MALICIOUS

Classifications: Ransomware | Backdoor | Wiper

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe**
ID	#3837110
MD5	e1e41506da591e55cee1825494ac8f42
SHA1	55aeda88fcbc314cf26a2f2bf41a2400d044a8bd
SHA256	ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027
File Size	2012.00 KB
Report Created	2022-03-18 10:23 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (14 rules, 58 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe modifies the content of multiple user files.			
5/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe deletes multiple user files.			
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) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe possibly drops ransom note files (creates 66 instances of the file "README.html" in different locations).			
3/5	Network Connection	All network connection attempts failed	1	-
	• Host "193.56.28.159" is unavailable.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Anti Analysis	Creates an unusually large number of processes	1	-
	• Above average number of processes were monitored.			
2/5	Network Connection	Sets up server that accepts incoming connections	2	Backdoor
	• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts a TCP server listening on port 49713. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts a TCP server listening on port 49723.			
1/5	Hide Tracks	Creates process with hidden window	43	-

Score	Category	Operation	Count	Classification
		• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #3) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #6) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #8) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #9) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #10) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #12) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #14) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #16) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #18) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #20) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #22) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #24) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #26) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #28) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #30) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #32) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #34) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #36) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #38) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #40) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #42) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #44) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #46) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #48) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #50) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #52) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #54) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #56) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #59) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #61) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #63) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #65) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #67) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #69) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #71) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #73) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #75) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #77) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #79) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #81) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #83) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #85) cmd.exe with a hidden window. • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe starts (process #87) cmd.exe with a hidden window.		
1/5	Network Connection	Connects to remote host	2	-
		• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe accepts an incoming TCP connection from host "193.56.28.159:80". • (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe opens an outgoing TCP connection to host "193.56.28.159:80".		
1/5	System Modification	Creates an unusually large number of files	1	-
		• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe creates an above average number of files.		

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-

• (Process #1) ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe resolves 44 API functions by name.

Mitre ATT&CK Matrix

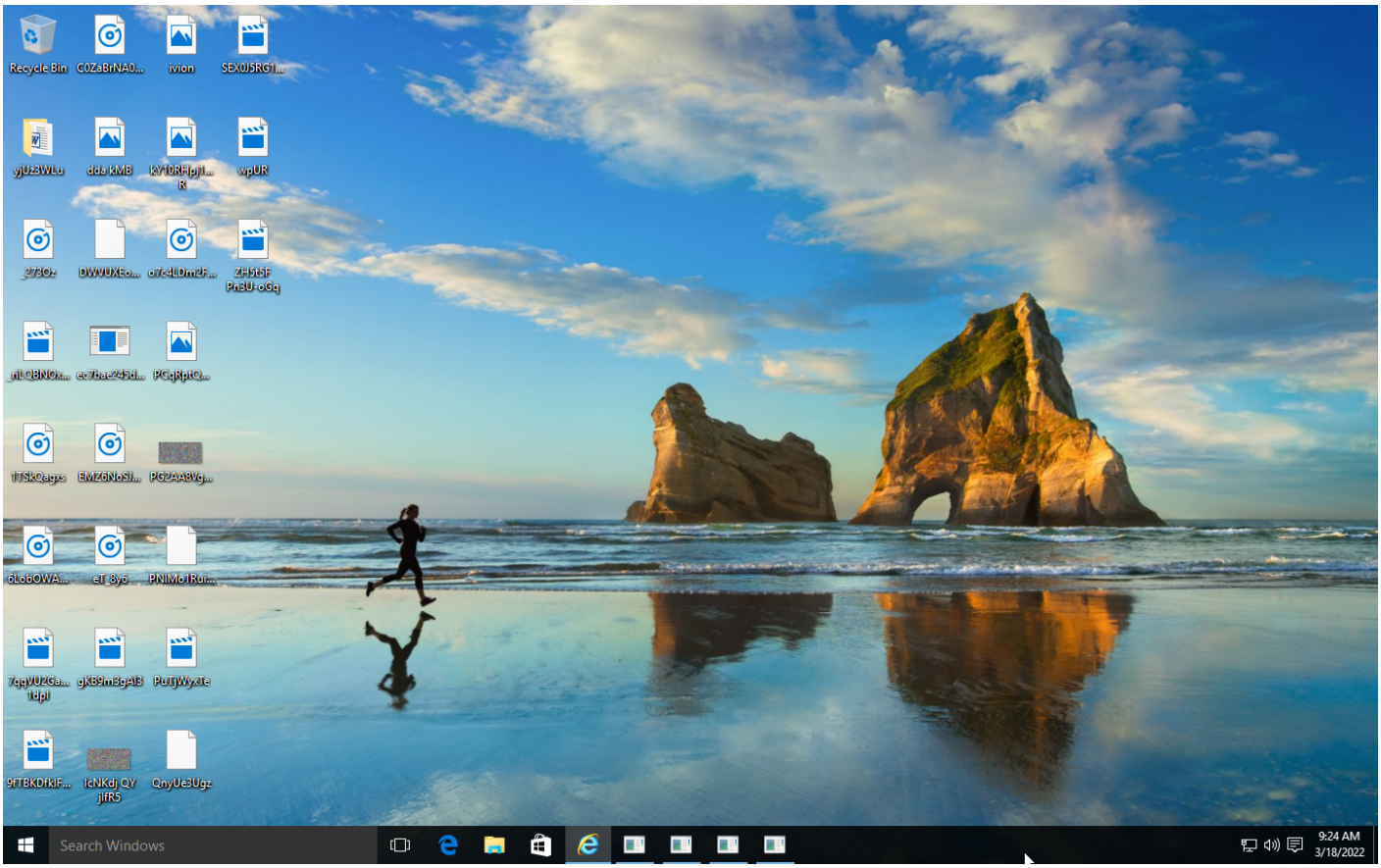
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection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

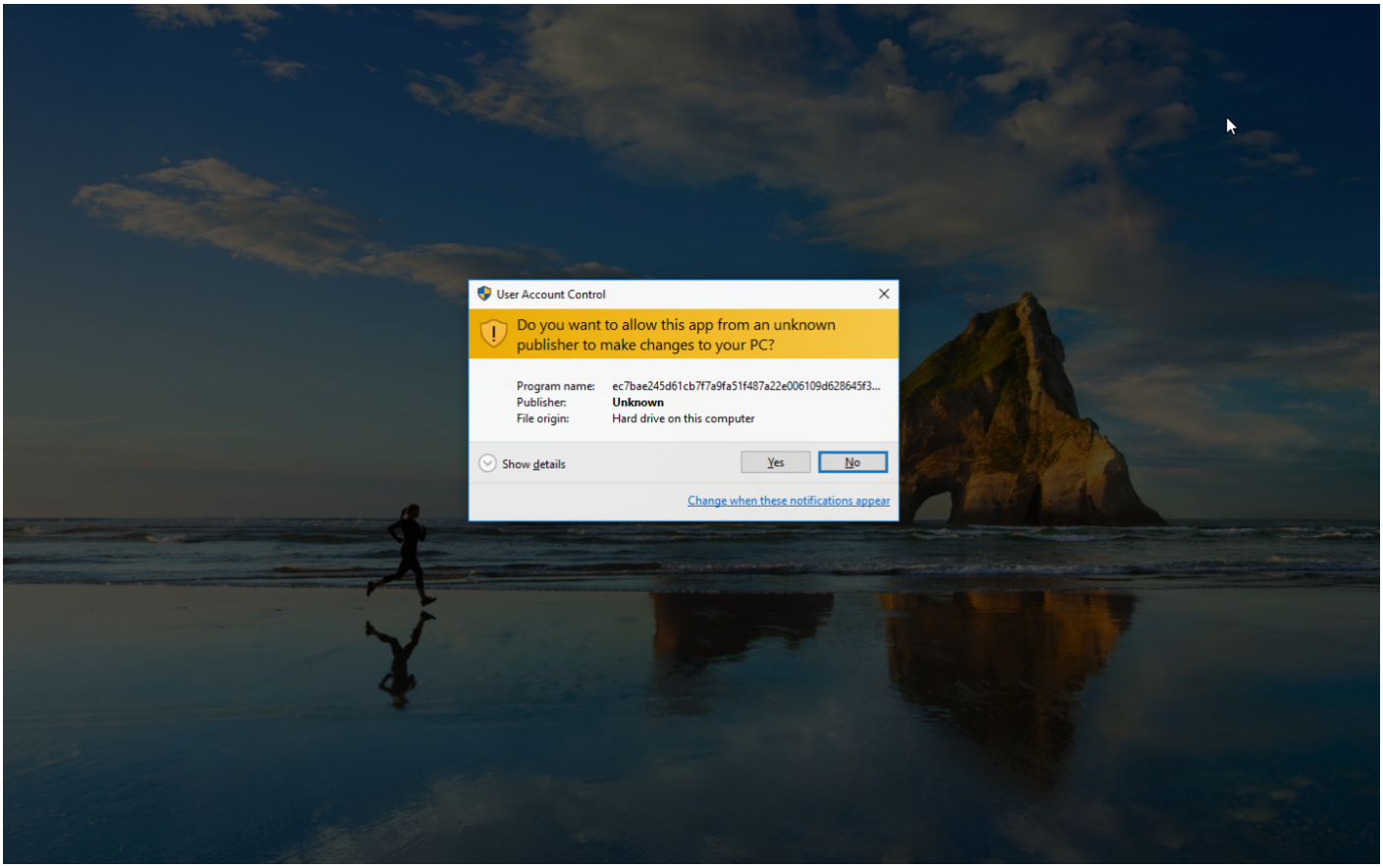
Sample Information

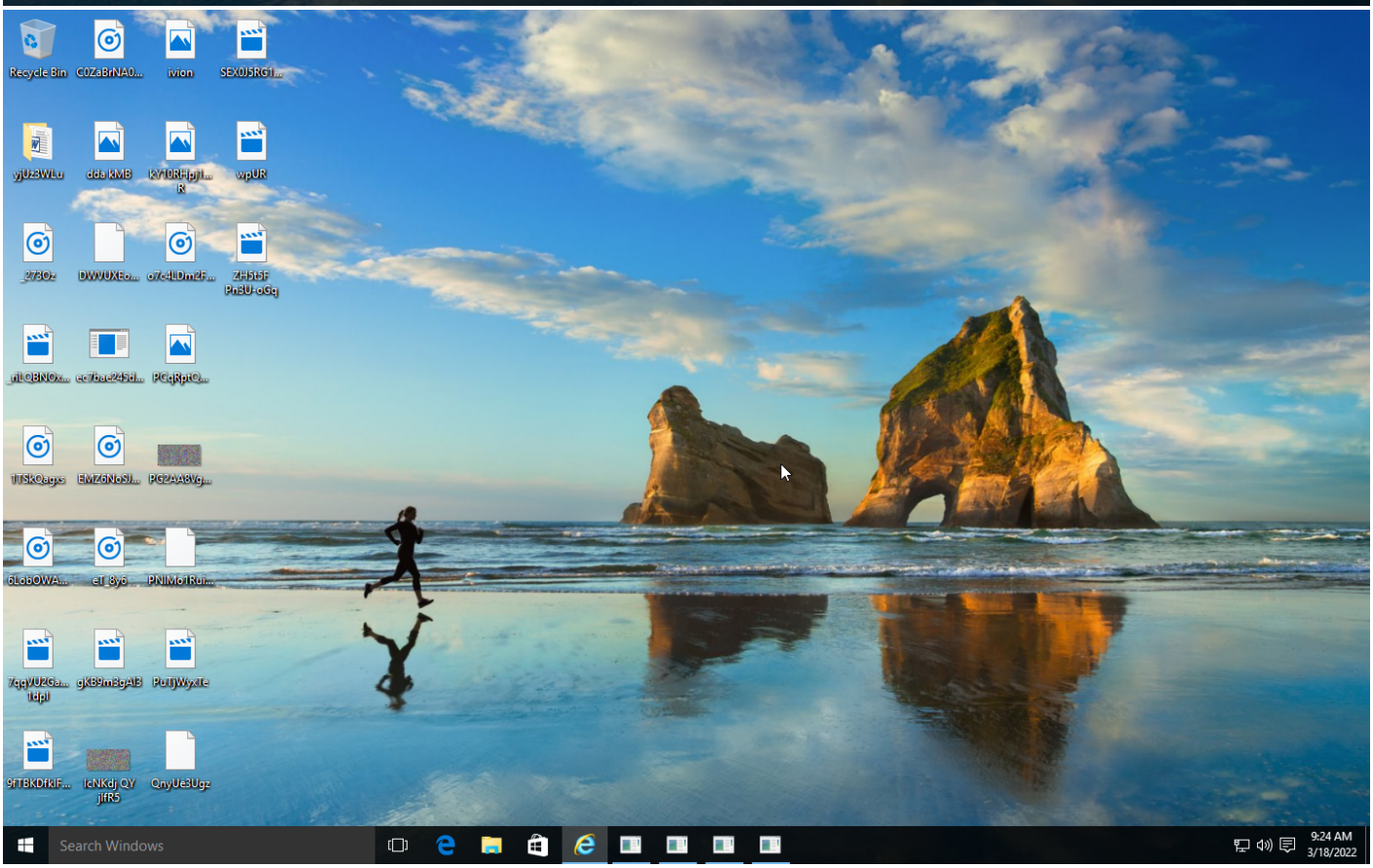
ID	#3837110
MD5	e1e41506da591e55cee1825494ac8f42
SHA1	55aeda88fcbc314cf26a2f2bf41a2400d044a8bd
SHA256	ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027
SSDeep	24576:fyWrQcBZS30+h+wuLWPh4O8USgIamJ4FWMQYO9C8vx9G9FUcUFJmpvgmISKg0P4J:TrQc63d+LLmh4n7P6gmmWwlG02Ul
ImpHash	96c44fa1eee2c4e9b9e77d7bf42d59e6
File Name	ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe
File Size	2012.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-03-18 10:23 (UTC+1)
Analysis Duration	00:03:52
Termination Reason	Timeout
Number of Monitored Processes	85
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
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: ec7bae245d61cb7f7a9fa51f487a22e006109d628645f3...
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

1 ports 80

1 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

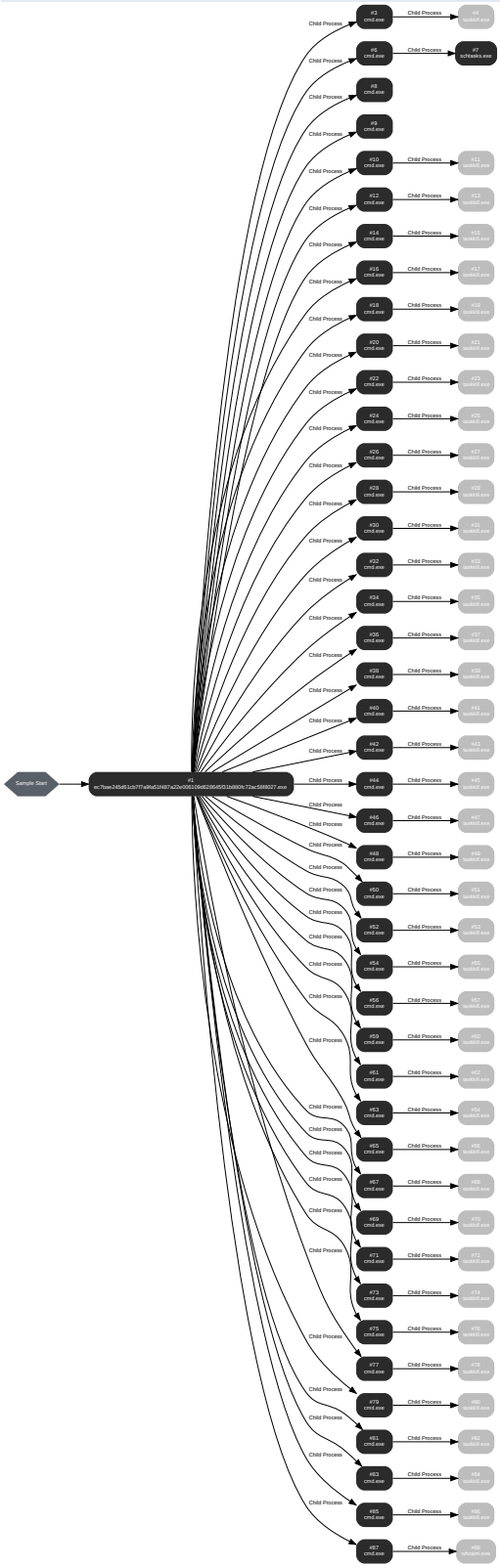
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 90914, Reason: Analysis Target
Unmonitor End Time	End Time: 322947, Reason: Terminated by Timeout
Monitor duration	232.03s
Return Code	Unknown
PID	4364
Parent PID	1184
Bitness	32 Bit

Dropped Files (201)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\utbfPsCYzd	1.67 KB	7dab70485d4de81700d23f0a5007c574e3ac4a66a56f407989711df86ab95836	✗
C:\PerfLogs\README.html	3.13 KB	9718159cbe798996e172405e0b10daa43085dad0a30d6e725d48e595f4b36d5c	✗
C:\Users\RDhJ0CNFevzX\Desktop\ZH5t5F Pn3U-oGq.mp4	1000.00 KB	46f339857c3409155aed24d6596fa7cf444c9d479c4b04ed76ba810e4a5e821c	✗
C:\Users\RDhJ0CNFevzX\Desktop\ZH5t5F Pn3U-oGq.mp4.locked	38.81 KB	0130f926ed949d38f7ae774ebb192c95cda11452a3e3fde10565b95a713f1e44	✗
C:\Users\RDhJ0CNFevzX\Desktop\EMZ6NoSJq0-2xx6IW.wav	1000.00 KB	bac19dace0fda3b8a12dc6bfca94de94dbb8df96343d09437edecdf34d68951c	✗
C:\Users\RDhJ0CNFevzX\Desktop\EMZ6NoSJq0-2xx6IW.wav.locked	91.44 KB	7c5fbc699323ca95871fb862bc4b7f7063d274b888b2a66853ec89cb2070b795	✗
C:\Users\RDhJ0CNFevzX\Desktop\1TSkQagxs.mp3	1000.00 KB	df358f622a9386942fcde745d9147799b72d9000d4c5134cba081f2188f189d6	✗
C:\Users\RDhJ0CNFevzX\Desktop\9fTBKDfkIFX1UCW.avi	1000.00 KB	1c28054cd4a5608a651773aab1dd96bf858e5f46543b4371f3e2e243ade9f06d	✗
C:\Users\RDhJ0CNFevzX\Desktop\7qqVU2GatTMCj 1dpl.mkv	1000.00 KB	274f2c79636c8b2dd29f2d0dcdf176402a90e6a4c6bdff5f62224f7455aab18f	✗
C:\Users\RDhJ0CNFevzX\Desktop\DWVUXEoQZyD.flv	1000.00 KB	1757a80c92f814b344d0901bb87b2f1a0505e5cc1138bceefb5f03cec2e30e36	✗
C:\Users\RDhJ0CNFevzX\Desktop_riLQBNOxB3yhpHCkj.mkv	1000.00 KB	e3c9c22c51369609eeaa58ec7b3f96665a4d8d0c5451ed993c7b10d9d20feb7b	✗
C:\Users\RDhJ0CNFevzX\Desktop\IcNKdj QY jIfR5.bmp	1000.00 KB	fd642dbd292204ed7ade0877ff0fbd309abaa6c2e7790bb48f11c5f56a13582d	✗
C:\Users\RDhJ0CNFevzX\Desktop\1TSkQagxs.mp3.locked	7.17 KB	5c758998b1a8fcc4a908f712022013a95dd69d0f53b2744f4f764965c67092e3	✗
C:\Users\RDhJ0CNFevzX\Desktop\dda kMB.jpg	1000.00 KB	a44fd0a02e46844bd82bba5b09d0f72adf8f1f2fad82de6fb7f51cb5a6c8e11c	✗
C:\Users\RDhJ0CNFevzX\Desktop\PNIMo1Rui9-Os7LqiJYf.swf	1000.00 KB	3bdb30eee41f93ac8a838c61cfcfc0b14c1a2b5706693af6939cdd4028678dac	✗
C:\Users\RDhJ0CNFevzX\Desktop\9fTBKDfkIFX1UCW.avi.locked	10.33 KB	12868e326d1cdb4d18c5952c3fba492c035abc317b79a382b435f95141399a38	✗
C:\Users\RDhJ0CNFevzX\Desktop\PG2AA8VgUaJQix3.bmp	1000.00 KB	1df7df6b8b17402d95ad9be9aa55a18d9590d2fd30af795ef0619ff03e8dcda4	✗
C:\Users\RDhJ0CNFevzX\Desktop\eT_8y6.mp3	1000.00 KB	7e06fe1df3c7cd787ddae4e3b812eb63581429f213745bb49bdc5bbd4cfb3201	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\PCqRptQW6vY1N.gif	1000.00 KB	b7bf1600d531f68e52cb2dc50cbc9144c05c0b5539635986674419b12ae14476	✗
C:\Users\RDhJ0CNFevzX\Desktop\7qqVU2GatTMCj1dpl.mkv.locked	57.12 KB	340280f09c93e8584621ccf5f1e504b629a141024520fb9605cbaa311fbef702	✗
C:\Users\RDhJ0CNFevzX\Desktop\DWVUXEoQZyD.flv.locked	33.53 KB	64d154ae155f7cf0fc8020bfbe38f5b59e00dc7581a60d20a876a09187f7b0d2	✗
C:\Users\RDhJ0CNFevzX\Desktop_273Oz.mp3	1000.00 KB	15d2eed348350e64ce6aae127605b2d10b1fb186569049a62844d9faee277d40	✗
C:\Users\RDhJ0CNFevzX\Desktop\dda kMB.jpg.locked	69.42 KB	e964527fdd8884e0ddb9e4646dd9febc734bd3cd168ea302dbdfa1f8789b2f3d	✗
C:\Users\RDhJ0CNFevzX\Desktop\IcNKdj QY jffR5.bmp.locked	69.53 KB	11f8401c77927358e74769522c26ff5d791041258637703bfa457521b3c66f16	✗
C:\Users\RDhJ0CNFevzX\Desktop_riLQBNOxB3yhpHCkj.mkv.locked	71.90 KB	551333eb9bbac3cea69210f6966df67ff72602fbead1f3d0fa7b027eb6bf60a8	✗
C:\Users\RDhJ0CNFevzX\Desktop\PNIMo1Rui9-Os7LqiJYf.swf.locked	97.74 KB	9e828e297d0cbd90a38cc2c771454b147e2e6a39c04d0a40731769015b115bf2	✗
C:\Users\RDhJ0CNFevzX\Desktop\PG2AA8VgUaJQix3.bmp.locked	58.09 KB	6aeacaba2377ba4418114c7603662af296feacf69af5dd0a69699e3a233f546f	✗
C:\Users\RDhJ0CNFevzX\Desktop\eT_8y6.mp3.locked	2.25 KB	28910f59815ecf14e97389d54adb7d20dca6474a044e4cf660cc44857c30fb6f	✗
C:\Users\RDhJ0CNFevzX\Desktop\PCqRptQW6vY1N.gif.locked	55.49 KB	6779db9e89823fbfa62e45320a7f3efc90171470442a80b63dab02a0ee93c750	✗
C:\Users\RDhJ0CNFevzX\Desktop_273Oz.mp3.locked	30.37 KB	9bb51b95db56c3b365331978788611ca76feef1ff6849ae40ca9ce00d16e738d	✗
C:\Users\RDhJ0CNFevzX\Desktop\QnyUe3Ugz.swf	1000.00 KB	ebceeec8ae6cc0200e8f21f0e2d19e79466b6dce71b987cd2d2eaf597d9cf111	✗
C:\Users\RDhJ0CNFevzX\Desktop\PuTjWyxTe.mp4	1000.00 KB	406b29834850bc8793f74559c8922b7f20721832641 66c60da03d31a49855a4c	✗
C:\Users\RDhJ0CNFevzX\Desktop\PuTjWyxTe.mp4.locked	65.59 KB	1779cb433e2172f60a81f4280e4dbde4129ed3fd4416df2ae701b4462c3ac6f6	✗
C:\Users\RDhJ0CNFevzX\Desktop\QnyUe3Ugz.swf.locked	47.10 KB	cab619da12d3934031a2357f70bd7a33ba7cd065e5fecb41b2f36e26f6d20d63	✗
C:\Users\RDhJ0CNFevzX\Desktop\SEX0J5RG1Om3TZ.mp4	1000.00 KB	57b4e8c1150744579500b9733d096a59a86db92abdfd15f9022bf94841936017	✗
C:\Users\RDhJ0CNFevzX\Desktop\SEX0J5RG1Om3TZ.mp4.locked	61.45 KB	e0cf58a211329a09b33f1e2a4a3d6d1881fff756031032fee69a26798885c262	✗
C:\Users\RDhJ0CNFevzX\Desktop\gKB9m3gAI3.mp4	1000.00 KB	66a0de9412bc8e07225dbb1dfb3eaf7a2051b2e0c3153bbc5388c3af1a644506	✗
C:\Users\RDhJ0CNFevzX\Desktop\ivion.png	1000.00 KB	af0c2f50a027001637cc32cab9357d11b5dd133e5c6aee31141c0eae4a9a28f1	✗
C:\Users\RDhJ0CNFevzX\Desktop\gKB9m3gAI3.mp4.locked	6.06 KB	3c9ddb6179eddf2c8e0daa83ccf176ff9e8515be6747776c9a21731d024f84a6	✗
C:\Users\RDhJ0CNFevzX\Desktop\ivion.png.locked	92.82 KB	308b7f9e412061777715a63ce55a972e9d65d432e713081bc6b58e66284a4775	✗
C:\Users\RDhJ0CNFevzX\Desktop\kY10RHpj1Ccj R.png	1000.00 KB	2bd40cc9adc73a27b9c2ae5ff81d02e984cdff2d3104a2bab8896f76d48b293a	✗
C:\Users\RDhJ0CNFevzX\Desktop\o7c4LDm2F7lcu2v.wav	1000.00 KB	e44dcf3117b1ca5c60b340524868de84ce9cdedbe46bdd438172dcd4fc539112	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\ZA606Y.rtf	1000.00 KB	6e3d6e4c1d8dccb8121d61d69a6ab3f7b2085ab3831344d6d78c7f561d45b1ac	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\0C0imTxCn.mp3	1000.00 KB	3115f55e4dec7239f612ada62f634515fdf34bf7ec9ca15224872c59eba61409	✗
C:\Users\RDhJ0CNFevzX\Desktop\o7c4LDm2F7lcu2v.wav.locked	4.34 KB	88b05e5b402e6ccee8890dd2019bfeed9a38f0f3bd15fe07fc624e5f7d53373b	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\ZA606Y.rtf.locked	58.39 KB	5e55ba7e245439512885932e92ea4efdf45eb5d74d753ead20aa9b9d4630e1d0	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\0C0imTxCn.mp3.locked	91.83 KB	7b8daee4b9a7b35ced48d2286f29d8e72e37647175bfe585713d5b7c484cff02	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\C5Fa.mkv	1000.00 KB	00f99228ffff505e53dbca6043cc42162f3a34ab1ab1142346028e60ca4b3bc2	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\C5Fa.mkv.locked	91.31 KB	02c0643cf06db0d07c3f4b674119ba506e4a2463b7e7790af04a9d2740f24c00	✗
C:\Users\RDhJ0CNFevzX\Desktop\wpUR.mp4	1000.00 KB	4590bf60768034519ab4d41ca2dd0702a09026a3f5953627201e798de69ab84f	✗
C:\Users\RDhJ0CNFevzX\Desktop\wpUR.mp4.locked	77.17 KB	80d2bfbb6e3b704554bedddee9ca055adfd4dad4fd0b1b89bc5b9945c5c02365	✗
C:\Users\RDhJ0CNFevzX\Desktop\kY10RHpj1Ccj R.png.locked	86.07 KB	65bd68accb0ac85426b9893ba91a8de1521fc5aee501cfdfa332091de1962804	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj_2Qs2D.odp	1000.00 KB	225410108acdeb269576578082ea9598410a9395c86e7291a9c47b3e6b61e48e	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj_2Qs2D.odp.locked	4.97 KB	6ce1fd442b45344283a13c3b81b84606c7e21e11d32b2545e59d1a6d10e3fc12	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\ynl0nO8fmos3T.mp4	1000.00 KB	4d648a5ce80d9288f4ba445a79e1773326004bbb3f65ec34f179326d29e7fd6c	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\7pK8Q9_TXKB_8t_99Nak.gif	1000.00 KB	d5c9b320c67cdf1ec7f73e8cfc90f4553b6230d8767e04b606a52a7d73db7891	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\ynl0nO8fmos3T.mp4.locked	64.07 KB	5207ca89e45d9182296af798ee1a540e65ebaa587fd54f9f3291a94893389837	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\pQ4D7olyLasPf6h0yK.flv	1000.00 KB	e5201b6cbc6946cc75437903a4dce7ddbfeb02c3cdc594950d30375477b7eb89	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\pQ4D7olyLasPf6h0yK.flv.locked	53.57 KB	9e0aac4a30f76a216f8575d1d19e304f938e44adc17d1a42ad47f0b2b06cc66b	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\7pK8Q9_TXKB_8t_99Nak.gif.locked	75.36 KB	31bf3eb483dc3644fabfd24dc5f0d07a54e15a76b34893f5e40288886a817f85	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\53CjZJnv.avi	1000.00 KB	3d3bedb4c4da7a67c8d7e1fc8cf456a3ac541e8fd1f084c7724053c04458eb49	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\53CjZJnv.avi.locked	15.35 KB	9240c572eae2a0115c0594f6b98780027cf0bd5ced0635d6bec79239645478eb	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\-tLx.jpg	1000.00 KB	4d4c58e0165c8dd45df96aefb7166a29fbb4ab93da5a080cf10800c6deb5ad31	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\-tLx.jpg.locked	50.30 KB	d85ace7327931a467ebad76ac93ed7c870f8cf2e537acb4d8ed187b5832d24db	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\WqsBnn5V5.flv	1000.00 KB	5be4ef565773f5a14b843595f5ea1b65080e58821c6b691b3e99095ffb365325	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\WqsBnn5V5.flv.locked	48.22 KB	06c4a5bb15161402e1bd494370abaf284020c32bcf38810056fb197befbbbd91	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\2I YP.mkv	1000.00 KB	9a007151d6178367b5806f315d5abd6be2711d38c2312be0398272a624971cec	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\2I YP.mkv.locked	70.25 KB	d74e0c2920e9dd98918c7b1335a784fa9f6104823528e84f043396869c002ab7	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\YRFgwGf0zYgcMX.flv	1000.00 KB	83c14d1e5a5a45cc453834d6aeb1fcc4bb88303a60498ba7ebe8952a9ce09b77	✗
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\zMPTOdNQ.jpg	1000.00 KB	4d641e6f56b3557c24a2fc3b5c2a2678d101609fde1b8ad7eb4160b1db39b29d	✗

File Name	File Size	SHA256	YARA Match
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\YRFgwGf0zYgcMX.flv.locked	20.53 KB	91d9e96f96337f84135d4b68cf1cf92ca7ba7a7ff9178f2724374627443533 0f	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\zMPTOdNQ.jpg.locked	67.86 KB	75118dba30c93e2d6632861d6fdaefc051214e7f61a1918b8cc709d1cb8ecc7b	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\P-STq-jQ5hYtJhlu5S.ots	1000.00 KB	b98d202317823f20d06b268d562a1e642b498c67054f8237ab6bc184c90 891cb	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\P-STq-jQ5hYtJhlu5S.ots.locked	99.37 KB	1dcb69984aee4888a95ef5305973e6688b8b07f1c708248607089bbcecb 690fd	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\7g-3nq2zvxE4Vlk.png	1000.00 KB	8f5eaa86b38a5db7b0bb07ecf5f2b2a7658a792807bb45018dc7be28121e f107	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\RqMHtJbqykr-i2R.jpg	1000.00 KB	62cf2a4c92217d067bdec832ad7d97bf80db7e9e63fcf8e96d45dc4604d4 9314	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\7g-3nq2zvxE4Vlk.png.locked	82.84 KB	f07d2a35204689504d5c86e357dffa319a1ee29110e907c3862b7d11597c ab4c	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\RqMHtJbqykr-i2R.jpg.locked	92.63 KB	5ac7129ffe9e16211c18a7f29171fc555ab4de90d2f381295b5a69d544a30 3e0	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\dbMm7g.png	1000.00 KB	b5054120b83b3afb89b2885d3c8edcbf451e2b407d367d394fd4d3c3bdd7 d5f9	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\dbMm7g.png.locked	42.67 KB	feeebc81478c3c50a5532e7238f9ebd7f5cd22de6632474100208dd4d9c3 66fe	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\1s4d3CDN.flv	1000.00 KB	1cd8845c7a70f64e877a208ef74c511bdd454687625a9a7a836567208dd 74bf8	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\1s4d3CDN.flv.locked	93.97 KB	8fd5cead50508768993d6eee7c710331d39455c684d00751d4e64e28b2d 50a23	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\pVnv3JR1eBRIl.xls	1000.00 KB	8be46b6d1b644539a8b48ec4e38722fbaca73beb45bca4fd003267be10e 495d6	✗
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\pVnv3JR1eBRIl.xls.locked	13.84 KB	efa0020c434254fbd16073d682aa7f0de53afd59505a0b9bbaa6445d7c59f cda	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\xxYCYyYbKsjdn.swf	1000.00 KB	135490743b2ea5d2280f2b300f9a41939a7433c9ac0ed6a00f6099142ab5 1ac2	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\YqAV-p.bmp	1000.00 KB	eebedae32c786be9e86454323110415afb8a5303ac4c4a6e9f617705f189 d10f	✗
C:\\Users\RDhJ0CNFevzX\Documents\4hjR_qw1PrF.docx	1000.00 KB	ac00e8510d80337baa045eb1e154eb2170c086ee9cad268179d366a50e bf8ceb	✗
C:\\Users\RDhJ0CNFevzX\Documents\4hjR_qw1PrF.docx.locked	9.93 KB	f6a400ba4dc86579c02fcf9e7d6c4c64cca73b1834de47085b418acf0afd7 9f5	✗
C:\\Users\RDhJ0CNFevzX\Documents\4R8gdYA15.docx	1000.00 KB	8ef4c87b0429b30f5bb800f50f751ae277ee33101f3b7b9f654d93e908109f 2e	✗
C:\\Users\RDhJ0CNFevzX\Documents\4R8gdYA15.docx.locked	49.95 KB	379e417377eaed3f14b2c6b775a793baa332e086a125a2dba17c49e528c f19ad	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\xxYCYyYbKsjdn.swf.locked	35.94 KB	d5c06a6393afe21a4b1d0c2bfad1fab89d6a76f79f2bb19d18ed16228694b 12d	✗
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\YqAV-p.bmp.locked	8.75 KB	e93a7279d3a83dc260bb7528dfbee464f3c7044fca619c4d5f6e8d7a12c8 ef5b	✗
C:\\Users\RDhJ0CNFevzX\Documents\CX3dvz.pptx	1000.00 KB	f49f835eb2240fd4995a597c4df1d3891349b245f8e23085854e54fa80f1b3 19	✗
C:\\Users\RDhJ0CNFevzX\Documents\CX3dvz.pptx.locked	79.35 KB	593e35e1f3ee39968d18850dc66ba3cdeb1155fcb1673bb13a7bcc8a4fc5 2287	✗
C:\\Users\RDhJ0CNFevzX\Documents\9Q7-bFR.xlsx	1000.00 KB	4bba66e28582e311f5da43570eb021292c99f7e206ebdddd5745ae9db75 e0a0c	✗
C:\\Users\RDhJ0CNFevzX\Documents\9Q7-bFR.xlsx.locked	89.61 KB	160c1e7b5231537b228392520372fd7e43ac978f7dbdae6f535a918b7101 9424	✗

File Name	File Size	SHA256	YARA Match
C:\\Users\RDhJ0CNFevzX\Documents\Ej4CnCJUCwn5 nF.docx	1000.00 KB	e076d82e0f0902840204365db0f0a11769a75ec0114048078c40acaff3b776af	✗
C:\\Users\RDhJ0CNFevzX\Documents\Ej4CnCJUCwn5 nF.docx.locked	85.51 KB	b5f080255531370992138922b58ce6c93f825803364f914629b83871b01fe69d	✗
C:\\Users\RDhJ0CNFevzX\Documents\Crvhk0MgLr2QKx _m.pdf	1000.00 KB	b26e03640fb92fc853a234d4783a0f32c5fb0de108ba71da50d4354f8023e7a1	✗
C:\\Users\RDhJ0CNFevzX\Documents\GPvOBFfXu_XAefB06.doc	1000.00 KB	af7433bff9bb5f6f13cb05d289ff22ad73dc1dade6000709d6864f54c0fc3f52	✗
C:\\Users\RDhJ0CNFevzX\Documents\GPvOBFfXu_XAefB06.doc.locked	30.13 KB	304ed6e28249765a8a25a383ad63361a180145006917ac6614460df06f3634f8	✗
C:\\Users\RDhJ0CNFevzX\Documents\PksQcVAF-FVG.docx	1000.00 KB	6512270250927a179594c364c927ccbaacd452149e539e4ba56ad45a8ec15a90	✗
C:\\Users\RDhJ0CNFevzX\Documents\PksQcVAF-FVG.docx.locked	68.76 KB	433bd3caa64069c428f338162e37e0bcd773a250d6f7b2947327ebed6946a936	✗
C:\\Users\RDhJ0CNFevzX\Documents\5yfr.docx	1000.00 KB	7f69ac5c64b05a826cd683e34f991797e935ee81c22363810e612c23ed79011c	✗
C:\\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	1000.00 KB	d30384b0fd662bff161b1b60412846e00f22d714cd805fbfc641d92234bd7943	✗
C:\\Users\RDhJ0CNFevzX\Documents\5yfr.docx.locked	39.39 KB	268817fe9b4b0ef357ad90f2dc7af6a709b9c10a167c997a1c877236e53f1740	✗
C:\\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.locked	265.12 KB	b1ba2598049bd30f9bd0056ae5f8a5c8a74e553664b2370fcb9f888258d72406	✗
C:\\Users\RDhJ0CNFevzX\Documents\Crvhk0MgLr2QKx _m.pdf.locked	8.83 KB	df823390cf6e18bd1708e65f06a64b5a837cde6a64884ddec3636922dfadf63f	✗
C:\\Users\RDhJ0CNFevzX\Documents\VupTUE7Pb.xls	1000.00 KB	4873be4a46d8e49bd558a0b1de217304b9869cc828242b0c4dc2fc5d59856152	✗
C:\\Users\RDhJ0CNFevzX\Documents\lfzi1.xlsx	1000.00 KB	283fdb30371e26b4370f341a041b71a17781d42c72d8b0e0b8fb05b0a0927cc1	✗
C:\\Users\RDhJ0CNFevzX\Documents\XxX9zS.ods	1000.00 KB	bc9141e194a179610fd8016e4bfb0eb7f9332cb9a5fb1ba2f2cb6b9a7b460f24	✗
C:\\Users\RDhJ0CNFevzX\Documents\baXS\00jJreyg.doc	1000.00 KB	2acf8925f41af1b414a34ca7e2a386d3a7d4ffaaa745bf5899a85a233df25fa9	✗
C:\\Users\RDhJ0CNFevzX\Documents\baXS\00jJreyg.doc.locked	9.56 KB	eda9e180d7cfc235ea2d6905e8897c8193b1ac58c9cc72b0349b0dc913b5d00f	✗
C:\\Users\RDhJ0CNFevzX\Documents\UYS dfMqbVg.xlsx	1000.00 KB	d4b461015c70516433e435efc92c5fb627fb5dcd4cc2b0522efe4893732e8f2a	✗
C:\\Users\RDhJ0CNFevzX\Documents\VupTUE7Pb.xls.locked	6.04 KB	ce24bbe8890b920357eb83c28fbe6f83e1823e007a311eae7a106d290e45a3f6	✗
C:\\Users\RDhJ0CNFevzX\Documents\lfzi1.xlsx.locked	99.82 KB	2a9230a27f5c45d9ac7ca7a388038b42fd3b06587e63899e31e0760580905472	✗
C:\\Users\RDhJ0CNFevzX\Documents\baXS\8NTFMxPNLnS-.xlsx	1000.00 KB	807632d166cd7a7dd2d525fefe768794799fd528e8300e811d0e07d5ec859d2b	✗
C:\\Users\RDhJ0CNFevzX\Documents\XxX9zS.ods.locked	9.00 KB	0d3116f74f33d7be4d892fcf22224b2c7fbef4bcbe8b504006295b0dc7b32e65	✗
C:\\Users\RDhJ0CNFevzX\Documents\baXS\8NTFMxPNLnS-.xlsx.locked	52.99 KB	ca9490a39e07d6b00aa1efe51adab1fe09744dbe52cb0cf55c46f56a517c0b28	✗
C:\\Users\RDhJ0CNFevzX\Documents\TP7qaB_8RwFo0zi2S F.ods	1000.00 KB	2ac492f6b6c5acdfad585daa708bb917558861ba6233ead834a3c471abf8903a	✗
C:\\Users\RDhJ0CNFevzX\Documents\UYS dfMqbVg.xlsx.locked	68.24 KB	7ce3ebc7e017ab16d263bd43a5c0aba4cbf6a82cd616210f53eb5b27e38971c3	✗
C:\\Users\RDhJ0CNFevzX\Documents\TP7qaB_8RwFo0zi2S F.ods.locked	24.86 KB	aadd90b2a04d4a5bf29db011c9d9ebf0c946244437ab7570b418c3abc6a6214d	✗
C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\0ToZccO18urTblN.rtf	1000.00 KB	fe819089a3934cba4856a4b160d39f277c4894a9a0bee3cc3961493e898935f0	✗
C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\0ToZccO18urTblN.rtf.locked	7.07 KB	78d5f197e2895f48be3e472d18aa86adf34b54e5f1a47e7afe22d4d9287d72ba	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\4bt-B2q.pdf	1000.00 KB	4df541c2ce2a78af6e134401ae20c0b78fbffa154bb7da9027cc564c4f67b3eb	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\6wvQVTWOr1.doc	1000.00 KB	675edf71e75b6eb717a0cc5cede59daae9f43a51f9267558d188332c60dc81b7	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\4bt-B2q.pdf.locked	68.35 KB	402b62bf82819c32cfb4dae436e5f210c80b6e0f9f304a8cc8469fcdbbbbeae6	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\6wvQVTWOr1.doc.locked	97.78 KB	8ae8a53987f5a526869c7aad5027f55452a9d385fab838f5c52e98f773fbc181	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\8BJrk8.pps	1000.00 KB	675207649ab053d16ece358265d7c98a3b7244a773ce144d1dd81e1cf05eaf98	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\7NGgJCF9p1sXP7bTM6Xc.odp	1000.00 KB	5b7ccb378565d28251469179d9bdb4b30641c251d87bd3b3e65eec23a32bfae8	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\CJfBVMezWzfCMgvFYwf.ots	1000.00 KB	9d7bd017aff1d9ba17d723a645e962922a5fb217ab91b831fd8bc8484f56e49a	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\8BJrk8.pps.locked	81.91 KB	dcbbf55e1ec038794272129ced08ab8ce57a977c97f9192323fd56ad32c92e45	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\7NGgJCF9p1sXP7bTM6Xc.odp.locked	19.39 KB	22ea756bc8b8817cbaa0f55a5048e59158af44edbd243deed0ce785fb46fe4d9	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\L-u71CPit811c.xls	1000.00 KB	80014362c63ed28cb1afcb865b2a8de2420f270c0c287a69962e2f4df280acad	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\CJfBVMezWzfCMgvFYwf.ots.locked	60.53 KB	737b8d02ebddb6c9b5e0202b727b7c2b7b12365122cea1a2ad8671d71bfa9740	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EzlWVPEgGWw7Xy7.ods	1000.00 KB	fa943eebc7fa03ddc82099666cb18f63e0c22ac40f4414b6427d619ec8248e8f	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\L-u71CPit811c.xls.locked	38.46 KB	704afe1f68cac1a0963ea7210441b32384f1e97678d44b79ecfd864c34e2a4f8	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EzlWVPEgGWw7Xy7.ods.locked	68.03 KB	a1b4d2a0b2f326f54dd72095350fc70993bd491e973dc6468918aaefc05d3817	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\GFqXQi80UXX3UPgD.pdf	1000.00 KB	1f771f822ff1697a5ddf5c61086c8051a77d78c8f9f10fa14f7c077131818de0	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\GFqXQi80UXX3UPgD.pdf.locked	10.14 KB	70b74d6178d2e54209a777fccb34a00088fae9d3d514018b12c269f4bf7d63ed	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EPo8_m0ryn 6ACWfcC.doc	1000.00 KB	812bd6f9e42110e5813151e1db9789d17e347086ec52b7baa9424723b28ded75	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EPo8_m0ryn 6ACWfcC.doc.locked	72.51 KB	384872b45a20e19d2e1018f065087430c857f7f3430314fc6866d85c4695ce6b	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\nRY0tYZ9Ff0noTxW-ck.pptx	1000.00 KB	40052ad93892329ebeb4a2259429345ccdd21353ccf0e7fccfddc17f962d3672	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\v4ns79y.pptx	1000.00 KB	46351e77ad05db8285e83c0394f400b413f56ff85b0e45cbe512dd29b062a1d9	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\O4XyZ4ZdDUL8nyTp.csv	1000.00 KB	91795ec5ded0ae2d9fb849f03141e94b01e2bd1f337c7b87be1fee233a4c4d42	✗
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\nRY0tYZ9Ff0noTxW-ck.pptx.locked	99.31 KB	e3c4459f266441abe87f4bf1e7823ba59a7b01617cafa4f23e78999b1ba587ef	✗

File Name	File Size	SHA256	YARA Match
C:\ \Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\ v4ns79y.pptx.locked	63.08 KB	8cc277a3a44b7e2d8dd83bc5ea7c045531ac45fd42fabc216a90e6c5bcc47a29	✗
C:\ \Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\ O4XyZ4ZdDUL8nyTp.csv.locked	16.06 KB	b3b25f48305f8e1a292f5726c744c19cc39de924117859706b8d7ebfd04decc5	✗
C:\ \Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\ vTjM.rtf	1000.00 KB	ec78013ddaaee1c6f91b5df1d8a28eb5dbef826c3ae325bc690597a4a450a0ea	✗
C:\ \Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\ vTjM.rtf.locked	30.33 KB	56bbffc9178f3d842167a63e5f926c61da005ce2075c08da705182cd8842f689	✗

Reduced dataset

Host Behavior

Type	Count
Module	51
System	2
Environment	175
-	21
File	4413
Process	43

Network Behavior

Type	Count
TCP	2

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: 124339, Reason: Child Process
Unmonitor End Time	End Time: 141915, Reason: Terminated
Monitor duration	17.58s
Return Code	128
PID	3756
Parent PID	4364
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: 125659, Reason: Child Process
Unmonitor End Time	End Time: 141458, Reason: Terminated
Monitor duration	15.80s
Return Code	128
PID	2972
Parent PID	3756
Bitness	32 Bit

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "schtasks /delete /tn WM /F "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 141697, Reason: Child Process
Unmonitor End Time	End Time: 144634, Reason: Terminated
Monitor duration	2.94s
Return Code	1
PID	2568
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #7: schtasks.exe

ID	7
File Name	c:\windows\syswow64\schtasks.exe
Command Line	schtasks /delete /tn WM /F
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 142061, Reason: Child Process
Unmonitor End Time	End Time: 144379, Reason: Terminated
Monitor duration	2.32s
Return Code	1
PID	3156
Parent PID	2568
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
-	3
COM	1
File	10

Process #8: cmd.exe

ID	8
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "del C:\e.bat"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 143764, Reason: Child Process
Unmonitor End Time	End Time: 145105, Reason: Terminated
Monitor duration	1.34s
Return Code	0
PID	3628
Parent PID	4364
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	21
Environment	12
System	1

Process #9: cmd.exe

ID	9
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "del C:\a.bat"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 144406, Reason: Child Process
Unmonitor End Time	End Time: 144973, Reason: Terminated
Monitor duration	0.57s
Return Code	0
PID	3908
Parent PID	4364
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	21
Environment	12
System	1

Process #10: cmd.exe

ID	10
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: 144635, Reason: Child Process
Unmonitor End Time	End Time: 147488, Reason: Terminated
Monitor duration	2.85s
Return Code	128
PID	928
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #11: taskkill.exe

ID	11
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: 144979, Reason: Child Process
Unmonitor End Time	End Time: 147146, Reason: Terminated
Monitor duration	2.17s
Return Code	128
PID	3932
Parent PID	928
Bitness	32 Bit

Process #12: cmd.exe

ID	12
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: 146750, Reason: Child Process
Unmonitor End Time	End Time: 149645, Reason: Terminated
Monitor duration	2.90s
Return Code	128
PID	1504
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #13: taskkill.exe

ID	13
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: 147156, Reason: Child Process
Unmonitor End Time	End Time: 149668, Reason: Terminated
Monitor duration	2.51s
Return Code	128
PID	1756
Parent PID	1504
Bitness	32 Bit

Process #14: cmd.exe

ID	14
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: 149455, Reason: Child Process
Unmonitor End Time	End Time: 152331, Reason: Terminated
Monitor duration	2.88s
Return Code	128
PID	3976
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #15: taskkill.exe

ID	15
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: 149777, Reason: Child Process
Unmonitor End Time	End Time: 151327, Reason: Terminated
Monitor duration	1.55s
Return Code	128
PID	3484
Parent PID	3976
Bitness	32 Bit

Process #16: cmd.exe

ID	16
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: 151397, Reason: Child Process
Unmonitor End Time	End Time: 153601, Reason: Terminated
Monitor duration	2.20s
Return Code	128
PID	4796
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #17: taskkill.exe

ID	17
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: 151939, Reason: Child Process
Unmonitor End Time	End Time: 153249, Reason: Terminated
Monitor duration	1.31s
Return Code	128
PID	2952
Parent PID	4796
Bitness	32 Bit

Process #18: cmd.exe

ID	18
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: 153253, Reason: Child Process
Unmonitor End Time	End Time: 155795, Reason: Terminated
Monitor duration	2.54s
Return Code	128
PID	1204
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #19: taskkill.exe

ID	19
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: 153509, Reason: Child Process
Unmonitor End Time	End Time: 154792, Reason: Terminated
Monitor duration	1.28s
Return Code	128
PID	3076
Parent PID	1204
Bitness	32 Bit

Process #20: cmd.exe

ID	20
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: 154826, Reason: Child Process
Unmonitor End Time	End Time: 157870, Reason: Terminated
Monitor duration	3.04s
Return Code	128
PID	4868
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #21: taskkill.exe

ID	21
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: 155273, Reason: Child Process
Unmonitor End Time	End Time: 157620, Reason: Terminated
Monitor duration	2.35s
Return Code	128
PID	3640
Parent PID	4868
Bitness	32 Bit

Process #22: cmd.exe

ID	22
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: 157622, Reason: Child Process
Unmonitor End Time	End Time: 159830, Reason: Terminated
Monitor duration	2.21s
Return Code	128
PID	3832
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #23: taskkill.exe

ID	23
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: 157872, Reason: Child Process
Unmonitor End Time	End Time: 159400, Reason: Terminated
Monitor duration	1.53s
Return Code	128
PID	5064
Parent PID	3832
Bitness	32 Bit

Process #24: cmd.exe

ID	24
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: 159401, Reason: Child Process
Unmonitor End Time	End Time: 162161, Reason: Terminated
Monitor duration	2.76s
Return Code	128
PID	4120
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #25: taskkill.exe

ID	25
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: 159835, Reason: Child Process
Unmonitor End Time	End Time: 161893, Reason: Terminated
Monitor duration	2.06s
Return Code	128
PID	2280
Parent PID	4120
Bitness	32 Bit

Process #26: cmd.exe

ID	26
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: 161898, Reason: Child Process
Unmonitor End Time	End Time: 166901, Reason: Terminated
Monitor duration	5.00s
Return Code	128
PID	1356
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #27: taskkill.exe

ID	27
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: 162163, Reason: Child Process
Unmonitor End Time	End Time: 165675, Reason: Terminated
Monitor duration	3.51s
Return Code	128
PID	1252
Parent PID	1356
Bitness	32 Bit

Process #28: cmd.exe

ID	28
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: 165933, Reason: Child Process
Unmonitor End Time	End Time: 168189, Reason: Terminated
Monitor duration	2.26s
Return Code	128
PID	4392
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #29: taskkill.exe

ID	29
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: 166176, Reason: Child Process
Unmonitor End Time	End Time: 167923, Reason: Terminated
Monitor duration	1.75s
Return Code	128
PID	1376
Parent PID	4392
Bitness	32 Bit

Process #30: cmd.exe

ID	30
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: 167927, Reason: Child Process
Unmonitor End Time	End Time: 170963, Reason: Terminated
Monitor duration	3.04s
Return Code	128
PID	1296
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #31: taskkill.exe

ID	31
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: 168349, Reason: Child Process
Unmonitor End Time	End Time: 170305, Reason: Terminated
Monitor duration	1.96s
Return Code	128
PID	4276
Parent PID	1296
Bitness	32 Bit

Process #32: cmd.exe

ID	32
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: 170013, Reason: Child Process
Unmonitor End Time	End Time: 172261, Reason: Terminated
Monitor duration	2.25s
Return Code	128
PID	3388
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #33: taskkill.exe

ID	33
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: 170308, Reason: Child Process
Unmonitor End Time	End Time: 171925, Reason: Terminated
Monitor duration	1.62s
Return Code	128
PID	4480
Parent PID	3388
Bitness	32 Bit

Process #34: cmd.exe

ID	34
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: 171929, Reason: Child Process
Unmonitor End Time	End Time: 175436, Reason: Terminated
Monitor duration	3.51s
Return Code	128
PID	4940
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #35: taskkill.exe

ID	35
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: 172264, Reason: Child Process
Unmonitor End Time	End Time: 174463, Reason: Terminated
Monitor duration	2.20s
Return Code	128
PID	4256
Parent PID	4940
Bitness	32 Bit

Process #36: cmd.exe

ID	36
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: 174467, Reason: Child Process
Unmonitor End Time	End Time: 178009, Reason: Terminated
Monitor duration	3.54s
Return Code	128
PID	4196
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #37: taskkill.exe

ID	37
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: 175538, Reason: Child Process
Unmonitor End Time	End Time: 176839, Reason: Terminated
Monitor duration	1.30s
Return Code	128
PID	4560
Parent PID	4196
Bitness	32 Bit

Process #38: cmd.exe

ID	38
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: 176841, Reason: Child Process
Unmonitor End Time	End Time: 181144, Reason: Terminated
Monitor duration	4.30s
Return Code	128
PID	392
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #39: taskkill.exe

ID	39
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: 177523, Reason: Child Process
Unmonitor End Time	End Time: 180175, Reason: Terminated
Monitor duration	2.65s
Return Code	128
PID	3520
Parent PID	392
Bitness	32 Bit

Process #40: cmd.exe

ID	40
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: 180178, Reason: Child Process
Unmonitor End Time	End Time: 182206, Reason: Terminated
Monitor duration	2.03s
Return Code	128
PID	2932
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #41: taskkill.exe

ID	41
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: 180415, Reason: Child Process
Unmonitor End Time	End Time: 181949, Reason: Terminated
Monitor duration	1.53s
Return Code	128
PID	3896
Parent PID	2932
Bitness	32 Bit

Process #42: cmd.exe

ID	42
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: 181962, Reason: Child Process
Unmonitor End Time	End Time: 184111, Reason: Terminated
Monitor duration	2.15s
Return Code	128
PID	4000
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #43: taskkill.exe

ID	43
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: 182208, Reason: Child Process
Unmonitor End Time	End Time: 183859, Reason: Terminated
Monitor duration	1.65s
Return Code	128
PID	3996
Parent PID	4000
Bitness	32 Bit

Process #44: cmd.exe

ID	44
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: 183861, Reason: Child Process
Unmonitor End Time	End Time: 187669, Reason: Terminated
Monitor duration	3.81s
Return Code	128
PID	5108
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #45: taskkill.exe

ID	45
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: 184114, Reason: Child Process
Unmonitor End Time	End Time: 186504, Reason: Terminated
Monitor duration	2.39s
Return Code	128
PID	5088
Parent PID	5108
Bitness	32 Bit

Process #46: cmd.exe

ID	46
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: 186692, Reason: Child Process
Unmonitor End Time	End Time: 191035, Reason: Terminated
Monitor duration	4.34s
Return Code	128
PID	4736
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #47: taskkill.exe

ID	47
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: 187034, Reason: Child Process
Unmonitor End Time	End Time: 190679, Reason: Terminated
Monitor duration	3.65s
Return Code	128
PID	4844
Parent PID	4736
Bitness	32 Bit

Process #48: cmd.exe

ID	48
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: 190795, Reason: Child Process
Unmonitor End Time	End Time: 194384, Reason: Terminated
Monitor duration	3.59s
Return Code	128
PID	3196
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #49: taskkill.exe

ID	49
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: 191036, Reason: Child Process
Unmonitor End Time	End Time: 193295, Reason: Terminated
Monitor duration	2.26s
Return Code	128
PID	1652
Parent PID	3196
Bitness	32 Bit

Process #50: cmd.exe

ID	50
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: 193413, Reason: Child Process
Unmonitor End Time	End Time: 200836, Reason: Terminated
Monitor duration	7.42s
Return Code	128
PID	3136
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #51: taskkill.exe

ID	51
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: 193641, Reason: Child Process
Unmonitor End Time	End Time: 200107, Reason: Terminated
Monitor duration	6.47s
Return Code	128
PID	2428
Parent PID	3136
Bitness	32 Bit

Process #52: cmd.exe

ID	52
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: 200557, Reason: Child Process
Unmonitor End Time	End Time: 203658, Reason: Terminated
Monitor duration	3.10s
Return Code	128
PID	2484
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #53: taskkill.exe

ID	53
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: 200837, Reason: Child Process
Unmonitor End Time	End Time: 202686, Reason: Terminated
Monitor duration	1.85s
Return Code	128
PID	4376
Parent PID	2484
Bitness	32 Bit

Process #54: cmd.exe

ID	54
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: 202691, Reason: Child Process
Unmonitor End Time	End Time: 204469, Reason: Terminated
Monitor duration	1.78s
Return Code	128
PID	3480
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #55: taskkill.exe

ID	55
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: 202913, Reason: Child Process
Unmonitor End Time	End Time: 204224, Reason: Terminated
Monitor duration	1.31s
Return Code	128
PID	2412
Parent PID	3480
Bitness	32 Bit

Process #56: cmd.exe

ID	56
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: 204229, Reason: Child Process
Unmonitor End Time	End Time: 206996, Reason: Terminated
Monitor duration	2.77s
Return Code	128
PID	2568
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #57: taskkill.exe

ID	57
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: 204472, Reason: Child Process
Unmonitor End Time	End Time: 206914, Reason: Terminated
Monitor duration	2.44s
Return Code	128
PID	3628
Parent PID	2568
Bitness	32 Bit

Process #59: cmd.exe

ID	59
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: 206021, Reason: Child Process
Unmonitor End Time	End Time: 208113, Reason: Terminated
Monitor duration	2.09s
Return Code	128
PID	3936
Parent PID	4364
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 infopath.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 206211, Reason: Child Process
Unmonitor End Time	End Time: 207805, Reason: Terminated
Monitor duration	1.59s
Return Code	128
PID	3932
Parent PID	3936
Bitness	32 Bit

Process #61: cmd.exe

ID	61
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: 207809, Reason: Child Process
Unmonitor End Time	End Time: 210303, Reason: Terminated
Monitor duration	2.49s
Return Code	128
PID	3140
Parent PID	4364
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 msaccess.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 208121, Reason: Child Process
Unmonitor End Time	End Time: 210012, Reason: Terminated
Monitor duration	1.89s
Return Code	128
PID	2156
Parent PID	3140
Bitness	32 Bit

Process #63: cmd.exe

ID	63
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: 210020, Reason: Child Process
Unmonitor End Time	End Time: 212031, Reason: Terminated
Monitor duration	2.01s
Return Code	128
PID	836
Parent PID	4364
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 mspub.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 210306, Reason: Child Process
Unmonitor End Time	End Time: 211645, Reason: Terminated
Monitor duration	1.34s
Return Code	128
PID	2400
Parent PID	836
Bitness	32 Bit

Process #65: cmd.exe

ID	65
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: 211647, Reason: Child Process
Unmonitor End Time	End Time: 215002, Reason: Terminated
Monitor duration	3.35s
Return Code	128
PID	3692
Parent PID	4364
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 onenote.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 212101, Reason: Child Process
Unmonitor End Time	End Time: 214344, Reason: Terminated
Monitor duration	2.24s
Return Code	128
PID	3672
Parent PID	3692
Bitness	32 Bit

Process #67: cmd.exe

ID	67
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: 214032, Reason: Child Process
Unmonitor End Time	End Time: 217133, Reason: Terminated
Monitor duration	3.10s
Return Code	0
PID	596
Parent PID	4364
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 outlook.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 214348, Reason: Child Process
Unmonitor End Time	End Time: 216295, Reason: Terminated
Monitor duration	1.95s
Return Code	0
PID	1640
Parent PID	596
Bitness	32 Bit

Process #69: cmd.exe

ID	69
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: 216166, Reason: Child Process
Unmonitor End Time	End Time: 218071, Reason: Terminated
Monitor duration	1.91s
Return Code	128
PID	752
Parent PID	4364
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 powerpnt.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 216398, Reason: Child Process
Unmonitor End Time	End Time: 218389, Reason: Terminated
Monitor duration	1.99s
Return Code	128
PID	4636
Parent PID	752
Bitness	32 Bit

Process #71: cmd.exe

ID	71
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: 217899, Reason: Child Process
Unmonitor End Time	End Time: 219607, Reason: Terminated
Monitor duration	1.71s
Return Code	128
PID	3076
Parent PID	4364
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 steam.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 218073, Reason: Child Process
Unmonitor End Time	End Time: 219358, Reason: Terminated
Monitor duration	1.28s
Return Code	128
PID	2096
Parent PID	3076
Bitness	32 Bit

Process #73: cmd.exe

ID	73
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: 219135, Reason: Child Process
Unmonitor End Time	End Time: 221679, Reason: Terminated
Monitor duration	2.54s
Return Code	128
PID	1204
Parent PID	4364
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 sqlservr.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 219362, Reason: Child Process
Unmonitor End Time	End Time: 221583, Reason: Terminated
Monitor duration	2.22s
Return Code	128
PID	4856
Parent PID	1204
Bitness	32 Bit

Process #75: cmd.exe

ID	75
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: 222406, Reason: Child Process
Unmonitor End Time	End Time: 224831, Reason: Terminated
Monitor duration	2.42s
Return Code	128
PID	3568
Parent PID	4364
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 thebat.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 222586, Reason: Child Process
Unmonitor End Time	End Time: 224182, Reason: Terminated
Monitor duration	1.60s
Return Code	128
PID	824
Parent PID	3568
Bitness	32 Bit

Process #77: cmd.exe

ID	77
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: 223699, Reason: Child Process
Unmonitor End Time	End Time: 225447, Reason: Terminated
Monitor duration	1.75s
Return Code	128
PID	3376
Parent PID	4364
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 thebat64.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 223912, Reason: Child Process
Unmonitor End Time	End Time: 225430, Reason: Terminated
Monitor duration	1.52s
Return Code	128
PID	2496
Parent PID	3376
Bitness	32 Bit

Process #79: cmd.exe

ID	79
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: 224887, Reason: Child Process
Unmonitor End Time	End Time: 227191, Reason: Terminated
Monitor duration	2.30s
Return Code	0
PID	2280
Parent PID	4364
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 thunderbird.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 225118, Reason: Child Process
Unmonitor End Time	End Time: 226763, Reason: Terminated
Monitor duration	1.65s
Return Code	0
PID	4120
Parent PID	2280
Bitness	32 Bit

Process #81: cmd.exe

ID	81
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: 226209, Reason: Child Process
Unmonitor End Time	End Time: 228427, Reason: Terminated
Monitor duration	2.22s
Return Code	128
PID	1252
Parent PID	4364
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 visio.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 226379, Reason: Child Process
Unmonitor End Time	End Time: 227659, Reason: Terminated
Monitor duration	1.28s
Return Code	128
PID	772
Parent PID	1252
Bitness	32 Bit

Process #83: cmd.exe

ID	83
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: 227469, Reason: Child Process
Unmonitor End Time	End Time: 229632, Reason: Terminated
Monitor duration	2.16s
Return Code	128
PID	1300
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #84: taskkill.exe

ID	84
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: 227658, Reason: Child Process
Unmonitor End Time	End Time: 229579, Reason: Terminated
Monitor duration	1.92s
Return Code	128
PID	4436
Parent PID	1300
Bitness	32 Bit

Process #85: cmd.exe

ID	85
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: 228656, Reason: Child Process
Unmonitor End Time	End Time: 231085, Reason: Terminated
Monitor duration	2.43s
Return Code	128
PID	4124
Parent PID	4364
Bitness	32 Bit

Host Behavior

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

Process #86: taskkill.exe

ID	86
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: 228831, Reason: Child Process
Unmonitor End Time	End Time: 231051, Reason: Terminated
Monitor duration	2.22s
Return Code	128
PID	4236
Parent PID	4124
Bitness	32 Bit

Process #87: cmd.exe

ID	87
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c "whoami >>C:\ProgramData\keEeR.txt"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 231518, Reason: Child Process
Unmonitor End Time	End Time: 236090, Reason: Terminated
Monitor duration	4.57s
Return Code	0
PID	3364
Parent PID	4364
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\keEeR.txt	6.32 KB	63422135392f683f9049b3b60daf70b13fc6607c1ff987ed93ffad30ec9bf3a9	✗

Host Behavior

Type	Count
Module	8
Registry	17
File	25
Environment	19
System	1
Process	1

Process #88: whoami.exe

ID	88
File Name	c:\windows\syswow64\whoami.exe
Command Line	whoami
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 232156, Reason: Child Process
Unmonitor End Time	End Time: 235996, Reason: Terminated
Monitor duration	3.84s
Return Code	0
PID	3224
Parent PID	3364
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027	C:\Users\RDhJ0CNFevzX\Desktop\ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe	Sample File	2012.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
9718159cbe798996e172405e0b10daa43085dad0a30d6e725d48e595f4b36d5c	C:\Users\Default\Saved Games\README.html, C:\Users\RDhJ0CNFevzX\Documents\README.html, C:\Users\RDhJ0CNFevzX\Documents\baXS\REA... ...Users\Default\Documents\README.html, C:\Users\Public\Pictures\README.html, C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\README.html	Dropped File	3.13 KB	text/html	Access, Write, Create	SUSPICIOUS
7dab70485d4de81700d23f0a5007c574e3ac4a66a56f407989711df86ab95836	C:\ProgramData\utbfPsCYzd	Dropped File	1.67 KB	text/plain	Access, Write, Create	CLEAN
46f339857c3409155aed24d6596fa7cf444c9d479c4b04ed76ba810e4a5e821c	C:\Users\RDhJ0CNFevzX\Desktop\ZH5t5F Pn3U-oGq.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
0130f926ed949d38f7ae774ebb192c95cda11452a3e3fde10565b95a713f1e44	C:\Users\RDhJ0CNFevzX\Desktop\ZH5t5F Pn3U-oGq.mp4.locked	Dropped File	38.81 KB	application/x-dosexec	Access, Write, Create	CLEAN
bac19dace0fda3b8a12dc6bfca94de94dbb8df96343d09437edecdf34d68951c	C:\Users\RDhJ0CNFevzX\Desktop\EMZ6NoSJq0-2xx6lW.wav	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
7c5fbc699323ca95871fb862bc4b7f7063d274b888b2a66853ec89cb2070b795	C:\Users\RDhJ0CNFevzX\Desktop\EMZ6NoSJq0-2xx6lW.wav.locked	Dropped File	91.44 KB	application/octet-stream	Access, Write, Create	CLEAN
df358f622a9386942fcde745d9147799b72d9000d4c5134cba081f2188f189d6	C:\Users\RDhJ0CNFevzX\Desktop\1TSkQagxs.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Write, Create	CLEAN
1c28054cd4a5608a651773aab1dd96bf858e5f46543b4371f3e2e243ade9f06d	C:\Users\RDhJ0CNFevzX\Desktop\9fTBKDfkIFX1UCW.avi	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
274f2c79636c8b2dd29f2d0dcdf176402a90e6a4c6bdff5f62224f7455aab18f	C:\Users\RDhJ0CNFevzX\Desktop\7qqVU2GatTMCj 1dpl.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
1757a80c92f814b344d0901bb87b2f1a0505e5cc1138bceefb5f03cec2e30e36	C:\Users\RDhJ0CNFevzX\Desktop\DWVUXEoQZyD.flv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
e3c9c22c51369609eeaa58ec7b3f96665a4d8d0c5451ed993c7b10d9d20feb7b	C:\Users\RDhJ0CNFevzX\Desktop_riLQBNOxB3yhpHCkj.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
fd642dbd292204ed7ade0877ff0fbd309abaa6c2e7790bb48f11c5f56a13582d	C:\Users\RDhJ0CNFevzX\Desktop\lcNKdj QY jlfR5.bmp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
5c758998b1a8fcc4a908f712022013a95dd69d0f53b2744f4f764965c67092e3	C:\Users\RDhJ0CNFevzX\Desktop\1TSkQagxs.mp3.locked	Dropped File	7.17 KB	application/octet-stream	Access, Write, Create	CLEAN
a44fd0a02e46844bd82bba5b09d0f72adf8f1f2fad82de6fb7f51cb5a6c8e11c	C:\Users\RDhJ0CNFevzX\Desktop\ddakMB.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
3bdb30eee41f93ac8a838c61cfcfc0b14c1a2b5706693af6939cdd4028678dac	C:\Users\RDhJ0CNFevzX\Desktop\PNIMo1Rui9-Os7LqiJYf.swf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
12868e326d1cdb4d18c5952c3fba492c035abc317b79a382b435f95141399a38	C:\Users\RDhJ0CNFevzX\Desktop\9fTBKDfkIFX1UCW.avi.locked	Dropped File	10.33 KB	application/octet-stream	Access, Create	CLEAN
1df7df6b8b17402d95ad9be9aa55a18d9590d2fd30af795ef0619ff03e8dcda4	C:\Users\RDhJ0CNFevzX\Desktop\PG2AA8VgUaJQix3.bmp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7e06fe1df3c7cd787ddae4e3b812eb63581429f213745bb49bdc5bbd4cfb3201	C:\Users\RDhJ0CNFevzX\Desktop\eT_8y6.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
b7bf1600d531f68e52cb2dc50cbc9144c05c0b5539635986674419b12ae14476	C:\Users\RDhJ0CNFevzX\Desktop\PCqRptQW6vY1N.gif	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
340280f09c93e8584621ccf5f1e504b629a141024520fb9605cbaa311fbef702	C:\Users\RDhJ0CNFevzX\Desktop\7qqVU2GatTMCj 1dpl.mkv.locked	Dropped File	57.12 KB	application/octet-stream	Access, Write, Create	CLEAN
64d154ae155f7cf0fc8020bfbe38f5b59e00dc7581a60d20a876a09187f7b0d2	C:\Users\RDhJ0CNFevzX\Desktop\DWVUXEoQZyD.flv.locked	Dropped File	33.53 KB	application/octet-stream	Access, Create	CLEAN
15d2eed348350e64ce6aae127605b2d10b1fb186569049a62844d9faee277d40	C:\Users\RDhJ0CNFevzX\Desktop_273Oz.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
e964527fdd8884e0ddb9e4646dd9febc734bd3cd168ea302dbdfa1f8789b2f3d	C:\Users\RDhJ0CNFevzX\Desktop\ddakMB.jpg.locked	Dropped File	69.42 KB	application/octet-stream	Access, Write, Create	CLEAN
11f8401c77927358e74769522c26ff5d7910412586377703bfa457521b3c66f16	C:\Users\RDhJ0CNFevzX\Desktop\IcNKdj QY jlfR5.bmp.locked	Dropped File	69.53 KB	application/octet-stream	Access, Write, Create	CLEAN
551333eb9bbac3cea69210f6966df67ff72602fbead1f3d0fa7b027eb6bf60a8	C:\Users\RDhJ0CNFevzX\Desktop_riLQBNOxB3yhpHCkj.mkv.locked	Dropped File	71.90 KB	application/octet-stream	Access, Write, Create	CLEAN
9e828e297d0cbd90a38cc2c771454b147e2e6a39c04d0a40731769015b115bf2	C:\Users\RDhJ0CNFevzX\Desktop\PNIMo1Rui9-Os7LqiJYf.swf.locked	Dropped File	97.74 KB	application/octet-stream	Access, Read, Write, Create	CLEAN
6aeacaba2377ba4418114c7603662af296feacf69af5dd0a69699e3a233f546f	C:\Users\RDhJ0CNFevzX\Desktop\PG2AA8VgUaJQix3.bmp.locked	Dropped File	58.09 KB	application/octet-stream	Access, Create	CLEAN
28910f59815ecf14e97389d54adb7d20dca6474a044e4cf660cc44857c30fb6f	C:\Users\RDhJ0CNFevzX\Desktop\eT_8y6.mp3.locked	Dropped File	2.25 KB	application/octet-stream	Access, Write, Create	CLEAN
6779db9e89823fbfa62e45320a7f3efc90171470442a80b63dab02a0ee93c750	C:\Users\RDhJ0CNFevzX\Desktop\PCqRptQW6vY1N.gif.locked	Dropped File	55.49 KB	application/octet-stream	Access, Write, Create	CLEAN
9bb51b95db56c3b365331978788611ca76feef1ff6849ae40ca9ce00d16e738d	C:\Users\RDhJ0CNFevzX\Desktop_273Oz.mp3.locked	Dropped File	30.37 KB	application/octet-stream	Access, Write, Create	CLEAN
ebceeec8ae6cc0200e8f21f0e2d19e79466b6dce71b987cd2d2eaf597d9cf111	C:\Users\RDhJ0CNFevzX\Desktop\QnyUe3Ugz.swf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
406b29834850bc8793f74559c8922b7f20721832641 66c60da03d31a49855a4c	C:\Users\RDhJ0CNFevzX\Desktop\PuTjWyxTe.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
1779cb433e2172f60a81f4280e4dbde4129ed3fd4416df2ae701b4462c3ac6f6	C:\Users\RDhJ0CNFevzX\Desktop\PuTjWyxTe.mp4.locked	Dropped File	65.59 KB	application/octet-stream	Access, Write, Create	CLEAN
cab619da12d3934031a2357f70bd7a33ba7cd065e5fecb41b2f36e26f6d20d63	C:\Users\RDhJ0CNFevzX\Desktop\QnyUe3Ugz.swf.locked	Dropped File	47.10 KB	application/octet-stream	Access, Write, Create	CLEAN
57b4e8c1150744579500b9733d096a59a86db92abdfd15f9022bf94841936017	C:\Users\RDhJ0CNFevzX\Desktop\SEX0J5RG1Om3TZ.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
e0cf58a211329a09b33f1e2a4a3d6d1881fff756031032fee69a26798885c262	C:\Users\RDhJ0CNFevzX\Desktop\SEX0J5RG1Om3TZ.mp4.locked	Dropped File	61.45 KB	application/octet-stream	Access, Write, Create	CLEAN
66a0de9412bc8e07225dbb1dfb3eaf7a2051b2e0c3153bbc5388c3af1a644506	C:\Users\RDhJ0CNFevzX\Desktop\gKB9m3gAI3.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
af0c2f50a027001637cc32cab9357d11b5dd133e5c6aee31141c0eae4a9a28f1	C:\Users\RDhJ0CNFevzX\Desktop\ivion.png	Dropped File	1000.00 KB	text/plain	Delete, Access, Write, Create	CLEAN
3c9ddb6179eddf2c8e0daa83ccf176ff9e8515be6747776c9a21731d024f84a6	C:\Users\RDhJ0CNFevzX\Desktop\gKB9m3gAI3.mp4.locked	Dropped File	6.06 KB	application/octet-stream	Access, Read, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
308b7f9e412061777715a63ce55a972e9d65d432e713081bc6b58e66284a4775	C:\Users\RDhJ0CNFevzX\Desktop\ivion.png.locked	Dropped File	92.82 KB	application/octet-stream	Access, Write, Create	CLEAN
2bd40cc9adc73a27b9c2ae5ff81d02e984cdff2d3104a2bab8896f76d48b293a	C:\Users\RDhJ0CNFevzX\Desktop\kY10RHpj1Ccj R.png	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
e44dcf3117b1ca5c60b340524868de84ce9cdedbe46bdd438172dcd4fc539112	C:\Users\RDhJ0CNFevzX\Desktop\o7c4LDm2F7lcu2v.wav	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
6e3d6e4c1d8dccb8121d61d69a6ab3f7b2085ab3831344d6d78c7f561d45b1ac	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\ZA606Y.rtf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
3115f55e4dec7239f612ada62f634515fdf34bf7ec9ca15224872c59eba61409	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\0C0imTxCn.mp3	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
88b05e5b402e6ccee8890dd2019bfeed9a38f0f3bd15fe07fc624e5f7d53373b	C:\Users\RDhJ0CNFevzX\Desktop\o7c4LDm2F7lcu2v.wav.locked	Dropped File	4.34 KB	application/octet-stream	Access, Read, Write, Create	CLEAN
5e55ba7e245439512885932e92ea4efdf45eb5d74d753ead20aa9b9d4630e1d0	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\ZA606Y.rtf.locked	Dropped File	58.39 KB	application/octet-stream	Access, Write, Create	CLEAN
7b8daee4b9a7b35ced48d2286f29d8e72e37647175bfe585713d5b7c484cff02	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\0C0imTxCn.mp3.locked	Dropped File	91.83 KB	application/octet-stream	Access, Write, Create	CLEAN
00f99228ffff505e53dbca6043cc42162f3a34ab1ab1142346028e60ca4b3bc2	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\C5Fa.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
02c0643cf06db0d07c3f4b674119ba506e4a2463b7e7790af04a9d2740f24c00	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\C5Fa.mkv.locked	Dropped File	91.31 KB	application/octet-stream	Access, Write, Create	CLEAN
4590bf60768034519ab4d41ca2dd0702a09026a3f5953627201e798de69ab84f	C:\Users\RDhJ0CNFevzX\Desktop\wpUR.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
80d2bfbb6e3b704554beddde9ca055adfd4dad4fd0b1b89bc5b9945c5c02365	C:\Users\RDhJ0CNFevzX\Desktop\wpUR.mp4.locked	Dropped File	77.17 KB	application/octet-stream	Access, Write, Create	CLEAN
65bd68accb0ac85426b9893ba91a8de1521fc5aee501cfdfa332091de1962804	C:\Users\RDhJ0CNFevzX\Desktop\kY10RHpj1Ccj R.png.locked	Dropped File	86.07 KB	application/octet-stream	Access, Write, Create	CLEAN
225410108acdeb269576578082ea9598410a9395c86e7291a9c47b3e6b61e48e	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj_2Qs2D.odp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
6ce1fd442b45344283a13c3b81b84606c7e21e11d32b2545e59d1a6d10e3fc12	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj_2Qs2D.odp.locked	Dropped File	4.97 KB	application/octet-stream	Access, Write, Create	CLEAN
4d648a5ce80d9288f4ba445a79e1773326004bbb3f65ec34f179326d29e7fd6c	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\ynl0nO8fmos3T.mp4	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
d5c9b320c67cdf1ec7f73e8cfc90f4553b6230d8767e04b606a52a7d73db7891	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\7pK8Q9_TXKB_8t_99Nak.gif	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
5207ca89e45d9182296af798ee1a540e65ebaa587fd54f9f3291a94893389837	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\ynl0nO8fmos3T.mp4.locked	Dropped File	64.07 KB	application/octet-stream	Access, Read, Create	CLEAN
e5201b6cbc6946cc75437903a4dce7ddbfeb02c3cdc594950d30375477b7eb89	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\pQ4D7olyLasPf6h0yK.flv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
9e0aac4a30f76a216f8575d1d19e304f938e44adc17d1a42ad47f0b2b06cc66b	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\pQ4D7olyLasPf6h0yK.flv.locked	Dropped File	53.57 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
31bf3eb483dc3644fabfd24dc5f0d07a54e15a76b34893f5e40288886a817f85	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\7pK8Q9_TXKB_8t_99Nak.gif.locked	Dropped File	75.36 KB	application/octet-stream	Access, Write, Create	CLEAN
3d3bedb4c4da7a67c8d7e1fc8cf456a3ac541e8fd1f084c7724053c04458eb49	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\53CjZJnv.avi	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
9240c572eae2a0115c0594f6b98780027cf0bd5ced0635d6bec79239645478eb	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\53CjZJnv.avi.locked	Dropped File	15.35 KB	application/octet-stream	Access, Write, Create	CLEAN
4d4c58e0165c8dd45df96aefb7166a29fbb4ab93da5a080cf10800c6deb5ad31	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\-tLx.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
d85ace7327931a467ebad76ac93ed7c870f8cf2e537acb4d8ed187b5832d24db	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\-tLx.jpg.locked	Dropped File	50.30 KB	application/octet-stream	Access, Write, Create	CLEAN
5be4ef565773f5a14b843595f5ea1b65080e58821c6b691b3e99095ffb365325	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\WqsBnn5V5.flv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
06c4a5bb15161402e1bd494370abaf284020c32bcf388100056fb197befbbbd91	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\WqsBnn5V5.flv.locked	Dropped File	48.22 KB	application/octet-stream	Access, Write, Create	CLEAN
9a007151d6178367b5806f315d5abd6be2711d38c2312be0398272a624971cec	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\2l YP.mkv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
d74e0c2920e9dd98918c7b1335a784fa9f6104823528e84f043396869c002ab7	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\2l YP.mkv.locked	Dropped File	70.25 KB	application/octet-stream	Access, Write, Create	CLEAN
83c14d1e5a5a45cc453834d6aeb1fcc4bb88303a60498ba7ebe8952a9ce09b77	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\YRFgwGf0zYgcMX.flv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
4d641e6f56b3557c24a2fc3b5c2a2678d101609fde1b8ad7eb4160b1db39b29d	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\zMPTOdNQ.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
91d9e96f96337f84135d4b68cf1cf92ca7ba7a7ff9178f27243746274435330f	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\YRFgwGf0zYgcMX.flv.locked	Dropped File	20.53 KB	application/octet-stream	Access, Write, Create	CLEAN
75118dba30c93e2d6632861d6fdaefc051214e7f61a1918b8cc709d1cb8ecc7b	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\zMPTOdNQ.jpg.locked	Dropped File	67.86 KB	application/octet-stream	Access, Write, Create	CLEAN
b98d202317823f20d06b268d562a1e642b498c67054f8237ab6bc184c90891cb	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\P-STq-jQ5hYtJhlu5S.ots	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
1dcb69984aee4888a95ef5305973e6688b8b07f1c708248607089bbcecb690fd	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\P-STq-jQ5hYtJhlu5S.ots.locked	Dropped File	99.37 KB	application/octet-stream	Access, Write, Create	CLEAN
8f5eaa86b38a5db7b0bb07ecf5f2b2a7658a792807bb45018dc7be28121ef107	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\7g-3nq2zvxE4VIk.png	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
62cf2a4c92217d067bdec832ad7d97bf80db7e9e63fcf8e96d45dc4604d49314	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\RqMHt Jbqykr-i2R.jpg	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
f07d2a35204689504d5c86e357dffa319a1ee29110e907c3862b7d11597cab4c	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\7g-3nq2zvxE4VIk.png.locked	Dropped File	82.84 KB	application/octet-stream	Access, Create	CLEAN
5ac7129ffe9e16211c18a7f29171fc555ab4de90d2f381295b5a69d544a303e0	C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\RqMHt Jbqykr-i2R.jpg.locked	Dropped File	92.63 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b5054120b83b3afb89b2885d3c8edcbf451e2b407d367d394fd4d3c3bdd7d5f9	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\dbMm7g.png	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
feeebc81478c3c50a5532e7238f9ebd7f5cd22de6632474100208dd4d9c366fe	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\dbMm7g.png.locked	Dropped File	42.67 KB	application/octet-stream	Access, Write, Create	CLEAN
1cd8845c7a70f64e877a208ef74c511bdd454687625a9a7a836567208dd74bf8	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\1s4d3CDN.flv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
8fd5cead50508768993d6eee7c710331d39455c684d00751d4e64e28b2d50a23	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\1s4d3CDN.flv.locked	Dropped File	93.97 KB	application/octet-stream	Access, Write, Create	CLEAN
8be46b6d1b644539a8b48ec4e38722fbaca73beb45bca4fd003267be10e495d6	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\pVnv3JR1eBRll.xls	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
efa0020c434254fbd16073d682aa7f0de53afd59505a0b9bbaa6445d7c59fcda	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\pVnv3JR1eBRll.xls.locked	Dropped File	13.84 KB	application/octet-stream	Access, Write, Create	CLEAN
135490743b2ea5d2280f2b300f9a41939a7433c9ac0ed6a00f6099142ab51ac2	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\xxYCYyYbKsjdn.swf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
eebedae32c786be9e86454323110415afb8a5303ac4c4a6e9f617705f189d10f	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\YqAV-p.bmp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
ac00e8510d80337baa045eb1e154eb2170c086ee9cad268179d366a50ebf8ceb	C:\Users\RDhJ0CNFevzX\Documents\4hjR_qw1PrF.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
f6a400ba4dc86579c02fcf9e7d6c4c64cca73b1834de47085b418acf0afd79f5	C:\Users\RDhJ0CNFevzX\Documents\4hjR_qw1PrF.docx.locked	Dropped File	9.93 KB	application/octet-stream	Access, Write, Create	CLEAN
8ef4c87b0429b30f5bb800f50f751ae277ee33101f3b7b9f654d93e908109f2e	C:\Users\RDhJ0CNFevzX\Documents\4R8gdYA15.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
379e417377eaed3f14b2c6b775a793baa332e086a125a2dba17c49e528cf19ad	C:\Users\RDhJ0CNFevzX\Documents\4R8gdYA15.docx.locked	Dropped File	49.95 KB	application/octet-stream	Access, Write, Create	CLEAN
d5c06a6393afe21a4b1d0c2bfad1fab89d6a76f79f2bb19d18ed16228694b12d	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\xxYCYyYbKsjdn.swf.locked	Dropped File	35.94 KB	application/octet-stream	Access, Read, Write, Create	CLEAN
e93a7279d3a83dc260bb7528dfbee464f3c7044fca619c4d5f6e8d7a12c8ef5b	C:\Users\RDhJ0CNFevzX\Desktop\yJUz3WLu\u5XgcDVp\YqAV-p.bmp.locked	Dropped File	8.75 KB	application/octet-stream	Access, Write, Create	CLEAN
f49f835eb2240fd4995a597c4df1d3891349b245f8e23085854e54fa80f1b319	C:\Users\RDhJ0CNFevzX\Documents\CX3dvz.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
593e35e1f3ee39968d18850dc66ba3cdeb1155fcb1673bb13a7bcc8a4fc52287	C:\Users\RDhJ0CNFevzX\Documents\CX3dvz.pptx.locked	Dropped File	79.35 KB	application/octet-stream	Access, Write, Create	CLEAN
4bba66e28582e311f5da43570eb021292c99f7e206ebddddd5745ae9db75e0a0c	C:\Users\RDhJ0CNFevzX\Documents\9Q7-bFR.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
160c1e7b5231537b228392520372fd7e43ac978f7dbdae6f535a918b71019424	C:\Users\RDhJ0CNFevzX\Documents\9Q7-bFR.xlsx.locked	Dropped File	89.61 KB	application/octet-stream	Access, Write, Create	CLEAN
e076d82e0f0902840204365db0f0a11769a75ec0114048078c40acaff3b776af	C:\Users\RDhJ0CNFevzX\Documents\Ej4CnCJUCwn5 nF.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
b5f080255531370992138922b58ce6c93f825803364f914629b83871b01fe69d	C:\Users\RDhJ0CNFevzX\Documents\Ej4CnCJUCwn5 nF.docx.locked	Dropped File	85.51 KB	application/octet-stream	Access, Write, Create	CLEAN
b26e03640fb92fc853a234d4783a0f32c5fb0de108ba71da50d4354f8023e7a1	C:\Users\RDhJ0CNFevzX\Documents\Crvhk0MgLr2QKx _m.pdf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
af7433bff9bb5f6f13cb05d289ff22ad73dc1dade6000709d6864f54c0fc3f52	C:\Users\RDhJ0CNFevzX\Documents\GPvOBFfXu_XAefB06.doc	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
304ed6e28249765a8a25a383ad63361a180145006917ac6614460df06f3634f8	C:\Users\RDhJ0CNFevzX\Documents\GPvOBFfXu_XAefB06.doc.locked	Dropped File	30.13 KB	application/octet-stream	Access, Write, Create	CLEAN
6512270250927a179594c364c927ccbaacd452149e539e4ba56ad45a8ec15a90	C:\Users\RDhJ0CNFevzX\Documents\PksQcVAF-FVG.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
433bd3caa64069c428f338162e37e0bcd773a250d6f7b2947327ebed6946a936	C:\Users\RDhJ0CNFevzX\Documents\PksQcVAF-FVG.docx.locked	Dropped File	68.76 KB	application/octet-stream	Access, Write, Create	CLEAN
7f69ac5c64b05a826cd683e34f991797e935ee81c22363810e612c23ed79011c	C:\Users\RDhJ0CNFevzX\Documents\5yfr.docx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
d30384b0fd662bff161b1b60412846e00f22d714cd805fbfc641d92234bd7943	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
268817fe9b4b0ef357ad90f2dc7af6a709b9c10a167c997a1c877236e53f1740	C:\Users\RDhJ0CNFevzX\Documents\5yfr.docx.locked	Dropped File	39.39 KB	application/octet-stream	Access, Write, Create	CLEAN
b1ba2598049bd30f9bd0056ae5f8a5c8a74e553664b2370fcb9f888258d72406	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.locked	Dropped File	265.12 KB	application/octet-stream	Access, Write, Create	CLEAN
df823390cf6e18bd1708e65f06a64b5a837cde6a64884ddec3636922dfadf63f	C:\Users\RDhJ0CNFevzX\Documents\Crvhk0MgLr2QKx _m.pdf.locked	Dropped File	8.83 KB	application/octet-stream	Access, Write, Create	CLEAN
4873be4a46d8e49bd558a0b1de217304b9869cc828242b0c4dc2fc5d59856152	C:\Users\RDhJ0CNFevzX\Documents\VupTUE7Pb.xls	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
283fdb30371e26b4370f341a041b71a17781d42c72d8b0e0b8fb05b0a0927cc1	C:\Users\RDhJ0CNFevzX\Documents\lfzi1.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
bc9141e194a179610fd8016e4bfb0eb7f9332cb9a5fb1ba2f2cb6b9a7b460f24	C:\Users\RDhJ0CNFevzX\Documents\XxX9zS.ods	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
2acf8925f41af1b414a34ca7e2a386d3a7d4ffaaa745bf5899a85a233df25fa9	C:\Users\RDhJ0CNFevzX\Documents\baXS\00jJreyg.doc	Dropped File	1000.00 KB	text/plain	Delete, Access, Write, Create	CLEAN
eda9e180d7cfc235ea2d6905e8897c8193b1ac58c9cc72b0349b0dc913b5d00f	C:\Users\RDhJ0CNFevzX\Documents\baXS\00jJreyg.doc.locked	Dropped File	9.56 KB	application/octet-stream	Access, Create	CLEAN
d4b461015c70516433e435efc92c5fb627fb5dcd4cc2b0522efe4893732e8f2a	C:\Users\RDhJ0CNFevzX\Documents\UYS dfMqbVg.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
ce24bbe8890b920357eb83c28fbe6f83e1823e007a311eae7a106d290e45a3f6	C:\Users\RDhJ0CNFevzX\Documents\VupTUE7Pb.xls.locked	Dropped File	6.04 KB	application/octet-stream	Access, Create	CLEAN
2a9230a27f5c45d9ac7ca7a388038b42fd3b06587e63899e31e0760580905472	C:\Users\RDhJ0CNFevzX\Documents\lfzi1.xlsx.locked	Dropped File	99.82 KB	application/octet-stream	Access, Write, Create	CLEAN
807632d166cd7a7dd2d525fefe768794799fd528e8300e811d0e07d5ec859d2b	C:\Users\RDhJ0CNFevzX\Documents\baXS\8NTFMxPNLnS-.xlsx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
0d3116f74f33d7be4d892fcf22224b2c7fbef4bcbe8b504006295b0dc7b32e65	C:\Users\RDhJ0CNFevzX\Documents\XxX9zS.ods.locked	Dropped File	9.00 KB	application/octet-stream	Access, Write, Create	CLEAN
ca9490a39e07d6b00aa1efe51adab1fe09744dbe52cb0cf55c46f56a517c0b28	C:\Users\RDhJ0CNFevzX\Documents\baXS\8NTFMxPNLnS-.xlsx.locked	Dropped File	52.99 KB	application/octet-stream	Access, Write, Create	CLEAN
2ac492f6b6c5acdfad585daa708bb917558861ba6233ead834a3c471abf8903a	C:\Users\RDhJ0CNFevzX\Documents\TP7qaB_8RwFo0zi2S F.ods	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
7ce3ebc7e017ab16d263bd43a5c0aba4cbf6a82cd616210f53eb5b27e38971c3	C:\Users\RDhJ0CNFevzX\Documents\UYS dfMqbVg.xlsx.locked	Dropped File	68.24 KB	application/octet-stream	Access, Read, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
aadd90b2a04d4a5bf29db011c9d9ebf0c946244437ab7570b418c3abc6a6214d	C:\\Users\RDhJ0CNFevzX\Documents\TP7qaB_8RwFo0zi2S F.ods.locked	Dropped File	24.86 KB	application/octet-stream	Access, Write, Create	CLEAN
fe819089a3934cba4856a4b160d39f277c4894a9a0bee3cc3961493e898935f0	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\0ToZccO18urTblN.rtf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
78d5f197e2895f48be3e472d18aa86adf34b54e5f1a47e7afe22d4d9287d72ba	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\0ToZccO18urTblN.rtf.locked	Dropped File	7.07 KB	application/octet-stream	Access, Write, Create	CLEAN
4df541c2ce2a78af6e134401ae20c0b78fbffa154bb7da9027cc564c4f67b3eb	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\4bt-B2q.pdf	Dropped File	1000.00 KB	text/plain	Delete, Access, Write, Create	CLEAN
675edf71e75b6eb717a0cc5cede59daae9f43a51f9267558d188332c60dc81b7	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\6wvQVTWOr1.doc	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
402b62bf82819c32cfb4dae436e5f210c80b6e0f9f304a8cc8469fcdbbbbeae6	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\4bt-B2q.pdf.locked	Dropped File	68.35 KB	application/octet-stream	Access, Write, Create	CLEAN
8ae8a53987f5a526869c7aad5027f55452a9d385fab838f5c52e98f773fbc181	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\6wvQVTWOr1.doc.locked	Dropped File	97.78 KB	application/octet-stream	Access, Write, Create	CLEAN
675207649ab053d16ece358265d7c98a3b7244a773ce144d1dd81e1cf05eaf98	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\8BJrk8.pps	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
5b7ccb378565d28251469179d9bdb4b30641c251d87bd3b3e65eec23a32bfae8	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\7NGgJCF9p1sXP7bTM6Xc.odp	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
9d7bd017aff1d9ba17d723a645e962922a5fb217ab91b831fd8bc8484f56e49a	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\CJfBVMezWzfCMgvFYwf.ots	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
dcbbf55e1ec038794272129ced08ab8ce57a977c97f9192323fd56ad32c92e45	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\8BJrk8.pps.locked	Dropped File	81.91 KB	application/octet-stream	Access, Write, Create	CLEAN
22ea756bc8b8817cbaa0f55a5048e59158af44edbd243deed0ce785fb46fe4d9	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\7NGgJCF9p1sXP7bTM6Xc.odp.locked	Dropped File	19.39 KB	application/octet-stream	Access, Write, Create	CLEAN
80014362c63ed28cb1afcb865b2a8de2420f270c0c287a69962e2f4df280acad	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\L-u71CPit811c.xls	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
737b8d02ebddb6c9b5e0202b727b7c2b7b12365122cea1a2ad8671d71bfa9740	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\CJfBVMezWzfCMgvFYwf.ots.locked	Dropped File	60.53 KB	application/octet-stream	Access, Write, Create	CLEAN
fa943eebc7fa03ddc82099666cb18f63e0c22ac40f4414b6427d619ec8248e8f	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EzIWVPEgGWw7Xy7.ods	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
704afe1f68cac1a0963ea7210441b32384f1e97678d44b79ecfd864c34e2a4f8	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\L-u71CPit811c.xls.locked	Dropped File	38.46 KB	application/octet-stream	Access, Write, Create	CLEAN
a1b4d2a0b2f326f54dd72095350fc70993bd491e973dc6468918aaefc05d3817	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EzIWVPEgGWw7Xy7.ods.locked	Dropped File	68.03 KB	application/octet-stream	Access, Write, Create	CLEAN
1f771f822ff1697a5ddf5c61086c8051a77d78c8f9f10fa14f7c077131818de0	C:\\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\GFqXQi80UXX3UPgD.pdf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
70b74d6178d2e54209a777fccb34a00088fae9d3d514018b12c269f4bf7d63ed	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\GFqXQi80UXX3UPgD.pdf.locked	Dropped File	10.14 KB	application/octet-stream	Access, Create	CLEAN
812bd6f9e42110e5813151e1db9789d17e347086ec52b7baa9424723b28ded75	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EPo8_m0ryn 6ACWfcC.doc	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Create	CLEAN
384872b45a20e19d2e1018f065087430c857f7f3430314fc6866d85c4695ce6b	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\EPo8_m0ryn 6ACWfcC.doc.locked	Dropped File	72.51 KB	application/octet-stream	Access, Write, Create	CLEAN
40052ad93892329ebeb4a2259429345ccdd21353ccf0e7fccfddc17f962d3672	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\nRY0tYZ9Ff0noTxW-ck.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
46351e77ad05db8285e83c0394f400b413f56ff85b0e45cbe512dd29b062a1d9	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\v4ns79y.pptx	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
91795ec5ded0ae2d9fb849f03141e94b01e2bd1f337c7b87be1fee233a4c4d42	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\O4XyZ4ZdDUL8nyTp.csv	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN
e3c4459f266441abe87f4bf1e7823ba59a7b01617cafa4f23e78999b1ba587ef	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\nRY0tYZ9Ff0noTxW-ck.pptx.locked	Dropped File	99.31 KB	application/octet-stream	Access, Write, Create	CLEAN
8cc277a3a44b7e2d8dd83bc5ea7c045531ac45fd42fabc216a90e6c5bcc47a29	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\v4ns79y.pptx.locked	Dropped File	63.08 KB	application/octet-stream	Access, Write, Create	CLEAN
b3b25f48305f8e1a292f5726c744c19cc39de924117859706b8d7ebfd04decc5	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\O4XyZ4ZdDUL8nyTp.csv.locked	Dropped File	16.06 KB	application/octet-stream	Access, Write, Create	CLEAN
ec78013ddaaee1c6f91b5df1d8a28eb5dbef826c3ae325bc690597a4a450a0ea	C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\vTjM.rtf	Dropped File	1000.00 KB	text/plain	Delete, Access, Read, Write, Create	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\\PerfLogs\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
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

File Name	Category	Operations	Verdict
NUL	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\e.bat	Accessed File	Access	CLEAN
C:\	Accessed File	Access	CLEAN
C:\a.bat	Accessed File	Access	CLEAN
C:\ProgramData\utbfPsCYzd	Dropped File	Access, Write, Create	CLEAN
C:\ProgramData\keEeR.txt	Dropped File	Access, Write, Create	CLEAN
A:\	Accessed File	Access	CLEAN
B:\	Accessed File	Access	CLEAN
C:\\PerfLogs	Accessed File	Access	CLEAN
C:\\Recovery	Accessed File	Access	CLEAN
C:\\Users	Accessed File	Access	CLEAN
C:\\Users\Default	Accessed File	Access	CLEAN
C:\\Users\Default\Desktop	Accessed File	Access	CLEAN
C:\\Users\Default\Documents	Accessed File	Access	CLEAN
C:\\Users\Default\Downloads	Accessed File	Access	CLEAN
C:\\Users\Default\Favorites	Accessed File	Access	CLEAN
C:\\Users\Default\Links	Accessed File	Access	CLEAN
C:\\Users\Default\Music	Accessed File	Access	CLEAN
C:\\Users\Default\Pictures	Accessed File	Access	CLEAN
C:\\Users\Default\Saved Games	Accessed File	Access	CLEAN
C:\\Users\Default\Videos	Accessed File	Access	CLEAN
C:\\Users\Public	Accessed File	Access	CLEAN
C:\\Users\Public\AccountPictures	Accessed File	Access	CLEAN
C:\\Users\Public\Desktop	Accessed File	Access	CLEAN
C:\\Users\Public\Documents	Accessed File	Access	CLEAN
C:\\Users\Public\Downloads	Accessed File	Access	CLEAN
C:\\Users\Public\Libraries	Accessed File	Access	CLEAN
C:\\Users\Public\Music	Accessed File	Access	CLEAN
C:\\Users\Public\Pictures	Accessed File	Access	CLEAN
C:\\Users\Public\Videos	Accessed File	Access	CLEAN
C:\\Users\RDhJ0CNFevzX	Accessed File	Access	CLEAN
C:\\Users\RDhJ0CNFevzX\Contacts	Accessed File	Access	CLEAN
C:\\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\baXS	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Downloads	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Favorites	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Favorites\Links	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Links	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\A_vsPrHANVz-cnbD2	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\Yjsf	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\YjsfljvLuJscJOug	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\YjsfljvLuJscJOug\ZvLJyDLOgo	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\YjsfljvLuJscJOug\ZvLJyDLOgo\YibDx1iNotnzBWQf	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\YjsfljvLuJscJOug\ZvLJyDLOgo\YibDx1iNotnzBWQf\8GJ8o0z9Qy_3x90hPI8	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\YjsfljvLuJscJOug\pqkT0R1dikE	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Music\Jbo1FZx\KcRwHRb9GRYnTCwA\w158lXmEu7fV	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\OneDrive	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks\MgwF6NEdCmu8wRMced1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks\MgwF6NEdCmu8wRMced1\Dju4ZgDG1-unlMg	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks\MgwF6NEdCmu8wRMced1\bOgs768mC0sZS6u	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks\MgwF6NEdCmu8wRMced1\zOpDqT28-XSK3u	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks\MgwF6NEdCmu8wRMced1\zOpDqT28-XSK3u\Y7n QDyh jI	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks\j5yJ	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\eDM5D-EmY4\EL7ncsIzIojJ_a9Ks\tX9_ewqicQ_n-v	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\wW1ws0e	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Saved Games	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Searches	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Videos	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Videos\UQ6zmB-l2xOZ	Accessed File	Access	CLEAN
D:\	Accessed File	Access	CLEAN
E:\	Accessed File	Access	CLEAN
F:\	Accessed File	Access	CLEAN
G:\	Accessed File	Access	CLEAN
H:\	Accessed File	Access	CLEAN
I:\	Accessed File	Access	CLEAN
J:\	Accessed File	Access	CLEAN
K:\	Accessed File	Access	CLEAN
L:\	Accessed File	Access	CLEAN
M:\	Accessed File	Access	CLEAN
N:\	Accessed File	Access	CLEAN
O:\	Accessed File	Access	CLEAN
P:\	Accessed File	Access	CLEAN
Q:\	Accessed File	Access	CLEAN
R:\	Accessed File	Access	CLEAN
S:\	Accessed File	Access	CLEAN
T:\	Accessed File	Access	CLEAN
U:\	Accessed File	Access	CLEAN
V:\	Accessed File	Access	CLEAN
W:\	Accessed File	Access	CLEAN
X:\	Accessed File	Access	CLEAN
Y:\	Accessed File	Access	CLEAN
Z:\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\\Recovery\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Desktop\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Documents\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Downloads\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Favorites\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Links\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Music\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Pictures\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Saved Games\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Default\Videos\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\AccountPictures\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\Desktop\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\Documents\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\Downloads\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\Libraries\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\Music\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\Pictures\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\Public\Videos\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\Contacts\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\Desktop\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\README.html	Dropped File	Access, Write, Create	CLEAN
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\b1s7y96Y6gVCDj\README.html	Dropped File	Access, Write, Create	CLEAN
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\bHSVytOE\README.html	Dropped File	Access, Write, Create	CLEAN
C:\ \Users\RDhJ0CNFevzX\Desktop\yjUz3WLu\u5XgcDVp\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\Documents\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\Documents\Outlook Files\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\Documents\baXS\README.html	Dropped File	Access, Write, Create	CLEAN
C:\ \Users\RDhJ0CNFevzX\Documents\baXS\AZLma79E0y7Lx7ST0eS\README.html	Dropped File	Access, Write, Create	CLEAN
C:\\Users\RDhJ0CNFevzX\Downloads\README.html	Dropped File	Access, Write, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Favorites\README.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Favorites\Links\README.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Links\README.html	Dropped File	Access, Write, Create	CLEAN

Reduced dataset

IP

IP Address	Domains	Country	Protocols	Verdict
193.56.28.159	-	United Kingdom	TCP	CLEAN

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
ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.exe	"C:\Users\RDhJ0CNFevzX\Desktop\ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027.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 "schtasks /delete /tn WM /F "	CLEAN

Process Name	Commandline	Verdict
schtasks.exe	schtasks /delete /tn WM /F	CLEAN
cmd.exe	cmd.exe /c "del C:\e.bat"	CLEAN
cmd.exe	cmd.exe /c "del C:\a.bat"	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
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

Process Name	Commandline	Verdict
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
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

Process Name	Commandline	Verdict
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
cmd.exe	cmd.exe /c "whoami >>C:\ProgramData\keEeR.txt"	CLEAN
whoami.exe	whoami	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