm09o.odt	1000.00 KB	be02d24e78664b4f8784421f09d4847b9864c73ad2f480d376674c46c630625d	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\ZjvJmA1w8wm09o.odt.locked	82.93 KB	6dc888e59cf9ee4a2c4758394e0717437c1243f149334700d84f399f42eb1a61	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\bPP6k2AtPCvK.odp	1000.00 KB	f9f0ac38a4cd220f20915b7c2c6df1e896bc74792d78c0eb8bfec3061709b68c	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\bPP6k2AtPCvK.odp.locked	82.49 KB	2cef7f23852bfb4210821c4d29414963bc17acef59d326d5e5236b9bb9d69ab2	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\8BmBuzkrBAz-1J-IShq.pdf	1000.00 KB	44ad6bba2e1868cf4b1890535c561bb0c6b9a6dd90c4a4c28828a3bf2b170e62	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\8BmBuzkrBAz-1J-IShq.pdf.locked	10.65 KB	abdc90fccae93deebd9abdd9231f509db489f2635e0f9866d5e97420d7238a46	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\R1iyoik0t.ppt	1000.00 KB	8926a7b659945b81d5102841e0cf2e4d3639320508b032578c455d77f2e6bf9e	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\R1iyoik0t.ppt.locked	14.75 KB	44c5d70caa46c9dc22317d0b64e9d10b59b544db654703af3663261159e3c49e	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\fAbqQJxC6j.xls	1000.00 KB	f388c1e7d136aceddf5556da363f1c7928e13f1399cf0efd2f6c41f2725cb011	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\fAbqQJxC6j.xls.locked	99.34 KB	8db19dc78c9951b274811d9349ec34ee1996e6046f534ce5b115056215c80927	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\qb50fmMABVOmckG.docx	1000.00 KB	3a96de32868203997b50abc1e427aa85e0916dd03e6a473c69f3fa09250bff68	✗
C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7S xtG\qb50fmMABVOmckG.docx.locked	76.03 KB	cb957aa09c92a04c1cc9f036f3768320bf57e396c1d12976d1828e2eda31c6cb	✗

Reduced dataset

Host Behavior

Type	Count
Module	44
System	2
Environment	161
-	6
File	7350
Process	39

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im msftesql.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109568, Reason: Child Process
Unmonitor End Time	End Time: 119999, Reason: Terminated
Monitor duration	10.43s
Return Code	128
PID	4624
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #4: taskkill.exe

ID	4
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im msftesql.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 110335, Reason: Child Process
Unmonitor End Time	End Time: 120003, Reason: Terminated
Monitor duration	9.67s
Return Code	128
PID	4620
Parent PID	4624
Bitness	32 Bit

Process #7: cmd.exe

ID	7
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im sqlagent.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 120039, Reason: Child Process
Unmonitor End Time	End Time: 122375, Reason: Terminated
Monitor duration	2.34s
Return Code	128
PID	5068
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #8: taskkill.exe

ID	8
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im sqlagent.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 120574, Reason: Child Process
Unmonitor End Time	End Time: 122202, Reason: Terminated
Monitor duration	1.63s
Return Code	128
PID	3292
Parent PID	5068
Bitness	32 Bit

Process #9: cmd.exe

ID	9
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im sqlbrowser.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 121970, Reason: Child Process
Unmonitor End Time	End Time: 124045, Reason: Terminated
Monitor duration	2.08s
Return Code	128
PID	1620
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #10: taskkill.exe

ID	10
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im sqlbrowser.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 122204, Reason: Child Process
Unmonitor End Time	End Time: 124351, Reason: Terminated
Monitor duration	2.15s
Return Code	128
PID	5080
Parent PID	1620
Bitness	32 Bit

Process #11: cmd.exe

ID	11
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im sqlservr.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 123653, Reason: Child Process
Unmonitor End Time	End Time: 125209, Reason: Terminated
Monitor duration	1.56s
Return Code	128
PID	4696
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #12: taskkill.exe

ID	12
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im sqlservr.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 123883, Reason: Child Process
Unmonitor End Time	End Time: 125331, Reason: Terminated
Monitor duration	1.45s
Return Code	128
PID	4672
Parent PID	4696
Bitness	32 Bit

Process #13: cmd.exe

ID	13
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im sqlwriter.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 124996, Reason: Child Process
Unmonitor End Time	End Time: 127169, Reason: Terminated
Monitor duration	2.17s
Return Code	128
PID	2472
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #14: taskkill.exe

ID	14
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im sqlwriter.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 125339, Reason: Child Process
Unmonitor End Time	End Time: 126774, Reason: Terminated
Monitor duration	1.44s
Return Code	128
PID	2408
Parent PID	2472
Bitness	32 Bit

Process #15: cmd.exe

ID	15
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im oracle.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 126777, Reason: Child Process
Unmonitor End Time	End Time: 128733, Reason: Terminated
Monitor duration	1.96s
Return Code	128
PID	2284
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #16: taskkill.exe

ID	16
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im oracle.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 127174, Reason: Child Process
Unmonitor End Time	End Time: 129253, Reason: Terminated
Monitor duration	2.08s
Return Code	128
PID	176
Parent PID	2284
Bitness	32 Bit

Process #17: cmd.exe

ID	17
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im ocssd.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 128443, Reason: Child Process
Unmonitor End Time	End Time: 130225, Reason: Terminated
Monitor duration	1.78s
Return Code	128
PID	2968
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #18: taskkill.exe

ID	18
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im ocssd.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 128735, Reason: Child Process
Unmonitor End Time	End Time: 130508, Reason: Terminated
Monitor duration	1.77s
Return Code	128
PID	3136
Parent PID	2968
Bitness	32 Bit

Process #19: cmd.exe

ID	19
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im dbsnmp.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 130229, Reason: Child Process
Unmonitor End Time	End Time: 131868, Reason: Terminated
Monitor duration	1.64s
Return Code	128
PID	2348
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #20: taskkill.exe

ID	20
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im dbsnmp.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 130508, Reason: Child Process
Unmonitor End Time	End Time: 131635, Reason: Terminated
Monitor duration	1.13s
Return Code	128
PID	4100
Parent PID	2348
Bitness	32 Bit

Process #21: cmd.exe

ID	21
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im synctime.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 131639, Reason: Child Process
Unmonitor End Time	End Time: 133667, Reason: Terminated
Monitor duration	2.03s
Return Code	128
PID	4124
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #22: taskkill.exe

ID	22
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im synctime.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 131868, Reason: Child Process
Unmonitor End Time	End Time: 133889, Reason: Terminated
Monitor duration	2.02s
Return Code	128
PID	4168
Parent PID	4124
Bitness	32 Bit

Process #23: cmd.exe

ID	23
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im mydesktopqos.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 133402, Reason: Child Process
Unmonitor End Time	End Time: 138448, Reason: Terminated
Monitor duration	5.05s
Return Code	128
PID	4348
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #24: taskkill.exe

ID	24
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im mydesktopqos.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 133670, Reason: Child Process
Unmonitor End Time	End Time: 137966, Reason: Terminated
Monitor duration	4.30s
Return Code	128
PID	4360
Parent PID	4348
Bitness	32 Bit

Process #25: cmd.exe

ID	25
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im agntsvc.exeisqlplussvc.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 138318, Reason: Child Process
Unmonitor End Time	End Time: 140247, Reason: Terminated
Monitor duration	1.93s
Return Code	128
PID	4440
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #26: taskkill.exe

ID	26
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im agntsvc.exeisqlplussvc.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 138666, Reason: Child Process
Unmonitor End Time	End Time: 141101, Reason: Terminated
Monitor duration	2.44s
Return Code	128
PID	4472
Parent PID	4440
Bitness	32 Bit

Process #27: cmd.exe

ID	27
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im xfssvccon.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 140249, Reason: Child Process
Unmonitor End Time	End Time: 142869, Reason: Terminated
Monitor duration	2.62s
Return Code	128
PID	4564
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #28: taskkill.exe

ID	28
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im xfssvccon.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 140671, Reason: Child Process
Unmonitor End Time	End Time: 141895, Reason: Terminated
Monitor duration	1.22s
Return Code	128
PID	4996
Parent PID	4564
Bitness	32 Bit

Process #29: cmd.exe

ID	29
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im mydesktopservice.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 141896, Reason: Child Process
Unmonitor End Time	End Time: 143581, Reason: Terminated
Monitor duration	1.69s
Return Code	128
PID	740
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #30: taskkill.exe

ID	30
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im mydesktopservice.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 142157, Reason: Child Process
Unmonitor End Time	End Time: 144276, Reason: Terminated
Monitor duration	2.12s
Return Code	128
PID	5092
Parent PID	740
Bitness	32 Bit

Process #31: cmd.exe

ID	31
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im ocautoupds.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 143414, Reason: Child Process
Unmonitor End Time	End Time: 144861, Reason: Terminated
Monitor duration	1.45s
Return Code	128
PID	4088
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #32: taskkill.exe

ID	32
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im ocautoupds.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 143585, Reason: Child Process
Unmonitor End Time	End Time: 144713, Reason: Terminated
Monitor duration	1.13s
Return Code	128
PID	2768
Parent PID	4088
Bitness	32 Bit

Process #33: cmd.exe

ID	33
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im agntsvc.exeagntsvc.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 144717, Reason: Child Process
Unmonitor End Time	End Time: 146261, Reason: Terminated
Monitor duration	1.54s
Return Code	128
PID	3116
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #34: taskkill.exe

ID	34
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im agntsvc.exeagntsvc.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 144961, Reason: Child Process
Unmonitor End Time	End Time: 146063, Reason: Terminated
Monitor duration	1.10s
Return Code	128
PID	3100
Parent PID	3116
Bitness	32 Bit

Process #35: cmd.exe

ID	35
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im agntsvc.exeencsvc.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 146070, Reason: Child Process
Unmonitor End Time	End Time: 147879, Reason: Terminated
Monitor duration	1.81s
Return Code	128
PID	1300
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #36: taskkill.exe

ID	36
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im agntsvc.exeencsvc.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 146262, Reason: Child Process
Unmonitor End Time	End Time: 147527, Reason: Terminated
Monitor duration	1.26s
Return Code	128
PID	1296
Parent PID	1300
Bitness	32 Bit

Process #37: cmd.exe

ID	37
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im firefoxconfig.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 147530, Reason: Child Process
Unmonitor End Time	End Time: 149804, Reason: Terminated
Monitor duration	2.27s
Return Code	128
PID	3464
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #38: taskkill.exe

ID	38
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im firefoxconfig.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 147883, Reason: Child Process
Unmonitor End Time	End Time: 149112, Reason: Terminated
Monitor duration	1.23s
Return Code	128
PID	4584
Parent PID	3464
Bitness	32 Bit

Process #39: cmd.exe

ID	39
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im tbirdconfig.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 149114, Reason: Child Process
Unmonitor End Time	End Time: 151420, Reason: Terminated
Monitor duration	2.31s
Return Code	128
PID	3672
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #40: taskkill.exe

ID	40
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im tbirdconfig.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 149905, Reason: Child Process
Unmonitor End Time	End Time: 150770, Reason: Terminated
Monitor duration	0.86s
Return Code	128
PID	2212
Parent PID	3672
Bitness	32 Bit

Process #41: cmd.exe

ID	41
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im ocomm.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 150773, Reason: Child Process
Unmonitor End Time	End Time: 153155, Reason: Terminated
Monitor duration	2.38s
Return Code	128
PID	236
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #42: taskkill.exe

ID	42
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im ocomm.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 151008, Reason: Child Process
Unmonitor End Time	End Time: 153649, Reason: Terminated
Monitor duration	2.64s
Return Code	128
PID	380
Parent PID	236
Bitness	32 Bit

Process #43: cmd.exe

ID	43
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im mysqld.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 152515, Reason: Child Process
Unmonitor End Time	End Time: 155934, Reason: Terminated
Monitor duration	3.42s
Return Code	128
PID	4620
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #44: taskkill.exe

ID	44
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im mysqld.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 153159, Reason: Child Process
Unmonitor End Time	End Time: 155622, Reason: Terminated
Monitor duration	2.46s
Return Code	128
PID	4624
Parent PID	4620
Bitness	32 Bit

Process #45: cmd.exe

ID	45
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im mysqld-nt.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 155624, Reason: Child Process
Unmonitor End Time	End Time: 157047, Reason: Terminated
Monitor duration	1.42s
Return Code	128
PID	5068
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #46: taskkill.exe

ID	46
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im mysqld-nt.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 155936, Reason: Child Process
Unmonitor End Time	End Time: 157590, Reason: Terminated
Monitor duration	1.65s
Return Code	128
PID	3312
Parent PID	5068
Bitness	32 Bit

Process #47: cmd.exe

ID	47
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im mysqld-opt.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 157014, Reason: Child Process
Unmonitor End Time	End Time: 158814, Reason: Terminated
Monitor duration	1.80s
Return Code	128
PID	1620
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #48: taskkill.exe

ID	48
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im mysqld-opt.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 157303, Reason: Child Process
Unmonitor End Time	End Time: 158556, Reason: Terminated
Monitor duration	1.25s
Return Code	128
PID	3480
Parent PID	1620
Bitness	32 Bit

Process #49: cmd.exe

ID	49
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im dbeng50.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 158560, Reason: Child Process
Unmonitor End Time	End Time: 164180, Reason: Terminated
Monitor duration	5.62s
Return Code	128
PID	4672
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #50: taskkill.exe

ID	50
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im dbeng50.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 158817, Reason: Child Process
Unmonitor End Time	End Time: 162995, Reason: Terminated
Monitor duration	4.18s
Return Code	128
PID	4696
Parent PID	4672
Bitness	32 Bit

Process #51: cmd.exe

ID	51
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im sqbcoreservice.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 163272, Reason: Child Process
Unmonitor End Time	End Time: 166159, Reason: Terminated
Monitor duration	2.89s
Return Code	128
PID	3176
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #52: taskkill.exe

ID	52
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im sqbcoreservice.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 163699, Reason: Child Process
Unmonitor End Time	End Time: 165697, Reason: Terminated
Monitor duration	2.00s
Return Code	128
PID	4716
Parent PID	3176
Bitness	32 Bit

Process #53: cmd.exe

ID	53
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im excel.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 165727, Reason: Child Process
Unmonitor End Time	End Time: 173905, Reason: Terminated
Monitor duration	8.18s
Return Code	128
PID	2828
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #54: taskkill.exe

ID	54
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im excel.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 165970, Reason: Child Process
Unmonitor End Time	End Time: 172424, Reason: Terminated
Monitor duration	6.45s
Return Code	128
PID	1884
Parent PID	2828
Bitness	32 Bit

Process #55: cmd.exe

ID	55
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im infopath.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 172873, Reason: Child Process
Unmonitor End Time	End Time: 175660, Reason: Terminated
Monitor duration	2.79s
Return Code	128
PID	2076
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #56: taskkill.exe

ID	56
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im infopath.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 173127, Reason: Child Process
Unmonitor End Time	End Time: 175532, Reason: Terminated
Monitor duration	2.40s
Return Code	128
PID	2736
Parent PID	2076
Bitness	32 Bit

Process #57: cmd.exe

ID	57
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im msaccess.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 174960, Reason: Child Process
Unmonitor End Time	End Time: 176796, Reason: Terminated
Monitor duration	1.84s
Return Code	128
PID	3156
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #58: taskkill.exe

ID	58
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im msaccess.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 175198, Reason: Child Process
Unmonitor End Time	End Time: 177108, Reason: Terminated
Monitor duration	1.91s
Return Code	128
PID	2696
Parent PID	3156
Bitness	32 Bit

Process #59: cmd.exe

ID	59
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im mspub.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 176563, Reason: Child Process
Unmonitor End Time	End Time: 179027, Reason: Terminated
Monitor duration	2.46s
Return Code	128
PID	2348
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #60: taskkill.exe

ID	60
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im mspub.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 176799, Reason: Child Process
Unmonitor End Time	End Time: 178675, Reason: Terminated
Monitor duration	1.88s
Return Code	128
PID	4180
Parent PID	2348
Bitness	32 Bit

Process #61: cmd.exe

ID	61
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im onenote.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 178048, Reason: Child Process
Unmonitor End Time	End Time: 180257, Reason: Terminated
Monitor duration	2.21s
Return Code	128
PID	4124
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #62: taskkill.exe

ID	62
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im onenote.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 178268, Reason: Child Process
Unmonitor End Time	End Time: 179816, Reason: Terminated
Monitor duration	1.55s
Return Code	128
PID	3600
Parent PID	4124
Bitness	32 Bit

Process #63: cmd.exe

ID	63
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im outlook.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 179275, Reason: Child Process
Unmonitor End Time	End Time: 181527, Reason: Terminated
Monitor duration	2.25s
Return Code	0
PID	4384
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #64: taskkill.exe

ID	64
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im outlook.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 179468, Reason: Child Process
Unmonitor End Time	End Time: 180891, Reason: Terminated
Monitor duration	1.42s
Return Code	0
PID	4376
Parent PID	4384
Bitness	32 Bit

Process #65: cmd.exe

ID	65
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im powerpnt.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 180627, Reason: Child Process
Unmonitor End Time	End Time: 182302, Reason: Terminated
Monitor duration	1.68s
Return Code	128
PID	4356
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #66: taskkill.exe

ID	66
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im powerpnt.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 180894, Reason: Child Process
Unmonitor End Time	End Time: 182714, Reason: Terminated
Monitor duration	1.82s
Return Code	128
PID	4408
Parent PID	4356
Bitness	32 Bit

Process #67: cmd.exe

ID	67
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im steam.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 182031, Reason: Child Process
Unmonitor End Time	End Time: 184414, Reason: Terminated
Monitor duration	2.38s
Return Code	128
PID	4536
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #68: taskkill.exe

ID	68
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im steam.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 182303, Reason: Child Process
Unmonitor End Time	End Time: 183414, Reason: Terminated
Monitor duration	1.11s
Return Code	128
PID	4512
Parent PID	4536
Bitness	32 Bit

Process #69: cmd.exe

ID	69
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im sqlservr.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183497, Reason: Child Process
Unmonitor End Time	End Time: 185092, Reason: Terminated
Monitor duration	1.59s
Return Code	128
PID	3168
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #70: taskkill.exe

ID	70
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im sqlservr.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183749, Reason: Child Process
Unmonitor End Time	End Time: 184959, Reason: Terminated
Monitor duration	1.21s
Return Code	128
PID	460
Parent PID	3168
Bitness	32 Bit

Process #71: cmd.exe

ID	71
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im thebat.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 184778, Reason: Child Process
Unmonitor End Time	End Time: 187089, Reason: Terminated
Monitor duration	2.31s
Return Code	128
PID	1376
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #72: taskkill.exe

ID	72
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im thebat.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 185093, Reason: Child Process
Unmonitor End Time	End Time: 187037, Reason: Terminated
Monitor duration	1.94s
Return Code	128
PID	3856
Parent PID	1376
Bitness	32 Bit

Process #73: cmd.exe

ID	73
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im thebat64.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186131, Reason: Child Process
Unmonitor End Time	End Time: 188050, Reason: Terminated
Monitor duration	1.92s
Return Code	128
PID	3852
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #74: taskkill.exe

ID	74
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im thebat64.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186348, Reason: Child Process
Unmonitor End Time	End Time: 188053, Reason: Terminated
Monitor duration	1.71s
Return Code	128
PID	3756
Parent PID	3852
Bitness	32 Bit

Process #75: cmd.exe

ID	75
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im thunderbird.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 187808, Reason: Child Process
Unmonitor End Time	End Time: 189578, Reason: Terminated
Monitor duration	1.77s
Return Code	0
PID	2152
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #76: taskkill.exe

ID	76
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im thunderbird.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 188052, Reason: Child Process
Unmonitor End Time	End Time: 189855, Reason: Terminated
Monitor duration	1.80s
Return Code	0
PID	3864
Parent PID	2152
Bitness	32 Bit

Process #77: cmd.exe

ID	77
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im visio.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 189291, Reason: Child Process
Unmonitor End Time	End Time: 191487, Reason: Terminated
Monitor duration	2.20s
Return Code	128
PID	3116
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #78: taskkill.exe

ID	78
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im visio.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 189586, Reason: Child Process
Unmonitor End Time	End Time: 191069, Reason: Terminated
Monitor duration	1.48s
Return Code	128
PID	556
Parent PID	3116
Bitness	32 Bit

Process #79: cmd.exe

ID	79
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im winword.exe "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 190530, Reason: Child Process
Unmonitor End Time	End Time: 192439, Reason: Terminated
Monitor duration	1.91s
Return Code	128
PID	1300
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #80: taskkill.exe

ID	80
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im winword.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 190765, Reason: Child Process
Unmonitor End Time	End Time: 191990, Reason: Terminated
Monitor duration	1.23s
Return Code	128
PID	1872
Parent PID	1300
Bitness	32 Bit

Process #81: cmd.exe

ID	81
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "taskkill /f /im wordpad.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 191781, Reason: Child Process
Unmonitor End Time	End Time: 194344, Reason: Terminated
Monitor duration	2.56s
Return Code	128
PID	3664
Parent PID	1556
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	16
Environment	20
System	1
Process	1

Process #82: taskkill.exe

ID	82
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /f /im wordpad.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 192001, Reason: Child Process
Unmonitor End Time	End Time: 194291, Reason: Terminated
Monitor duration	2.29s
Return Code	128
PID	2296
Parent PID	3664
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965	C:\Users\RDhJ0CNFevzX\Desktop\b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe	Sample File	3196.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
f4dc1835c4945dd1a3b1d990ded128984218c279a67219110d60f77121727c00	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\README.html, C:\Users\RDhJ0CNFevzX\README.html, C:\Users\Default\README.html, C:\Use... ...ME.html, C:\Users\RDhJ0CNFevzX\Downloads\README.html, C:\Users\RDhJ0CNFevzX\Music\README.html, C:\Users\Default\Videos\README.html	Dropped File	3.13 KB	text/html	Access, Write, Create	SUSPICIOUS
f17946a4b13a3880ab0380888d05c17ee0c6adfc5879e5016774d80e155709c1	C:\Users\RDhJ0CNFevzX\windows	Dropped File	1.67 KB	text/plain	Access, Write, Create	CLEAN
56c956eadd553541e64b28a0ff8014b1717c60bf1ccc528d48c714f850e818e0	C:\Users\RDhJ0CNFevzX\Desktop\1svsBULw6E2suU5FLV.gif	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
46c89b4be487ac2d3bf6e18da7eaf442c3db13b50b18b292d721f7f3badc5fa6	C:\Users\RDhJ0CNFevzX\Desktop\1svsBULw6E2suU5FLV.gif.locked	Dropped File	3.14 KB	application/octet-stream	Access, Write, Create	CLEAN
d2a2357e75768a4dcc255f9f25e6c613f2b1b7ddc73bc30172bad6948e998ed7	C:\Users\RDhJ0CNFevzX\Desktop\6ag5kfsiaVq.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
ee207e016b7634c79fbdb6a3472d827aecb842bb51b445cf6f8f60c4f302a7b5	C:\Users\RDhJ0CNFevzX\Desktop\6ag5kfsiaVq.mp4.locked	Dropped File	9.53 KB	application/octet-stream	Access, Write, Create	CLEAN
b06004f30d1e202f660abe6e594687f21aec1c80c626a09bf34f782523ea35f6	C:\Users\RDhJ0CNFevzX\Desktop\9dmrU1YjBAS.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
aa4ecaf31d7e8301c3778e97d78b5f141cff2d4af3cb18e6704754e18da104de	C:\Users\RDhJ0CNFevzX\Desktop\9dmrU1YjBAS.xlsx.locked	Dropped File	72.26 KB	application/octet-stream	Access, Write, Create	CLEAN
a9d2b2e983afe860bc4e5cfeb24f99a6f0e402fa31afae49884cf4a3ddf55f85	C:\Users\RDhJ0CNFevzX\Desktop\A7lggNk.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
e0acb1199d8a6510da90a8ca084145d5579a434f1c76d7ec17566e11f180c665	C:\Users\RDhJ0CNFevzX\Desktop\A7lggNk.mkv.locked	Dropped File	22.95 KB	application/octet-stream	Access, Write, Create	CLEAN
e44b49b444030e3ce8363c5a423662779fe1b8ee8db70e8ff5a102b465958052	C:\Users\RDhJ0CNFevzX\Desktop\C0syXD_bv.odt	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
a94129ce33a3346692f7c6b4f6568cad3a342402160f042d2801557d24174d58	C:\Users\RDhJ0CNFevzX\Desktop\C0syXD_bv.odt.locked	Dropped File	63.93 KB	application/octet-stream	Access, Write, Create	CLEAN
510d9e524395f851fcd15c5bba0903697e82ca57c89bff9cfbc859bbb56324f5	C:\Users\RDhJ0CNFevzX\Desktop\DiFuL.swf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
06639bec533d6c37714a2bafe6db0304f2e58ee8a6f40e7370e97f0662ed5ffa	C:\Users\RDhJ0CNFevzX\Desktop\DiFuL.swf.locked	Dropped File	94.81 KB	application/octet-stream	Access, Write, Create	CLEAN
3e3d3d5f575681b7bb94187fd68d1a87a5f159c74b7b9de09f73181da60b3a7e	C:\Users\RDhJ0CNFevzX\Desktop\Dyb9xZeWpRv.swf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
dbf50a3fd46136fa860e0d8722cbfad5a4e72f78bb0d87e29f0b9fc99bc1a7cf	C:\Users\RDhJ0CNFevzX\Desktop\Dyb9xZeWpRv.swf.locked	Dropped File	15.80 KB	application/octet-stream	Access, Write, Create	CLEAN
7a2208c31f931382e0f1b5ce320d8e63f2962452c69cf42e3d6f967431bb3575	C:\Users\RDhJ0CNFevzX\Desktop\L1OM5.png	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
86f5e85ededd0c0f357cad2cc95aca2e6f401e3df6ceb35c7f1c45e19950cbbd	C:\Users\RDhJ0CNFevzX\Desktop\L1OM5.png.locked	Dropped File	22.28 KB	application/octet-stream	Access, Write, Create	CLEAN
52420db4ef48203a00eac41c6943085e5bea1d66cd69f5dbb7addea14fd5d18e	C:\Users\RDhJ0CNFevzX\Desktop\LcNUIHK9lEvgMQ7.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
a71b6be246997c7bea957839eb1ea553ed0aaa109a5aba89e99884de1463b85c	C:\Users\RDhJ0CNFevzX\Desktop\LcNUIHK9lEvgMQ7.jpg.locked	Dropped File	14.42 KB	application/octet-stream	Access, Write, Create	CLEAN
e2514b14d479909bd67bc999c087670059a57032ae854d2a670a46163539d071	C:\Users\RDhJ0CNFevzX\Desktop\Lvtr1Ydb7MIz.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
46afb2a9171bb6c606f33d51d1d3273046d0e9242e85d44acb1e4e1a64a7ee62	C:\Users\RDhJ0CNFevzX\Desktop\Lvtr1Ydb7MIz.mkv.locked	Dropped File	24.14 KB	application/octet-stream	Access, Write, Create	CLEAN
3b73846292ca5cb5f8cf76afd888165c9a118f5c37d2d3825b76d0c51c9c9791	C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\0RzD7W9keho8x2.gif	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
8d2b115d97bec1cafcd3f526eb3913f1f97757033db99e06abf5d4165a5f82cb	C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\0RzD7W9keho8x2.gif.locked	Dropped File	48.37 KB	application/octet-stream	Access, Write, Create	CLEAN
dd470399e663d825f486ec8eb377ebba60add29b533bfd7748b93851ed5b90d7	C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\UQjVL.png	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
8dd90f0ceedd1ae25106e9968df0f9a9d6f4c10305f84ee084c57ae62900ab04	C:\Users\RDhJ0CNFevzX\Desktop\MJtStno\UQjVL.png.locked	Dropped File	42.42 KB	application/octet-stream	Access, Write, Create	CLEAN
a50a9834abc2bee1dbb6db615052c9d4fdfd0232b9dd29386731f441cd888e0a	C:\Users\RDhJ0CNFevzX\Desktop\QixwzNIhzqpngSpTJiG.avi	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
dbb045a2e4b33d514c2a38754b5c4b08a8d78697555f8e4078e84e7d8c578b92	C:\Users\RDhJ0CNFevzX\Desktop\QixwzNIhzqpngSpTJiG.avi.locked	Dropped File	57.63 KB	application/octet-stream	Access, Write, Create	CLEAN
b900b2c5b44764fdf3a9c54c3e4e1c214508c5a4d248a73ca3412347b1f6f05c	C:\Users\RDhJ0CNFevzX\Desktop\R3MdJzJmTt.ods	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
267841eaac9aea99758d3a8067c8cb579665f6f07f04ab07a6273f24aed97cdc	C:\Users\RDhJ0CNFevzX\Desktop\R3MdJzJmTt.ods.locked	Dropped File	93.49 KB	application/octet-stream	Access, Write, Create	CLEAN
0b6a70e93ea97fba2b3c0d01902133cd22e6a44851c426a008fadd2422456ebd	C:\Users\RDhJ0CNFevzX\Desktop\S-eoW0hMerDLmPid.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
2ee99dffdf472a2450dd370794c506404b18580ad97beed53c21887cbf448f69	C:\Users\RDhJ0CNFevzX\Desktop\S-eoW0hMerDLmPid.mp4.locked	Dropped File	17.25 KB	application/octet-stream	Access, Write, Create	CLEAN
62827cb044d0b66e2e7d6f4ee7e8e718268e48fd8cede1fae47c06751c070757	C:\Users\RDhJ0CNFevzX\Desktop\SFjU-GGjjEg.wav	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
15d927151aae287a94e8a5ae7352d97ddbdde7c4b87ea5a81aa0fd016db74781	C:\Users\RDhJ0CNFevzX\Desktop\SFjU-GGjjEg.wav.locked	Dropped File	66.74 KB	application/octet-stream	Access, Write, Create	CLEAN
afc263cbcd82e7359589c54466f1bbce56bad04462e1ffee5d00de035e24791b	C:\Users\RDhJ0CNFevzX\Desktop\SJsz9b80pOXI.wav	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
59c8c9e2f4c8c909f43ece3618fdd60fe85b40905851392093e3a272aa801a1a	C:\Users\RDhJ0CNFevzX\Desktop\SJsz9b80pOXI.wav.locked	Dropped File	82.29 KB	application/octet-stream	Access, Write, Create	CLEAN
028b2a1f8f6512da8ac142c9a1449a92d8601390c2f2026556adc378959e50b5	C:\Users\RDhJ0CNFevzX\Desktop\Sp32K2MJT8oGwSN.gif	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
f742dcc0ba7f4988f315de3a7619fe7b2381ea07e05e681838ef92866ab322fe	C:\Users\RDhJ0CNFevzX\Desktop\Sp32K2MJT8oGwSN.gif.locked	Dropped File	58.36 KB	application/octet-stream	Access, Write, Create	CLEAN
cae22c82669b96970efb8fd945d2844730f08943b23248cbceb07d4f9b73847b	C:\Users\RDhJ0CNFevzX\Desktop\WYG6ic.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f060645abcf83af491125e739e4a2f2cf366a58758a53f1e677034cdad066e02	C:\Users\RDhJ0CNFevzX\Desktop\WYG6ic.jpg.locked	Dropped File	13.81 KB	application/octet-stream	Access, Write, Create	CLEAN
04de5f09381081b6b47a9ff6c44527f372569edaeae21f42fb9ef22130b2e9ec	C:\Users\RDhJ0CNFevzX\Desktop\YUi--Xwk3SNHRau.bmp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
7e821cf2a4abb0f7da10f5b7de46bce13ae90c370f160eb339e4231c20c3c340	C:\Users\RDhJ0CNFevzX\Desktop\YUi--Xwk3SNHRau.bmp.locked	Dropped File	85.70 KB	application/octet-stream	Access, Write, Create	CLEAN
b5d738b4493475a857a64ceab256ba3e5830f5e642d4fc113085626c1a19f343	C:\Users\RDhJ0CNFevzX\Desktop\ZKt7SKs8.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
b10533907df5ab74a3d40b1870d0f85a23ba11d18e21039da72878ab7be40909	C:\Users\RDhJ0CNFevzX\Desktop\ZKt7SKs8.mp4.locked	Dropped File	10.31 KB	application/octet-stream	Access, Write, Create	CLEAN
465fda221fca6e17fd78af63687d2b2bc23e1fc0e23154e4b38305c95ae7e1e1	C:\Users\RDhJ0CNFevzX\Desktop\aOaBV.bmp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
cc9a2823bcd64c901f17ca211e56565d1e82e7c40f25707b7a50edc2a1550c98	C:\Users\RDhJ0CNFevzX\Desktop\aOaBV.bmp.locked	Dropped File	16.41 KB	application/octet-stream	Access, Write, Create	CLEAN
a49dc0f910f841ee85d698edac02198ac5decfc2d769fa09e8d3bd446f5bc307	C:\Users\RDhJ0CNFevzX\Desktop\bYMSr1.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
5bb2de92da9cbd4397151a95b6ab2cc144b696cdb57c37c21ab0f32b6539676e	C:\Users\RDhJ0CNFevzX\Desktop\bYMSr1.mkv.locked	Dropped File	24.80 KB	application/octet-stream	Access, Write, Create	CLEAN
43f182df9ecf7825a6bccc09588a83e99d20ac78e3f85ffcdcdc5806a72f3554	C:\Users\RDhJ0CNFevzX\Desktop\cDIqglnt.pps	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
d53e4d280f815de87c7132a3d8278c61a9822cc21ed5362871b01e6104d216d8	C:\Users\RDhJ0CNFevzX\Desktop\cDIqglnt.pps.locked	Dropped File	37.33 KB	application/x-dosexec	Access, Write, Create	CLEAN
982c580a49fa03a6bf058ef0e3b79d081fddbc955ba7beb5a35f7f9be4b21db9	C:\Users\RDhJ0CNFevzX\Desktop\joFK1K4FpCy.odt	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
d60162c1f31f979c18686bc6406bf099c22025160a63fd4d3647c57f43717dc9	C:\Users\RDhJ0CNFevzX\Desktop\joFK1K4FpCy.odt.locked	Dropped File	27.26 KB	application/octet-stream	Access, Write, Create	CLEAN
76b71ef39217c8995eb651fa6cbd303bf05b4bbdb5abb56e8203551fe5f69117	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\27JfCEVulMHbbO.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
e0b55af099041861a20e4c70778df0e817f9f362879521330 8c5f6f1468bec53	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\27JfCEVulMHbbO.mp3.locked	Dropped File	16.62 KB	application/octet-stream	Access, Write, Create	CLEAN
d2bf2a730dd8478649f55a39229e394a4f8cdfa336cd77e4adc19b0d625de800	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\9Vntf.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
1435cd76bac95d35a9f0e8aad7011f51f4b2c6e64473b64f9592930fafe33611	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\9Vntf.mkv.locked	Dropped File	53.05 KB	application/octet-stream	Access, Write, Create	CLEAN
78f673b8564763f614b2ecdccf2d65d8d01f1e8d9b8e3e5711b6482c5b0614a9	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\kfCcoa0Kn4e.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
31cfa5bf2a594423f3c0f4d955349824a04cb60ef577c6479cb92d9a8e10c2cd	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\kfCcoa0Kn4e.mp3.locked	Dropped File	47.60 KB	application/octet-stream	Access, Write, Create	CLEAN
19271e7ef63c5163e92c0ef85f58c12ada8561b7732769f242bed082eeafdddd	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\lkG90.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
2fc7888b36c372d90b70da48ce2ccd5c24640b7ea190691c02789629b52863df	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\lkG90.jpg.locked	Dropped File	8.40 KB	application/octet-stream	Access, Write, Create	CLEAN
d6603040b9e7f4f181826890b901b1082669239a09ff85fc780c4d4b4befc843	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\w8O0bav5Ww_S.pdf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b2be9af5b09740471120e08be793ddc8eb9bf56b505f802f174309af509fb77c	C:\Users\RDhJ0CNFevzX\Desktop\jqRKACI6\w8O0bav5Ww_S.pdf.locked	Dropped File	95.34 KB	application/octet-stream	Access, Write, Create	CLEAN
b7b67aabbfb47069e1840d2b274aee7593939a901934610e9fee7575bf9b0459	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\D-Cg-mvfsgn.flv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
5d81d02d86323e15210db22af3d351015c8e2d83edcba9441baadf53b9d07aa3	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\D-Cg-mvfsgn.flv.locked	Dropped File	4.89 KB	application/octet-stream	Access, Write, Create	CLEAN
29b4805b8be70bff0b471adc691a3c21ea1f49cd5d76362c40d8d4080ed9515f	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\KBe56raX.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
247d7337165b2a27a5c1c568c8b09f5be1dbae1364d48bc7ddcdc22631da9676	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\KBe56raX.jpg.locked	Dropped File	14.57 KB	application/octet-stream	Access, Write, Create	CLEAN
5677e2cb5d666bfa137af30e7346b80c4b8969e9f4094240f935c0a2c5225704	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\UyGAh1goU67sQ4n_bFy.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
fada929b7f22f74292efe12b33fcb74de92031ab1270aa28ca9d06d40ed741fd	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\UyGAh1goU67sQ4n_bFy.mp3.locked	Dropped File	18.08 KB	application/octet-stream	Access, Write, Create	CLEAN
a09c6d65c28f1a3302a9dd7f8a5f59be3d91a1af4f332431275439461fcd035a	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\pmRHoZn51.avi	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
bd3c4aa89e01b886f5faee099ad8aa0ba515dd5e4782bbb1ab33835feb62cfa1	C:\Users\RDhJ0CNFevzX\Desktop\l2CI\pmRHoZn51.avi.locked	Dropped File	82.28 KB	application/octet-stream	Access, Write, Create	CLEAN
73e798c0ea206fe9e841a0e5105bae7caf25a1e21adc0387fb9bcbddc59dd4bd	C:\Users\RDhJ0CNFevzX\Desktop\pgIQZ6vV6.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
f376ae9e7de1343e9a91ef1112b2f51f9adb246d4dae53e307065d7c04fb1304	C:\Users\RDhJ0CNFevzX\Desktop\pgIQZ6vV6.mkv.locked	Dropped File	65.81 KB	application/octet-stream	Access, Write, Create	CLEAN
ece913d714c2b991a89975162850de8a1af1efd06bc3692af0f5a20372f4d41d	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\4m1VwisQwNYyO.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
b85f34a1791299ace654022b289c159d6645dbce4010ef39dc009d3d76f6463f	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\4m1VwisQwNYyO.mp3.locked	Dropped File	95.92 KB	application/octet-stream	Access, Write, Create	CLEAN
bdaafdeaee19cb204b67b0e26cb72a4995ed461e0669424c3ef5f086192560de	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drlHYf6Q54DMKd0A\3_vtHE.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
f3f53a25134df8e3cc5dcee88b7da6200b2cc303c39554ef3f1d0b0a38915026	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drlHYf6Q54DMKd0A\3_vtHE.pptx.locked	Dropped File	68.36 KB	application/octet-stream	Access, Write, Create	CLEAN
797d35946436b04c072eeb7a27994ae601afaddd11692bdb30f8e2a2972df8ac	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drlHYf6Q54DMKd0A\664ei1-x8f0_Yk6d9oEE.png	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
4ff9a5b1bf27f87e63e12f6f7a0ebeda24e6e70d386e67b59e474b38b7032364	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drlHYf6Q54DMKd0A\664ei1-x8f0_Yk6d9oEE.png.locked	Dropped File	11.64 KB	application/octet-stream	Access, Write, Create	CLEAN
d29dbd8bd703a6ad3fa28c3e1267b74d2c03a416434769dd35a1293c93c2bcc4	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drlHYf6Q54DMKd0A\zeUh4blJhKCdE8.swf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
4b5d7e57499730e02e4dde9af5b9a9bb54a07ed83be6c68a8fdff1e7f513e71b	C:\Users\RDhJ0CNFevzX\Desktop\uFbh\q0drlHYf6Q54DMKd0A\zeUh4blJhKCdE8.swf.locked	Dropped File	78.86 KB	application/octet-stream	Access, Write, Create	CLEAN
a3dcc595dafb405dc807798bc1bbfb2b563724b751509ec86567c107c9f0eada	C:\Users\RDhJ0CNFevzX\Documents\2kmOhs9S25.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
b24f5a9dd65ebe862239800b5f387df564d423a7ea2b0a73a39842c3f6b98ec6	C:\Users\RDhJ0CNFevzX\Documents\2kmOhs9S25.xlsx.locked	Dropped File	47.22 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4880804cdb76879c7be131ba6fe69756977ab7661b7c77a7f6ff9d4d0b1b1a8c	C:\Users\RDhJ0CNFevzX\Documents\5pf90.rtf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
849abb3aa62738cdb26883a6b5f1f0e4bc3b32961aec9d0dab68f60da51c59c4	C:\Users\RDhJ0CNFevzX\Documents\5pf90.rtf.locked	Dropped File	47.76 KB	application/octet-stream	Access, Write, Create	CLEAN
3ad7fe5f7689c4ec5ef202aa26940ce05f99f19b00f9bcf05f20f05e0c388ae2	C:\Users\RDhJ0CNFevzX\Documents\6gmL5X_4sIK-0_B6U.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
3e9d4e0016cac6ca52563e303851f873a3f937366fd5db728f348ca7bd0a20ab	C:\Users\RDhJ0CNFevzX\Documents\6gmL5X_4sIK-0_B6U.xlsx.locked	Dropped File	9.10 KB	application/octet-stream	Access, Write, Create	CLEAN
5a376e46b2d3e3b77ecffdff0e7d5297f3806d6e095e54b0ef77f1388d8698d3	C:\Users\RDhJ0CNFevzX\Documents\7GBj_BHQB3gjCk60.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
6ed16a005ee52e80a37efaf7cee90062d2bd74fe342760dbe3f41aa487d43f78	C:\Users\RDhJ0CNFevzX\Documents\7GBj_BHQB3gjCk60.docx.locked	Dropped File	34.16 KB	application/octet-stream	Access, Write, Create	CLEAN
1bb4151798964ae3ff3a5b6a6f610b6d7d215a76ad5b73fac23e3a5da0ba5b12	C:\Users\RDhJ0CNFevzX\Documents\8Y_umCxII.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
5ff5c5641c6326d8edb27023683ed4164a6bdf7a93ea60002eb1cb63809e6d98	C:\Users\RDhJ0CNFevzX\Documents\8Y_umCxII.xlsx.locked	Dropped File	28.94 KB	application/octet-stream	Access, Write, Create	CLEAN
2735dd0f63b377a05100da8a15c92cfa6ccddda9875b4ba939960bed025b4160	C:\Users\RDhJ0CNFevzX\Documents\GAL0vICrqtbz5.ots	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
534257e4fbb8f9f6efd600a79131052255a22bef4872d22101488dc005c567ce	C:\Users\RDhJ0CNFevzX\Documents\GAL0vICrqtbz5.ots.locked	Dropped File	30.66 KB	application/octet-stream	Access, Write, Create	CLEAN
b6bd6ce1de92f12456f0e7d82a30594a0e72e5fc960086fd92032bda815c819f	C:\Users\RDhJ0CNFevzX\Documents\Nv-fQq_ b.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
88d7cc8586c30b451c0525072c35ec7b0ede3f24cb4f1bf64ddb242cc6902ae0	C:\Users\RDhJ0CNFevzX\Documents\Nv-fQq_ b.pptx.locked	Dropped File	7.08 KB	application/octet-stream	Access, Write, Create	CLEAN
47dbe12984799f370541228799a9f975f1a696487030a74e149966825a6ee2ef	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
8308f09745acd3f8933592e4d2b6675cd3c18feeb7922e063f0b5bbb0507bff6	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.locked	Dropped File	265.12 KB	application/octet-stream	Access, Write, Create	CLEAN
eb9429e6db28689a46665dbd9d69d2a36915463e9abd1665bee52e0e8b242262	C:\Users\RDhJ0CNFevzX\Documents\SfN_7SLvBv6HWGGZ.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
1f979f7805b29aff4f275089ad3eccc14a140e4fb7e5a13860a61f1f2df9dfab	C:\Users\RDhJ0CNFevzX\Documents\SfN_7SLvBv6HWGGZ.docx.locked	Dropped File	38.48 KB	application/octet-stream	Access, Write, Create	CLEAN
2ea233be47c3b6986054a87ba6a28831390013cda71592268b94da583c661979	C:\Users\RDhJ0CNFevzX\Documents\TaxhME.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
87feade60556f8542817febcf84ed6e514e59d8bb98e6f689b557c67673a9347	C:\Users\RDhJ0CNFevzX\Documents\TaxhME.pptx.locked	Dropped File	12.01 KB	application/octet-stream	Access, Write, Create	CLEAN
82aa1bfe55d7d1020288ff1ca22c9efbacf6c7d3e82262fdb5d3cf2b5cb4de0a	C:\Users\RDhJ0CNFevzX\Documents\XlenjhZeamfDvL.odt	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
5024b442f395b3a7e89d7ec9ba8489fb9c32f6a5238214becc661d4eccc35a2b	C:\Users\RDhJ0CNFevzX\Documents\XlenjhZeamfDvL.odt.locked	Dropped File	15.57 KB	application/octet-stream	Access, Write, Create	CLEAN
2d0eac453dd131013110f1d992e6ba5d88c9a09ce6f7c74031cfdd3c5d595658	C:\Users\RDhJ0CNFevzX\Documents\YKkR7 10Jqcina5HGOD.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
9ffa51149977e9e9d42043ae2e3b7f4242005eb42c7f355c1f189a6beadb549c	C:\Users\RDhJ0CNFevzX\Documents\YKkR7 10Jqcina5HGOD.pptx.locked	Dropped File	93.35 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2d4612a496f218629dd27a97f8c01313bbd17eeb996f3c0dd266d00552702b9b	C:\Users\RDhJ0CNFevzX\Documents\Zx_PeYMMp5W-Vj0.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
fb6094bb0161408125411f5b113f475190cb8482d2b78832837ec2a486946a7e	C:\Users\RDhJ0CNFevzX\Documents\Zx_PeYMMp5W-Vj0.xlsx.locked	Dropped File	76.77 KB	application/octet-stream	Access, Write, Create	CLEAN
20fb11714d984a7a76c1bcf2ff271d2337d2648937ba590826162f7bef997da3	C:\Users\RDhJ0CNFevzX\Documents\eBPMR.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
f0ebc663a443ca21e7f83e2010b20f845688aa453db0875111942cce16f35318	C:\Users\RDhJ0CNFevzX\Documents\eBPMR.pptx.locked	Dropped File	35.70 KB	application/octet-stream	Access, Write, Create	CLEAN
99592d59d4cb2717c295becc70277a66a5bc95f0fd1e0a321a33ea84e2919f6d	C:\Users\RDhJ0CNFevzX\Documents\eau-Oo1pPUvz4w8PX.ppt	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
a0d78e1c293d592fcd5ad4b9e063cbdec23ff321e27071d2c63c874dcd1a8cb6	C:\Users\RDhJ0CNFevzX\Documents\eau-Oo1pPUvz4w8PX.ppt.locked	Dropped File	45.76 KB	application/octet-stream	Access, Write, Create	CLEAN
4ee26b626744940ed70bf735521cf2ef7faa107ff738c50ce4d73f82ae486469	C:\Users\RDhJ0CNFevzX\Documents\gRpk8Z1c.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
79c8d752d8b033d0347330a0874c82ecb0a8b75f852404ef3f42b195aa4733bb	C:\Users\RDhJ0CNFevzX\Documents\gRpk8Z1c.docx.locked	Dropped File	76.90 KB	application/octet-stream	Access, Write, Create	CLEAN
8918f31f3b0ffb1b052bde1b73e77903e64bff55fc7078e39b72af0acd63c8cd	C:\Users\RDhJ0CNFevzX\Documents\jaCxkmZM5HvA.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
0b7bace5157a8a2dce4b3de0e08c2e705e8859eba96bd2fca1ffd695d76c4295	C:\Users\RDhJ0CNFevzX\Documents\jaCxkmZM5HvA.docx.locked	Dropped File	75.31 KB	application/octet-stream	Access, Write, Create	CLEAN
c25cbeedff6478885c9643c862fc8a0719fe7d8c02abcec0051a8c0a26be7405	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\6ah1b.odp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
9d261d21fa605d42e626a9e47d93ed3afe5764d726bb6bb4513b8a8ad6b31f33	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\6ah1b.odp.locked	Dropped File	89.17 KB	application/octet-stream	Access, Write, Create	CLEAN
7840e46c2638e72710e3964e3413b63e7215fd9de854fe4558d793684d0395f8	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\uMIP.pps	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
9439ea10d700ce1df3bd9659c1be74faba963b48bdb1e801283170df291e0dd7	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\uMIP.pps.locked	Dropped File	86.34 KB	application/octet-stream	Access, Write, Create	CLEAN
f425751cdb3f2df2b98df4a3c3ec7736a12534cf2329d746a95f8ad1fd316f12	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\3Zq4EcajsIY7PFQKVsvW.pdf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
9735d3500549a4959b0d83d10d71e4e0a4c64ff7fd61c251b45e6174cf45d689	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\3Zq4EcajsIY7PFQKVsvW.pdf.locked	Dropped File	26.55 KB	application/octet-stream	Access, Write, Create	CLEAN
6a8c3457b179fe43d2a90e6ccb95d09f3386c3a2d4e4a03dc8576b5f17894ff1	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\9RRM_.csv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
cf1c225e48bb705080c2c8e28c998fd6e9f73bf346ce31bc30126bb59f421824	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\9RRM_.csv.locked	Dropped File	12.82 KB	application/octet-stream	Access, Write, Create	CLEAN
4e86d73318b19034615d4be799a0ee95c162b8ec3264f5c3321e30422cd8b85f	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\H9ZYmL.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
eeee5b74068de51b045e97b25c9bb117a769ed8c693b5a4fb13494161ec0fa99	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\H9ZYmL.pptx.locked	Dropped File	97.12 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a388ea78fa468bc98e4f964078f520c4f0aeb1672dc67ac9a5838b4086d4f72f	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\-iqW_.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
9bc7e4d177c69e6a0a480ac68696b55f16c7b4af4dc8ed88e38c2d66006a9a6b	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\-iqW_.pptx.locked	Dropped File	55.33 KB	application/octet-stream	Access, Write, Create	CLEAN
e530aed9411237e1821616c47917228748ac5f9f8ad44d8bce76ad7678110f5d	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\Q8qlBA 30gG.ods	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
52644d8bc87964ba8d8e72166f6093369a45a3e8872f7361f397f082f4a91ca2	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\Q8qlBA 30gG.ods.locked	Dropped File	42.00 KB	application/octet-stream	Access, Write, Create	CLEAN
957cbcbd059f6c760407d7e4807c4ee2e8a1c2859ca1b1222facd7747acd3446	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\VNJUeKMIKE5Ysn n.rtf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
befb361243ef7090fc7c5d46c80ac13ce59fa53b9bb38c3d543c03320a694df2	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\VNJUeKMIKE5Ysn n.rtf.locked	Dropped File	54.14 KB	application/octet-stream	Access, Write, Create	CLEAN
315b901ec3e5b8df0bbae4f9b7a53e5809f1efdc8d7c319e9d4370aab475f1af	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\xgy7j.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
4561956a65afec745c32adabd2c0dcda586184497a64d8ebfbf22ef82b1e9fa5	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\xgy7j.pptx.locked	Dropped File	33.77 KB	application/octet-stream	Access, Write, Create	CLEAN
29fe4695ed925cd18b9819c7525d00e7e3e4d2235da016ea2e359038ab58d273	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\zIPqwuKy.rtf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
c613ade9d3bcf87a0e86dca7ade78827091c9072db6f1484055ca41f821afe1d	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\5A5KELPEB3fxvrO\zIPqwuKy.rtf.locked	Dropped File	72.29 KB	application/octet-stream	Access, Write, Create	CLEAN
50b7de5ce870c22203c9ce0ae3066cb8ab6d938f913cdfe77c28e7f96dcb0572	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\LtbtPfDoTJ77Qjxw.odt	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
15e2e76b4bb35c643dbd9598c2b4a9527fda055f0653cf794435571ee15e28d1	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\LtbtPfDoTJ77Qjxw.odt.locked	Dropped File	65.91 KB	application/octet-stream	Access, Write, Create	CLEAN
f22fc6f6ea74e52bf7e0fa6e9197f1c60507520c1182d20254c25c468f64677e	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\Mh6oNy9bLKM5.pps	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
167f60a902860fcecc06e5a5b35023c3e0f966cf185db220746f385858b3a96e	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\Mh6oNy9bLKM5.pps.locked	Dropped File	22.21 KB	application/octet-stream	Access, Write, Create	CLEAN
be02d24e78664b4f8784421f09d4847b9864c73ad2f480d376674c46c630625d	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\IQnC\ZjvJmA1w8wm09o.odt	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6dc888e59cf9ee4a2c4758394e0717437c1243f149334700d84f399f42eb1a61	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\ZjvJmA1w8wm09o.odt.locked	Dropped File	82.93 KB	application/octet-stream	Access, Write, Create	CLEAN
f9f0ac38a4cd220f20915b7c2c6df1e896bc74792d78c0eb8bfec3061709b68c	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\bPP6k2AtPCvK.odp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
2cef7f23852bfb4210821c4d29414963bc17acef59d326d5e5236b9bb9d69ab2	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\lQnC\bPP6k2AtPCvK.odp.locked	Dropped File	82.49 KB	application/octet-stream	Access, Write, Create	CLEAN
44ad6bba2e1868cf4b1890535c561bb0c6b9a6dd90c4a4c28828a3bf2b170e62	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7SxtG\8BmBuzkrBAz-1J-IShq.pdf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
abdc90fccae93deebd9abdd9231f509db489f2635e0f9866d5e97420d7238a46	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7SxtG\8BmBuzkrBAz-1J-IShq.pdf.locked	Dropped File	10.65 KB	application/octet-stream	Access, Write, Create	CLEAN
8926a7b659945b81d5102841e0cf2e4d3639320508b032578c455d77f2e6bf9e	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7SxtG\R1iyoik0t.ppt	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
44c5d70caa46c9dc22317d0b64e9d10b59b544db654703af3663261159e3c49e	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7SxtG\R1iyoik0t.ppt.locked	Dropped File	14.75 KB	application/octet-stream	Access, Write, Create	CLEAN
f388c1e7d136aceddf5556da363f1c7928e13f1399cf0efd2f6c41f2725cb011	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7SxtG\fAbqQJxC6j.xls	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
8db19dc78c9951b274811d9349ec34ee1996e6046f534ce5b115056215c80927	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7SxtG\fAbqQJxC6j.xls.locked	Dropped File	99.34 KB	application/octet-stream	Access, Write, Create	CLEAN
3a96de32868203997b50abc1e427aa85e0916dd03e6a473c69f3fa09250bff68	C:\Users\RDhJ0CNFevzX\Documents\l0xtaApata393X0pssf\vJv2RbfkMNDaXqowjBc\TVGDzH\LdD7SxtG\qb50fmMABVOmckG.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\README.html	Dropped File	Access, Write, Create	SUSPICIOUS
cmd.exe	Accessed File	Access	CLEAN
cmd.exe.com	Accessed File	Access	CLEAN
cmd.exe.exe	Accessed File	Access	CLEAN
cmd.exe.bat	Accessed File	Access	CLEAN
cmd.exe.cmd	Accessed File	Access	CLEAN
cmd.exe.vbs	Accessed File	Access	CLEAN
cmd.exe.vbe	Accessed File	Access	CLEAN
cmd.exe.js	Accessed File	Access	CLEAN
cmd.exe.jse	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
cmd.exe.wsf	Accessed File	Access	CLEAN
cmd.exe.wsh	Accessed File	Access	CLEAN
cmd.exe.msc	Accessed File	Access	CLEAN
C:\Windows\system32\cmd.exe	Accessed File	Access	CLEAN
NUL	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\windows	Dropped File	Access, Write, Create	CLEAN
A:\	Accessed File	Access	CLEAN
B:\	Accessed File	Access	CLEAN
C:\	Accessed File	Access	CLEAN
C:\$Recycle.Bin	Accessed File	Access	CLEAN
C:\$Recycle.Bin\S-1-5-18	Accessed File	Access	CLEAN
C:\$Recycle.Bin\S-1-5-18\desktop.ini	Accessed File	Access	CLEAN
C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000	Accessed File	Access	CLEAN
C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini	Accessed File	Access	CLEAN
C:\BOOTNXT	Accessed File	Access	CLEAN
C:\BOOTSECT.BAK	Accessed File	Access	CLEAN
C:\Boot	Accessed File	Access	CLEAN
C:\Boot\BCD	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG1	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG2	Accessed File	Access	CLEAN
C:\Boot\BOOTSTAT.DAT	Accessed File	Access	CLEAN
C:\Boot\Fonts	Accessed File	Access	CLEAN
C:\Boot\Fonts\chs_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\cht_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\jpn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\kor_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\malgun_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\malgunn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\meiryo_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\meiryon_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\msjh_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\msjhn_boot.ttf	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\Fonts\msyh_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\msyhn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\segmono_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\segoe_slboot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\segoen_slboot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\wgl4_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Resources	Accessed File	Access	CLEAN
C:\Boot\Resources\bootres.dll	Accessed File	Access	CLEAN
C:\Boot\Resources\en-US	Accessed File	Access	CLEAN
C:\Boot\Resources\en-US\bootres.dll.mui	Accessed File	Access	CLEAN
C:\Boot\bg-BG	Accessed File	Access	CLEAN
C:\Boot\bg-BG\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\bootvhd.dll	Accessed File	Access	CLEAN
C:\Boot\cs-CZ	Accessed File	Access	CLEAN
C:\Boot\cs-CZ\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\cs-CZ\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\da-DK	Accessed File	Access	CLEAN
C:\Boot\da-DK\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\da-DK\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\de-DE	Accessed File	Access	CLEAN
C:\Boot\de-DE\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\de-DE\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\el-GR	Accessed File	Access	CLEAN
C:\Boot\el-GR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\el-GR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\en-GB	Accessed File	Access	CLEAN
C:\Boot\en-GB\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\en-US	Accessed File	Access	CLEAN
C:\Boot\en-US\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\en-US\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\es-ES	Accessed File	Access	CLEAN
C:\Boot\es-ES\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\es-ES\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\es-MX	Accessed File	Access	CLEAN
C:\Boot\es-MX\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\et-EE	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\et-EE\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fi-FI	Accessed File	Access	CLEAN
C:\Boot\fi-FI\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fi-FI\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fr-CA	Accessed File	Access	CLEAN
C:\Boot\fr-CA\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fr-FR	Accessed File	Access	CLEAN
C:\Boot\fr-FR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fr-FR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\hr-HR	Accessed File	Access	CLEAN
C:\Boot\hr-HR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\hu-HU	Accessed File	Access	CLEAN
C:\Boot\hu-HU\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\hu-HU\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\it-IT	Accessed File	Access	CLEAN
C:\Boot\it-IT\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\it-IT\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ja-JP	Accessed File	Access	CLEAN
C:\Boot\ja-JP\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ja-JP\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ko-KR	Accessed File	Access	CLEAN
C:\Boot\ko-KR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ko-KR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\lt-LT	Accessed File	Access	CLEAN
C:\Boot\lt-LT\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\lv-LV	Accessed File	Access	CLEAN
C:\Boot\lv-LV\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\memtest.exe	Accessed File	Access	CLEAN
C:\Boot\nb-NO	Accessed File	Access	CLEAN
C:\Boot\nb-NO\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\nb-NO\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\nl-NL	Accessed File	Access	CLEAN
C:\Boot\nl-NL\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\nl-NL\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pl-PL	Accessed File	Access	CLEAN
C:\Boot\pl-PL\bootmgr.exe.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\pl-PL\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pt-BR	Accessed File	Access	CLEAN
C:\Boot\pt-BR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pt-BR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pt-PT	Accessed File	Access	CLEAN
C:\Boot\pt-PT\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pt-PT\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\qps-ploc	Accessed File	Access	CLEAN
C:\Boot\qps-ploc\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\qps-ploc\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ro-RO	Accessed File	Access	CLEAN
C:\Boot\ro-RO\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ru-RU	Accessed File	Access	CLEAN
C:\Boot\ru-RU\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ru-RU\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sk-SK	Accessed File	Access	CLEAN
C:\Boot\sk-SK\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sl-SI	Accessed File	Access	CLEAN
C:\Boot\sl-SI\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sr-Latn-CS	Accessed File	Access	CLEAN
C:\Boot\sr-Latn-CS\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sr-Latn-CS\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sr-Latn-RS	Accessed File	Access	CLEAN
C:\Boot\sr-Latn-RS\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sv-SE	Accessed File	Access	CLEAN
C:\Boot\sv-SE\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sv-SE\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\tr-TR	Accessed File	Access	CLEAN
C:\Boot\tr-TR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\tr-TR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\uk-UA	Accessed File	Access	CLEAN
C:\Boot\uk-UA\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\zh-CN	Accessed File	Access	CLEAN

Reduced dataset

Registry

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

Process

Process Name	Commandline	Verdict
b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe	"C:\Users\RDhJ0CNFevzX\Desktop\b40db2ff2f7b61092ec9962bfefe8eca240d3a4238e9e96ebe48e840dcdc5965.exe"	MALICIOUS
cmd.exe	cmd.exe /c "taskkill /f /im msftesql.exe "	CLEAN
taskkill.exe	taskkill /f /im msftesql.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im sqlagent.exe "	CLEAN
taskkill.exe	taskkill /f /im sqlagent.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im sqlbrowser.exe "	CLEAN
taskkill.exe	taskkill /f /im sqlbrowser.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im sqlservr.exe "	CLEAN
taskkill.exe	taskkill /f /im sqlservr.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im sqlwriter.exe "	CLEAN
taskkill.exe	taskkill /f /im sqlwriter.exe	CLEAN

Process Name	Commandline	Verdict
cmd.exe	cmd.exe /c "taskkill /f /im oracle.exe "	CLEAN
taskkill.exe	taskkill /f /im oracle.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im ocssd.exe "	CLEAN
taskkill.exe	taskkill /f /im ocssd.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im dbsnmp.exe "	CLEAN
taskkill.exe	taskkill /f /im dbsnmp.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im synctime.exe "	CLEAN
taskkill.exe	taskkill /f /im synctime.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im mydesktopqos.exe "	CLEAN
taskkill.exe	taskkill /f /im mydesktopqos.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im agntsvc.exeisqlplussvc.exe "	CLEAN
taskkill.exe	taskkill /f /im agntsvc.exeisqlplussvc.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im xfssvccon.exe "	CLEAN
taskkill.exe	taskkill /f /im xfssvccon.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im mydesktopservice.exe "	CLEAN
taskkill.exe	taskkill /f /im mydesktopservice.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im ocautoupds.exe "	CLEAN
taskkill.exe	taskkill /f /im ocautoupds.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im agntsvc.exeagntsvc.exe "	CLEAN
taskkill.exe	taskkill /f /im agntsvc.exeagntsvc.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im agntsvc.exeencsvc.exe "	CLEAN
taskkill.exe	taskkill /f /im agntsvc.exeencsvc.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im firefoxconfig.exe "	CLEAN
taskkill.exe	taskkill /f /im firefoxconfig.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im tbirdconfig.exe "	CLEAN
taskkill.exe	taskkill /f /im tbirdconfig.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im ocomm.exe "	CLEAN
taskkill.exe	taskkill /f /im ocomm.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im mysqld.exe "	CLEAN
taskkill.exe	taskkill /f /im mysqld.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im mysqld-nt.exe "	CLEAN
taskkill.exe	taskkill /f /im mysqld-nt.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im mysqld-opt.exe "	CLEAN
taskkill.exe	taskkill /f /im mysqld-opt.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im dbeng50.exe "	CLEAN
taskkill.exe	taskkill /f /im dbeng50.exe	CLEAN

Process Name	Commandline	Verdict
cmd.exe	cmd.exe /c "taskkill /f /im sqbcoreservice.exe "	CLEAN
taskkill.exe	taskkill /f /im sqbcoreservice.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im excel.exe "	CLEAN
taskkill.exe	taskkill /f /im excel.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im infopath.exe "	CLEAN
taskkill.exe	taskkill /f /im infopath.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im msaccess.exe "	CLEAN
taskkill.exe	taskkill /f /im msaccess.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im mspub.exe "	CLEAN
taskkill.exe	taskkill /f /im mspub.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im onenote.exe "	CLEAN
taskkill.exe	taskkill /f /im onenote.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im outlook.exe "	CLEAN
taskkill.exe	taskkill /f /im outlook.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im powerpnt.exe "	CLEAN
taskkill.exe	taskkill /f /im powerpnt.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im steam.exe "	CLEAN
taskkill.exe	taskkill /f /im steam.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im thebat.exe "	CLEAN
taskkill.exe	taskkill /f /im thebat.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im thebat64.exe "	CLEAN
taskkill.exe	taskkill /f /im thebat64.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im thunderbird.exe "	CLEAN
taskkill.exe	taskkill /f /im thunderbird.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im visio.exe "	CLEAN
taskkill.exe	taskkill /f /im visio.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im winword.exe "	CLEAN
taskkill.exe	taskkill /f /im winword.exe	CLEAN
cmd.exe	cmd.exe /c "taskkill /f /im wordpad.exe"	CLEAN
taskkill.exe	taskkill /f /im wordpad.exe	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	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.16 / 2022-03-11 16:16:43
YARA Built-in Ruleset Version	4.4.1.16

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows