MALICIOUS

Classifications: Ransomware | Spyware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe**
ID	#5504523
MD5	cefa3818648f481c93acb3e95241e211
SHA1	c6d9addf290419d825724909f8bd01d44f2067a7
SHA256	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a
File Size	316.50 KB
Report Created	2022-09-22 22:35 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 19 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #2) tmp_asdqwd2.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #2) tmp_asdqwd2.exe renames multiple user files.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: git, Internet Explorer / Edge, The Bat!.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as Mal/Generic-S. • Reputation analysis labels file "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe" as Mal/Generic-S.			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #2) tmp_asdqwd2.exe possibly drops ransom note files (creates 275 instances of the file "READ_ME.htm" in different locations).			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #2) tmp_asdqwd2.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #2) tmp_asdqwd2.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) tmp_asdqwd2.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe".			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe creates mutex with name "Global\.net clr networking".			
1/5	Input Capture	Monitors mouse movements and clicks	1	-
	• (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe frequently reads the state of a mouse button by API.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe resolves host name "www.free-website-hit-counter.com" to IP "158.176.65.249". • (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe resolves host name "pastebin.com" to IP "104.20.68.143".			
1/5	Network Connection	Connects to remote host	3	-

Score	Category	Operation	Count	Classification
		• (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe opens an outgoing TCP connection to host "104.20.68.143:443". • (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe opens an outgoing TCP connection to host "158.176.65.249:80". • (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe opens an outgoing TCP connection to host "104.20.68.143:80".		
1/5	Execution	Drops PE file	1	-
		• (Process #1) fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe drops file "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe".		
1/5	Execution	Executes dropped PE file	1	-
		• Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe".		

Mitre ATT&CK Matrix

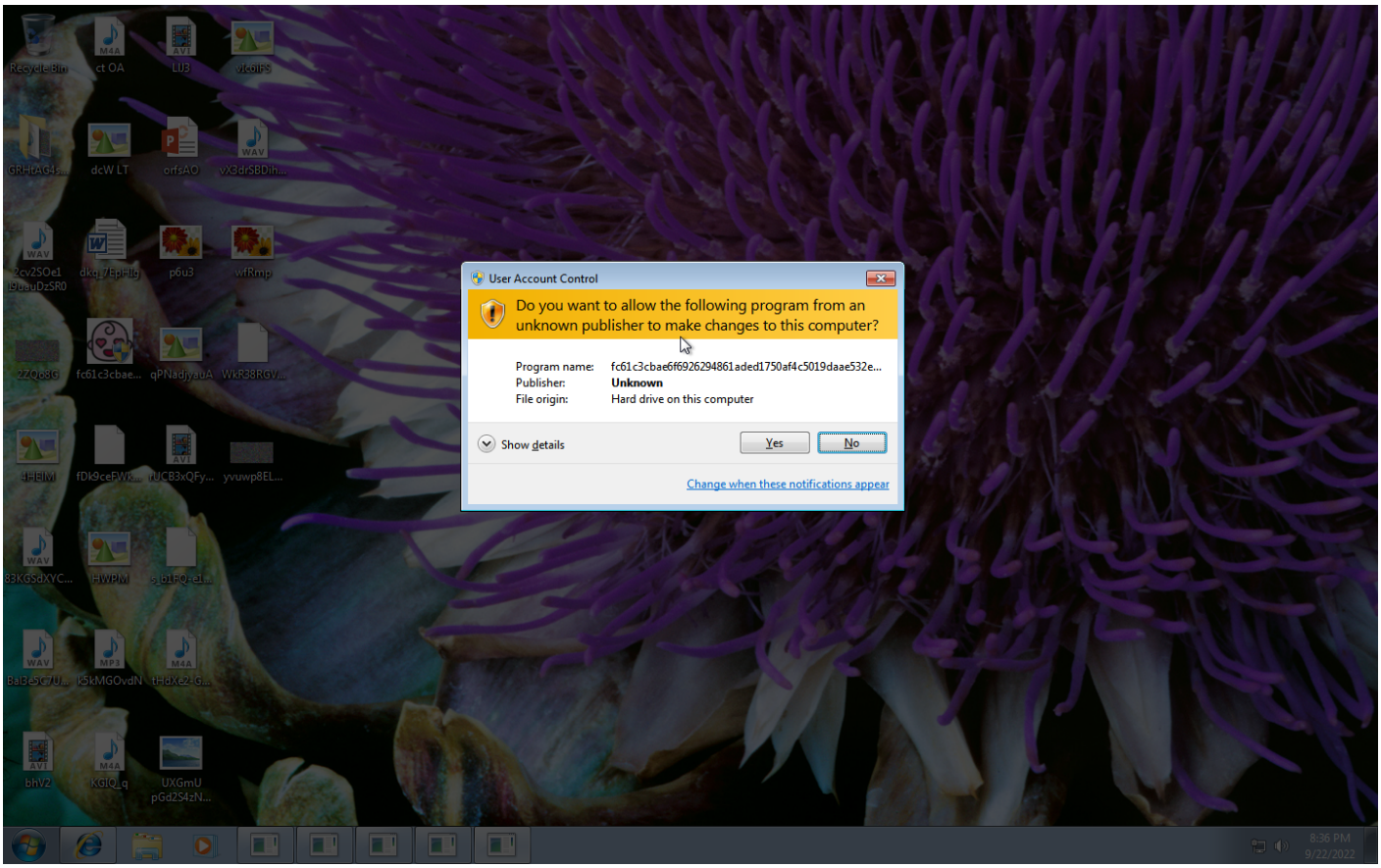
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
					#T1056 Input Capture	#T1083 File and Directory Discovery		#T1056 Input Capture			#T1486 Data Encrypted for Impact
					#T1081 Credentials in Files			#T1119 Automated Collection			
								#T1005 Data from Local System			

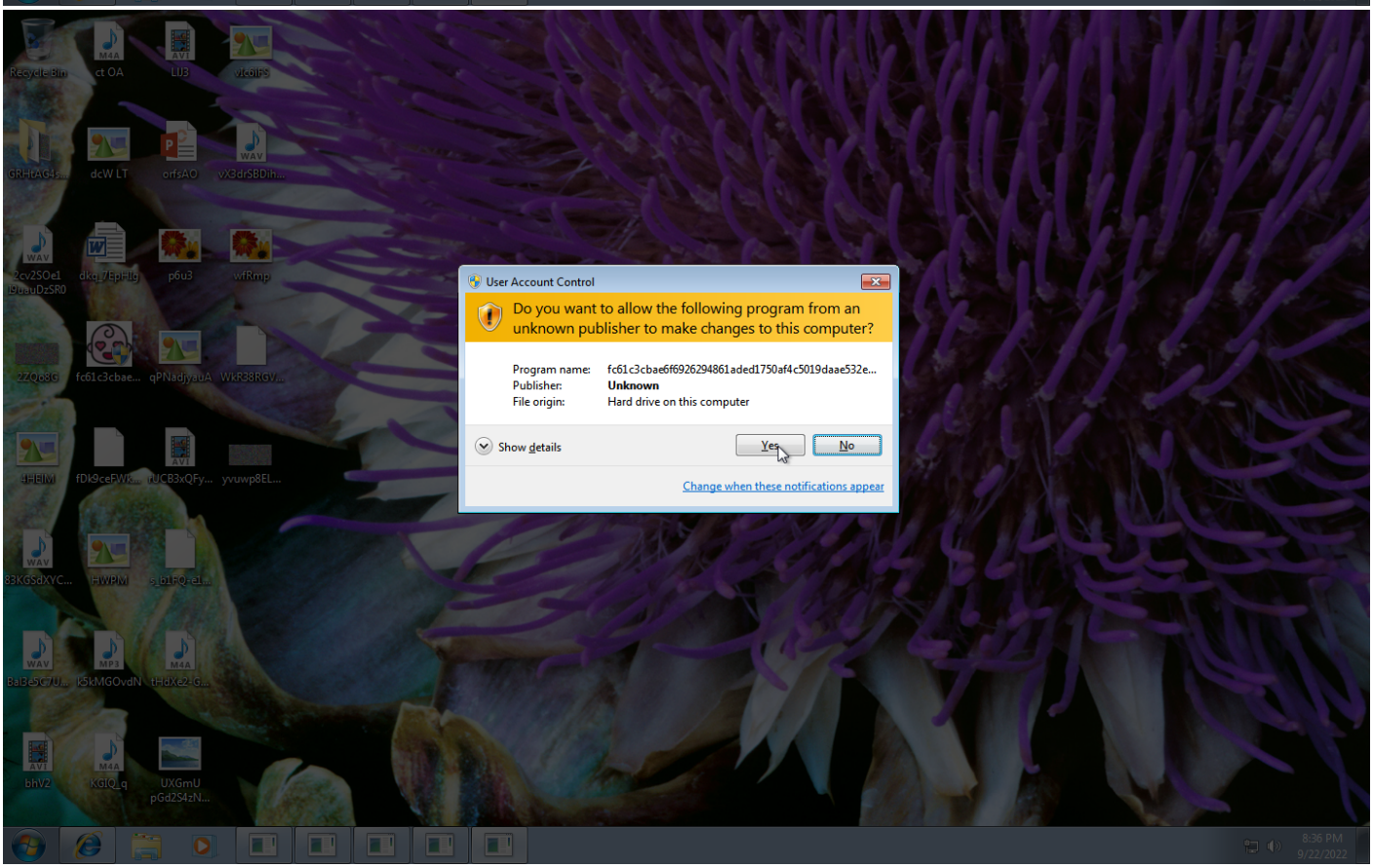
Sample Information

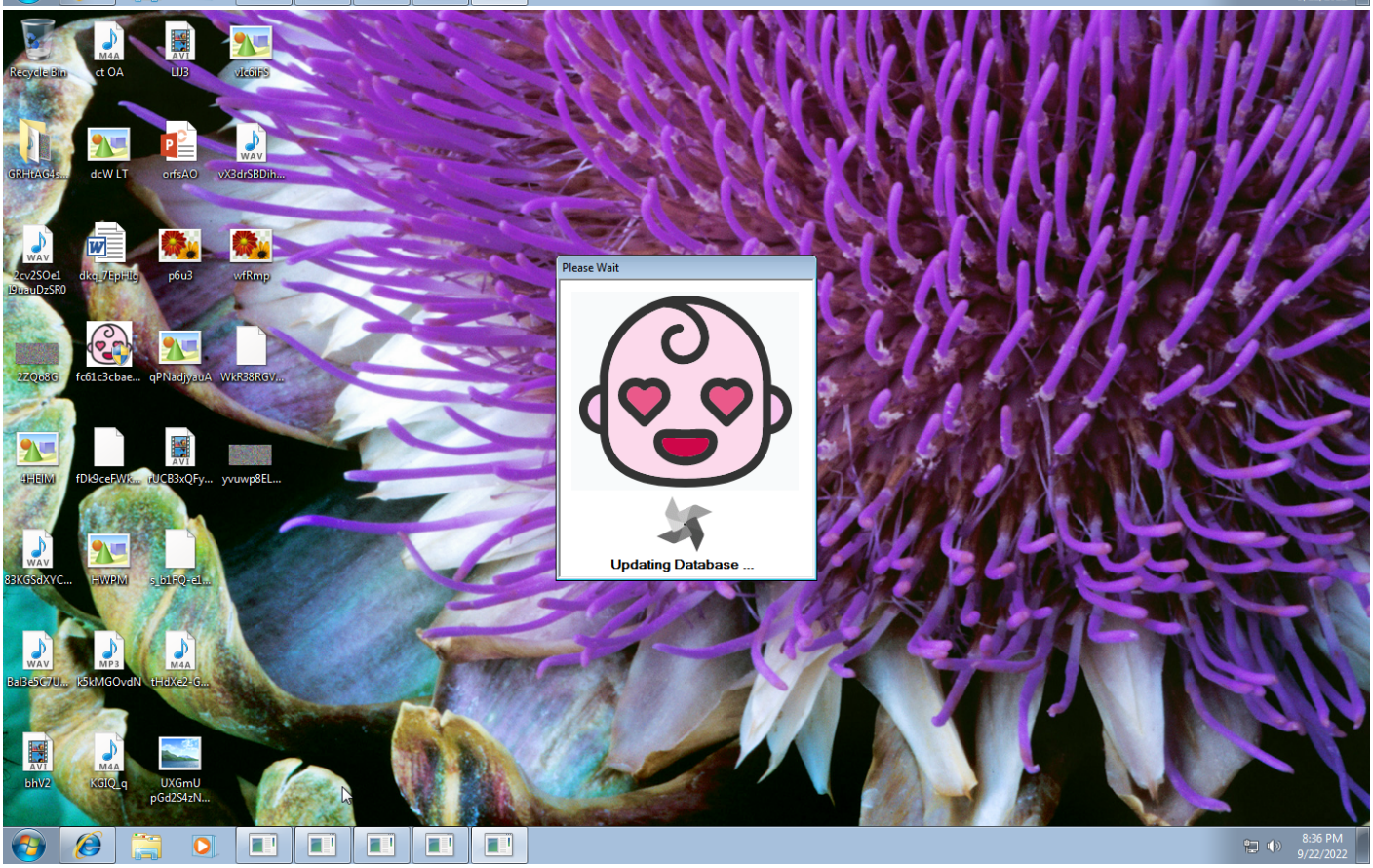
ID	#5504523
MD5	cefa3818648f481c93acb3e95241e211
SHA1	c6d9addf290419d825724909f8bd01d44f2067a7
SHA256	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a
SSDeep	6144:0tH1Q69RgUnTtcUx5rlxQamSsDan8ddaS/nEG54KcEGhlCJyyo:G97gSt7QamSsYUaM/KKcEGhcU
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe
File Size	316.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-09-22 22:35 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
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


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: fc61c3cbae6ff6926294861aded1750af4c5019daae532e...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: fc61c3cbae6ff6926294861aded1750af4c5019daae532e...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

3.27 KB total sent

10.37 KB total received

4 ports 80, 443, 53, 445

3 contacted IP addresses

1 URLs extracted

4 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 2 servers

5 sessions, 3.13 KB sent, 10.04 KB received

HTTP Requests

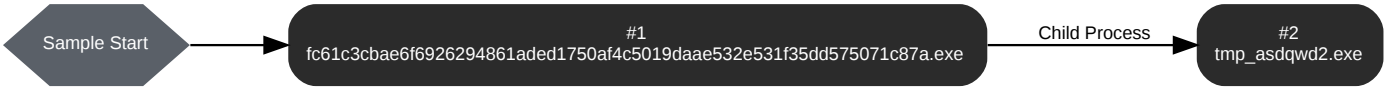
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.free-website-hit-counter.com/c.php?d=9&id=123252&s=2	-	-		0 bytes	NA
GET	http://www.free-website-hit-counter.com/c.php?d=9&id=123086&s=16	-	-		0 bytes	NA
GET	http://pastebin.com/raw/f1TMQySv	-	-		0 bytes	NA
GET	https://localbitcoins.com/guides/how-to-buy-bitcoins	-	-		0 bytes	NA
GET	https://pastebin.com/raw/f1TMQySv	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.free-website-hit-counter.com, free-website-hit-counter.com	NO_ERROR	158.176.65.249	free-website-hit-counter.com	NA
A	pastebin.com	NO_ERROR	104.20.68.143, 172.67.34.170, 104.20.67.143		NA

BEHAVIOR

Process Graph



Process #1: fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64942, Reason: Analysis Target
Unmonitor End Time	End Time: 179918, Reason: Terminated
Monitor duration	114.98s
Return Code	0
PID	3772
Parent PID	1888
Bitness	64 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe	160.50 KB	c78fe2783012de1f4771b380d1607b7d6822d80a3c62602bfe28678f384b54ba	✖
-	8.03 KB	c5e68bc6ec9388f0b0be98a6100459c5573044e269a87f804dac29c025505f52	✖
-	108.54 KB	07bb5948a0a337ab0cd2d6db088d56d8106f7ae2df40ee9ec86537d3b835f302	✖

Host Behavior

Type	Count
System	641
Module	23
Window	7
Registry	24
File	22
Keyboard	323
Process	1
-	10
Mutex	33
-	3

Network Behavior

Type	Count
HTTP	2
HTTPS	1
DNS	2
TCP	3

Process #2: tmp_asdqwd2.exe

ID	2
File Name	c:\users\keecfmwgj\appdata\local\temp\tmp_asdqwd2.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115933, Reason: Child Process
Unmonitor End Time	End Time: 178436, Reason: Terminated
Monitor duration	62.50s
Return Code	0
PID	3852
Parent PID	3772
Bitness	64 Bit

Dropped Files (539)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\TsyPWpsnMPhL\P55qinM.flv.air6xs	19.72 KB	fc97659f8b7b7dee75cbef363ded982b2c8e55c7e5e512a8c200c31880f394e6	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\avR1UifnHmhlJS.jpg.2786ed	88.55 KB	f1f3d9c7ac9dc5abeec7a168aec72b0ec73eb16ff7ae88774677c7a3ae591193	✖
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\LZmok.pdf.vdlv3o	87.23 KB	c12d470247806e37c1071aeb1dae6dccdb2be684b9fa8bb974b58759305318ed	✖
C:\Users\kEecfMwgj\Documents\xzzxF rzoZd o7Cf.pptx.pfb411	11.50 KB	e63e335fcb05432a185e1aabe954f7a8f636c8b5469b96561506897bee8e0205	✖
C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\X7gt.mp4.z0bvmw	75.34 KB	7aebcf84e1bafc09b2bf29c634c85a344981c20530233441abea4ea74bc25110	✖
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\lXgZA3JD1f_.rtf.2f13fx	75.12 KB	b96f440caef7fb6ff55b998248fdcad2f6e53b8734fa9bc845e421303cc3390e	✖
C:\Users\kEecfMwgj\AppData\Roaming\XNfiHAeLkxT6WxYO.m4a.pvi9ve	20.80 KB	94c6c5e0b926c955a9e89884af2bc461a2c3b7feff6e2433c6178337c6e51967	✖
C:\Users\kEecfMwgj\Pictures\Ap5aZoqdUEP.png.s2ypyd	94.25 KB	0bbab701df0d0c07575db201584a8907ebc064e134f1b3bdcd9319cfc841b2ed	✖
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.e6qpy0	5.16 KB	759470df58d112edf17e956d8037763b7f7d3084213ae2d3a21d72317a371665	✖
C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\t8c4sQgxZhGJp90o\G3cproBxiH\YkFaHc49kE 0.jpg.web6cn	91.44 KB	7d1d708ebefb2dc5260e03deb4fcb8cec0e4326ac0449ed345984bb8ee874e60	✖
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\MasterDescriptor.en-us.xml.xo1phl	21.86 KB	645defd44dc8e2e3a2b3dceff67b1d7c582c47892f953e7099bd8534c09cea5d	✖
C:\Users\kEecfMwgj\Documents\zIcOMqefwlUm\vXkkwtyn7WU6A.xls.516tp7	24.11 KB	8cdf16146aed9f4f0fb459286517f2af86d8a5add04b76f216303db206141806	✖
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.spt7cg	2.12 KB	00a0c56b1786128fd435caedeb3d535de974d2fb890c5663db6d1e35083eb2a1	✖
C:\Users\Public\Pictures\Sample Pictures\Koala.jpg.94f43u	762.53 KB	5eb059aa07103951295fbb76121ad209a63c6bf59141dba226bbea960cda445c	✖
C:\Users\kEecfMwgj\AppData\Roaming\RWmilgBZ3oS-YZH.gif.i9r11n	72.14 KB	1c1b42bb81ba32a4d5758d73421046a84cc7b3583ae7dca2a41c090ee2656fdd	✖
C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg.2tf4m6	858.80 KB	eece0800bc01bb462a39ca2039e7b6534a193920aaaeccd7f42bedfa1d58dfcb	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\xuKD9lnbmJOIcf\dadCFjWoK75rYQp0Ycn.flv.lc80hd	30.19 KB	2144b0c4fb0131f848be85a30cd693931bccd8081e8a96e22868e67f1b7a1fe2	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.png.qreinu	10.00 KB	620fd8a14212f9de613f87f97c7b5c16fd8b2e0c0d0e1fe07a02b4a2779e6a04	✖
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml.ap83un	16.72 KB	3a913adba810b2abb92d0e3a31d8fac8d503d339d6be4452f3ee31834f0b06c4	✖
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.0fm26x	1.19 KB	ff3b2e67a3c9d2dec43c65508d801481e075ab42c90d4ae241bd2439236c228a	✖
C:\Users\kEecfMwgj\Documents\j5g-Xfr8dqgh7T\H9Ph1__8iq0eDkOhCO.rtf.bs3gvh	82.83 KB	d985313ebf3650e2864d9bc585dcb9f7abdb1c2469a7f698f10e2acedecdd008	✖
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.2q5bez	2.72 KB	ceb531fc67347ded419ff54d7bf1b911887b89eac60f5a97b3910a7c013dcb3a	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\bJiFgZ6houa47UyvW.mp4.ylh0l1	40.12 KB	f0aabe960a368950d39ca44bb3000ecb219582b1c89be001e8b472fcad4c9839	✖
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml.22n576	4.89 KB	ecbc54e7d874e7e8a734d60b6f3e3581d9671164729506e00a8bc9b28efc3e84	✖
C:\Users\kEecfMwgj\Music\fXs7dyEh5KRVvZ0H\2KcT02McQ-LKwXH.m4a.v1unnn	92.28 KB	fc77bd492e068e11bb5188ae6050fa2b2148346828907700e800485df0dfa9b4	✖
C:\Users\kEecfMwgj\Pictures\xXMg NqTxoBvoofJbN8.gif.jgkx27	82.08 KB	5910051d0690a8f8fa4d89ff0f542f9cc7a4b703e5b7e56e307790d07fdcd985	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.gif.ck3ano	374.25 KB	88b68d5089b4ba5dfbac5937e265858a88c4b9167f94dd738d2d26d1cd3ce5dd	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\4n7INBARZ3VQX4.gif.qhuhy6	91.31 KB	cbaa9b3e346e851fdf4e2fa6d9f3260121249317a80d02b36c3e222734b35a32	✖
C:\Users\kEecfMwgj\Desktop\tHdXe2-Gmf-Jn.m4a.zq8ar0	53.97 KB	b21c25d507d3359b58a30f0b452c2d6c9ed156f6e63bd62a26a69f6f5e677527	✖
C:\Users\kEecfMwgj\Documents\j5g-Xfr8dqgh7T\J_lvk4yknnivy.ods.iwq3vk	85.41 KB	28cfab3491c360e0aedca938b623e2554dc4585c4d9a24ed6671e61d1985dfa1	✖
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml.aumo8t	3.78 KB	ce8fad00842e927d277bee525db6da755765a5f352d31d335edfec55da4d4cad	✖
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml.ahvgss	1.11 KB	c53619b40e3ae4151acd5c22ee592cdf511b41230e43b9426cb3431daf809b84	✖
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml.n3voag	1.53 KB	7c0ee63fb0b4c791b1796bf9ff182e18a783cc0c924a10cd8d3f3bfadd5f5f59	✖
C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\2rQiSlDpO4fwQ3nAaWxD.jpg.cxzxwr	6.73 KB	94a5ec8cfcdbe8f31ad67b7ae29acf55c1eb5a36b7019caeaa3d1af494617958	✖
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml.yufkg1	1.11 KB	6fe0c93f46f44829604a5b31c4d5098003f0cdacf6102760e6e4ad8d13f5c220	✖
C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg.fq7bxl	548.12 KB	a1f2d9ff972e24f210c5e6b4c9822180634ce4fea93e065ac883aaf8180da286	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\X7OTvBAgdZbJ.flv.gacda2	67.55 KB	bb5d01d20384697ec842d3601e480a565a90a705d47115ed795d3d845835acee	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\xuKD9lnbmJOlcf\UieYy.mp4.3m4q6i	1.30 KB	059d7c6303a2af008451e3c9d755e5fc075ad9e156cff790a101f801254d95fa	✖
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.xml.jro710	1.02 KB	61432ad691883767120d6d34bd9a0a74b091de0c3774b9af7c2fecc94cefbc3f	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\setup\logs\2021-02-22_125735_3c4-a98.log.nfscjj	17.14 KB	92f3c609aa4212bc34d24fb18a7047a2fa280f75f75bac4e9a73c220b1cd53c5	✖
C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg.h5q05d	581.34 KB	70745c9bcd4d579676f8138365bc1506bac8b09c57ddc3ce489667bab1217d3f	✖

File Name	File Size	SHA256	YARA Match
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml.j9ll6l	8.30 KB	f86f7d31d86cdfd059ca6933908cf6117755ecf85c387348e4085174be573329	✖
C:\Users\Public\Videos\Sample Videos\Wildlife.wmv.fliq06	10240.00 KB	fcc20470bcbf5dce30a3af58054414adf98441d91e593a61119c9a8c90ff2ad9	✖
C:\Users\kEecfMwgj\Desktop\dkq_7EpHIg.doc.7qpp12	4.22 KB	99ad6cba330824d048e695652fd69e0b53ca86923011d7ddacf0b367e357c308	✖
C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\L9bVBQTdPu.gif.hzus44	81.19 KB	d8dc74b1bc3cfd80aeb1fff424b2a1aa87e4a193920616bcda4fed8488ae0c38	✖
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml.jcr1h6	2.44 KB	69b365eaa1316884287acab54e4d1e4143c7df3784dd08379e9ccf5dcd76a03e	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\lOKKHz-jj1T03E2Exf\V2mn8JsxE2Wt-PJaw2f.mp4.smsk4z	78.80 KB	a1be88005896f7686e6568a97805d4c357b22023e2dfd56a9eb1669e0c54d196	✖
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.xml.u7jbaj	1.64 KB	c5ecf1bb76bfc1c98ab1468523692431585885e68d01e49394385099b265d4b3	✖
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml.0is9v9	2.00 KB	5b0f934630cc3a6eb567a39348980c3792114a597cdcafddaa4a54558fad5538	✖
C:\Users\kEecfMwgj\Desktop\qPNadjyauA.gif.4rurbq	70.80 KB	32ad865dafe570e511f710cc99eab9beb2e03d5d97f94b9394e6d358997cf333	✖
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml.lshxtz	3.06 KB	6bca28befd7ff554143fcaef3f59b5b73d7d85245f3050ba5b4e8fdf127d673b	✖
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml.8izi4i	2.41 KB	c7587995d6a5c81add75a61abed5174ceda34f41872404a5ebdf0fc01224032b	✖
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml.9721g8	2.53 KB	457887ba6b206e7f70cae3a9cf6a534718e90e95b859ceae66c4fd7e755f72de	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.ehptp5	11.92 KB	3d1e521dda8a5422174183d66c32cec791726c65b7c2095f8c0637ec59edf4f4	✖
C:\Users\kEecfMwgj\Documents\LtH-\ml1qaw b9lT2Kv6H0.ppt.iftoq9	5.14 KB	03efb94efa99bf2104b7cd4788295dae4f05e6c83594a72265d3428ff9b2dbe3	✖
C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.0.xml.1nwo7w	1.94 KB	1d691ca4086b87ddbec5137a96a82d470a1a3ce4c47b716cfcc9eac12f52bcc8	✖
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.s6qkht	1.20 KB	2977eefd4e84748e123195f5716adfdf737fff6c38f89f536b3d4cbcd919dfa0	✖
C:\Users\kEecfMwgj\Documents\LtH-\DCMx8oRdsb2P_vnN.xlsx.tk5rbt	61.25 KB	fc6c9e32c6d2fbd80fed0e1d0a5530e7eba4c7a305b945705874ea211d09fbd6	✖
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.gjao61	1.78 KB	c2c7c46711ee6ce4ca78009bddf7cfcd0327f40f4c3f19d471eef4ea26a80e39	✖
C:\Users\kEecfMwgj\Videos\9Af6Yl_3rtjrz2wEmaF.avi.puq588	36.06 KB	6f722a7074c0e855892a15fee1a2d734ca73455814f23b5caee0dd8318c21d18	✖
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml.l9ecyc	1.02 KB	50e5e30db93d4cae20fcfec95d8886c6b72568c80c5a7a16934ff6a9d33ae027	✖
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml.9oec2w	27.14 KB	f38df64fea9292adf71bd05f3a8a42e855586a2a8fedd89817f67bbe87c3ba13	✖
C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\t8c4sQgxZhGJp90o\U05NyfhFoOH.png.t95t8q	99.78 KB	f95c2ef86cbe4908adaf48e657b0d9492b8f54e22fa66dddc3c35d7642c9473b	✖
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\8aikgzugk.odt.xdemuf	96.78 KB	a7957a3a14fc54fc76da783dc13f3f7017472dc29b24c03aa0342845bd319216	✖
C:\Users\kEecfMwgj\Desktop\orfsAO.odp.feaooi	30.08 KB	7abd21da488152d6373a461324f8b8b59f4912302cbd8e7a4522605253fcd151	✖
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\branding.xml.oxal5s	328.44 KB	c56e964e0e89cac16ddaa5fc102c9cdb888d96c529fa70179def70a382cdd34b	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\C_98-V0.png.0tr42v	5.22 KB	49fca3375c6c85aa2fce31fc9cf643d4fcfa204d4d1d2cd9de9601f8e6c27293	✖
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.wqgmxy	1.77 KB	4632b39f8e911d0a1e1a0ca8b385c2305a58f64977385be5464afb142fa7a4a8	✖
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml.zln0j2	1.20 KB	315cbd62a6c09587254e0810b92cd69597fb20eba4a60b5691f0bb19fc35fd70	✖
C:\Users\kEecfMwgj\Documents\zIcOMqefwIUm\hOuHh_SwDbliUgNTQ.ppt.d5m7h1	53.11 KB	b32e2dbe80052ccb0a4541f27096658a14eb3967f59fbf48ac5932035878c29a	✖
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.372qjb	1.77 KB	e026d965faab230df7729e3fe622a9c293a6a8e247cd484cb93654807fb11afc	✖
C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\E-uYSW4Do.avi.l4ynmq	30.34 KB	f6508a076d3ca932ceb510f8903aa08c4ce7909bf1f5ae0713ca6b047960c4f1	✖
C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.1.xml.q20imu	1.94 KB	4cfe7fee0b5f4e18382048a5d370e274ce84baa8a15a5a78d4bae856cf04bfb8	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\xuKD9InbmJOIcf\CBZ05GkRAEgsJx 7.avi.e0jmia	56.41 KB	2b393606967cb5e6ac1855432af7abe57fb8b1ac658354602139ece61b9c8449	✖
C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.ykkkg1	11.92 KB	6ba05849b6bd9e62c8b9385dc83a960606ac76393afa73c93eb2fdf5fbb02ca9	✖
C:\Users\kEecfMwgj\AppData\Roaming\MzZay9cJsQOsYylg.gif.k9krsd	74.25 KB	efa812bea48f7c35c4f47838604ab5ef0f71208277116a64a4ef2b7b9d682cf4	✖
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.p4of38	1.02 KB	f7d3cdb34d2a56541efe7d738137865b128fbc8a94a8c3fbc05c7fc8244d3790	✖
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.fs3y21	1.75 KB	c1a17058856db049aedf0588738a86e85f7a44caea06bd1daab96f30a3e19ef0	✖
C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg.46zt8o	606.34 KB	affcd384aec8478c3253e266dfe8be2bde31ca97a328eebd342cebb1ecab3993	✖
C:\Users\Default\AppData\Local\Temp\FXSAPIDebugLogFile.txt.my5n59	16 bytes	c4d8677b592e0cf2c272d051a1b424abce9cc8ea45e41898e872d7e347481738	✖
C:\Users\kEecfMwgj\Pictures\4_gCpVi\V1tLRl90VOX8.png.mjm4gs	67.97 KB	6f33db7d9279454071d23b329a64b2c76267ed31f38b8aefd1535465e1bdd92b	✖
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\O5hM2sANeBEXGTf3mc.pdf.l8v5n1	94.19 KB	77a42c7a97c7fd9181e1af6ee075d254316597236655ea5990e194dcb5a019f1	✖
C:\Users\kEecfMwgj\AppData\Roaming\cpj-qQBHP_mKPrmP-k.jpg.014hhh	86.78 KB	d8edbc05e0630473157002219d9836c09c87bc791b775c4efd160f30ad1502ea	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\setup\logs\2021-02-22_125735_4d4-a74.log.uigyjm	7.83 KB	be881f2d695855ac822ae1bd68150708416bcd65079cfaaf214a639d3f366309	✖
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.r5i6uy	2.06 KB	239584da44cb9af6fcce8e4b0ac1ee44bee6034b9a67c5fa4029dc79559f0ed7	✖
C:\Users\kEecfMwgj\Music\4waS\aice20.m4a.mcap17	90.33 KB	06a6fc6ec76d67f1330a0db3fc3d001b2a469eb72a57a6f300a49e230bde6752	✖
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.1ebw4e	1.44 KB	b2909ad924d5475318863f8da4f3fd36cba007c3c4eac6cfda5606e0312dcbbd	✖
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.ll6jcd	1.78 KB	d48be6e5ee33f51228a2669feb2981fa7a817c0c8210ce5f70cfe0b8739c37d2	✖
C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg.fa0ws0	759.61 KB	8502d9d60f41d4c27b846bf527aa314d1501b01229fc811b1b4f2dcdc52e3518	✖
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml.w47ucz	1.62 KB	ea25944f78e9d7947d122bca8df70287468c60f7b073a5a677dfe8cfa6d86b8f	✖
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.xml.rnlrql	1.64 KB	3532213584b5ca2036236cd7a20be0ec1a60f19178789c4c6b37c814528ebbab	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Music\0Gi9jAAneSNZB2RiMYa\Hj4upkRDF60Y UCaU Lrc.m4a.qdw7kn	79.75 KB	03da4c1cfa3b8322b62f31c9e2ff96d61fcf6e8f5f5ec0fb5063d69d0fa396a4	✖
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.y51l5q	2.03 KB	44d819b8e533c41899fa22e20115429562ec7a368cea5507645228b66f8faf0f	✖
C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.3rraty	265.02 KB	1a470173268625ecb7409783f7ad46fbf6042b8cecf087b7dee76637bbc0faf6	✖
C:\Users\kEecfMwgj\AppData\Roaming\h1YIXDOe1dpX6GMny-.gif.ioof6z	27.31 KB	e46d299516a44c3574ef2f1ab366ce7dc4e5425a9c7793e463ff69d1a2cc01ad	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\b8T3auYtVogPw5aYbN8s.gif.90vseg	8.22 KB	53721f3da71fe295360527058d2708cd0c576941a47ce1581166e76509f5e610	✖
C:\Users\kEecfMwgj\Music\fXs7dyEh5KRVvZ0H\3WvCbF\xEnzmTd-.m4a.dsvy3z	41.61 KB	e5a7d8022da5adfce36ffd2c63b2275fe4efc4f1f3256a2b93d77d00ef7e82c7	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\rjMao5c8LjOzfjEul.avi.4oc6sd	78.31 KB	ffb8ca74462c82eef67e6ccaa59051c66366a68e35a4439ef0534df8b1e0150c	✖
C:\Users\kEecfMwgj\Documents\bjeZGjCALbyoQVDOz.xlsx.32cbio	98.77 KB	fa305c0d075480ac338f2babb924a92f2584088f0f7a0c1eceedb281745178b6	✖
C:\Users\kEecfMwgj\Pictures\4_gCpVi\UfIU4AupJZ3uu6WTr4v.jpg.ojft9j	11.70 KB	7345f730255f43d457bbe084c06403ff9fb79dfa9076d08f6e72bb759ac456cb	✖
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\xymCfQvs0a.xls.72ykhx	1.23 KB	a48d399eeee1a47b52e0e9cd64a9e1276a62a072008376825945442cf4526f86	✖
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.xml.769aog	1.42 KB	f7d4285217e2e5432f0c72416020eddc38cbf84f8746b71fc3c07392b74748b8	✖
C:\Users\Public\Pictures\Sample Pictures\Desert.jpg.hkno0p	826.12 KB	368de5ccc6dd66b9b4e92b018a68b265c77cd7c016aec7bcec118eeeb2f30b98	✖
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.0cgvfm	2.78 KB	46c7fdb6c7392ec16e1aa63c0911836b44e7ef9856712a2d0caaf40b32efdbe7	✖
C:\Users\kEecfMwgj\Documents\QblbR\eUc2ZnHoSmyslPJGT.docx.5vq8c1	29.33 KB	62fe7fd3851aceba0a2cc616f753aefb596a80227543ffe4593cb6d6d5172d8b	✖
C:\Users\kEecfMwgj\Documents\3CgFzZIG5azlFPRBrK.docx.k0b23c	93.64 KB	a70f9cec35a1fcc8270d96bef8515bb30bbf2a32bc624f1bfe1e2f4da8ece283	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\dvnjFpGyCrr4q.odp.pl1oog	89.11 KB	051770425e40162ffc645b61235b2a0c0bb173ddcdf2b64f640ff2658168d082	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\dsXGshyj.xlsx.rIteh8	97.55 KB	6dc83f682afd7dde6ad4c631dccbf5379fb83ffe82fef3bb0389a16ba6c356f2	✖
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.41gmdo	1.88 KB	e6a18fa1241a6caa7b708b60a0c5669e3da1b87e6d43395efa574a5acbed0808	✖
C:\Users\kEecfMwgj\Documents\DG0rAqFzdHUG15.csv.ktemy1	91.94 KB	be6fec859553357dae6bcdd7e1f7aed45fd28bdb842fd0f392de7103622f0727	✖
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.1v9a9r	1.61 KB	c71c52dcba65a3923bcffefe869a65320ded314973893e9a71304d57a7927fbd	✖
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.14t4b9	1.66 KB	5fde7c5d5607c656da2badf592d5765c22f8af8adaf5afccafa7fabc2aff621d	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\Tg9U9jjSqkvBNtKz.mp4.4l6y33	67.62 KB	d03a3b0ad800d2c32b12ac2c169c0b6c5b9afdafc4e69dd4b8a8d59443168fbe	✖
C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.2.xml.o1gru5	1.36 KB	1bbed2e4896985823a9f89f9bd25546c2150b435d63cf94140bf3fc814bd233e	✖
C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\READ_ME.htm	1.78 KB	612cef3e4facd583dcce79f3c985337cb7ae4fd19f2e9a81e7e698cbd1f59cd6	✖
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.jh7mub	5.94 KB	28e955b5c54135f88c9548308d47ad89356030122a025dbec5176d6d1195fafe	✖

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\MasterDescriptor.x-none.xml.3rvlpy	20.55 KB	a646e4fc87b24dfba68c62b618740533188ebd76a5281e6d2034bb20f6a48f8b	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ExclusionList.xml.xu45my	19.59 KB	656c63fa20f0da797ee19010d0afe69c286c4802cf35e6144cf13ce5e7d2f285	✖
C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg.orihz5	757.53 KB	f3dd3bc5f5a0cd0842e3456ad7f780acbd8ed6adeb2e0c97144342ceb9c3acb2	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\DNuRUiZ.mp4.6p6vk5	68.39 KB	68cc57925ccdbed866eaaa0d490e607c6876f941c202df99cab4ffb45ba7088b	✖
C:\Users\kEecfMwgj\Documents\Xy9pNIL0lNohzVp4.docx.b0zv1t	17.17 KB	3b40a84da79b915545af22cdc443e1b4886f9a2eccb759bb86bea026c8805e53	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\dvwxkOLliLo8iOIR.pdf.ghibwm	36.22 KB	ebedf3577fe5a76f91a051570ba73bc7225d7cb7696d4629f16ad16e4ef939ec	✖
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\gohAPDYvxpiV5JD.ppt.rqnezo	96.83 KB	a7c4d9dae7cef5542b4d882208c207dcc30e97b367cb5db7ef1096b27fe019a4	✖
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml.ofmwoh	1.62 KB	11669fab4ad07dc89fb9a0a0abfe4f8e20df8c238fb3462d8a1218c9fc4571a6	✖
C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\qs5-GxiBYrtogzhqzA1S.png.m3pobg	39.52 KB	f7c45a4649e0b3b27c2170754e28f6bca7d7dcb75a1bc8a51b4dbb847491d880	✖
C:\Users\kEecfMwgj\Pictures\nFvnUcfZr2ciaqvGBH.gif.mzjhl5	88.64 KB	3f28781e58902f6494d420b81c527b3ceeae6a37eafe87ec4915606b3f0fef28	✖
C:\Users\kEecfMwgj\AppData\Roaming\EPBdPl2nUBwLxi2a.gif.bk1t6w	75.23 KB	e1aaa83400cb48d9cd1cfed035ddc55b287d74f9f965cc04d22c5e083d50acf6	✖
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml.eptbtw	1.02 KB	43d27943144a429074238a2a1550f898879727937ee9384dd4b44dbb9759dd44	✖
C:\Users\kEecfMwgj\AppData\Roaming\4n0L _Me_g-.m4a.b2x8a9	56.80 KB	85564416d9d4570ab9967c72cd02f1c9d7289827081120dc4679fa3993728d82	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\TsyPWpsnMPhL\vEsxlZJ6fy_JVYxR43.pptx.9hyf53	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\af\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\Documents\j5g-Xfr8dqgh7T\fIAl.docx.15psg9	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\quz-pe\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Document Building Blocks\1033\16\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Feeds\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\Documents\QblbR\6RjpQT8xrF.xls.ehdew2	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\pXTOnk25mpA16xy.odp.lrypin	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ha-latn-ng\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\16.0\officec2rclient.exe_Rules.xml.u9ydcp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\Documents\FQRLvgP_7y0.pptx.64ehxa	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Crypto\RSA\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\Videos_6W_tOp4\OScpcujUrV9u.avi.6lzous	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\kEecfMwgj\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\READ_ME.htm	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Reduced dataset

Host Behavior

Type	Count
System	18
Environment	1
Module	18
Window	8
Registry	3
File	6366
Process	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a	C:\Users\kEecfMwgj\Desktop\fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	Sample File	316.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c78fe2783012de1f4771b380d1607b7d6822d80a3c62602bfe28678f384b54ba	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe	Dropped File	160.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
fc97659f8b7b7dee75cbef363ded982b2c8e55c7e5e512a8c200c31880f394e6	C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\TsyPWpsnMPhL\P55qinM.flv.air6xs	Dropped File	19.72 KB	application/octet-stream	Access, Create, Write	CLEAN
f1f3d9c7ac9dc5abeec7a168aec72b0ec73eb16ff7ae88774677c7a3ae591193	C:\Users\kEecfMwgj\AppData\Local\Temp\avR1UifnHmhlJS.jpg.2786ed	Dropped File	88.55 KB	application/octet-stream	Access, Create, Write	CLEAN
c12d470247806e37c1071aeb1dae6dccdb2be684b9fa8bb974b58759305318ed	C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\LZmok.pdf.vdlv3o	Dropped File	87.23 KB	application/octet-stream	Access, Create, Write	CLEAN
e63e335fcb05432a185e1aabe954f7a8f636c8b5469b96561506897bee8e0205	C:\Users\kEecfMwgj\Documents\xzzxFrzoZd o7Cf.pptx.pfb411	Dropped File	11.50 KB	application/octet-stream	Access, Create, Write	CLEAN
7aebcf84e1bafc09b2bf29c634c85a344981c20530233441abea4ea74bc25110	C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\X7gt.mp4.z0bvmw	Dropped File	75.34 KB	application/octet-stream	Access, Create, Write	CLEAN
b96f440caef7fb6ff55b998248fdcad2f6e53b8734fa9bc845e421303cc3390e	C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\lXgZA3JD1f_.rtf.2f13fx	Dropped File	75.12 KB	application/octet-stream	Access, Create, Write	CLEAN
94c6c5e0b926c955a9e89884af2bc461a2c3b7feff6e2433c6178337c6e51967	C:\Users\kEecfMwgj\AppData\Roaming\XNfiHAeLkxT6WxYO.m4a.pvi9ve	Dropped File	20.80 KB	application/octet-stream	Access, Create, Write	CLEAN
0bbab701df0d0c07575db201584a8907ebc064e134f1b3bdcd9319cfc841b2ed	C:\Users\kEecfMwgj\Pictures\Ap5aZoqdUEP.png.s2ypyd	Dropped File	94.25 KB	application/octet-stream	Access, Create, Write	CLEAN
b6df767e9e023e8bfa1b354c106f585fbbf984d1e17e2a4c1ca1019d851b2030	-	Downloaded File	783 bytes	image/gif	-	CLEAN
759470df58d112edf17e956d8037763b7f7d3084213ae2d3a21d72317a371665	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.e6qpy0	Dropped File	5.16 KB	application/octet-stream	Access, Create, Write	CLEAN
7d1d708ebefb2dc5260e03deb4fcb8cec0e4326ac0449ed345984bb8ee874e60	C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\t8c4sQgxZhGJp90o\G3cproBxiH\YkFaHc49kE 0.jpg.web6cn	Dropped File	91.44 KB	application/octet-stream	Access, Create, Write	CLEAN
645defd44dc8e2e3a2b3dceff67b1d7c582c47892f953e7099bd8534c09cea5d	C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\MasterDescriptor.en-us.xml.xo1phl, C:\ProgramData\Microsoft\ClickToRun\634EF343-54B0-4B56-9FD9-A785E3F22968\en-us.16\MasterDescriptor.en-us.xml.9tat37	Dropped File	21.86 KB	application/octet-stream	Access, Create, Write	CLEAN
8cdf16146aed9f4f0fb459286517f2af86d8a5add04b76f216303db206141806	C:\Users\kEecfMwgj\Documents\zIcOMqefwIUm\vXkkwtyn7WU6A.xls.516tp7	Dropped File	24.11 KB	application/octet-stream	Access, Create, Write	CLEAN
00a0c56b1786128fd435caedeb3d535de974d2fb890c5663db6d1e35083eb2a1	C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.spt7cg	Dropped File	2.12 KB	application/octet-stream	Access, Create, Write	CLEAN
5eb059aa07103951295fbb76121ad209a63c6bf59141dba226bbea960cda445c	C:\Users\Public\Pictures\Sample Pictures\Koala.jpg.94f43u	Dropped File	762.53 KB	application/octet-stream	Access, Create, Write	CLEAN
1c1b42bb81ba32a4d5758d73421046a84cc7b3583ae7dca2a41c090ee2656fdd	C:\Users\kEecfMwgj\AppData\Roaming\RWmilgBZ3oS-YZH.gif.i9r11n	Dropped File	72.14 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
eece0800bc01bb462a39ca2039e7b6534a193920aaaeccd7f42bedfa1d58dfcb	C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg.2tf4m6	Dropped File	858.80 KB	application/octet-stream	Access, Create, Write	CLEAN
bff32a9f8c9ba4555bf54ddbe650304ba6b8022f5ed8fef7ef3f949ff4d3da47	-	Downloaded File	776 bytes	image/gif	-	CLEAN
2144b0c4fb0131f848be85a30cd693931bccd8081e8a96e22868e67f1b7a1fe2	C:\Users\kEecfMwgj\Videos_6W_tOp4\xuKD9lnbmJOIcf\dadCFjWoK75rYQp0Ycn.flv.lc80hd	Dropped File	30.19 KB	application/octet-stream	Access, Create, Write	CLEAN
620fd8a14212f9de613f87f97c7b5c16fd8b2e0c0d0e1fe07a02b4a2779e6a04	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.png.qreinu	Dropped File	10.00 KB	application/octet-stream	Access, Create, Write	CLEAN
3a913adba810b2abb92d0e3a31d8fac8d503d339d6be4452f3ee31834f0b06c4	C:\MSOCache\All Users\{90160000-0011-0000-0000-000000000FF1CE}-C\ProPlusWW.xml.ap83un	Dropped File	16.72 KB	application/octet-stream	Access, Create, Write	CLEAN
ff3b2e67a3c9d2dec43c65508d801481e075ab42c90d4ae241bd2439236c228a	C:\MSOCache\All Users\{90160000-0090-0409-0000-000000000FF1CE}-C\DCFMUI.xml.0fm26x	Dropped File	1.19 KB	application/octet-stream	Access, Create, Write	CLEAN
d985313ebf3650e2864d9bc585dcb9f7abdb1c2469a7f698f10e2acedecdd008	C:\Users\kEecfMwgj\Documents\j5g-Xfr8dqgh7T\H9Ph1__8iq0eDkOhCO.rtf.bs3gvh	Dropped File	82.83 KB	application/octet-stream	Access, Create, Write	CLEAN
ceb531fc67347ded419ff54d7bf1b911887b89eac60f5a97b3910a7c013dcb3a	C:\MSOCache\All Users\{90160000-001B-0409-0000-000000000FF1CE}-C\Setup.xml.2q5bez	Dropped File	2.72 KB	application/octet-stream	Access, Create, Write	CLEAN
f0aabe960a368950d39ca44bb3000ecb219582b1c89be001e8b472fcad4c9839	C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\bJiFgZ6houa47UyvW.mp4.yIh0l1	Dropped File	40.12 KB	application/octet-stream	Access, Create, Write	CLEAN
ecbc54e7d874e7e8a734d60b6f3e3581d9671164729506e00a8bc9b28efc3e84	C:\MSOCache\All Users\{90160000-0011-0000-0000-000000000FF1CE}-C\Office64WW.xml.22n576	Dropped File	4.89 KB	application/octet-stream	Access, Create, Write	CLEAN
fc77bd492e068e11bb5188ae6050fa2b2148346828907700e800485df0dfa9b4	C:\Users\kEecfMwgj\Music\fXs7dyEh5KRVvZ0H\2KcT02McQ-LKwXH.m4a.v1unnn	Dropped File	92.28 KB	application/octet-stream	Access, Create, Write	CLEAN
5910051d0690a8f8fa4d89ff0f542f9cc7a4b703e5b7e56e3077790d07fdcd985	C:\Users\kEecfMwgj\Pictures\xXMgNqTxoBvoofJbN8.gif.jgkx27	Dropped File	82.08 KB	application/octet-stream	Access, Create, Write	CLEAN
88b68d5089b4ba5dfbac5937e265858a88c4b9167f94dd738d2d26d1cd3ce5dd	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.gif.ck3ano	Dropped File	374.25 KB	application/octet-stream	Access, Create, Write	CLEAN
cbaa9b3e346e851fdf4e2fa6d9f3260121249317a80d02b36c3e222734b35a32	C:\Users\kEecfMwgj\AppData\Local\Temp\4n7INBARZ3VQX4.gif.qhuhy6	Dropped File	91.31 KB	application/octet-stream	Access, Create, Write	CLEAN
b21c25d507d3359b58a30f0b452c2d6c9ed156f6e63bd62a26a69f6f5e677527	C:\Users\kEecfMwgj\Desktop\tHdXe2-Gmf-Jn.m4a.zq8ar0	Dropped File	53.97 KB	application/octet-stream	Access, Create, Write	CLEAN
28cfab3491c360e0aedca938b623e2554dc4585c4d9a24ed6671e61d1985dfa1	C:\Users\kEecfMwgj\Documents\j5g-Xfr8dqgh7T\J_lvk4yknnivy.ods.iwq3vk	Dropped File	85.41 KB	application/octet-stream	Access, Create, Write	CLEAN
ce8fad00842e927d277bee525db6da755765a5f352d31d335edfec55da4d4cad	C:\MSOCache\All Users\{90160000-001A-0409-0000-000000000FF1CE}-C\Setup.xml.aumo8t	Dropped File	3.78 KB	application/octet-stream	Access, Create, Write	CLEAN
c53619b40e3ae4151acd5c22ee592cdf511b41230e43b9426cb3431daf809b84	C:\MSOCache\All Users\{90160000-00BA-0409-0000-000000000FF1CE}-C\GrooveMUI.xml.ahvgss	Dropped File	1.11 KB	application/octet-stream	Access, Create, Write	CLEAN
7c0ee63fb0b4c791b1796bf9ff182e18a783cc0c924a10cd8d3f3bfadd5f5f59	C:\MSOCache\All Users\{90160000-002C-0409-0000-000000000FF1CE}-C\Proof.en\Proof.xml.n3voag	Dropped File	1.53 KB	application/octet-stream	Access, Create, Write	CLEAN
94a5ec8cfcdbe8f31ad67b7ae29acf55c1eb5a36b7019caeaa3d1af494617958	C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\2rQiSlDpO4fwQ3nAaWxD.jpg.cxzxwr	Dropped File	6.73 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6fe0c93f46f44829604a5b31c4d5098003f0cdacf6102760e6e4ad8d13f5c220	C:\MSOCache\All Users\{90160000-00E1-0409-0000-000000FF1CE}-C\OSMMUI.xml.yufkg1	Dropped File	1.11 KB	application/octet-stream	Access, Create, Write	CLEAN
a1f2d9ff972e24f210c5e6b4c9822180634ce4fea93e065ac883aaf8180da286	C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg.fq7bxl	Dropped File	548.12 KB	application/octet-stream	Access, Create, Write	CLEAN
bb5d01d20384697ec842d3601e480a565a90a705d47115ed795d3d845835acee	C:\Users\kEecfMwgj\Videos_6W_tOp4\X7OTvBAgdZbJ.flv.gacda2	Dropped File	67.55 KB	application/octet-stream	Access, Create, Write	CLEAN
059d7c6303a2af008451e3c9d755e5fc075ad9e156cff790a101f801254d95fa	C:\Users\kEecfMwgj\Videos_6W_tOp4\xuKD9lnbmJOIcf\UieYy.mp4.3m4q6i	Dropped File	1.30 KB	application/octet-stream	Access, Create, Write	CLEAN
61432ad691883767120d6d34bd9a0a74b091de0c3774b9af7c2fecc94cefbc3f	C:\MSOCache\All Users\{90160000-0117-0409-0000-000000FF1CE}-C\AccessMUISet.xml.jro710	Dropped File	1.02 KB	application/octet-stream	Access, Create, Write	CLEAN
92f3c609aa4212bc34d24fb18a7047a2fa280f75f75bac4e9a73c220b1cd53c5	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\setup\logs\2021-02-22_125735_3c4-a98.log.nfscjj	Dropped File	17.14 KB	application/octet-stream	Access, Create, Write	CLEAN
70745c9bcd4d579676f8138365bc1506bac8b09c57ddc3ce489667bab1217d3f	C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg.h5q05d	Dropped File	581.34 KB	application/octet-stream	Access, Create, Write	CLEAN
f86f7d31d86cdfd059ca6933908cf6117755ecf85c387348e4085174be573329	C:\MSOCache\All Users\{90160000-0115-0409-0000-000000FF1CE}-C\Setup.xml.j9ll6l	Dropped File	8.30 KB	application/octet-stream	Access, Create, Write	CLEAN
fcc20470bcbf5dce30a3af58054414adf98441d91e593a61119c9a8c90ff2ad9	C:\Users\Public\Videos\Sample Videos\Wildlife.wmv.fliq06	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN
99ad6cba330824d048e695652fd69e0b53ca86923011d7ddacf0b367e357c308	C:\Users\kEecfMwgj\Desktop\dkq_7EpHIg.doc.7qpp12	Dropped File	4.22 KB	application/octet-stream	Access, Create, Write	CLEAN
d8dc74b1bc3cfd80aeb1fff424b2a1aa87e4a193920616bcda4fed8488ae0c38	C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\L9bVBQTdPu.gif.hzus44	Dropped File	81.19 KB	application/octet-stream	Access, Create, Write	CLEAN
69b365eaa1316884287acab54e4d1e4143c7df3784dd08379e9ccf5dcd76a03e	C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\Setup.xml.jcr1h6	Dropped File	2.44 KB	application/octet-stream	Access, Create, Write	CLEAN
a1be88005896f7686e6568a97805d4c357b22023e2dfd56a9eb1669e0c54d196	C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\lOKKHz-jj1T03E2Exf\V2mn8JsxE2Wt-PJaw2f.mp4.smsk4z	Dropped File	78.80 KB	application/octet-stream	Access, Create, Write	CLEAN
c5ecf1bb76bfc1c98ab1468523692431585885e68d01e49394385099b265d4b3	C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.es\Proof.xml.u7jbaj	Dropped File	1.64 KB	application/octet-stream	Access, Create, Write	CLEAN
5b0f934630cc3a6eb567a39348980c3792114a597cdcafddaa4a54558fad5538	C:\MSOCache\All Users\{90160000-00E1-0409-0000-000000FF1CE}-C\Setup.xml.0is9v9	Dropped File	2.00 KB	application/octet-stream	Access, Create, Write	CLEAN
32ad865dafe570e511f710cc99eab9beb2e03d5d97f94b9394e6d358997cf333	C:\Users\kEecfMwgj\Desktop\qPNadjyauA.gif.4rurbq	Dropped File	70.80 KB	application/octet-stream	Access, Create, Write	CLEAN
6bca28befd7ff554143fcaef3f59b5b73d7d85245f3050ba5b4e8fdf127d673b	C:\MSOCache\All Users\{90160000-0116-0409-1000-000000FF1CE}-C\Setup.xml.lshxtz	Dropped File	3.06 KB	application/octet-stream	Access, Create, Write	CLEAN
c7587995d6a5c81add75a61abed5174ceda34f41872404a5ebdf0fc01224032b	C:\MSOCache\All Users\{90160000-00E2-0409-0000-000000FF1CE}-C\Setup.xml.8izi4i	Dropped File	2.41 KB	application/octet-stream	Access, Create, Write	CLEAN
457887ba6b206e7f70cae3a9cf6a534718e90e95b859ceae66c4fd7e755f72de	C:\MSOCache\All Users\{90160000-0117-0409-0000-000000FF1CE}-C\Setup.xml.9721g8	Dropped File	2.53 KB	application/octet-stream	Access, Create, Write	CLEAN
e26dc05f3f66277f5ab92cd0e156d71034f2a0d67aebe00c2554119ff0d66320	-	Downloaded File	1.41 KB	image/gif	-	CLEAN
3d1e521dda8a5422174183d66c32cec791726c65b7c2095f8c0637ec59edf4f4	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.ehptp5	Dropped File	11.92 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
03efb94efa99bf2104b7cd4788295dae4f05e6c83594a72265d3428ff9b2dbe3	C:\Users\kEecfMwgj\Documents\LtH-\ml1qaw b9lT2Kv6H0.ppt.iftoq9	Dropped File	5.14 KB	application/octet-stream	Access, Create, Write	CLEAN
1d691ca4086b87ddbec5137a96a82d470a1a3ce4c47b716cfcc9eac12f52bcc8	C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.0.xml.1nwo7w	Dropped File	1.94 KB	application/octet-stream	Access, Create, Write	CLEAN
2977eefd4e84748e123195f5716adfdf737fff6c38f89f536b3d4cbcd919dfa0	C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.s6qkht	Dropped File	1.20 KB	application/octet-stream	Access, Create, Write	CLEAN
fc6c9e32c6d2fbd80fed0e1d0a5530e7eba4c7a305b945705874ea211d09fbd6	C:\Users\kEecfMwgj\Documents\LtH-\DCMx8oRdsb2P_vnN.xlsx.tk5rbt	Dropped File	61.25 KB	application/octet-stream	Access, Create, Write	CLEAN
c2c7c46711ee6ce4ca78009bddf7cfcd0327f40f4c3f19d471eef4ea26a80e39	C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.gjao61	Dropped File	1.78 KB	application/octet-stream	Access, Create, Write	CLEAN
6f722a7074c0e855892a15fee1a2d734ca73455814f23b5caee0dd8318c21d18	C:\Users\kEecfMwgj\Videos\9Af6Yl_3rtjrz2wEmaF.avi.puq588	Dropped File	36.06 KB	application/octet-stream	Access, Create, Write	CLEAN
50e5e30db93d4cae20fcfec95d8886c6b72568c80c5a7a16934ff6a9d33ae027	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml.l9ecyc	Dropped File	1.02 KB	application/octet-stream	Access, Create, Write	CLEAN
f38df64fea9292adf71bd05f3a8a42e855586a2a8fedd89817f67bbe87c3ba13	C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml.9oec2w	Dropped File	27.14 KB	application/octet-stream	Access, Create, Write	CLEAN
f95c2ef86cbe4908adaf48e657b0d9492b8f54e22fa66dddc3c35d7642c9473b	C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\t8c4sQgxZhGJp90o\U05NyfhFoOH.png.t95t8q	Dropped File	99.78 KB	application/octet-stream	Access, Create, Write	CLEAN
a7957a3a14fc54fc76da783dc13f3f7017472dc29b24c03aa0342845bd319216	C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\8 aikgzugk.odt.xdemuf	Dropped File	96.78 KB	application/octet-stream	Access, Create, Write	CLEAN
7abd21da488152d6373a461324f8b8b59f4912302cbd8e7a452605253fcd151	C:\Users\kEecfMwgj\Desktop\orfsAO.odp.feaooi	Dropped File	30.08 KB	application/octet-stream	Access, Create, Write	CLEAN
c56e964e0e89cac16ddaa5fc102c9cdb888d96c529fa70179def70a382cdd34b	C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\branding.xml.oxal5s, C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml.ak2ni4	Dropped File	328.44 KB	application/octet-stream	Access, Create, Write	CLEAN
49fca3375c6c85aa2fce31fc9cf643d4fcfa204d4d1d2cd9de9601f8e6c27293	C:\Users\kEecfMwgj\AppData\Local\Temp\C_98-V0.png.0tr42v	Dropped File	5.22 KB	application/octet-stream	Access, Create, Write	CLEAN
4632b39f8e911d0a1e1a0ca8b385c2305a58f64977385be5464afb142fa7a4a8	C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.wqgmxy	Dropped File	1.77 KB	application/octet-stream	Access, Create, Write	CLEAN
315cbd62a6c09587254e0810b92cd69597fb20eba4a60b5691f0bb19fc35fd70	C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml.zln0j2	Dropped File	1.20 KB	application/octet-stream	Access, Create, Write	CLEAN
b32e2dbe80052ccb0a4541f27096658a14eb3967f59fbf48ac5932035878c29a	C:\Users\kEecfMwgj\Documents\zIcOMqefwIUm\hOuHh_SwDbliUgNTQ.ppt.d5m7h1	Dropped File	53.11 KB	application/octet-stream	Access, Create, Write	CLEAN
e026d965faab230df7729e3fe622a9c293a6a8e247cd484cb93654807fb11afc	C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.372qjb	Dropped File	1.77 KB	application/octet-stream	Access, Create, Write	CLEAN
f6508a076d3ca932ceb510f8903aa08c4ce7909bf1f5ae0713ca6b047960c4f1	C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\E-uYSW4Do.avi.l4ynmq	Dropped File	30.34 KB	application/octet-stream	Access, Create, Write	CLEAN
4cfe7fee0b5f4e18382048a5d370e274ce84baa8a15a5a78d4bae856cf04bfb8	C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.1.xml.q20imu	Dropped File	1.94 KB	application/octet-stream	Access, Create, Write	CLEAN
3e08fe3b99d139f714d0b213727b084b4baacf83df0459ab07b991206f26ba0c	-	Downloaded File	64 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c5e68bc6ec9388f0b0be98a6100459c5573044e269a87f804dac29c025505f52	-	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
2b393606967cb5e6ac1855432af7abe57fb8b1ac658354602139ece61b9c8449	C:\Users\kEecfMwgj\Videos_6W_tOp4\xuKD9lnbmJOlcf\CBZ05GkRAEgsJx7.avi.e0jmia	Dropped File	56.41 KB	application/octet-stream	Access, Create, Write	CLEAN
6ba05849b6bd9e62c8b9385dc83a960606ac76393afa73c93eb2fdf5fbb02ca9	C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.ykkkg1	Dropped File	11.92 KB	application/octet-stream	Access, Create, Write	CLEAN
efa812bea48f7c35c4f47838604ab5ef0f71208277116a64a4ef2b7b9d682cf4	C:\Users\kEecfMwgj\AppData\Roaming\MzZay9cJsQOsYylg.gif.k9krsd	Dropped File	74.25 KB	application/octet-stream	Access, Create, Write	CLEAN
f7d3cdb34d2a56541efe7d738137865b128fbc8a94a8c3fbc05c7fc8244d3790	C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proofing.xml.p4of38	Dropped File	1.02 KB	application/octet-stream	Access, Create, Write	CLEAN
c1a17058856db049aedf0588738a86e85f7a44caea06bd1daab96f30a3e19ef0	C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelMUI.xml.fs3y21	Dropped File	1.75 KB	application/octet-stream	Access, Create, Write	CLEAN
affcd384aec8478c3253e266dfe8be2bde31ca97a328eebd342cebb1ecab3993	C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg.46zt8o	Dropped File	606.34 KB	application/octet-stream	Access, Create, Write	CLEAN
c4d8677b592e0cf2c272d051a1b424abce9cc8ea45e41898e872d7e347481738	C:\Users\Default\AppData\Local\Temp\FXSAPIDebugLogFile.txt.my5n59	Dropped File	16 bytes	application/octet-stream	Access, Create, Write	CLEAN
6f33db7d9279454071d23b329a64b2c76267ed31f38b8aefd1535465e1bdd92b	C:\Users\kEecfMwgj\Pictures\4_gCpVi\V1tLRl90VOX8.png.mjm4gs	Dropped File	67.97 KB	application/octet-stream	Access, Create, Write	CLEAN
77a42c7a97c7fd9181e1af6ee075d254316597236655ea5990e194dcb5a019f1	C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\O5hM2sANeBEXGTf3mc.pdf.l8v5n1	Dropped File	94.19 KB	application/octet-stream	Access, Create, Write	CLEAN
d8edbc05e06304731570022219d9836c09c87bc791b775c4efd160f30ad1502ea	C:\Users\kEecfMwgj\AppData\Roaming\cpj-qQBHP_mKPrmP-k.jpg.014hhh	Dropped File	86.78 KB	application/octet-stream	Access, Create, Write	CLEAN
be881f2d695855ac822ae1bd68150708416bcd65079cfaaf214a639d3f366309	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\setup\logs\2021-02-22_125735_4d4-a74.log.uigyjm	Dropped File	7.83 KB	application/octet-stream	Access, Create, Write	CLEAN
239584da44cb9af6fcce8e4b0ac1ee44bee6034b9a67c5fa4029dc79559f0ed7	C:\MSOCache\All Users\{90160000-001B-0409-0000-000000FF1CE}-C\WordMUI.xml.r5i6uy	Dropped File	2.06 KB	application/octet-stream	Access, Create, Write	CLEAN
06a6fc6ec76d67f1330a0db3fc3d001b2a469eb72a57a6f300a49e230bde6752	C:\Users\kEecfMwgj\Music\4waS\aice20.m4a.mcap17	Dropped File	90.33 KB	application/octet-stream	Access, Create, Write	CLEAN
b2909ad924d5475318863f8da4f3fd36cba007c3c4eac6cfda5606e0312dcbbd	C:\MSOCache\All Users\{90160000-00E2-0409-0000-000000FF1CE}-C\OSMUXMUI.xml.1ebw4e	Dropped File	1.44 KB	application/octet-stream	Access, Create, Write	CLEAN
d48be6e5ee33f51228a2669feb2981fa7a817c0c8210ce5f70cfe0b8739c37d2	C:\MSOCache\All Users\{90160000-00A1-0409-0000-000000FF1CE}-C\OneNoteMUI.xml.ll6jcd	Dropped File	1.78 KB	application/octet-stream	Access, Create, Write	CLEAN
8502d9d60f41d4c27b846bf527aa314d1501b01229fc811b1b4f2dcdc52e3518	C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg.fa0ws0	Dropped File	759.61 KB	application/octet-stream	Access, Create, Write	CLEAN
ea25944f78e9d7947d122bca8df70287468c60f7b073a5a677dfe8cfa6d86b8f	C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PublisherMUI.xml.w47ucz	Dropped File	1.62 KB	application/octet-stream	Access, Create, Write	CLEAN
3532213584b5ca2036236cd7a20be0ec1a60f19178789c4c6b37c814528ebbab	C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.fr\Proof.xml.rnlrql	Dropped File	1.64 KB	application/octet-stream	Access, Create, Write	CLEAN
03da4c1cfa3b8322b62f31c9e2ff96d61fcf6e8f5f5ec0fb5063d69d0fa396a4	C:\Users\kEecfMwgj\Music\0Gi9jAAneSNZB2RiMYa\Hj4upkRDF60YUCaULrc.m4a.qdw7kn	Dropped File	79.75 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
44d819b8e533c41899fa22e20115429562ec7a368cea5507645228b66f8faf0f	C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.y51l5q	Dropped File	2.03 KB	application/octet-stream	Access, Create, Write	CLEAN
1a470173268625ecb7409783f7ad46fbf6042b8cecf087b7dee76637bbc0faf6	C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.3rraty	Dropped File	265.02 KB	application/octet-stream	Access, Create, Write	CLEAN
07bb5948a0a337ab0cd2d6db088d56d8106f7ae2df40ee9ec86537d3b835f302	-	Dropped File	108.54 KB	application/octet-stream	-	CLEAN
e46d299516a44c3574ef2f1ab366ce7dc4e5425a9c7793e463ff69d1a2cc01ad	C:\Users\kEecfMwgj\AppData\Roaming\h1YIXDOe1dpX6GMny-.gif.ioof6z	Dropped File	27.31 KB	application/octet-stream	Access, Create, Write	CLEAN
53721f3da71fe295360527058d2708cd0c576941a47ce1581166e76509f5e610	C:\Users\kEecfMwgj\AppData\Local\Temp\b8T3auYtVogPw5aYbN8s.gif.90vseg	Dropped File	8.22 KB	application/octet-stream	Access, Create, Write	CLEAN
e5a7d8022da5adfce36ffd2c63b2275fe4efc4f1f3256a2b93d77d00ef7e82c7	C:\Users\kEecfMwgj\Music\fXs7dyEh5KRVvZ0H\3WvCbF\xEnzmTd-.m4a.dsvy3z	Dropped File	41.61 KB	application/octet-stream	Access, Create, Write	CLEAN
ffb8ca74462c82eef67e6ccaa59051c66366a68e35a4439ef0534df8b1e0150c	C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\rjMao5c8LjOzfjEul.avi.4oc6sd	Dropped File	78.31 KB	application/octet-stream	Access, Create, Write	CLEAN
fa305c0d075480ac338f2babb924a92f2584088f0f7a0c1eceedb281745178b6	C:\Users\kEecfMwgj\Documents\bjeZGjCALbyoQVDOz.xlsx.32cbio	Dropped File	98.77 KB	application/octet-stream	Access, Create, Write	CLEAN
7345f730255f43d457bbe084c06403ff9fb79dfa9076d08f6e72bb759ac456cb	C:\Users\kEecfMwgj\Pictures\4_gCpVi\UfIU4AupJZ3uu6W Tr4v.jpg.ojft9j	Dropped File	11.70 KB	application/octet-stream	Access, Create, Write	CLEAN
a48d399eeee1a47b52e0e9cd64a9e1276a62a072008376825945442cf4526f86	C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\xymCfQvs0a.xls.72ykhx	Dropped File	1.23 KB	application/octet-stream	Access, Create, Write	CLEAN
f7d4285217e2e5432f0c72416020eddc38cbf84f8746b71fc3c07392b74748b8	C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.xml.769aog	Dropped File	1.42 KB	application/octet-stream	Access, Create, Write	CLEAN
368de5ccc6dd66b9b4e92b018a68b265c77cd7c016aec7bcec118eeeb2f30b98	C:\Users\Public\Pictures\Sample Pictures\Desert.jpg.hkno0p	Dropped File	826.12 KB	application/octet-stream	Access, Create, Write	CLEAN
46c7fdb6c7392ec16e1aa63c0911836b44e7ef9856712a2d0caaf40b32efdbe7	C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.0cgvfm	Dropped File	2.78 KB	application/octet-stream	Access, Create, Write	CLEAN
62fe7fd3851aceba0a2cc616f753aefb596a80227543ffe4593cb6d6d5172d8b	C:\Users\kEecfMwgj\Documents\QblbR\eUc2ZnHoSmyslPJGT.docx.5vq8c1	Dropped File	29.33 KB	application/octet-stream	Access, Create, Write	CLEAN
a70f9cec35a1fcc8270d96bef8515bb30bbf2a32bc624f1bfe1e2f4da8ece283	C:\Users\kEecfMwgj\Documents\3CgFzZIG5azIFPRBrK.docx.k0b23c	Dropped File	93.64 KB	application/octet-stream	Access, Create, Write	CLEAN
051770425e40162ffc645b61235b2a0c0bb173ddcdf2b64f640ff2658168d082	C:\Users\kEecfMwgj\AppData\Local\Temp\dvnjFpGyCrr4q.odp.pl1oog	Dropped File	89.11 KB	application/octet-stream	Access, Create, Write	CLEAN
6dc83f682afd7dde6ad4c631dccbf5379fb83ffe82fef3bb0389a16ba6c356f2	C:\Users\kEecfMwgj\AppData\Local\Temp\dsXGshyj.xlsx.rIteh8	Dropped File	97.55 KB	application/octet-stream	Access, Create, Write	CLEAN
e6a18fa1241a6caa7b708b60a0c5669e3da1b87e6d43395efa574a5acbed0808	C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.41gmdo	Dropped File	1.88 KB	application/octet-stream	Access, Create, Write	CLEAN
be6fec859553357dae6bcdd7e1f7aed45fd28bdb842fd0f392de7103622f0727	C:\Users\kEecfMwgj\Documents\DG0rAqFzdHUG15.csv.ktemy1	Dropped File	91.94 KB	application/octet-stream	Access, Create, Write	CLEAN
c71c52dcba65a3923bcffefe869a65320ded314973893e9a71304d57a7927fbd	C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.1v9a9r	Dropped File	1.61 KB	application/octet-stream	Access, Create, Write	CLEAN
5fde7c5d5607c656da2badf592d5765c22f8af8adaf5afccafa7fabc2aff621d	C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.14t4b9	Dropped File	1.66 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d03a3b0ad800d2c32b12ac2c169c0b6c5b9afdafc4e69dd4b8a8d59443168fbe	C:\Users\kEecfMwgj\Videos_6W_tOp4\Tg9U9jjSqkvBNtKz.mp4.4l6y33	Dropped File	67.62 KB	application/octet-stream	Access, Create, Write	CLEAN
1bbed2e4896985823a9f89f9bd25546c2150b435d63cf94140bf3fc814bd233e	C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.2.xml.o1gru5	Dropped File	1.36 KB	application/octet-stream	Access, Create, Write	CLEAN
612cef3e4facd583dcce79f3c985337cb7ae4fd19f2e9a81e7e698cbd1f59cd6	C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\READ_ME.htm, C:\PerfLogs\READ_ME.htm, C:\ProgramData\Microsoft\Net... ... \Users\kEecfMwgj\Pictures\READ_ME.htm, C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}v14.25.28508\READ_ME.htm	Dropped File	1.78 KB	text/html	Access, Create, Write	CLEAN
28e955b5c54135f88c9548308d47ad89356030122a025dbec5176d6d1195fafe	C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.jh7mub	Dropped File	5.94 KB	application/octet-stream	Access, Create, Write	CLEAN
a646e4fc87b24dfba68c62b618740533188ebd76a5281e6d2034bb20f6a48f8b	C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\MasterDescriptor.x-none.xml.3rvlpy, C:\ProgramData\Microsoft\ClickToRun\634EF343-54B0-4B56-9FD9-A785E3F22968\x-none.16\MasterDescriptor.x-none.xml.17z02j	Dropped File	20.55 KB	application/octet-stream	Access, Create, Write	CLEAN
656c63fa20f0da797ee19010d0afe69c286c4802cf35e6144cf13ce5e7d2f285	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ExclusionList.xml.xu45my	Dropped File	19.59 KB	application/octet-stream	Access, Create, Write	CLEAN
f3dd3bc5f5a0cd0842e3456ad7f780acbd8ed6adeb2e0c97144342ceb9c3acb2	C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg.orihz5	Dropped File	757.53 KB	application/octet-stream	Access, Create, Write	CLEAN
68cc57925ccdbed866eaaa0d490e607c6876f941c202df99cab4ffb45ba7088b	C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\DNuRUiZ.mp4.6p6vk5	Dropped File	68.39 KB	application/octet-stream	Access, Create, Write	CLEAN
3b40a84da79b915545af22cdc443e1b4886f9a2eccb759bb86bea026c8805e53	C:\Users\kEecfMwgj\Documents\Xy9pNIL0lNohzVp4.docx.b0zv1t	Dropped File	17.17 KB	application/octet-stream	Access, Create, Write	CLEAN
ebedf3577fe5a76f91a051570ba73bc7225d7cb7696d4629f16ad16e4ef939ec	C:\Users\kEecfMwgj\AppData\Local\Temp\dvwxkOLliLo8iOIR.pdf.ghibwm	Dropped File	36.22 KB	application/octet-stream	Access, Create, Write	CLEAN
a7c4d9dae7cef5542b4d882208c207dcc30e97b367cb5db7ef1096b27fe019a4	C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\gohAPD YvxpiV5JD.ppt.rqnezo	Dropped File	96.83 KB	application/octet-stream	Access, Create, Write	CLEAN
11669fab4ad07dc89fb9a0a0abfe4f8e20df8c238fb3462d8a1218c9fc4571a6	C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml.ofmwoh	Dropped File	1.62 KB	application/octet-stream	Access, Create, Write	CLEAN
f7c45a4649e0b3b27c2170754e28f6bca7d7dcb75a1bc8a51b4dbb847491d880	C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\qs5-GxiBYrtogzhqzA1S.png.m3pobg	Dropped File	39.52 KB	application/octet-stream	Access, Create, Write	CLEAN
3f28781e58902f6494d420b81c527b3ceeae6a37eafe87ec4915606b3f0fef28	C:\Users\kEecfMwgj\Pictures\nFvnUcfZr2ciaqvGBH.gif.mzjhl5	Dropped File	88.64 KB	application/octet-stream	Access, Create, Write	CLEAN
e1aaa83400cb48d9cd1cfed035ddc55b287d74f9f965cc04d22c5e083d50acf6	C:\Users\kEecfMwgj\AppData\Roaming\EPBdPl2nUBwLxi2a.gif.bk1t6w	Dropped File	75.23 KB	application/octet-stream	Access, Create, Write	CLEAN
43d27943144a429074238a2a1550f898879727937ee9384dd4b44dbb9759dd44	C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml.eptbtw	Dropped File	1.02 KB	application/octet-stream	Access, Create, Write	CLEAN
85564416d9d4570ab9967c72cd02f1c9d7289827081120dc4679fa3993728d82	C:\Users\kEecfMwgj\AppData\Roaming\4n0L _Me_g-.m4a.b2x8a9	Dropped File	56.80 KB	application/octet-stream	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	Sample File, VM File	-	MALICIOUS
C:\PerfLogs\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\RAC\Outbound\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
c:\users\default\appdata\roaming\microsoft\windows\sendto\read_me.htm	Dropped File, Modified File	-	CLEAN
C:\Users\kEecfMwgj\Desktop\GRHtAG4s9qD-ME4UNQ5d\TsyPWpsnMPhL\vEsxlZJ6fy_JVYxR43.pptx.9hyf53	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\af\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\Default\AppData\Local\Temporary Internet Files\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\All Users\Oracle\Java\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Documents\j5g-Xfr8dqgh7T\flAl.docx.15psg9	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ScreenshotOptIn.png	Accessed File, Modified File, Not Extracted	Access, Create, Delete, Read, Write	CLEAN
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml	Accessed File, Modified File, Not Extracted	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\quz-pe\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.0fm26x	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Boot\sv-SE\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Document Building Blocks\1033\16\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\rjMao5c8LjOzfjEul.avi.4oc6sd	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\Public\Pictures\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Feeds\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Documents\QblbR\6RjpQT8xrF.xls.ehdew2	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\locallow\sun\java\deployment\cache\6.0\60\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\DZo4\pXTOnk25mpA16xy.odp.lrypin	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ha-latn-ng\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\16.0\officec2rclient.exe_Rules.xml.u9ydcp	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
c:\users\default\appdata\local\microsoft\windows\temporary internet files\read_me.htm	Dropped File, Modified File	-	CLEAN

File Name	Category	Operations	Verdict
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml.n3voag	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Documents\FQRLvgP_7y0.pptx.64ehxa	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\Default\AppData\Local\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png	Accessed File	Access, Create, Read	CLEAN
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\templates\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\kEecfMwgj\Music\fXs7dyEh5KRVvZ0H\2KcT02McQ-LKwXH.m4a.v1unnn	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\ClickToRun\UserData\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Crypto\RSA\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\roaming\microsoft\systemcertificates\my\certificates\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\behavior.xml	Accessed File	Access, Create, Read	CLEAN
C:\Users\kEecfMwgj\Desktop\tHdXe2-Gmf-Jn.m4a.zq8ar0	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\C_98-V0.png.0tr42v	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft OneDrive\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\locallow\sun\java\deployment\cache\6.0\45\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\Default\AppData\LocalLow\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Videos_6W_tOp4\OScpcujUrV9u.avi.6lzous	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\Default\Local Settings\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\Public\Documents\My Music\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\All Users\Package Cache\{B175520C-86A2-35A7-8619-86DC379688B9}v11.0.61030\packages\vcRuntimeAdditional_x86\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Boot\de-DE\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\All Users\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}v12.0.21005\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.14t4b9	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}v14.25.28508\packages\vcRuntimeMinimum_x86\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\Crypto\RSA\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ru\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ur\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\WJt-fDxLG.pdf.rvbyn5	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.e6qpy0	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Boot\cs-CZ\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Pictures\4_gCpVi\UfIU4AupJZ3uu6WTr4v.jpg.ojft9j	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\dKTFQ.m4a.ttyipk	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\All Users\Start Menu\READ_ME.htm	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\33GmwDyrWLVGP.flv.5x0la6	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\Default\Favorites\Links\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\be\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
c:\programdata\package cache\{cf2bea3c-26ea-32f8-aa9b-331f7e34ba97}v11.0.61030\read_me.htm	Dropped File, Modified File	-	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\Integration\ShortcutBackups\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\ClickToRun\634EF343-54B0-4B56-9FD9-A785E3F22968\x-none.16\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Pictures\hdQc_udJ4lFbk4Ni\t8c4sQgxZhGJp90o\G3cproBxiH\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Sun\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\mr\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ca\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Favorites\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\Office\Heartbeat\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\UserData\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\Recovery\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\16.0\winword.exe_Rules.xml.7fhvk5	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Documents\LtH-\DCMx8oRdsb2P_vnN.xlsx.tk5rbt	Dropped File, Accessed File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\READ_ME.htm	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\Default\AppData\Local\Application Data\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Outlook\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\Documents\3CgFzZlG5azlFPRBrK.docx.k0b23c	Dropped File, Accessed File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\onedrive\17.3.4604.0120\si-lk\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\Public\Downloads\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\tt\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\kEecfMwgj\Music\4waS\Bdv8RAzkZflDNMLATEh_5hWa8db7rvReOJ3u\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\MzZay9cJsQOsYylg.gif.k9krsd	Dropped File, Accessed File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\onedrive\17.3.4604.0120\sw\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}v14.25.28508\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\locallow\sun\java\deployment\cache\6.0\53\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\MasterDescriptor.en-us.xml.xo1phl	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\lOKKHz-jj1T03E2Exf\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\locallow\sun\java\deployment\cache\6.0\46\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\All Users\Microsoft\NetFramework\BreadcrumbStore\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\dvnjFpGyCrr4q.odp.pl1oog	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\Default\Desktop\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\mn\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.wqgmxy	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
c:\users\default\appdata\local\microsoft\windows\history\read_me.htm	Dropped File, Modified File	-	CLEAN
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml.9721g8	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\hi\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\lt\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\ProgramData\Oracle\Java\installcache_x64\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\40\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Videos\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Documents\vqpLNVtnZe\VrEWF.odp.qaqzuc	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\ClickToRun\634EF343-54B0-4B56-9FD9-A785E3F22968\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\bn-bd\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\Default\Pictures\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\34\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\uk\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\All Users\Oracle\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\locallow\sun\java\deployment\cache\6.0\7\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.2q5bez	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\RAC\PublishedData\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\ProgramData\Microsoft\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Documents\My Music\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Videos_6W_tOp4\zJQm10_Pj\DNuRUiZ.mp4.6p6vk5	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\SendTo\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml	Accessed File, Modified File, Not Extracted	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\10\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Downloads\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml	Accessed File, Modified File, Not Extracted	Access, Create, Delete, Read, Write	CLEAN
C:\Users\All Users\Package Cache\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
c:\programdata\package cache\{929fbd26-9020-399b-9a7a-751d61f0b942} v12.0.21005\packages\read_me.htm	Dropped File, Modified File	-	CLEAN
C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\C_98-V0.png	Accessed File, Modified File, Not Extracted	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\1\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\LocalLow\Sun\Java\Deployment\cache\6.0\11\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
C:\Documents and Settings\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Word\STARTUP\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\onedrive\17.3.4604.0120\sk\read_me.htm	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\eu\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Feeds Cache\1NBUR4HR\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\hu\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\All Users\Microsoft OneDrive\READ_ME.htm	Accessed File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\tk-tm\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\cs\READ_ME.htm	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	CLEAN
C:\Boot\ko-KR\READ_ME.htm	Dropped File, Accessed File, Modified File	Access, Create, Write	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://localbitcoins.com/guides/how-to-buy-bitcoins	-	-	-	-	CLEAN
http://www.free-website-hit-counter.com/c.php?d=9&id=123086&s=16	-	158.176.65.249	-	GET	CLEAN
http://pastebin.com/raw/f1TMQySv	-	104.20.68.143, 172.67.34.170, 104.20.67.143	-	GET	CLEAN
https://pastebin.com/raw/f1TMQySv	-	104.20.68.143, 172.67.34.170, 104.20.67.143	-	GET	CLEAN
http://www.free-website-hit-counter.com/c.php?d=9&id=123252&s=2	-	158.176.65.249	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
localbitcoins.com	-	-	-	CLEAN
free-website-hit-counter.com	158.176.65.249	-	TCP, DNS, HTTP	CLEAN
pastebin.com	104.20.68.143, 172.67.34.170, 104.20.67.143	-	TCP, HTTPS, DNS, HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www.free-website-hit-counter.com	158.176.65.249	-	TCP, DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
172.67.34.170	pastebin.com	United States	DNS	CLEAN
158.176.65.249	free-website-hit-counter.com, www.free-website-hit-counter.com	United States	TCP, DNS, HTTP	CLEAN
104.20.68.143	pastebin.com	-	TCP, HTTPS, DNS, HTTP	CLEAN
104.20.67.143	pastebin.com	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\.net clr networking	delete, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance	access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\CategoryOptions	read, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	tmp_asdqwd2.exe, fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	tmp_asdqwd2.exe, fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	tmp_asdqwd2.exe, fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\First Counter	read, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\FileMappingSize	read, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\Library	read, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\Counter Names	read, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\IsMultiInstance	read, access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance	access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	CLEAN

Process

Process Name	Commandline	Verdict
fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe	"C:\Users\kEecfMwgj\Desktop\fc61c3cbae6f6926294861aded1750af4c5019daae532e531f35dd575071c87a.exe"	MALICIOUS
tmp_asdqwd2.exe	"C:\Users\kEecfMwgj\AppData\Local\Temp\tmp_aSDqwd2.exe"	SUSPICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.2.24 / 2022-09-07 15:06:41
Link Detonation Heuristics Version	4.6.2.24 / 2022-09-07 15:06:41
Smart Memory Dumping Rules Version	4.6.2.24 / 2022-09-07 15:06:41
Config Extractors Version	4.6.2.26 / 2022-09-09 12:20:50
Signature Trust Store Version	4.6.2.24 / 2022-09-07 15:06:41
VMRay Threat Identifiers Version	4.6.2.26 / 2022-09-09 12:20:50
YARA Built-in Ruleset Version	4.6.2.26

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp

System Root	C:\Windows