MALICIOUS

Classifications: Ransomware, Wiper

Threat Names: Gen:Heur.Ransom.MSIL.1

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
Sample Name	**333.exe**
ID	#2182084
MD5	162cde379f01cda83e24ada7e04a2964
SHA1	990932e10b61de6357afa716fe2e66a6cedad25e
SHA256	ebfa81cf52743de40734c2aea01466c47d8c18d9fa663c897614756652e56b5c
File Size	314.50 KB
Report Created	2021-04-26 15:04 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 12 matches)

Score	Category	Operation	Count	Classification
4/5	System Modification	Disables a crucial system tool	1	-
	• (Process #1) 333.exe disables the Task Manager via registry.			
4/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) 333.exe modifies the content of multiple user files.			
4/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #1) 333.exe deletes multiple user files.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Gen:Heur.Ransom.MSIL.1".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) 333.exe adds "empty" to Windows startup via registry.			
1/5	Hide Tracks	Changes folder appearance	4	-
	• (Process #1) 333.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures". • (Process #1) 333.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\camera roll". • (Process #1) 333.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\saved pictures". • (Process #1) 333.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\documents".			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 333.exe enables process privilege "SeDebugPrivilege".			
1/5	Input Capture	Monitors mouse movements and clicks	1	-
	• (Process #1) 333.exe frequently reads the state of a mouse button by API.			
1/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #1) 333.exe creates an above average number of files.			

Mitre ATT&CK Matrix

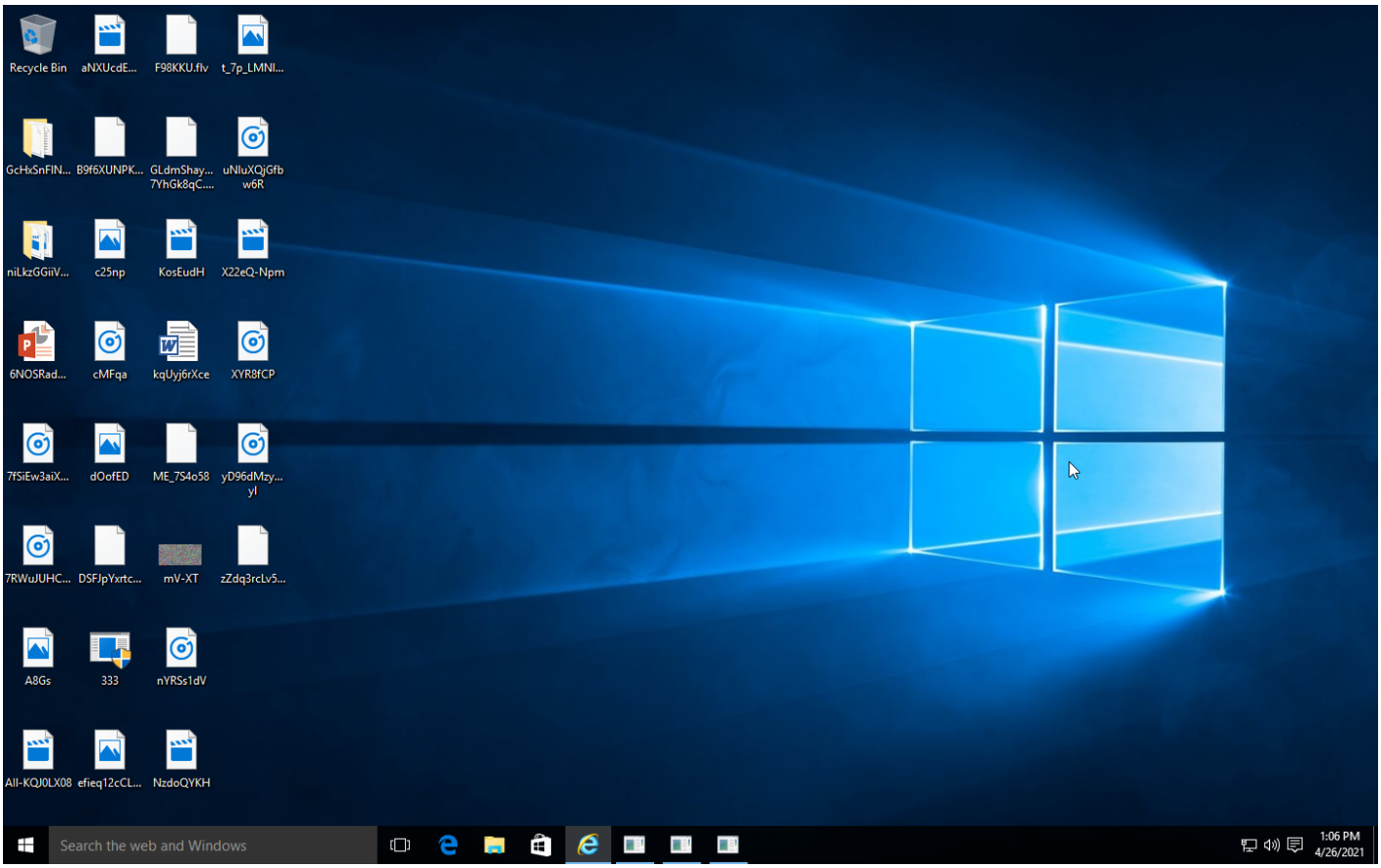
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	-	#T1060 Registry Run Keys / Startup Folder	-	-	-	-	-	-	-	-	-
-	-	-	-	#T1112 Modify Registry	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	#T1490 Inhibit System Recovery
-	-	-	-	-	-	-	-	-	-	-	#T1486 Data Encrypted for Impact
-	-	-	-	-	-	-	-	-	-	-	#T1485 Data Destruction
-	-	-	-	#T1036 Masquerading	-	-	-	-	-	-	-
-	-	-	-	-	#T1056 Input Capture	-	-	#T1056 Input Capture	-	-	-

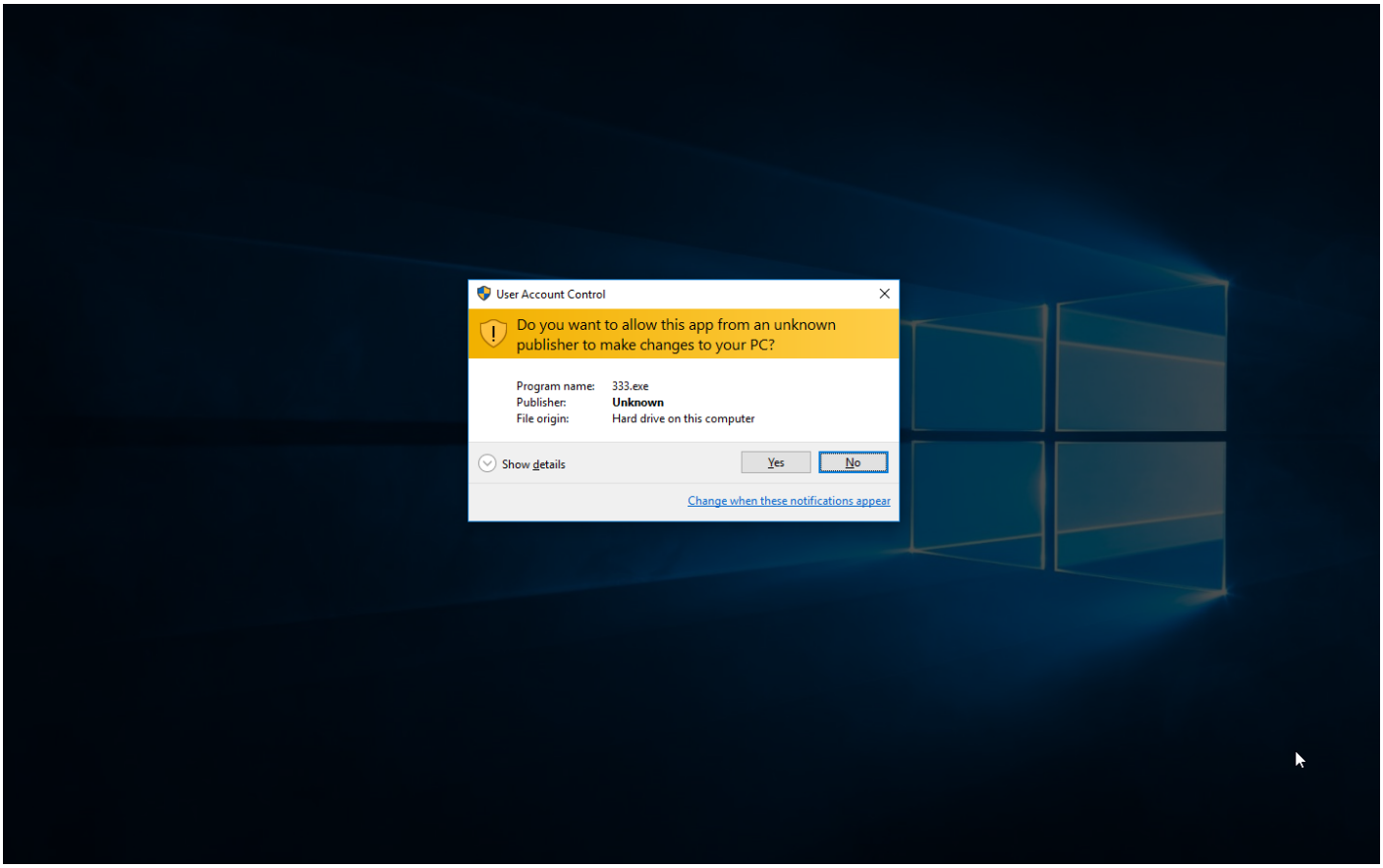
Sample Information

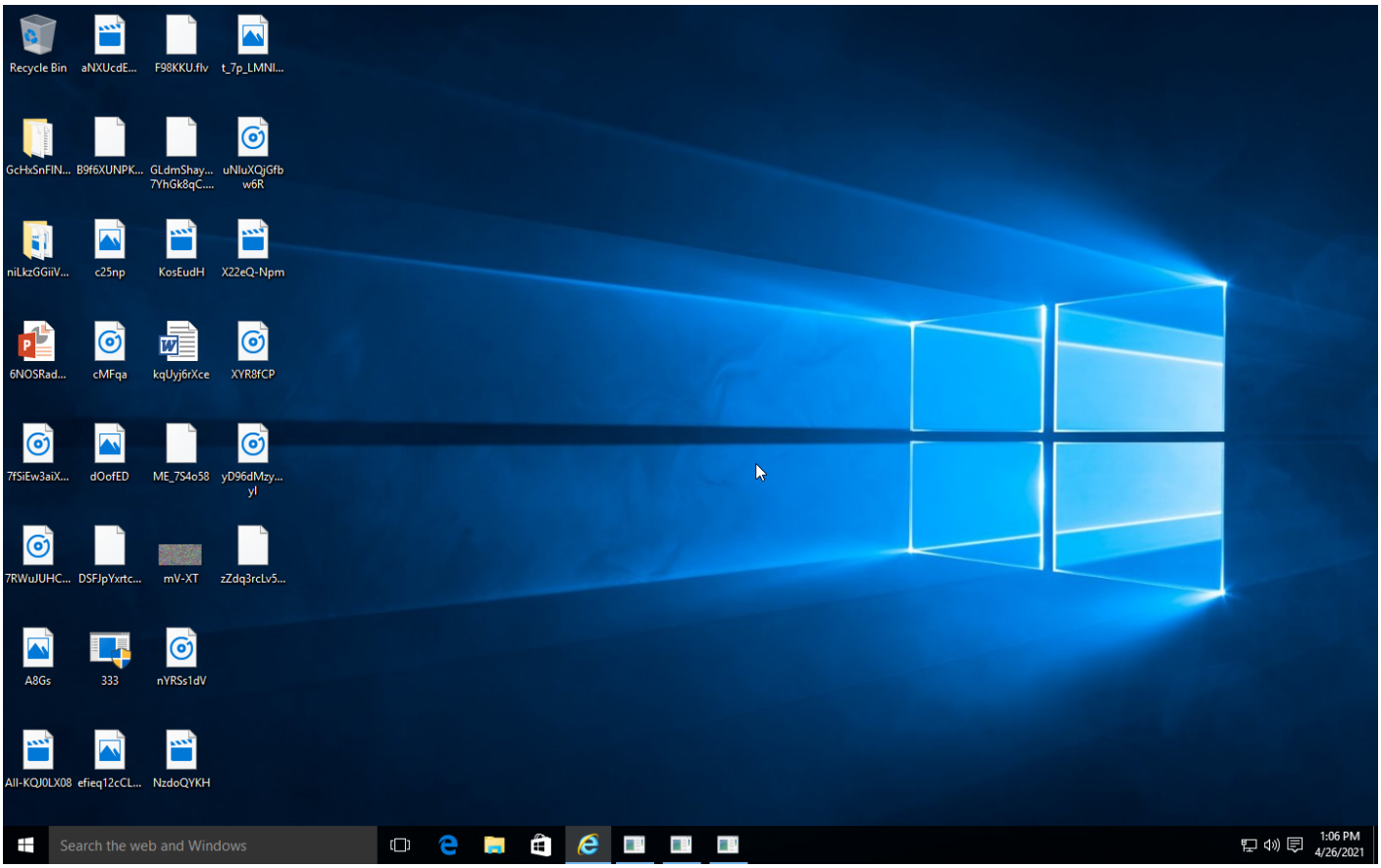
ID	5897454
MD5	162cde379f01cda83e24ada7e04a2964
SHA1	990932e10b61de6357afa716fe2e66a6cedad25e
SHA256	ebfa81cf52743de40734c2aea01466c47d8c18d9fa663c897614756652e56b5c
SSDeep	6144:iwa1MIjEPJ3W15N2PUH43IOuDdTDscYkqGBM+tAPEr8xuY:ejEPNW1n2a4VupfTf5nAM83
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
Filename	333.exe
File Size	314.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

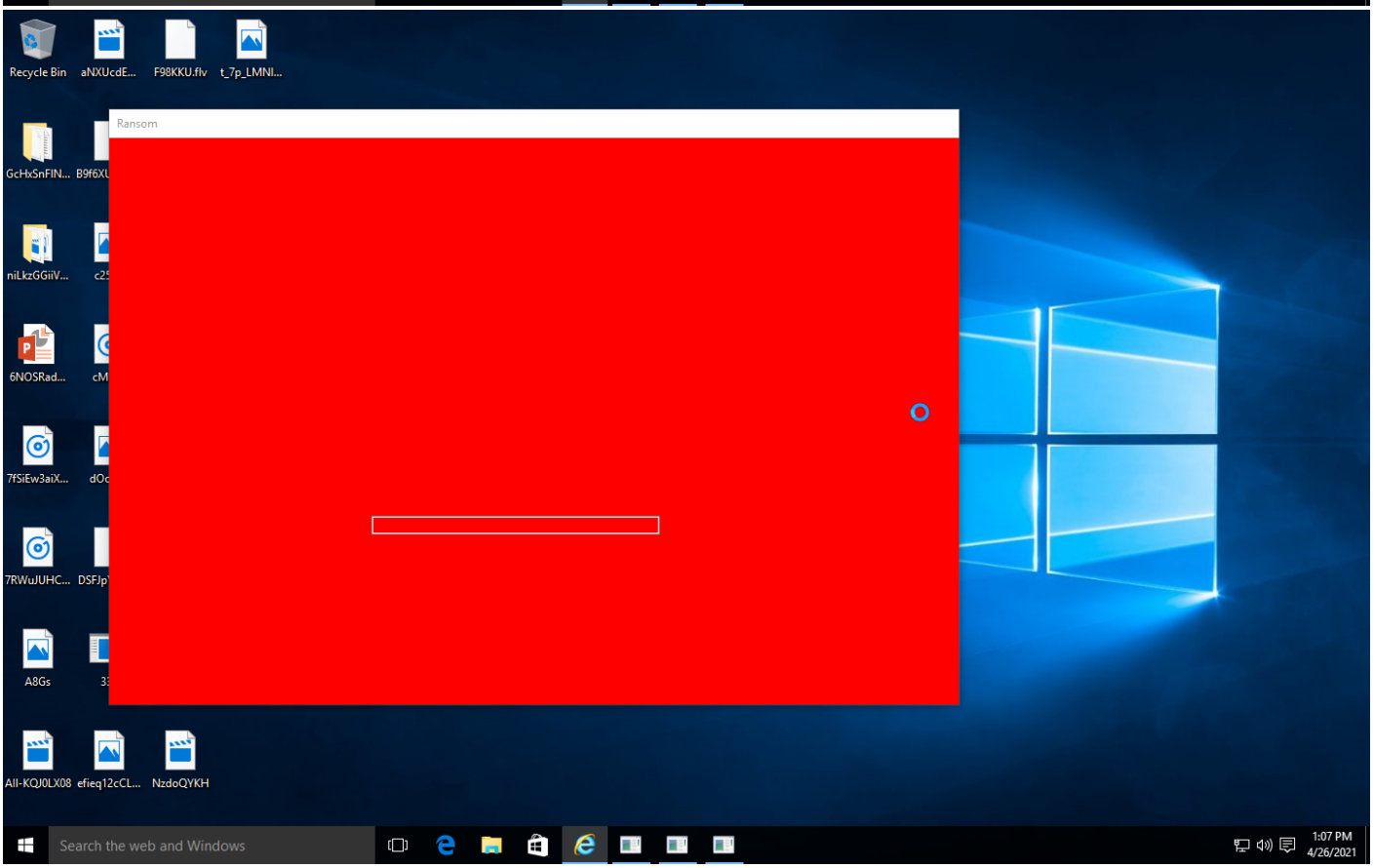
Analysis Information

Creation Time	2021-04-26 15:04 (UTC+2)
Analysis Duration	00:03:40
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successfull	False
Reputation Analysis Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
aNXUcdE...
F98KKU.flv
t_7p_LMNI...
GcHxSnFIN...
B9f6XUNPK...
GLdmShay...
7YhGk8qC....
uNluXQjGfb
w6R
niLkzGGiiV...
c25np
KosEudH
X22eQ-Npm
6NOSRad...
cMFqa
kqUyj6rXce
XYR8fCP
7fSiEw3aiX...
dOofED
ME_7S4o58
yD96dMzy...
yl
7RWuJUHC...
DSFJpYxrtc...
mV-XT
zZdq3rcLv5...
A8Gs
333
nYRSs1dV
All-KQJ0LX08
efieq12cCL...
NzdoQYKH
Search the web and Windows
1:06 PM
4/26/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 333.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots trunkated.

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes recivied

DNS Requests

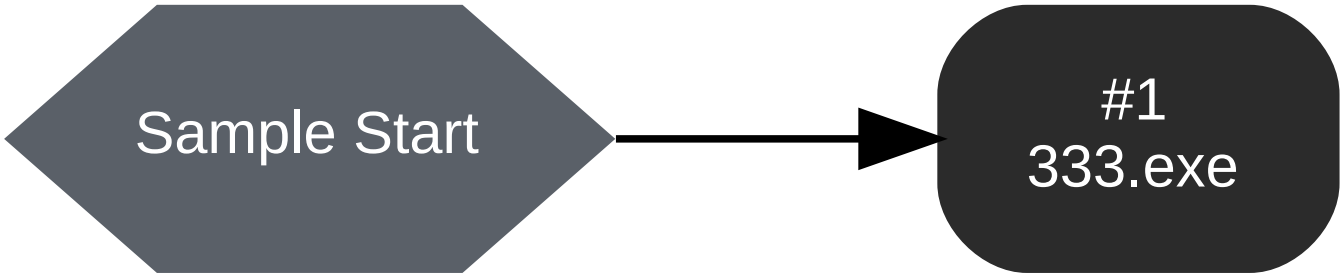
-

HTTP Requests

-

BEHAVIOR

Process Graph



Process #1: 333.exe

ID	1
Filename	c:\users\rdhj0cnfevzx\desktop\333.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\333.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 102952, Reason: Analysis Target
Unmonitor End Time	End Time: 321641, Reason: Terminated by Timeout
Monitor Duration	218.69s
Return Code	Unknown
PID	4120
Parent PID	2132
Bitness	64 Bit

Dropped Files (85)

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\333.exe.kfuald	32 bytes	e9eab25a0a5c2977fe7ca8d71aaf040b46889f4999ef1ed17789753fa11fad6e	✕
C:\Users\RDhJ0CNFevzX\Pictures\0_sc8lpuOR-.png.kfuald	82.42 KB	8c2d27c332560a4ea5d1a97af5bbd115f98ea9061b4cbf9d7b81e9f39e750802	✕
C:\Users\RDhJ0CNFevzX\Pictures\8ngyV20QtMP.jpg.kfuald	52.95 KB	a43630d86b763e1de33cac609ce49e1b357c97390c0249856e8e074c56a2f554	✕
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.kfuald	544 bytes	fe9f7c4940e11585db786ea6914b7940f089a6a795a6e680d18a9baf42b1f128	✕
C:\Users\RDhJ0CNFevzX\Pictures\DJ11q92YZCfOl_L.jpg.kfuald	62.72 KB	f80ea9899b117a55825b3f7d452eec3e55f7e1c26790c0c3276c9f2d439f4161	✕
C:\Users\RDhJ0CNFevzX\Pictures\FeW8I.gif.kfuald	86.22 KB	b306f8eccb396309eb8bece7062080df3a65de354496a274a099ad4b23e30fc9	✕
C:\Users\RDhJ0CNFevzX\Pictures\fGdy9UGlpL6.gif.kfuald	3.58 KB	4f312d84953199374cb1776aec097411791a7d485001471e69a34805f11c69fd	✕
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\9oTZGBQn6POhNzuW4cC9.gif.kfuald	86.77 KB	c3adab7cc46e27a0e83f5eafd13a6f96464bebbefa3f1ee9f10a769dd2a6c24e	✕
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\AQnQQQ8Qa.jpg.kfuald	99.86 KB	74a2b848e1ab2b29b592884b7ca5acd8b45a5165a9c1c9a271bae315d0aa310e	✕
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\vU7dn.png.kfuald	81.09 KB	8c013c45c156f31846c13819f130ecf95a5b0ea999e27934d4c92ecd26180368	✕
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn_8te40cGFqB.jpg.kfuald	8.27 KB	7e4347047c2ca29c3a247e94eb4ea43fed83c980d5855363702a680f52b35961	✕
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.kfuald	224 bytes	6f4da6365190abca713b62704964469b404eb8fa697fd05e7e039f01f3474edf	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\2z8r-rInMai4ng0l.png.kfuald	18.06 KB	15d1a0c8c70500e91ae8c2dc5dd51bca07c400d2bdb8ad85d693b96b373cb44c	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\428yCMsP5H.gif.kfuald	84.16 KB	0495e22d01a6cfab7b5e5b4901642db3abcdd53643acf96a19f00dfb4dc1d5c8	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bbhrwdO7CREtkiTfhwvG.bmp.kfuald	28.00 KB	9e74ecb09c8df0f00d6c392f1116924b4aa70f91d8117ac013784019e1263d8d	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bZ5iXwv8rJ.jpg.kfuald	31.22 KB	acae1a340b415bbba518c5f71cece3dc8e40bb50f80edeb17b2113dbb3941138	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\l8EnCbTqzZ.jpg.kfuald	28.69 KB	89aa1183428f02223f85436ba629df80818f4965910cac59ac74f426ff193d52	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\hHSY.gif.kfuald	25.55 KB	5df31071e47865ab36743f3dba1df78ceb57592af23de2bcca4f913433e0d3f0	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\kjoMFWZGlcEZGTaT.jpg.kfuald	20.91 KB	42b410d0de265793ed55bc7f185a7af3fb0e16914f4f483847dc578b649a9028	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\UabbxPnk9mFO9n0-.jpg.kfuald	91.69 KB	4d12fff38da339475f40852236a4eea0c17b546432cf0c0bde3d2eda5a4a5f59	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\ycvWF35JmUHZD9TF.jpg.kfuald	25.58 KB	d9446be5467c08486db0f1f97e9be9c54b5eef5806d0d88f4b754d53dfbe8b0d	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\4EC-NIq9H6XQjHrgH2.gif.kfuald	40.58 KB	8ba1f68f0756f99329d3ff3bedbe74c09d717aee6f1f40c93d26a987bda715a1	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\60RYSwKb4I8t.gif.kfuald	57.31 KB	c1bd372e1116790344cf46b0144a9528063d6938d2231d4ae85054f2d45b5256	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\bXEt8I6nq.bmp.kfuald	48.83 KB	59899a09a3b51ff179f120f4c640fcd1883993b0e862d9d543a78673d7e7dd46	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\M92sNjfyoi.png.kfuald	59.05 KB	b57ccb04f842f4e6b791651cab0ad3d3d67d3c7879e7ca8db9d7435ca39d8e2e	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\ZLNmgOE4O9pXPtAxNhVy.jpg.kfuald	30.05 KB	e5a984e1abb2a61ebbdb3ae1ac281428b2d6a2691c77ecbfe8a90cd056f23fb9	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fqei3XX5BBIz\BfmHAaxu.bmp.kfuald	46.59 KB	aab563b71688011d023e938417e047411eb33f11f691903f7e84a5153146af35	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fqei3XX5BBIz\tqmHJ4dmir9XV.bmp.kfuald	64.52 KB	1ec2164e71c9b9e67b76c6423d865989ef33e6025bafb411918b2a4254b0f961	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\-JhjDC2AIcrMU1Sqww.bmp.kfuald	6.12 KB	f1efa7eea637539ea9dc212f845298aa42825e5469aca9878c5cab7bf7a6fa79	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\lorQxNzqYxpX475.bmp.kfuald	49.89 KB	e915b0a482d16de8426c0b1b1294641f99cc3f3f8b5c8afcbeab089369d276db	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\8fSQ8UtOL.png.kfuald	71.38 KB	922a0c4fc999c59c84c06dabcbd32150ff0659c6daa3d1a05414b658ce06b6ef	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\DQaWtpbPalB66C0Zbv.bmp.kfuald	20.77 KB	aa3ea068dd57f196ad6d2e2a1ff6f6c984d88bab3b12525a2dddad75e6d079a6	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\KFDMiHEziC1N_EC.jpg.kfuald	37.30 KB	9da253a0d5d78d939bdd4129cea7f97b91b8db9ff66936eeb8a9c902658a6a34	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\kspB96BT5Kro-.bmp.kfuald	41.42 KB	4ddab9c9fb9fd2a8477642292f558f6f2836534e224518e5bacc379245f174aa	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\ejyC4n6QiKyh.gif.kfuald	4.91 KB	e951fa8da0f04ddb47bdb7114b5ba93142e8a930a93525ef3db56dbb3b8d49e8	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\fDtUSYBe.png.kfuald	5.64 KB	b941237e43d6678da2d4c8497fa81f34bc97b03b9be1370f20dd757ce752dd31	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\QDHUaG.jpg.kfuald	83.78 KB	beba564d72542051920d20a63d73a0d6e465ca18c11409a81dc4a813bb748316	✕
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\w3qvBj.jpg.kfuald	7.94 KB	f74d8a8aee648c7bc17c7198203959513315a01ac94a055c03af816f74761f80	✕
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.kfuald	224 bytes	e2f01f15741b918004c65d055338a021dc53a528baeec583bb90480dfeef47d3	✕
C:\Users\RDhJ0CNFevzX\Documents\0A931C.rtf.kfuald	60.94 KB	a6769277339af1d621b8ab9395da8145b54ac51490a01260025694a9d549aee9	✕
C:\Users\RDhJ0CNFevzX\Documents\7JpA4Ax39L.pptx.kfuald	94.16 KB	f78d8920530da0a90ffb765c449bbd92ba10a3667ab8b866c771c5502680ceca	✕
C:\Users\RDhJ0CNFevzX\Documents\9ndEkH.xlsx.kfuald	77.83 KB	b029858960df0b543d544720907432afaa883a08951a695c23e71d29bae6e9eb	✕
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.kfuald	448 bytes	d17c03717b4438b77138d5d401c3d5c09008aeb16311c3f973071670f9f4def4	✕
C:\Users\RDhJ0CNFevzX\Documents\e1mHtEVePp6n5SIIH2.ods.kfuald	55.16 KB	e3d269d6d26ad730962458bf620e8357e9f3544b28e6435e75e325e60376aadb	✕
C:\Users\RDhJ0CNFevzX\Documents\fvRJbkxezpybfmolJ.pptx.kfuald	3.08 KB	9da135f7afe0384d0af800bf86c5b1169e2a1ca75c12f9d5468a8f626fc4b47f	✕
C:\Users\RDhJ0CNFevzX\Documents\h7rmmJ75EUvYTZU.pptx.kfuald	54.86 KB	ab465310e4e5e78891219b252fc31f5b06eee282ec850af8eba281ea4217c73c	✕
C:\Users\RDhJ0CNFevzX\Documents\iZLXf9f3fQ-q.xls.kfuald	91.89 KB	72f80a263e2c8b2f7f8ff947dfa1fa800687ff6d1ff25ddb24be7558503ff4c1	✕
C:\Users\RDhJ0CNFevzX\Documents\jB6tZPmpB7d5JGJ.pptx.kfuald	88.67 KB	8a6d073556585d99c61a06b8279e12951c3210495ea07ac0dc2895d378847e74	✕
C:\Users\RDhJ0CNFevzX\Documents\krM-01YH_.docx.kfuald	86.25 KB	8f17ede90ced4b74a38be1e5c79f0836c899e1f5bb8ae47a2631ca02fab37a7f	✕
C:\Users\RDhJ0CNFevzX\Documents\KV2Njrt.ods.kfuald	11.25 KB	cb893839e1e01fd18c792c196d9455cf2e99c75934e749a6ec6f6dff64f6c781	✕
C:\Users\RDhJ0CNFevzX\Documents\Moeyr9UzHNHZH.xlsx.kfuald	72.58 KB	7ec75d7062f04836e72bc33d329ecd3e53a8a25a6f51d29062e4a8ae34fafaf8	✕
C:\Users\RDhJ0CNFevzX\Documents\MSKvEq.docx.kfuald	29.08 KB	a54ef854546956c23285590c7c980446d977472abdbc65337b37926f4cf2110c	✕
C:\Users\RDhJ0CNFevzX\Documents\onXIIelcJCBs2_atOn.ots.kfuald	39.58 KB	3c45aa41131e1a5c37f85be51cde051106b02c4a684784364aeb68257d4b947f	✕
C:\Users\RDhJ0CNFevzX\Documents\OV9cjW1KRPMZD6.xlsx.kfuald	28.52 KB	3d7bfe616263c96960635ff1825948b98ea35f54b3702abfeb64c874c999e178	✕
C:\Users\RDhJ0CNFevzX\Documents\peIc9.ppt.kfuald	27.17 KB	0e8e61d9774ea6b3ee02bda1c15d02e5604d3dfbe429905395242fe5f6f21a52	✕
C:\Users\RDhJ0CNFevzX\Documents\Q74iOtUSt-LdEt.xlsx.kfuald	16.03 KB	d046fe384715790b5cf5c9200104d962893b8813f6f573768cebe15558f4ae0d	✕
C:\Users\RDhJ0CNFevzX\Documents\QhvyDDZeU925SNWZ.xlsx.kfuald	33.47 KB	3bd613c2a3d151cbf9567bccd3b831e9ada4a23552872a8ac948ecb39f180abe	✕
C:\Users\RDhJ0CNFevzX\Documents\r5y7X6BeH79.pptx.kfuald	15.23 KB	73435576b03aa651e4d0cb3bcd754d335a14e34f1def874730c22df768ed4aad	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\Sa0.docx.kfuald	87.45 KB	bfc7b572855fa6f66f57f62dd1ef140c3b79d8a0f8403af73b67899abbc73d5d	✕
C:\Users\RDhJ0CNFevzX\Documents\Sh8o9ZbL4AXv5mdqw aT.docx.kfuald	18.33 KB	989575f627bd3e690f24bd57eb6f4977623eca15bc270e1cc0944d7f5c3111b8	✕
C:\Users\RDhJ0CNFevzX\Documents\vof9fF.pptx.kfuald	98.25 KB	08781efd01d25c0d80bda315eb62c03f5696464cb9053855b3a7bca92743146d	✕
C:\Users\RDhJ0CNFevzX\Documents\vS_gwWgi0tn.odp.kfuald	17.20 KB	6c7cc4924fe850c2e18c6eb956ece1bc282f703ad5f0aab45a0da364b6a8f145	✕
C:\Users\RDhJ0CNFevzX\Documents\VZPaIxcz7GLW.docx.kfuald	91.36 KB	b6131b27d07cf05beb7cfab014bad5f46e3094ad594095063a9219b3da5f8fb4	✕
C:\Users\RDhJ0CNFevzX\Documents\wljK1MkFwCn3.xls.kfuald	10.39 KB	161e89b2d88c524a695d6f88962d20e958320baf3b238f5c97d362f3c9380667	✕
C:\Users\RDhJ0CNFevzX\Documents\xU9MjOwvWLJY.csv.kfuald	18.88 KB	6ca86fadeaf4e94fe02ad9d0e4eab70badf3bbf1e1d90cd16a43f2fd606c64dd	✕
C:\Users\RDhJ0CNFevzX\Documents\yCEpdF.odt.kfuald	95.23 KB	264da6c11ba4f1052e871982d446357ef93df92c9c055ff3aa495aa0881daf50	✕
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.kfuald	265.05 KB	52b7151ea797db7b45afe1755397cb4110be278b4565a7a161f96b7167f9cd3d	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\-k2S G9eplCimY582CS.xls.kfuald	6.86 KB	6c62b12dabf349ad109fbe6f664f3eda24f291fd4fb7b2b480e8c68a3e15a157	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\2aGiB5Vu8dFo.pdf.kfuald	74.00 KB	f25671789cf1dfb578e6f215a34ad9565d82ad563a7e1b2e498854805887658c	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZ zpPoDQpQ8qTR.docx.kfuald	66.34 KB	d0074e9ca3e92d397a7234fa4bc56f2bed64105dd1e8f913f0c19d3686aebe0e	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZ8oHM1.pptx.kfuald	31.38 KB	6a9872a34d0e5be653e1ec84298162a4d04fc9f738f871b894567532d0655d9e	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\ECUe.pps.kfuald	4.27 KB	d849cfa1731ea762b9f30ad802c4739801c64b815766acc230be5a8d8a13bdef	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\iMLPUH5839SPlcf.doc.kfuald	28.73 KB	93dfee2c1e7ec33b85924ca885a79513e2cb7f71ef9491e53adc7fd318c2f63d	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\lrbahn2XTjt0vqe9HfL.pptx.kfuald	83.72 KB	4892609907fe2c517cfe28468af156d9a9d417990cad0e908646c14afdcb86c5	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\JxIpV.xls.kfuald	58.06 KB	6dc9518b47ae4b2c578903ba8eedc8ccecc20cb122b46f30c506654947a153d6	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\r3nAsVal.odp.kfuald	12.06 KB	bb06f5b03003041e7c588a5e3898261cdbdabc9c84c9421f78d2043580242d7c	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\2DW7QXR64oz.xlsx.kfuald	81.22 KB	4f8f7f12a8dc15c26b430e48bc1f2742e66e490aedb147747bd6a55aec9de6b8	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\4hP4g805ELYzX.xls.kfuald	80.83 KB	982a741bdf22d945a09977c2002d96700704c75698dc6f6ecec74b58590229f6	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\eHFVA333EtxT.xlsx.kfuald	59.45 KB	756e6364755066b4813ef8dd9408b3d0edbd7b1d41c12168b45bcb334049bd1e	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\G0G_AVyyXuVQrqvU8.doc.kfuald	47.03 KB	f2d1403aa65bc0d782f7e7c785cc1f2954c2089a92de3d3d19469a4c231b7f86	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\iPE90PQEnBDU.pps.kfuald	64.08 KB	bdc8cf8a05637ab153d81d992858093b25f53498c651c1760f35d964646a9d4b	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\nfPv2sbT6Wvhi16E.odp.kfuald	84.41 KB	38033aea153fbd455ecabc945bb0c6a17cfcbeedace2ac9696e8156626f68110	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\WZZFbk7EZqKXbeD.ods.kfuald	32.17 KB	a34b98aff2c1fb75758f2de41ca90dd880586c8b9088e9bf042bf28045760338	✕
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\XYhte4teKs65RLuMnq7.pps.kfuald	98.83 KB	75884a6afd2ffe65def824047be11eeaf853cfc55905b5e2224d5a8ba8732c7a	✕
C:\Users\RDhJ0CNFevzX\Desktopyour files have been encrypted.kfuald.txt	5.54 KB	de449357e30c550f0d5dde47e862f158c605613a37f0c618d0f33b78fa5df474	✕

Host Behavior

Type	Count
Module	391
System	810
Window	346
Registry	13
File	995
Keyboard	607
User	1

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
ebfa81cf52743de40734c2aea01466c47d8c18d9fa663c897614756652e56b5c	C:\Users\RDhJ0CNFevzX\Desktop\333.exe	Sample File	314.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
e9eab25a0a5c2977fe7ca8d71aaf040b46889f4999ef1ed17789753fa11fad6e	C:\Users\RDhJ0CNFevzX\Desktop\333.exe.kfuald	Dropped File	32 bytes	application/octet-stream	Write, Access, Create	CLEAN
8c2d27c332560a4ea5d1a97af5bbd115f98ea9061b4cbf9d7b81e9f39e750802	C:\Users\RDhJ0CNFevzX\Pictures\0_sc8lpuOR-.png.kfuald	Dropped File	82.42 KB	application/octet-stream	Write, Access, Create	CLEAN
a43630d86b763e1de33cac609ce49e1b357c97390c0249856e8e074c56a2f554	C:\Users\RDhJ0CNFevzX\Pictures\8ngyV20QtMP.jpg.kfuald	Dropped File	52.95 KB	application/octet-stream	Write, Access, Create	CLEAN
fe9f7c4940e11585db786ea6914b7940f089a6a795a6e680d18a9baf42b1f128	C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.kfuald	Dropped File	544 bytes	application/octet-stream	Write, Access, Create	CLEAN
f80ea9899b117a55825b3f7d452eec3e55f7e1c26790c0c3276c9f2d439f4161	C:\Users\RDhJ0CNFevzX\Pictures\DJ11q92YZCfOl_L.jpg.kfuald	Dropped File	62.72 KB	application/octet-stream	Write, Access, Create	CLEAN
b306f8eccb396309eb8bece7062080df3a65de354496a274a099ad4b23e30fc9	C:\Users\RDhJ0CNFevzX\Pictures\FeW8I.gif.kfuald	Dropped File	86.22 KB	application/octet-stream	Write, Access, Create	CLEAN
4f312d84953199374cb1776aec097411791a7d485001471e69a34805f11c69fd	C:\Users\RDhJ0CNFevzX\Pictures\fGdy9UGlpL6.gif.kfuald	Dropped File	3.58 KB	application/octet-stream	Write, Access, Create	CLEAN
c3adab7cc46e27a0e83f5eafd13a6f96464bebbefa3f1ee9f10a769dd2a6c24e	C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\9oTZGBQn6POhNzuW4cC9.gif.kfuald	Dropped File	86.77 KB	application/octet-stream	Write, Access, Create	CLEAN
74a2b848e1ab2b29b592884b7ca5acd8b45a5165a9c1c9a271bae315d0aa310e	C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\AQnQQQ8Qa.jpg.kfuald	Dropped File	99.86 KB	application/octet-stream	Write, Access, Create	CLEAN
8c013c45c156f31846c13819f130ecf95a5b0ea999e27934d4c92ecd26180368	C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\vU7dn.png.kfuald	Dropped File	81.09 KB	application/octet-stream	Write, Access, Create	CLEAN
7e4347047c2ca29c3a247e94eb4ea43fed83c980d5855363702a680f52b35961	C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn_8te40cGFqB.jpg.kfuald	Dropped File	8.27 KB	application/octet-stream	Write, Access, Create	CLEAN
6f4da6365190abca713b62704964469b404eb8fa697fd05e7e039f01f3474edf	C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.kfuald	Dropped File	224 bytes	application/octet-stream	Write, Access, Create	CLEAN
15d1a0c8c70500e91ae8c2dc5dd51bca07c400d2bdb8ad85d693b96b373cb44c	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\2z8r-rInMai4ng0l.png.kfuald	Dropped File	18.06 KB	application/octet-stream	Write, Access, Create	CLEAN
0495e22d01a6cfab7b5e5b4901642db3abcdd53643acf96a19f00dfb4dc1d5c8	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\428yCMsP5H.gif.kfuald	Dropped File	84.16 KB	application/octet-stream	Write, Access, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
9e74ecb09c8df0f00d6c392f1116924b4aa70f91d8117ac013784019e1263d8d	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bbhrwdO7CREtkiTfhwvG.bmp.kfuald	Dropped File	28.00 KB	application/octet-stream	Write, Access, Create	CLEAN
acae1a340b415bbba518c5f71cece3dc8e40bb50f80edeb17b2113dbb3941138	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bZ5iXwv8rJ.jpg.kfuald	Dropped File	31.22 KB	application/octet-stream	Write, Access, Create	CLEAN
89aa1183428f02223f85436ba629df80818f4965910cac59ac74f426ff193d52	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\l8EnCbTqzZ.jpg.kfuald	Dropped File	28.69 KB	application/octet-stream	Write, Access, Create	CLEAN
5df31071e47865ab36743f3dba1df78ceb57592af23de2bcca4f913433e0d3f0	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\hHSY.gif.kfuald	Dropped File	25.55 KB	application/octet-stream	Write, Access, Create	CLEAN
42b410d0de265793ed55bc7f185a7af3fb0e16914f4f483847dc578b649a9028	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\kjoMFWZGlcEZGTaT.jpg.kfuald	Dropped File	20.91 KB	application/octet-stream	Write, Access, Create	CLEAN
4d12fff38da339475f40852236a4eea0c17b546432cf0c0bde3d2eda5a4a5f59	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\UabbxPnk9mFO9n0-.jpg.kfuald	Dropped File	91.69 KB	application/octet-stream	Write, Access, Create	CLEAN
d9446be5467c08486db0f1f97e9be9c54b5eef5806d0d88f4b754d53dfbe8b0d	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\ycvWF35JmUHZD9TF.jpg.kfuald	Dropped File	25.58 KB	application/octet-stream	Write, Access, Create	CLEAN
8ba1f68f0756f99329d3ff3bedbe74c09d717aee6f1f40c93d26a987bda715a1	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\4EC-NIq9H6XQjHrgH2.gif.kfuald	Dropped File	40.58 KB	application/octet-stream	Write, Access, Create	CLEAN
c1bd372e1116790344cf46b0144a9528063d6938d2231d4ae85054f2d45b5256	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\60RYSwKb4I8t.gif.kfuald	Dropped File	57.31 KB	application/octet-stream	Write, Access, Create	CLEAN
59899a09a3b51ff179f120f4c640fcd1883993b0e862d9d543a78673d7e7dd46	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\bXEt8I6nq.bmp.kfuald	Dropped File	48.83 KB	application/octet-stream	Write, Access, Create	CLEAN
b57ccb04f842f4e6b791651cab0ad3d3d67d3c7879e7ca8db9d7435ca39d8e2e	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\M92sNjfyoi.png.kfuald	Dropped File	59.05 KB	application/octet-stream	Write, Access, Create	CLEAN
e5a984e1abb2a61ebbdb3ae1ac281428b2d6a2691c77ecbfe8a90cd056f23fb9	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\ZLNmgOE4O9pXPtAxNhVy.jpg.kfuald	Dropped File	30.05 KB	application/octet-stream	Write, Access, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
aab563b71688011d023e938417e047411eb33f11f691903f7e84a5153146af35	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fqei3XX5BBIz\BfmHAaxu.bmp.kfuald	Dropped File	46.59 KB	application/octet-stream	Write, Access, Create	CLEAN
1ec2164e71c9b9e67b76c6423d865989ef33e6025bafb411918b2a4254b0f961	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fqei3XX5BBIz\tqmHJ4dmir9XV.bmp.kfuald	Dropped File	64.52 KB	application/octet-stream	Write, Access, Create	CLEAN
f1efa7eea637539ea9dc212f845298aa42825e5469aca9878c5cab7bf7a6fa79	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\-JhjDC2AIcrMU1Sqww.bmp.kfuald	Dropped File	6.12 KB	application/octet-stream	Write, Access, Create	CLEAN
e915b0a482d16de8426c0b1b1294641f99cc3f3f8b5c8afcbeab089369d276db	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\lorQxNzqYxpX475.bmp.kfuald	Dropped File	49.89 KB	application/octet-stream	Write, Access, Create	CLEAN
922a0c4fc999c59c84c06dabcbd32150ff0659c6daa3d1a05414b658ce06b6ef	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\8fSQ8UtOL.png.kfuald	Dropped File	71.38 KB	application/octet-stream	Write, Access, Create	CLEAN
aa3ea068dd57f196ad6d2e2a1ff6f6c984d88bab3b12525a2dddad75e6d079a6	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\DQaWtpbPalB66C0Zbv.bmp.kfuald	Dropped File	20.77 KB	application/octet-stream	Write, Access, Create	CLEAN
9da253a0d5d78d939bdd4129cea7f97b91b8db9ff66936eeb8a9c902658a6a34	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\KFDMiHEziC1N_EC.jpg.kfuald	Dropped File	37.30 KB	application/octet-stream	Write, Access, Create	CLEAN
4ddab9c9fb9fd2a8477642292f558f6f2836534e224518e5bacc379245f174aa	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\kspB96BT5Kro-.bmp.kfuald	Dropped File	41.42 KB	application/octet-stream	Write, Access, Create	CLEAN
e951fa8da0f04ddb47bdb7114b5ba93142e8a930a93525ef3db56dbb3b8d49e8	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\ejyC4n6QiKyh.gif.kfuald	Dropped File	4.91 KB	application/octet-stream	Write, Access, Create	CLEAN
b941237e43d6678da2d4c8497fa81f34bc97b03b9be1370f20dd757ce752dd31	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\fDtUSYBe.png.kfuald	Dropped File	5.64 KB	application/octet-stream	Write, Access, Create	CLEAN
beba564d725420519020d20a63d73a0d6e465ca18c11409a81dc4a813bb748316	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\QDHUaG.jpg.kfuald	Dropped File	83.78 KB	application/octet-stream	Write, Access, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
f74d8a8aee648c7bc17c71982039595133 15a01ac94a055c03af816f74761f80	C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\w3qvBj.jpg.kfuald	Dropped File	7.94 KB	application/octet-stream	Write, Access, Create	CLEAN
e2f01f15741b918004c65d055338a021dc53a528baeec583bb90480dfeef47d3	C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.kfuald	Dropped File	224 bytes	application/octet-stream	Write, Access, Create	CLEAN
a6769277339af1d621b8ab9395da8145b54ac51490a01260025694a9d549aee9	C:\Users\RDhJ0CNFevzX\Documents\0A931C.rtf.kfuald	Dropped File	60.94 KB	application/octet-stream	Write, Access, Create	CLEAN
f78d8920530da0a90ffb765c449bbd92ba10a3667ab8b866c771c5502680ceca	C:\Users\RDhJ0CNFevzX\Documents\7JpA4Ax39L.pptx.kfuald	Dropped File	94.16 KB	application/octet-stream	Write, Access, Create	CLEAN
b029858960df0b543d544720907432afaa883a0895 1a695c23e71d29bae6e9eb	C:\Users\RDhJ0CNFevzX\Documents\9ndEkH.xlsx.kfuald	Dropped File	77.83 KB	application/x-dosexec	Write, Access, Create	CLEAN
d17c03717b4438b77138d5d401c3d5c09008aeb16311c3f973071670f9f4def4	C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.kfuald	Dropped File	448 bytes	application/octet-stream	Write, Access, Create	CLEAN
e3d269d6d26ad730962458bf620e8357e9f3544b28e6435e75e325e60376aadb	C:\Users\RDhJ0CNFevzX\Documents\e1mHtEVeP p6n5SIIH2.ods.kfuald	Dropped File	55.16 KB	application/octet-stream	Write, Access, Create	CLEAN
9da135f7afe0384d0af800bf86c5b1169e2a1ca75c12f9d5468a8f626fc4b47f	C:\Users\RDhJ0CNFevzX\Documents\fvRJbkxezpybfmolJ.pptx.kfuald	Dropped File	3.08 KB	application/octet-stream	Write, Access, Create	CLEAN
ab465310e4e5e78891219b252fc31f5b06eee282ec850af8eba281ea4217c73c	C:\Users\RDhJ0CNFevzX\Documents\h7rmmJ75EUvYTZU.pptx.kfuald	Dropped File	54.86 KB	application/octet-stream	Write, Access, Create	CLEAN
72f80a263e2c8b2f7f8ff947dfa1fa800687ff6d1ff25ddb24be7558503ff4c1	C:\Users\RDhJ0CNFevzX\Documents\iZLXf9f3fQ-q.xls.kfuald	Dropped File	91.89 KB	application/octet-stream	Write, Access, Create	CLEAN
8a6d073556585d99c61a06b8279e12951c3210495ea07ac0dc2895d378847e74	C:\Users\RDhJ0CNFevzX\Documents\jB6tZPmpB7d5JGJ.pptx.kfuald	Dropped File	88.67 KB	application/octet-stream	Write, Access, Create	CLEAN
8f17ede90ced4b74a38be1e5c79f0836c899e1f5bb8ae47a2631ca02fab37a7f	C:\Users\RDhJ0CNFevzX\Documents\krM-01YH_.docx.kfuald	Dropped File	86.25 KB	application/octet-stream	Write, Access, Create	CLEAN
cb893839e1e01fd18c792c196d9455cf2e99c75934e749a6ec6f6dff64f6c781	C:\Users\RDhJ0CNFevzX\Documents\KV2Njrt.ods.kfuald	Dropped File	11.25 KB	application/octet-stream	Write, Access, Create	CLEAN
7ec75d7062f04836e72bc33d329ecd3e53a8a25a6f51d29062e4a8ae34fafaf8	C:\Users\RDhJ0CNFevzX\Documents\Moeyr9UzHNHZH.xlsx.kfuald	Dropped File	72.58 KB	application/octet-stream	Write, Access, Create	CLEAN
a54ef854546956c23285590c7c980446d977472abdbc65337b37926f4cf2110c	C:\Users\RDhJ0CNFevzX\Documents\MSKvEq.docx.kfuald	Dropped File	29.08 KB	application/octet-stream	Write, Access, Create	CLEAN
3c45aa41131e1a5c37f85be51cde051106b02c4a684784364aeb68257d4b947f	C:\Users\RDhJ0CNFevzX\Documents\onXlIelcJCBs2_atOn.ots.kfuald	Dropped File	39.58 KB	application/octet-stream	Write, Access, Create	CLEAN
3d7bfe616263c96960635ff1825948b98ea35f54b3702abfeb64c874c999e178	C:\Users\RDhJ0CNFevzX\Documents\OV9cjW1KRPMZD6.xlsx.kfuald	Dropped File	28.52 KB	application/octet-stream	Write, Access, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
0e8e61d9774ea6b3ee02bda1c15d02e5604d3dfbe429905395242fe5f6f21a52	C:\Users\RDhJ0CNFevzX\Documents\pelc9.ppt.kfuald	Dropped File	27.17 KB	application/octet-stream	Write, Access, Create	CLEAN
d046fe384715790b5cf5c9200104d962893b8813f6f573768cebe15558f4ae0d	C:\Users\RDhJ0CNFevzX\Documents\Q74iOtU St-LdEt.xlsx.kfuald	Dropped File	16.03 KB	application/octet-stream	Write, Access, Create	CLEAN
3bd613c2a3d151cbf9567bccd3b831e9ada4a23552872a8ac948ecb39f180abe	C:\Users\RDhJ0CNFevzX\Documents\QhvyDDZeU925SNWZ.xlsx.kfuald	Dropped File	33.47 KB	application/octet-stream	Write, Access, Create	CLEAN
73435576b03aa651e4d0cb3bcd754d335a14e34f1def874730c22df768ed4aad	C:\Users\RDhJ0CNFevzX\Documents\r5y7X6BeH79.pptx.kfuald	Dropped File	15.23 KB	application/octet-stream	Write, Access, Create	CLEAN
bfc7b572855fa6f66f57f62dd1ef140c3b79d8a0f8403af73b67899abbc73d5d	C:\Users\RDhJ0CNFevzX\Documents\Sa0.docx.kfuald	Dropped File	87.45 KB	application/octet-stream	Write, Access, Create	CLEAN
989575f627bd3e690f24bd57eb6f4977623eca15bc270e1cc0944d7f5c3111b8	C:\Users\RDhJ0CNFevzX\Documents\Sh8o9ZbL4AXv5mdqwaT.docx.kfuald	Dropped File	18.33 KB	application/octet-stream	Write, Access, Create	CLEAN
08781efd01d25c0d80bda315eb62c03f5696464cb9053855b3a7bca92743146d	C:\Users\RDhJ0CNFevzX\Documents\vof9fF.pptx.kfuald	Dropped File	98.25 KB	application/octet-stream	Write, Access, Create	CLEAN
6c7cc4924fe850c2e18c6eb956ece1bc282f703ad5f0aab45a0da364b6a8f145	C:\Users\RDhJ0CNFevzX\Documents\vS_gwWgi0tn.odp.kfuald	Dropped File	17.20 KB	application/octet-stream	Write, Access, Create	CLEAN
b6131b27d07cf05beb7cfab014bad5f46e3094ad594095063a9219b3da5f8fb4	C:\Users\RDhJ0CNFevzX\Documents\VZPaIxcz7GLW.docx.kfuald	Dropped File	91.36 KB	application/octet-stream	Write, Access, Create	CLEAN
161e89b2d88c524a695d6f88962d20e958320baf3b238f5c97d362f3c9380667	C:\Users\RDhJ0CNFevzX\Documents\wljK1MkFwCn3.xls.kfuald	Dropped File	10.39 KB	application/octet-stream	Write, Access, Create	CLEAN
6ca86fadeaf4e94fe02ad9d0e4eab70badf3bbf1e1d90cd16a43f2fd606c64dd	C:\Users\RDhJ0CNFevzX\Documents\xU9MjOwvWLJY.csv.kfuald	Dropped File	18.88 KB	application/octet-stream	Write, Access, Create	CLEAN
264da6c11ba4f1052e871982d446357ef93df92c9c055ff3aa495aa0881daf50	C:\Users\RDhJ0CNFevzX\Documents\yCEpdF.odt.kfuald	Dropped File	95.23 KB	application/octet-stream	Write, Access, Create	CLEAN
52b7151ea797db7b45afe1755397cb4110be278b4565a7a161f96b7167f9cd3d	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.kfuald	Dropped File	265.05 KB	application/octet-stream	Write, Access, Create	CLEAN
6c62b12dabf349ad109fbe6f664f3eda24f291fd4fb7b2b480e8c68a3e15a157	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\-k2SG9eplCimY582CS.xls.kfuald	Dropped File	6.86 KB	application/octet-stream	Write, Access, Create	CLEAN
f25671789cf1dfb578e6f215a34ad9565d82ad563a7e1b2e498854805887658c	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\2aGiB5Vu8dFo.pdf.kfuald	Dropped File	74.00 KB	application/octet-stream	Write, Access, Create	CLEAN
d0074e9ca3e92d397a7234fa4bc56f2bed64105dd1e8f913f0c19d3686aebe0e	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZzpPoDQpQ8qTR.docx.kfuald	Dropped File	66.34 KB	application/octet-stream	Write, Access, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
6a9872a34d0e5be653e1ec84298162a4d04fc9f738f871b894567532d0655d9e	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZ8oHM1.pptx.kfuald	Dropped File	31.38 KB	application/octet-stream	Write, Access, Create	CLEAN
d849cfa1731ea762b9f30ad802c4739801c64b815766acc230be5a8d8a13bdef	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\ECUe.pps.kfuald	Dropped File	4.27 KB	application/octet-stream	Write, Access, Create	CLEAN
93dfee2c1e7ec33b85924ca885a79513e2cb7f71ef9491e53adc7fd318c2f63d	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\iMLPUH5839SPlcf.doc.kfuald	Dropped File	28.73 KB	application/octet-stream	Write, Access, Create	CLEAN
4892609907fe2c517cfe28468af156d9a9d417990cad0e908646c14afdcb86c5	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\Irbahn2XTjt0vqe9HfL.pptx.kfuald	Dropped File	83.72 KB	application/octet-stream	Write, Access, Create	CLEAN
6dc9518b47ae4b2c578903ba8eedc8ccecc20cb122b46f30c506654947a153d6	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\JxIpV.xls.kfuald	Dropped File	58.06 KB	application/octet-stream	Write, Access, Create	CLEAN
bb06f5b03003041e7c588a5e3898261cdbdabc9c84c9421f78d2043580242d7c	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\r3nAsVaI.odp.kfuald	Dropped File	12.06 KB	application/octet-stream	Write, Access, Create	CLEAN
4f8f7f12a8dc15c26b430e48bc1f2742e66e490aedb147747bd6a55aec9de6b8	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\2DW7QXR64oz.xlsx.kfuald	Dropped File	81.22 KB	application/octet-stream	Write, Access, Create	CLEAN
982a741bdf22d945a09977c2002d96700704c75698dc6f6ecec74b58590229f6	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\4hP4g805ELYzX.xls.kfuald	Dropped File	80.83 KB	application/octet-stream	Write, Access, Create	CLEAN
756e6364755066b4813ef8dd9408b3d0edbd7b1d41c12168b45bcb334049bd1e	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\eHFVA333EtxT.xlsx.kfuald	Dropped File	59.45 KB	application/octet-stream	Write, Access, Create	CLEAN
f2d1403aa65bc0d782f7e7c785cc1f2954c2089a92de3d3d19469a4c231b7f86	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\G0G_AVyyXuVQrqvU8.doc.kfuald	Dropped File	47.03 KB	application/octet-stream	Write, Access, Create	CLEAN
bdc8cf8a05637ab153d81d992858093b25f53498c651c1760f35d964646a9d4b	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\iPE90PQEnBDU.pps.kfuald	Dropped File	64.08 KB	application/octet-stream	Write, Access, Create	CLEAN
38033aea153fbd455ecabc945bb0c6a17cfcbeedace2ac9696e8156626f68110	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\nfPv2sbT6Wvhi16E.odp.kfuald	Dropped File	84.41 KB	application/octet-stream	Write, Access, Create	CLEAN
a34b98aff2c1fb75758f2de41ca90dd880586c8b9088e9bf042bf28045760338	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\WZZFbk7EZqKXbeD.ods.kfuald	Dropped File	32.17 KB	application/octet-stream	Write, Access, Create	CLEAN
75884a6afd2ffe65def824047be11eeaf853cfc55905b5e2224d5a8ba8732c7a	C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\xwVGQbDcVJE1vA2\XYhte4teKs65RLuMnq7.pps.kfuald	Dropped File	98.83 KB	application/octet-stream	Write, Access, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
de449357e30c550f0d5dde47e862f158c605613a37f0c618d0f33b78fa5df474	C:\Users\RDhJ0CNFevzX\Desktopyour files have been encrypted.kfuald.txt	Dropped File	5.54 KB	text/plain	Write, Access, Create	CLEAN

Filename

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\333.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\333.exe.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\333.exe	Sample File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\0_sc8lpuOR-.png.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\0_sc8lpuOR-.png	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\8ngyV20QtMP.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\8ngyV20QtMP.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\DJ11q92YZCfOl_L.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\DJ11q92YZCfOl_L.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\FeW8I.gif.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\FeW8I.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\fGdy9UGlpL6.gif.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\fGdy9UGlpL6.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\9oTZGBQn6POhNzuW4cC9.gif.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\9oTZGBQn6POhNzuW4cC9.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\AQnQQQ8Qa.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\AQnQQQ8Qa.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\vU7dn.png.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn\vU7dn.png	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn_8te40cGFqB.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\7q5Igh3ZHbzUE8nJTn_8te40cGFqB.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\2z8r-rInMai4ng0l.png.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\2z8r-rInMai4ng0l.png	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\428yCMsP5H.gif.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\428yCMsP5H.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bbhrwdO7CREtkiTfhwvG.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bbhrwdO7CREtkiTfhwvG.bmp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bZ5iXwv8rJ.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\bZ5iXwv8rJ.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\l8EnCbTqzZ.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\l8EnCbTqzZ.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\hHSY.gif.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\hHSY.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\kjoMFWZGlcEZGTaT.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\kjoMFWZGlcEZGTaT.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\UabbxPnk9mFO9n0-.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\UabbxPnk9mFO9n0-.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\ycvWF35JmUHZD9TF.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\-56LEi\ycvWF35JmUHZD9TF.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\4EC-NIq9H6XQjHrgH2.gif.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\4EC-NIq9H6XQjHrgH2.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\60RYSwKb4l8t.gif.kfuald	Dropped File	Write, Access, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\60RYSwKb4l8t.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\bXEt8I6nq.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\bXEt8I6nq.bmp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\M92sNjfyoi.png.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\M92sNjfyoi.png	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\ZLNmgOE4O9pXPtAxNhVy.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\ZLNmgOE4O9pXPtAxNhVy.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fq ei3XX5BBIz\BfmHAaxu.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fq ei3XX5BBIz\BfmHAaxu.bmp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fq ei3XX5BBIz\tqmHJ4dmir9XV.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\1X8Fq ei3XX5BBIz\tqmHJ4dmir9XV.bmp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\-JhjDC2AIcrMU1Sqww.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\-JhjDC2AIcrMU1Sqww.bmp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\IorQxNzqYx pX475.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\IorQxNzqYx pX475.bmp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\8fSQ8UtOL.png.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\8fSQ8UtOL.png	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\DQaWtpbPalB66C0Zbv.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\DQaWtpbPalB66C0Zbv.bmp	Accessed File	Delete, Access, Read	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\KFDMiHEziC1N_EC.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\KFDMiHEziC1N_EC.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\kspB96BT5Kro-.bmp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\l89y8z_sLA-3S7Jz4\KW-60E\bohzfm\kspB96BT5Kro-.bmp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\ejyC4n6QiKyh.gif.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\ejyC4n6QiKyh.gif	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\fDtUSYBe.png.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\fDtUSYBe.png	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\QDHUaG.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\QDHUaG.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\w3qvBj.jpg.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\qT-ecW9Dhu4cNPJGZ7c\BcRV_GQSK2\Ptrhjh\w3qvBj.jpg	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0A931C.rtf.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0A931C.rtf	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\7JpA4Ax39L.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\7JpA4Ax39L.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9ndEkH.xlsx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9ndEkH.xlsx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Accessed File	Delete, Access, Read	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\e1mHtEVePp6n5SIIH2.ods.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\e1mHtEVePp6n5SIIH2.ods	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fvRJbkxezpybfmolJ.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fvRJbkxezpybfmolJ.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\h7rmmJ75EUvYTZU.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\h7rmmJ75EUvYTZU.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\iZLXf9f3fQ-q.xls.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\iZLXf9f3fQ-q.xls	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\jB6tZPmpB7d5JGJ.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\jB6tZPmpB7d5JGJ.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\krM-01YH_.docx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\krM-01YH_.docx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\KV2Njrt.ods.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\KV2Njrt.ods	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Moeyr9UzHNHZH.xlsx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Moeyr9UzHNHZH.xlsx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\MSKvEq.docx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\MSKvEq.docx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\onXIIelcJCBs2_atOn.ots.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\onXIIelcJCBs2_atOn.ots	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\OV9cjW1KRPMZD6.xlsx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\OV9cjW1KRPMZD6.xlsx	Accessed File	Delete, Access, Read	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\peIc9.ppt.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\peIc9.ppt	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Q74iOtUSt-LdEt.xlsx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Q74iOtUSt-LdEt.xlsx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\QhvyDDZeU925SNWZ.xlsx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\QhvyDDZeU925SNWZ.xlsx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\r5y7X6BeH79.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\r5y7X6BeH79.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Sa0.docx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Sa0.docx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Sh8o9ZbL4AXv5mdqw aT.docx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Sh8o9ZbL4AXv5mdqw aT.docx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vof9fF.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vof9fF.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vS_gwWgi0tn.odp.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vS_gwWgi0tn.odp	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\VZPaIxcz7GLW.docx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\VZPaIxcz7GLW.docx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\wljK1MkFwCn3.xls.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\wljK1MkFwCn3.xls	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\xU9MjOwvWLJY.csv.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\xU9MjOwvWLJY.csv	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\yCEpdF.odt.kfuald	Dropped File	Write, Access, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\yCEpdF.odt	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\-k2S G9eplCimY582CS.xls.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\-k2S G9eplCimY582CS.xls	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\2aGiB5Vu8dFo.pdf.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\2aGiB5Vu8dFo.pdf	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZ zpPoDQpQ8qTR.docx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZ zpPoDQpQ8qTR.docx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZ8oHM1.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\CZ8oHM1.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\ECUe.pps.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\ECUe.pps	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\iMLPUH5839SPlcf.doc.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\iMLPUH5839SPlcf.doc	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\Irbahn2XTjt0vqe9HfL.pptx.kfuald	Dropped File	Write, Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\Irbahn2XTjt0vqe9HfL.pptx	Accessed File	Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vTuZUcXSG-8c_\JxIpV.xls.kfuald	Dropped File	Write, Access, Create	CLEAN

Reduced dataset

URL

-

Domain

-

IP

-

Email

-

Email Address

-

Mutex

-

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr	write, access, read	333.exe	MALICIOUS
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	333.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	333.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	333.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Desktop	access	333.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Desktop\Wallpaper	write, access, read	333.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	access	333.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	write, access, read	333.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	access, create	333.exe	CLEAN

Process

Process Name	Commandline	Verdict
333.exe	"C:\Users\RDhJ0CNFevzX\Desktop\333.exe"	MALICIOUS

YARA / AV

Antivirus (1)

File Type	Threat Name	Filename	Verdict
SAMPLE	Gen:Heur.Ransom.MSIL.1	C:\Users\RDhJ0CNFevzX\Desktop\333.exe	MALICIOUS

ENVIRONMENT

Virtual Machine Information

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

Analyzer Information

Analyzer Version	4.1.1
Dynamic Engine Version	4.1.1 / 02/08/2021 15:19
Static Engine Version	1.6.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (November 12, 2020)
Built-in AV Database Update Release Date	2021-04-26 09:13:57+00:00
VTI Ruleset Version	3.8
YARA Built-in Ruleset Version	1.5
Analysis Report Layout Version	10

Software Information

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