MALICIOUS

Classifications: -

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe**
ID	#4211493
MD5	5dc438c8c9ab91ccadba1de82ab481d9
SHA1	a4a80d386948fcd3edb6da1611ac43454124d997
SHA256	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1
File Size	112.00 KB
Report Created	2022-04-28 15:50 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 112 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 2454 files by appending the extension ".pxj".			
5/5	User Data Modification	Modifies Windows automatic backups	1	-
	• (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe deletes Windows volume shadow copies.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: git, AbleFTP, Total Commander.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
2/5	Data Collection	Reads sensitive ftp data	2	-
	• (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe tries to read sensitive data of ftp application "AbleFTP" by file. • (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe tries to read sensitive data of application "git" by file.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe creates mutex with name "XVFXGW DOUBLE SET".			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe starts (process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe with a hidden window. • (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe starts Anonymous Process with a hidden window.			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files\common files\99m9l9xg2pvu-fl.png".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files\common files\99m9l9xg2pvu-fl.png.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files\common files\gwfgft_br_n0vy16u6.gif".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files\common files\gwfgft_br_n0vy16u6.gif.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files\common files\x3dqavt3.jpg".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files\common files\x3dqavt3.jpg.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\appxmanifest.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\appxmanifest.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\filesystemmetadata.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\filesystemmetadata.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\common files\designer\msaddndr.olb".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\common files\designer\msaddndr.olb.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\internet explorer\signup\install.ins".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\internet explorer\signup\install.ins.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0015-0000-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0015-0000-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0015-0409-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0015-0409-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0016-0000-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0016-0000-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0016-0409-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0016-0409-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0018-0000-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0018-0000-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0018-0409-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0018-0409-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0019-0000-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0019-0000-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0019-0409-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0019-0409-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001a-0000-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001a-0000-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001a-0409-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001a-0409-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001b-0000-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001b-0000-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001b-0409-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001b-0409-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-0409-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-0409-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-040c-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-040c-0000-0000000ff1ce.xml.pxj".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-0c0a-0000-0000000ff1ce.xml".
- (Process #1) 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe modifies "c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-0c0a-0000-0000000ff1ce.xml.pxj".

Mitre ATT&CK Matrix

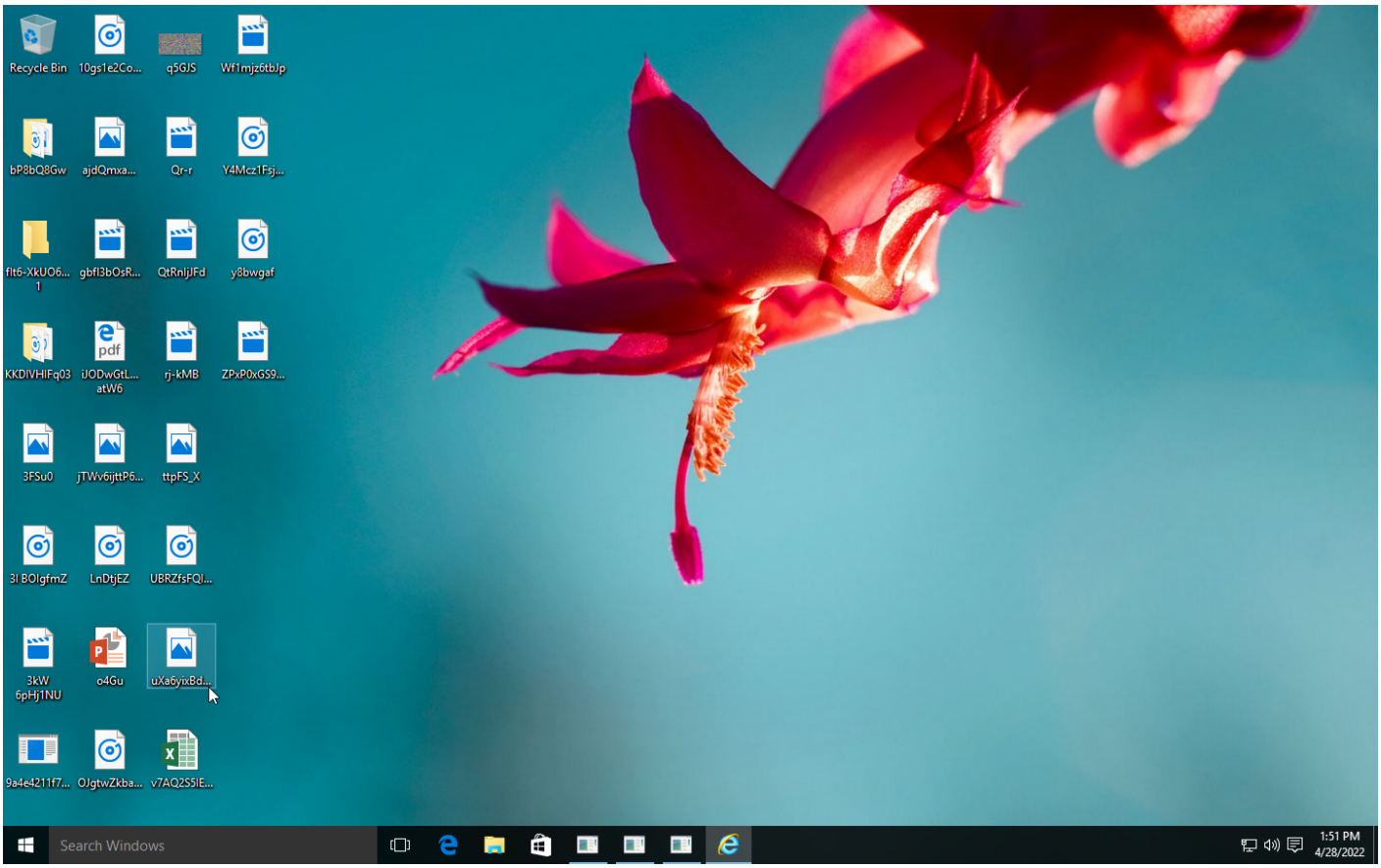
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
								#T1005 Data from Local System			#T1490 Inhibit System Recovery

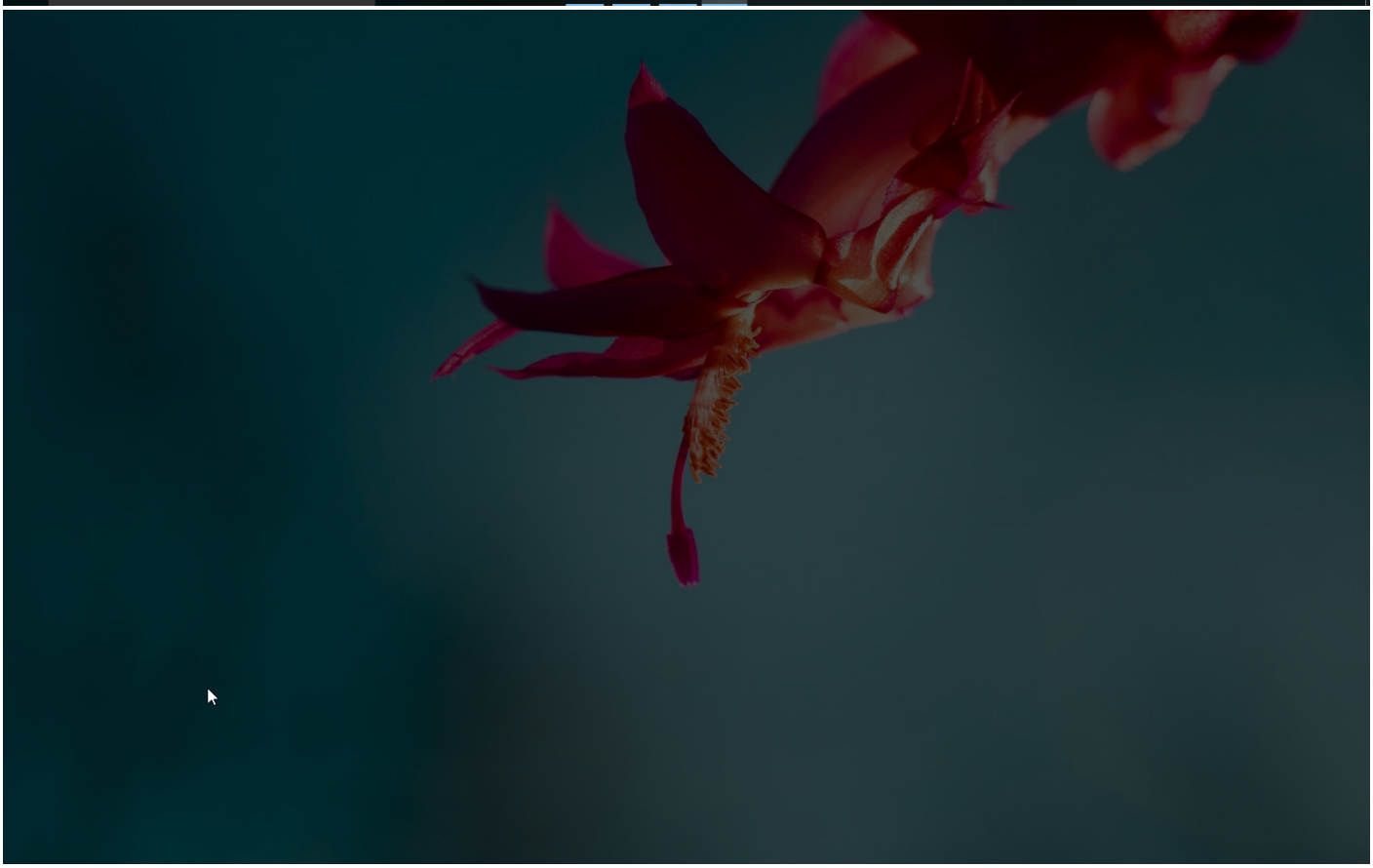
Sample Information

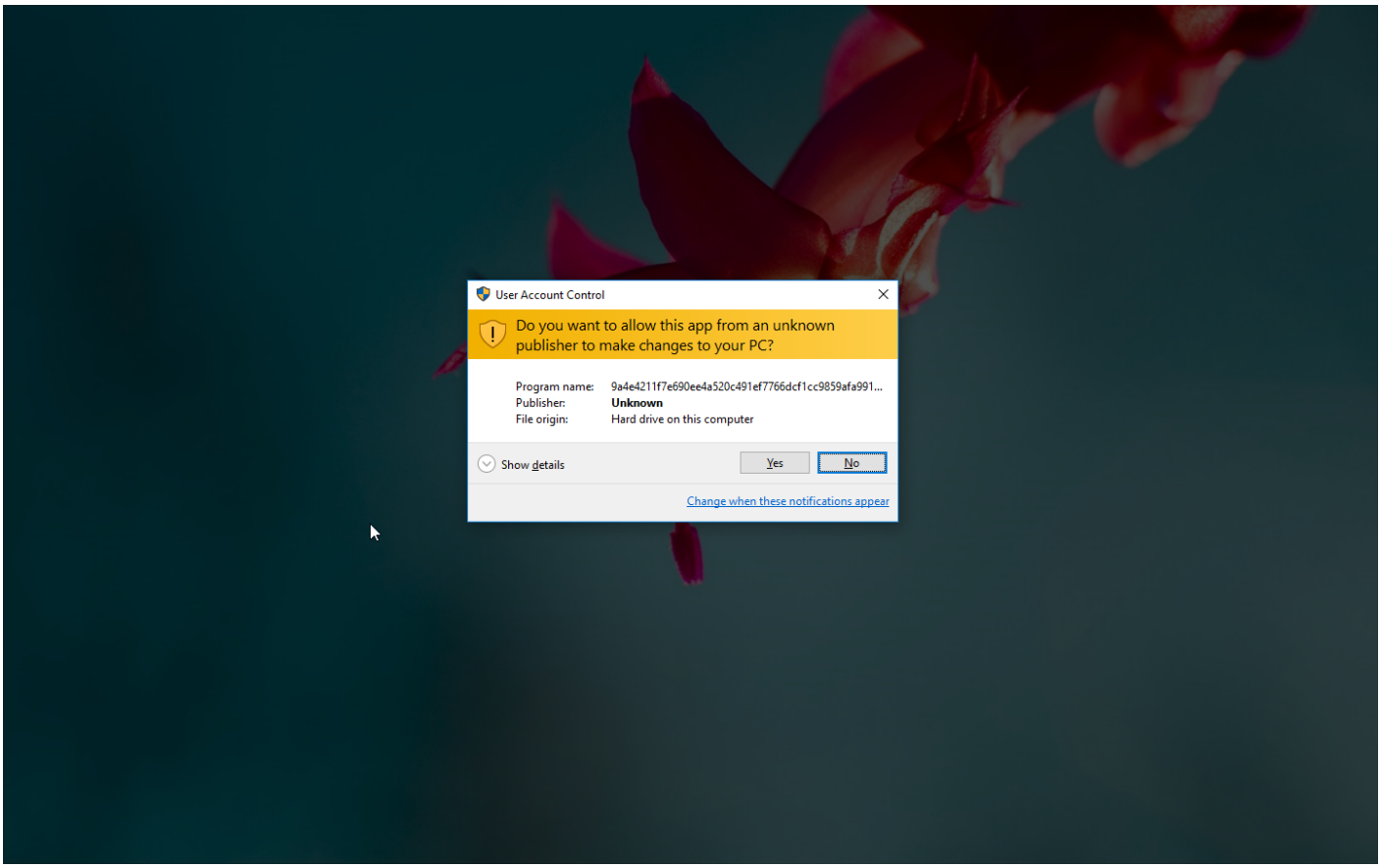
ID	#4211493
MD5	5dc438c8c9ab91ccadba1de82ab481d9
SHA1	a4a80d386948fcd3edb6da1611ac43454124d997
SHA256	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1
SSDeep	3072:W/QaMUCb9ybN2Rt5h48gn8OMqqDJppFm:W/QaM/U8gnuqqD7p
ImpHash	94059925f46c5497a958eb141fea0a0d
File Name	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe
File Size	112.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

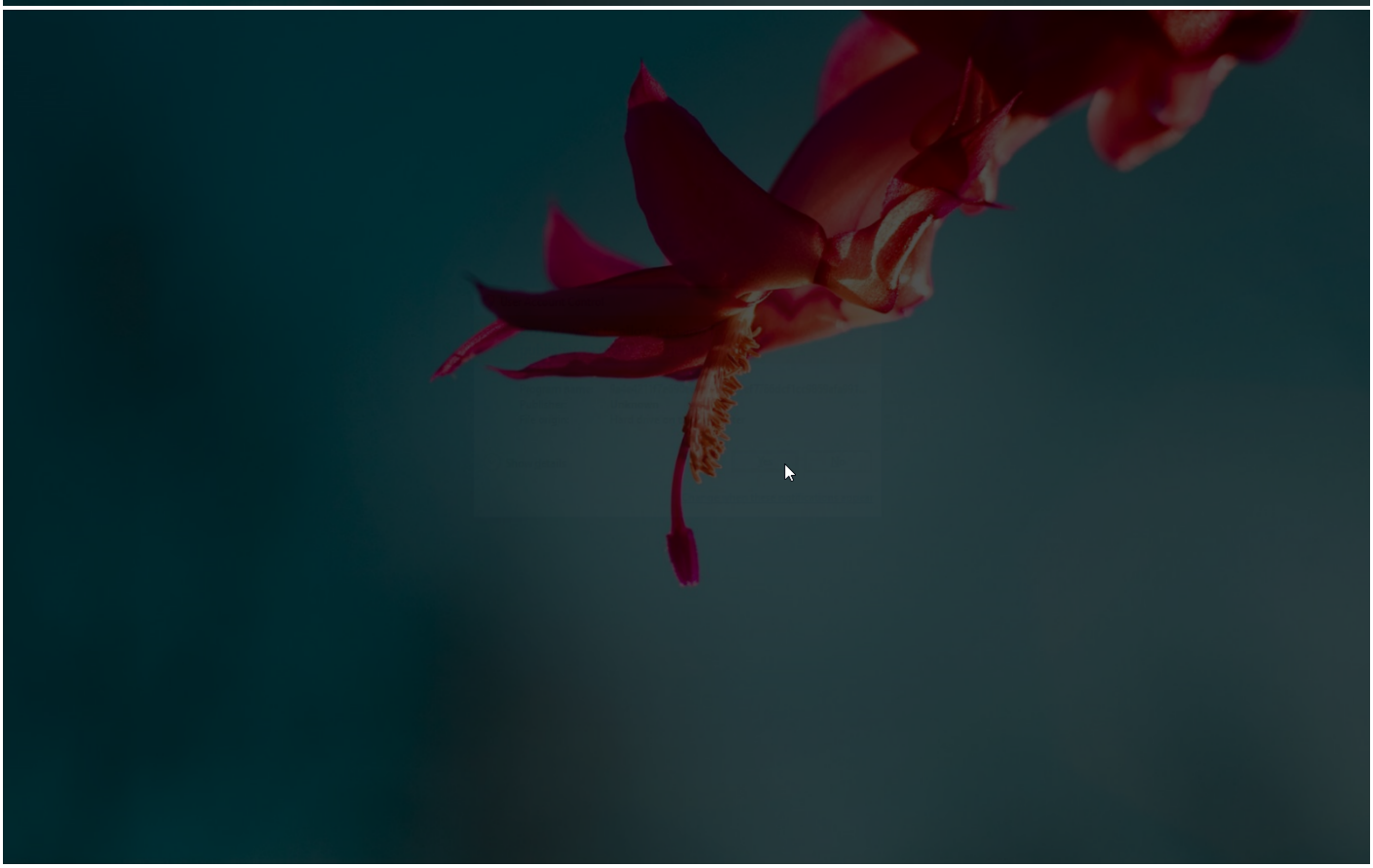
Analysis Information

Creation Time	2022-04-28 15:50 (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


Recycle Bin
10gs1e2Co...
q5GJS
Wf1mjz6tbJp
bP8bQ8Gw
ajdQmxa...
Qr-r
Y4Mcz1Fsj...
flt6-XkUO6...
1
gbfl3bOsR...
QtRnljJFd
y8bwgaf
KKDIVHIFq03
iODwGtL...
atW6
rj-kMB
ZPxP0xGS9...
3FSu0
jTWv6ijttP6...
ttpFS_X
3l BOlgfmZ
LnDtjEZ
UBRZfsFQI...
3kW
6pHj1NU
o4Gu
uXa6yixBd...
9a4e4211f7...
OJgtwZkba...
v7AQ2S5lE...
Search Windows
1:51 PM
4/28/2022







Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

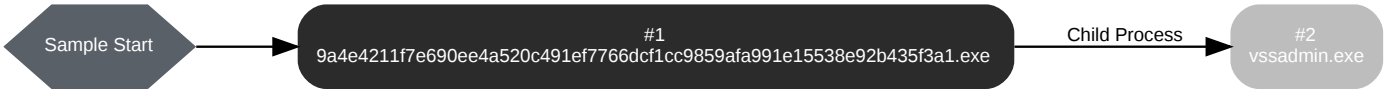
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81302, Reason: Analysis Target
Unmonitor End Time	End Time: 321559, Reason: Terminated by timeout
Monitor duration	240.26s
Return Code	Unknown
PID	3024
Parent PID	1932
Bitness	32 Bit

Dropped Files (2456)

File Name	File Size	SHA256	YARA Match
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001a-0409-0000-0000000ff1ce.xml.pxj	19.26 KB	780101ba245fb03c1783f719ef4456f39f3482b5e004e120ccabbd277b717fd8	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-040c-0000-0000000ff1ce.xml.pxj	2.37 KB	ef43dccc182ffe171b1e41f8a45445a8036f21e0bcec637fa42b62c7d5dd256e	✖
c:\users\rdhj0cnfevzx\documents\dhsdwsuvr.pptx.pxj	76.93 KB	8c94257b2354f3098001cabba62f30427c9db04ce12c1c14585bee057d824a46	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Proof.en-us.msi.16.en-us.tree.dat.pxj	19.02 KB	9a6445fcbe0caea3481ee261cd9a02834a82e234feae5fd292312fd5edf86bf0	✖
c:\programdata\package cache\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\vc_redist.x64.exe.pxj	632.79 KB	08fcec29d081857e0e62330f485c724edd451615e9fef56bae56a92fc67eff06	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\proof.es-es.msi.16.es-es.tree.dat.pxj	23.88 KB	686cad79a132284b17c6b52e6d37dd053eb2d80f4881a198663489003e219751	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\excel.x-none.msi.16.x-none.boot.tree.dat.pxj	166.20 KB	5f577cb9e77ec03df13450b1e2f40417683f1a6456308c3b1b388baf711176a7	✖
c:\program files\common files\microsoft shared\clicktorun\api-ms-win-core-file-l2-1-0.dll.pxj	18.45 KB	c10299669e0731d6118a952907a323c52e3d215048dbd2a4996fe07fbb205482	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml.pxj	648 bytes	a437d24d7cdf4e07d7820e6c27721c1e70a3c57bfa60105bbb1769b633f68361	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml.pxj	1.49 KB	ee0d4fe62e40de86cc6582aacb9d6e1f0e91b441d4dcdb55b04489ac94316802	✖
C:\Users\RDhJ0CNFevzX\Documents\JVuaF.ots.pxj	17.65 KB	f4d889dfe233d5c44d667928ad0d3a9f22b5a8f9ce99d798ffface723c9dcecc	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\office64muiset.msi.16.en-us.boot.tree.dat.pxj	1.95 KB	b03bd3dd738a393c95a5330bfd15c42d42e4a6fdef1a59ff621b3e283c5feaaa	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml.pxj	4.30 KB	af4ce45192283ca5e2aca9b87d4bf08d37717e1021cd6a888f30d5a3e86f2188	✖
c:\users\rdhj0cnfevzx\pictures\kwv8d1m_xerjis4ig.jpg.pxj	74.32 KB	f6edfc1eadf81cdb987d4d9397b12296cd527d86621752b534313e1a222dabd4	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0116-0409-1000-0000000ff1ce.xml.pxj	1.49 KB	0c516e20038fc6bcd47efcf84a6101530714931d44b247dbabe35a28f8129451	✖
c:\users\rdhj0cnfevzx\documents\4oz_p78.docx.pxj	93.76 KB	bdb5c8ac91e614a5ff9696657552dfc11a472f2fcb8aac14db0cf988700928a1	✖
C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB.pxj	15.87 KB	787659d75d4af3a778019f5524f1f57c73e10651657505c07113d74a52f50c81	✖

File Name	File Size	SHA256	YARA Match
c:\program files (x86)\microsoft office\root\rsodwow6432\proof.fr-fr.msi.16.fr-fr.tree.dat.pxj	23.95 KB	a4dd3e755c6144568981f9fddfb1dd9247de44418970070ef934bb2d3170dfc2	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-xstate-l2-1-0.dll.pxj	11.60 KB	8876657b0ed9f1c5c1e325170a5209febe563db5597aa65918145884284633b0	✖
c:\program files (x86)\microsoft.net\primary interop assemblies\msdatasrc.dll.pxj	12.32 KB	7dde84f7d00446f31bf5a654c688e1098732515a885ce0b33ce9080055668a89	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-stdio-l1-1-0.dll.pxj	24.45 KB	3eef532215198e752baf78adfc9e0327827ecab19ba44c5fec9e924bd663d6be	✖
c:\users\rdhj0cnfevzx\desktop\y8bwgaf.wav.pxj	97.37 KB	54bc3b007a5894fb3f32f6a47b02a5a577c730cc8659048e7f627ddc5777fcc5	✖
C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe.pxj	445.30 KB	331933131842ec561a8511926b7318171f6d6e7d8bc390508a1d8cd9e8b26402	✖
c:\users\rdhj0cnfevzx\desktop\ubrzfsfqiiguhptn.mp3.pxj	52.79 KB	49fbe8b105556712c5b09615f00bc1afa800ef5ed4f689838ed12ea027a7eeba	✖
C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.002.etl.pxj	12.26 KB	7a315839c65c68ad2dc29c0a8a19dfd9b5b57f7fc50fec4492ef9876cb60b8f9	✖
C:\Users\RDhJ0CNFevzX\Desktop\gbfl3bOsRvBD1R.mp4.pxj	29.98 KB	88bd3193f4982743e65a79f3090392e905b9307b462dbd80a45834daf89b5886	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\IntegratedOffice.exe.pxj	1067.88 KB	ab9e41d1f3b65bdde7830679f2e5cd3293ce951bf5b5c0487da6a8445dd128c9	✖
C:\Users\RDhJ0CNFevzX\Documents\cF4DGiix-UPJ.pptx.pxj	64.32 KB	0683711b2f49086268b72f780d4993cee11fb5c757be398f40b6daeb77eff4b2	✖
C:\Users\RDhJ0CNFevzX\Desktop\rj-kMB.mkv.pxj	56.30 KB	1e208a9fce49a197d6b02cd48849514be7e29393989375b4311b16e3d343c526	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\officemuiset.msi.16.en-us.tree.dat.pxj	4.82 KB	bb34ac591a12773b7fab42f339bca0f10ae412a5aba52b43df5f17882923be36	✖
C:\Users\RDhJ0CNFevzX\Pictures\WxUzKFkgu_fy5.gif.pxj	84.49 KB	d8d9661f560f7d06f3da371db0d42453a8635fc33df15fb4ec2c92169533d340	✖
c:\users\rdhj0cnfevzx\documents\zvx04_f1i1z9rufq15x.docx.pxj	76.80 KB	a7f31274d14054d18f0861a643e079f3ce2c7fef4953cc946744c990c81c6cd8	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml.pxj	1.76 KB	8492415e97283b80a354d4121686293dbfc708153a6d5e45b2a0e71c34d912a0	✖
c:\users\rdhj0cnfevzx\documents\oitf3cbvpsy_.pptx.pxj	29.32 KB	06b03d96402cb5989ee94310199ca583cf81cce90318dbf8bc74e682f390d037	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00a1-0000-0000-0000000ff1ce.xml.pxj	54.93 KB	680ef46531c4b7f41471159f833ac4ccc2f978a31f5fe38c68b07ab52a795cd5	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml.pxj	4.93 KB	0b2ccbd84fac7dc8a338e7b1c76c6e250e476fe3ac24e1e491779ac32821afaa	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-private-l1-1-0.dll.pxj	69.45 KB	7f2c781168225c8930288faaeda3c8619e2e4ed07a6faf28fd49fb452245149c	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml.pxj	1.49 KB	22cc50d1267920ce97097eed1c91d79a0262ecbc42046c1e1f171a51d35de447	✖
c:\program files\common files\microsoft shared\clicktorun\officec2rcom.dll.pxj	973.48 KB	9bd1ede987a4592c2c05e374184c2eda6db0d73b1a7d5150c2e38d9259d72772	✖
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Office 16 Click-to-Run Localization Component.swidtag.pxj	1.30 KB	0e1136d699ff8aef4e2018d99677a3281dbaa67a2d6ff40d82daf8090d71565d	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00ba-0409-0000-0000000ff1ce.xml.pxj	1.49 KB	0b299980675046da48be595ddf7d9a13ed15fcd9dbcd033dee228215e056be9c	✖
C:\Users\RDhJ0CNFevzX\Documents\lL qiypjS419b.pptx.pxj	53.73 KB	2ffdaf6bed85b388350f9c7a5ee73b3cf41cdce281e301145a825b3457f7cb9d	✖
C:\Users\RDhJ0CNFevzX\Videos\9Wec6D64kyBAn0qJ_5E.avi.pxj	56.90 KB	167efdce92c716cebf8ba1b0c968bc40fd83237303c41c52091cedeb5c72268f	✖
C:\ProgramData\Package Cache\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\state.rsm.pxj	1.04 KB	d9682743f61d723dc56e8b5df6f5f2618f74a6ea121bcd7d310caad74ef7a602	✖

File Name	File Size	SHA256	YARA Match
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest. 90160000-00e2-0409-0000-0000000ff1ce.xml.pxj	1.49 KB	6c4a2e94ecc07770924bc95b6f643c9a1960d03cc7277c2e45ea907ebc4c8ea2	✖
C:\Users\RDhJ0CNFevzX\Music\6P6Dok-d9o.m4a.pxj	27.16 KB	51fc6402445797e424386aca986986f3b5fe5ede888956e0f5de85116c2610ba	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmuxmui.msi.16.en-us.tree.dat.pxj	9.29 KB	51e7d5974cc7875f76d957402bd223f6520cac29574d26946907bc6edfe54b7e	✖
C:\Users\RDhJ0CNFevzX\Desktop\uXa6yixBdTufjOde5f.jpg.pxj	11.82 KB	9a0fe1604b619ab1eadd79417b02d3183f34d8e4290e8457505fb733cfd29a38	✖
c:\users\rdhj0cnfevzx\desktop\zpxp0xgs9ush4tgnr.mp4.pxj	81.51 KB	7b797a81e1865d476d3d3866ffb6c098e1b37bb9b89ae37ffa180fcfa61b2e8f	✖
c:\users\rdhj0cnfevzx\documents\qh--wkythvdi7yqhmto.ots.pxj	37.76 KB	bb6ec5a255a0bc2b9cff12e79461fc0294475bd5d49ea08516ffb3d72c508c21	✖
c:\program files (x86)\internet explorer\signup\install.ins.pxj	728 bytes	5e5b6ee31e4794791e3abf3d0b0d8c03fe1810aea7bac59ddad2dd149f18b4b1	✖
c:\users\rdhj0cnfevzx\documents\r qq1bkjumf5k.xlsx.pxj	44.82 KB	9c69f879b497b361216e92cac91cee25a41bf861b7070238800e435f8af6286f	✖
C:\Users\RDhJ0CNFevzX\Desktop\3l BOlgfmZ.wav.pxj	59.87 KB	b058c1e631c3ffc4adb180e78a1452003df7c755c0a1ed0eb224cbf110c2393a	✖
c:\users\rdhj0cnfevzx\videos\mnt8n-etnj4iwx.mkv.pxj	12.23 KB	0e4783241db9a84cacd1984604658d1f150a5a205b9f07f4ed1390c41640e314	✖
C:\Users\RDhJ0CNFevzX\Desktop\Y4Mcz1FsjYq4n.m4a.pxj	45.41 KB	e35519cbb6173d29ab62b878839cc174c601f417e85b40ee1c99b3c93fb77433	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest. 90160000-0090-0409-0000-0000000ff1ce.xml.pxj	1.49 KB	623e11308f2ec3c3094eed69a85fb85b867f493dd9472fd70953fe69dfd87a18	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\vccorlib140.dll.pxj	381.43 KB	77ceb7e988752773c32f8a45e4eb1f0f53f513448f79edf4b295aa01804e3ac0	✖
c:\users\rdhj0cnfevzx\desktop\qtrnijjfd.avi.pxj	40.12 KB	9055ca49408d939f7ffb0f9b96e208d4d1ff30e232741584ad82cba1eea22b21	✖
c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-filesystem-l1-1-0.dll.pxj	20.45 KB	114730a7a507419621368edf4d2ef140b3665756e454c50b16642af5f7e151b4	✖
c:\program files\common files\x3dqavt3.jpg.pxj	13.55 KB	733cc42d4183d9dc8f3175dc83c9a12e083c821dd635a3585bb92230fbeb3b49	✖
c:\program files (x86)\microsoft office\office16\ospp.htm.pxj	170.70 KB	3c580e7b8f9c298f6bf8e92743c5ead2c70415c71c27bf8a5772d1fc1fffabbf	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest. 90160000-00E1-0409-0000-0000000FF1CE.xml.pxj	1.49 KB	9a571b1e5c269292137edb038659f4fbba12912aa8f407a433e93053a9e0c6a6	✖
c:\program files\common files\microsoft shared\clicktorun\officec2rclient.exe.pxj	5828.37 KB	326a19169f1013cd3aade59b5486767f05be7085cb94539e4856dbb11726ec14	✖
C:\Users\RDhJ0CNFevzX\Music\F34KZnz.wav.pxj	81.91 KB	ed13d8591854c31ef9c7f566b522b563892927ba6b4d81d831bd6b9246ff0442	✖
c:\users\rdhj0cnfevzx\links\downloads.lnk.pxj	1.21 KB	13ec996e5bdd88cd105252e6f13a406faf754a7fa2d52e9c3763c3f388e0491d	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\outlookmui.msi.16.en-us.tree.dat.pxj	74.98 KB	2a9124e850137a9f198ef7f1dfcdd766517d2996ae35cad006ce161c92c83646	✖
c:\program files\internet explorer\signup\install.ins.pxj	728 bytes	06d568b87bc71ef24aceb78370ee4f27f17e38fbc4cd51138c9e8b25a5be083b	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\officemuiset.msi.16.en-us.boot.tree.dat.pxj	2.51 KB	7dd8dedc889275ec73f11c15a5f4f5a69ddbf45d45b8516d5fdd3854a53352cb	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVScripting.dll.pxj	500.48 KB	7d1b5687c4508e5b92b5131c541f635db44dcc305da7351e1cbd2be6dfaf715a	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\office64mui.msi.16.en-us.boot.tree.dat.pxj	6.95 KB	340ca2ed55ccf4888ecc2ab80cf5834263c1aba1293f62611954760a4a81ab5d	✖
c:\programdata\usoshared\logs\updatesessionorchestration.009.etl.pxj	4.26 KB	8bfe61b33fd3fc54715c94e73f90d43fd5fa52043c98a8f5ff6790ba297dabfa	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest. 90160000-00e2-0000-0000-0000000ff1ce.xml.pxj	3.93 KB	87ca215e5b70b15d480a4353d93380a18b11140a6c76df08a9bdf9c8ce652f7d	✖

File Name	File Size	SHA256	YARA Match
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-file-l1-2-0.dll.pxj	18.45 KB	424c776eea9e38fd4d6caa6051606cc9fe6c7272ef188b49acc12cb25278fc38	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00ba-0000-0000-0000000ff1ce.xml.pxj	9.26 KB	1b045f876842ed21a783387e98f7d513229ad5388539bb1948c446294d9795b8	✖
c:\users\rdhj0cnfevzx\desktop\qr-r.mkv.pxj	48.54 KB	24da9e72bb85174c450534cfe28e57655c9002b5024b7a08acd4cc31d8a10cf4	✖
c:\users\rdhj0cnfevzx\videos\pklzhb14u2fpdy.mp4.pxj	15.20 KB	376229dd1054d0ec92fd125c0f3aed975e34ea9b82ce5023729321c545d2dddc	✖
C:\ProgramData\Package Cache\{3c3aafc8-d898-43ec-998f-965ffdae065a}\vcredist_x64.exe.pxj	452.43 KB	939af0be23ede46bd02da70ad898de15473605ab4fbee14ee2067c2424f8f780	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml.pxj	1.49 KB	d90d631dc7366083afc14cf9cce702391b4d6bd9d7f5443c0278465b05652456	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\lyncmui.msi.16.en-us.boot.tree.dat.pxj	8.90 KB	950b9b259466d2af0a4d12f832ad199e8a531183d69fc270d4542b1686abacf7	✖
c:\users\rdhj0cnfevzx\documents\h4zgddgxc.docx.pxj	31.15 KB	16d63727793ef936755ab77beaf07331b8a0e4020c7e13f45faae29f2a569e93	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\powerpointmui.msi.16.en-us.boot.tree.dat.pxj	14.68 KB	5fee95d8cb77d1fadbf0b9294100e8418009455fc368f23cd74aab4e505a1823	✖
c:\users\rdhj0cnfevzx\desktop\3kw 6phj1nu.mp4.pxj	25.49 KB	9beb3c4dc049b6ed870a863013a71ec56bab29f6461f3baf2c53cb6c592769b7	✖
c:\programdata\usosharedlogs\updatesessionorchestration.003.etl.pxj	12.26 KB	1a3af86e247fc4020caa9ed2aeeefd9f36eb8477499d18c04afb9aac1941674d	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml.pxj	720.85 KB	8cd9c44c35cd27b1e33496ea18ecd061fa3eed04efce58789f223062dbc76164	✖
C:\Users\RDhJ0CNFevzX\Videos\WwNHxljnQ8Fh_KvDi.mp4.pxj	85.73 KB	7647eb67a842883e92cf91611395d312011e055d4a41e6e4646e44ac6035688f	✖
c:\program files\common files\microsoft shared\clicktorun\appvisvsubsystems64.dll.pxj	2232.43 KB	989c17f4eaa5fdb3b02786372949b80483ac4f2ad6c9f3f7e6c897aee65d63da	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash.pxj	376 bytes	e888279d08685b379ac2652222f8be552c5b3febb73d559acc2ff43f3d998d54	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\excelmui.msi.16.en-us.boot.tree.dat.pxj	19.66 KB	c100b89298110b8d995d91ea2c8b5afac4a7a3f04a2bf90b6ff34d4d3f2495f0	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\outlook.x-none.msi.16.x-none.tree.dat.pxj	581.90 KB	e7a1ca814c5df138f5a0b5793f70bd2d5685778809078967 42fe719641645eec	✖
C:\Users\RDhJ0CNFevzX\Music\56SXCIp.m4a.pxj	7.10 KB	1db85199132d60d9ea9e44794a123448c51f5f2f9fd223f631727846546fc5b3	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\groove.x-none.msi.16.x-none.boot.tree.dat.pxj	9.10 KB	4eba523461e0a72d8f96e71c8525b6af00db0334697ea81b26e36e5a308bf654	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.common.xml.pxj	1951.24 KB	fd8da5a08158700f51bb2a538f6c7948123bd27fb4cffeb5a4b033e3be5a482b	✖
c:\users\rdhj0cnfevzx\videos\8ooufkkqdq_ci1.flv.pxj	5.82 KB	d204ddc6fe352e2af5e948bdbf4a70d5379c29f41adfa8ff59fd31ba1a9f593e	✖
c:\users\rdhj0cnfevzx\documents\3oc5blwnmi_d.pptx.pxj	95.32 KB	132feb293339ff720f798eed4d8cd2ec84bb80fc793ec607f4b32aa47e4a33bd	✖
C:\Users\RDhJ0CNFevzX\Desktop\ajdQmxaQYMm_L.bmp.pxj	22.60 KB	ad87fac02da39735cee230bea47fa18015f2affdff2278c484fb30ea897e775d	✖
c:\users\rdhj0cnfevzx\documents\onljyqjpwbk.xlsx.pxj	67.34 KB	a615a0735e6ad5b44c3deb2826cbe7c67fc8f2dc7a762474a7ce934b3a59c1c3	✖
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Office 16 Click-to-Run Licensing Component.swidtag.pxj	1.30 KB	7ec90bc32c3e61338de65fcf1997f6f841193b0503d9e190950368159528dbb9	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\access.x-none.msi.16.x-none.boot.tree.dat.pxj	48.12 KB	ee645cd56f0d4a81bcea2268396e47e2b8f94d4cbea230ed55b3db9096b2f44a	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\dcf.x-none.msi.16.x-none.boot.tree.dat.pxj	9.12 KB	33f6c61bf539b270ef9d1e36aeeebf1ef6514222268bfe5017e69b536d87cc77	✖

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\placeholder.txt.pxj	632 bytes	c68d3554c6a569b23067ed2b4300e2317aaa4d512133495cb6b069521f1f17a7	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml.pxj	314.84 KB	3ec6137267020f5438f6e4ba6e2b354830fe596282e42e37830a5e5ecf69d0b4	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml.pxj	1.49 KB	abf1e6b926cd33f030664b3b95f4e878c3d7b3aaf6930205204633f6d26eba52	✖
c:\users\rdhj0cnfevzx\music\zfxe-iab.wav.pxj	79.70 KB	675b2c9285b7fad14aae359785632460cb863d728bc0120a9120515033ef379a	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\powerpivot.x-none.msi.16.x-none.boot.tree.dat.pxj	446.79 KB	c0d1531a803d382d0dc017f596cb71bb90f8b83ed93ff11d79e6e68e6829152f	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\powerpointmui.msi.16.en-us.tree.dat.pxj	18.90 KB	4710b81c12383406581a876c6b90e9e84e23211b01830c2e29e5cc11f0fe7b3a	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-locale-l1-1-0.dll.pxj	18.95 KB	be6d7edf554a98fe7dd6c97ff581b509c882f2fef71a8d8d1c78c7a8778b44f2	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\officemui.msi.16.en-us.boot.tree.dat.pxj	62.91 KB	8ffe3ea923d1d64311a06f91ad6cd38e83c3c8b1d25859fc073d0fc44a9d7798	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-002a-0000-1000-0000000ff1ce.xml.pxj	34.15 KB	2b85980d4cf404e9ef4ef217d3a5fc994af9c8d04c26c5999aa5e51bc2001ff3	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-runtime-l1-1-0.dll.pxj	22.95 KB	199b30a2b560fc84b1ff3bfde95136fdc2f3ab0c785617ac120c5632ccd20474	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\ucrtbase.dll.pxj	959.95 KB	cf3c75cca5f31ca0749c080910563c3f3ed124649868a7800951b2f3fdb103a5	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\dcfmui.msi.16.en-us.boot.tree.dat.pxj	5.77 KB	9080e6e868550de905a0de13d90bcf3654d1d80bcf7b0f060a60f0b22b120df4	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmuxmui.msi.16.en-us.boot.tree.dat.pxj	6.34 KB	71cb187c2b1f53cef3a666d197817696467bc6de05b12ebaa7f25fd2c24da4e9	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-006e-0409-0000-0000000ff1ce.xml.pxj	14.48 KB	3b6e2f058e8202e1bbb16677de28ce946f0a8b62843a9d178910d50f8dd836ca	✖
c:\program files\microsoft office 15\clientx64\officeclicktorun.exe.pxj	1067.88 KB	ba8453f8443681bbc6faad001a840f11562ac9805663ca9565bfed76fc835524	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-3101-0000-0000-0000000ff1ce.xml.pxj	3.55 KB	7f9fbbc2471efcc427d771e1e0e9d5dd5b28c99380d2a923cc29eb3bc4bdbf63	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\onenotemui.msi.16.en-us.boot.tree.dat.pxj	10.79 KB	0140b489f769d0e2cfd4931bb4b33115d4d8f997038f45114875f16978704a79	✖
c:\programdata\package cache\{65e650ff-30be-469d-b63a-418d71ea1765}\vc_redist.x86.exe.pxj	632.99 KB	b9feaa41497f2051f45702fdf7e96ee93d6bc975dfa91ae6df3d602108ee918f	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Proof.fr-fr.msi.16.fr-fr.boot.tree.dat.pxj	15.96 KB	56250aacb9fdd8560cf8e6dbf1c04c3cfc89036dac1ade7992710557d1775520	✖
c:\programdata\usosharedlogs\updatesessionorchestration.010.etl.pxj	4.26 KB	0ff7eecd8dc0f928119fc76e35e4425cd3c044bd4a270ce71e753df3b4f9af8f	✖
c:\program files\common files\gwfgft_br_n0vy16u6.gif.pxj	36.57 KB	11c908f07fe393884b23f127c6a9ebba096c38b0f549ec0e4d64a717701fb1ea	✖
C:\Users\RDhJ0CNFevzX\Pictures\VZ7J2h1NNIuHd_.png.pxj	72.90 KB	5646eb6e25cc061095624d927e9a951e2b3a233b09599e36fc496bae6ceb2cf2	✖
C:\Users\RDhJ0CNFevzX\Documents\koDg-zIFaXRKP63Q3p2.xlsx.pxj	38.49 KB	a0a24ab1b6355ae55766d3d4a5485ac7e4273d78c86be1edd0d09c681aa14e32	✖
C:\Users\RDhJ0CNFevzX\Desktop\3FSu0.gif.pxj	40.52 KB	13f8c9afa23b28d465183f9d5116860d0fe6822b4ae1ae52949d3219a5ab86ef	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\proof.es-es.msi.16.es-es.boot.tree.dat.pxj	15.96 KB	db4221beb611a56879385bb3d33e2c69892a0f2618b5f115b6115366c5135556	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-time-l1-1-0.dll.pxj	20.95 KB	892d7fa18b8dd600e365c25f94cceb8d96372e5974b658a8cd6a2511c0cec390	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-processthreads-l1-1-1.dll.pxj	18.95 KB	bdcd1ba759384358ed4a4173fff530261e915dc7d966b91ae995545f67f23b8c	✖

File Name	File Size	SHA256	YARA Match
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00a1-0409-0000-0000000ff1ce.xml.pxj	1.49 KB	96e66866caf8ebee1d155ac4e272c6c2e4667f5c2637f85869e794e26ed6374a	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml.pxj	1.49 KB	58ca5d3a02e38c9a2d434e1f8c0d65aac8142d562fec8e3590cc778489b86995	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\accessmuiset.msi.16.en-us.boot.tree.dat.pxj	2.51 KB	bad278ed356e2d88787226180c1d1f122e2ac55edda4719a3a5c7927c4a0309a	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-synch-l1-2-0.dll.pxj	18.95 KB	f3566531825301d6c24ed72cd9c898660c5bd074dd687d25b3a771848defc7d1	✖
C:\ProgramData\Package Cache\{3c3aafc8-d898-43ec-998f-965ffdae065a}\state.rsm.pxj	904 bytes	b1e9d20aaa2b3a110d9f30364c554a98ae6d38fb6ba2d9828ddb528fdc657874	✖
c:\programdata\package cache\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\state.rsm.pxj	904 bytes	1369e1e14566dd4d136046a56783438bf74624edac77d8122436f544648c5395	✖
C:\Users\RDhJ0CNFevzX\Documents\W9Zb9GI99.odt.pxj	42.51 KB	5ddfe4551b3dd12511f0b128a750d5ca2f4fc855f5e015eaf08285690fa6d752	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml.pxj	1.49 KB	48a5ba1bcb2c6fd1db2b67b481bf3ac74b4092741db200b53c2ef82760230151	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\osmmui.msi.16.en-us.boot.tree.dat.pxj	2.80 KB	431f7355add6d58b7c095c45604a47c9fea31bcee597187be5e399702bbc80ae	✖
C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.004.etl.pxj	12.26 KB	b3b7ed8db4bf66c6325283d1d977144e9408b2aeba569a32294307f8ca9ec982	✖
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmmui.msi.16.en-us.tree.dat.pxj	5.18 KB	55980d372e528b484e05fcd2c6e701406986617b070ad9348dec565cbd76c6ac	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml.pxj	453.37 KB	19ec4b95c9da7733ef33d8fe81776cf1ad2a80107747fede26a73afa8ce6c269	✖
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml.pxj	758.16 KB	8e12e6d2aac6c12f8b7c067053aa7e5d29afa8ece0e3b7c5821131f2f503889b	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifestloc.en-us.xml.pxj	9.87 KB	9bb622c0e0221da3e715c4d6355a1cbe43e46d652b83b378dc9c9724f1f28712	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-string-l1-1-0.dll.pxj	24.45 KB	cfee2d4b810a7f904d6bbba64ac53bf69228259f514131532e40f7566d48ca98	✖
c:\program files (x86)\microsoft office\root\rsodwow6432\groovemui.msi.16.en-us.boot.tree.dat.pxj	3.85 KB	70fb52ba3ddefc1cdd7a801fe07bdc0cad37d1aa104217ccd3f3f23592a3f49e	✖
c:\program files (x86)\microsoft office\office16\slerror.xml.pxj	35.74 KB	5f68f3b005a32816ceb5dfbebd4d5fc19b4e6a2a65450a047492d25ee3c17801	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-environment-l1-1-0.dll.pxj	18.95 KB	02f63fc1bfefd2d98c19965c75dac70bf271ecff37731aa5c79bd5c2257e2138	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-conio-l1-1-0.dll.pxj	19.45 KB	83af66bc316c7daae3cb3045d2f8e27e03c28fb3a09021f315fe5cdae43e61d9	✖
c:\programdata\usoshared\logs\updatesessionorchestration.005.etl.pxj	12.26 KB	b4febd50db795e01fb82f217d08afe0357bb717a9356c285b640ac429034a7da	✖
c:\users\rdhj0cnfevzx\desktop\10gs1e2cow2stsot.mp3.pxj	95.29 KB	714822afe82b60f56783c0a95ba4d809377ecadeb2ec97eda44814fdaafe3fad	✖
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-012a-0000-0000-0000000ff1ce.xml.pxj	516.54 KB	9a653932ef0c54276ea15e75709b1509321186a269ce40d43474ad2365cdb4c9	✖
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-timezone-l1-1-0.dll.pxj	18.45 KB	dba6b592d01e4762659afdb908011e6b808b4f685eb1a32ae70622d577bf8681	✖
c:\users\rdhj0cnfevzx\desktop\o4gu.pptx.pxj	28.71 KB	b1efa75452c0665ed3648bbee640978dd7994734d4f3998c5cf3e79cfa2fdfb2	✖

Reduced dataset

Host Behavior

Type	Count
File	54520

Type	Count
Mutex	1
Module	9
Process	5
System	1
Window	2
Environment	1

Process #2: vssadmin.exe

ID	2
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin.exe delete shadows /all /quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 113989, Reason: Child Process
Unmonitor End Time	End Time: 135892, Reason: Terminated
Monitor duration	21.90s
Return Code	2
PID	3236
Parent PID	3024
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1	C:\Users\RDhJ0CNFevzX\Desktop\9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe	Sample File	112.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
780101ba245fb03c1783f719ef4456f39f3482b5e004e120ccabbd277b717fd8	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001a-0409-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml.pxj	Dropped File	19.26 KB	application/octet-stream	Access, Create, Write	CLEAN
ef43dccc182ffe171b1e41f8a45445a8036f21e0bcec637fa42b62c7d5dd256e	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-040c-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-040C-0000-0000000FF1CE.xml.pxj	Dropped File	2.37 KB	application/octet-stream	Access, Create, Write	CLEAN
8c94257b2354f3098001cabba62f30427c9db04ce12c1c14585bee057d824a46	c:\users\rdhj0cnfevzx\documents\dhsdwsuvr.pptx.pxj, C:\Users\RDhJ0CNFevzX\Documents\dHsDwSUvr.pptx.pxj	Dropped File	76.93 KB	application/octet-stream	Access, Create, Write	CLEAN
9a6445fcbe0caea3481ee261cd9a02834a82e234feae5fd292312fd5edf86bf0	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Proof.en-us.msi.16.en-us.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\proof.en-us.msi.16.en-us.tree.dat.pxj	Dropped File	19.02 KB	application/octet-stream	Access, Create, Write	CLEAN
08fcec29d081857e0e62330f485c724edd451615e9fef56bae56a92fc67eff06	c:\programdata\package cache\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\vc_redist.x64.exe.pxj, C:\ProgramData\Package Cache\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\VC_redist.x64.exe.pxj	Dropped File	632.79 KB	application/octet-stream	Access, Create, Write	CLEAN
686cad79a132284b17c6b52e6d37dd053eb2d80f4881a198663489003e219751	c:\program files (x86)\microsoft office\root\rsodwow6432\proof.es-es.msi.16.es-es.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Proof.es-es.msi.16.es-es.tree.dat.pxj	Dropped File	23.88 KB	application/octet-stream	Access, Create, Write	CLEAN
5f577cb9e77ec03df13450b1e2f40417683f1a6456308c3b1b388baf711176a7	c:\program files (x86)\microsoft office\root\rsodwow6432\excel.x-none.msi.16.x-none.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Excel.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File	166.20 KB	application/octet-stream	Access, Create, Write	CLEAN
c10299669e0731d6118a952907a323c52e3d215048dbd2a4996fe07fbb205482	c:\program files\common files\microsoft shared\clicktorun\api-ms-win-core-file-l2-1-0.dll.pxj, C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-file-l2-1-0.dll.pxj	Dropped File	18.45 KB	application/octet-stream	Access, Create, Write	CLEAN
a437d24d7cdf4e07d7820e6c27721c1e70a3c57bfa60105bbb1769b633f68361	C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\authoredextensions.xml.pxj	Dropped File	648 bytes	application/octet-stream	Access, Create, Write	CLEAN
ee0d4fe62e40de86cc6582aacb9d6e1f0e91b441d4dcdb55b04489ac94316802	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001b-0409-0000-0000000ff1ce.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f4d889dfe233d5c44d667928ad0d3a9f22b5a8f9ce99d798ffface723c9dcecc	C:\Users\RDhJ0CNFevzX\Documents\JVuaF.ots.pxj, c:\users\rdhj0cnfevzx\documents\jvuaf.ots.pxj	Dropped File	17.65 KB	application/octet-stream	Access, Create, Write	CLEAN
b03bd3dd738a393c95a5330bfd15c42d42e4a6fdef1a59ff621b3e283c5feaaa	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\office64muiset.msi.16.en-us.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\office64muiset.msi.16.en-us.boot.tree.dat.pxj	Dropped File	1.95 KB	application/octet-stream	Access, Create, Write	CLEAN
af4ce45192283ca5e2aca9b87d4bf08d37717e1021cd6a888f30d5a3e86f2188	C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml.pxj, c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.pxj	Dropped File	4.30 KB	application/octet-stream	Access, Create, Write	CLEAN
f6edfc1eadf81cdb987d4d9397b12296cd527d86621752b534313e1a222dabd4	c:\users\rdhj0cnfevzx\pictures\kwv8d1m_xerjis4ig.jpg.pxj, C:\Users\RDhJ0CNFevzX\Pictures\kWV8D1M_XERjis4IG.jpg.pxj	Dropped File	74.32 KB	application/octet-stream	Access, Create, Write	CLEAN
0c516e20038fc6bcd47efcf84a6101530714931d44b247dbabe35a28f8129451	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0116-0409-1000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
bdb5c8ac91e614a5ff9696657552dfc11a472f2fcb8aac14db0cf988700928a1	c:\users\rdhj0cnfevzx\documents\4oz_p78.docx.pxj, C:\Users\RDhJ0CNFevzX\Documents\4oz_P78.docx.pxj	Dropped File	93.76 KB	application/octet-stream	Access, Create, Write	CLEAN
787659d75d4af3a778019f5524f1f57c73e10651657505c07113d74a52f50c81	C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB.pxj, c:\program files (x86)\common files\designer\msaddndr.olb.pxj	Dropped File	15.87 KB	application/octet-stream	Access, Create, Write	CLEAN
a4dd3e755c6144568981f9fddfb1dd9247de44418970070ef934bb2d3170dfc2	c:\program files (x86)\microsoft office\root\rsodwow6432\proof.fr-fr.msi.16.fr-fr.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Proof.fr-fr.msi.16.fr-fr.tree.dat.pxj	Dropped File	23.95 KB	application/octet-stream	Access, Create, Write	CLEAN
8876657b0ed9f1c5c1e325170a5209febe563db5597aa65918145884284633b0	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-xstate-l2-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-core-xstate-l2-1-0.dll.pxj	Dropped File	11.60 KB	application/octet-stream	Access, Create, Write	CLEAN
7dde84f7d00446f31bf5a654c688e1098732515a885ce0b33ce9080055668a89	c:\program files (x86)\microsoft.net\primary interop assemblies\msdatasrc.dll.pxj, C:\Program Files (x86)\Microsoft.NET\Primary Interop Assemblies\msdatasrc.dll.pxj	Dropped File	12.32 KB	application/octet-stream	Access, Create, Write	CLEAN
3eef532215198e752baf78adfc9e0327827ecab19ba44c5fec9e924bd663d6be	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-stdio-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-stdio-l1-1-0.dll.pxj	Dropped File	24.45 KB	application/octet-stream	Access, Create, Write	CLEAN
54bc3b007a5894fb3f32f6a47b02a5a577c730cc8659048e7f627ddc5777fcc5	c:\users\rdhj0cnfevzx\desktop\y8bwgaf.wav.pxj, C:\Users\RDhJ0CNFevzX\Desktop\y8bwgaf.wav.pxj	Dropped File	97.37 KB	application/octet-stream	Access, Create, Write	CLEAN
331933131842ec561a8511926b7318171f6d6e7d8bc390508a1d8cd9e8b26402	C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe.pxj, c:\programdata\package cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe.pxj	Dropped File	445.30 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
49fbe8b105556712c5b09615f00bc1afa800ef5ed4f689838ed12ea027a7eeba	c:\users\rdhj0cnfevzx\desktop\ubrzfsfqiiguhptn.mp3.pxj, C:\Users\RDhJ0CNFevzX\Desktop\UBRZfsFQIIGuhpTN.mp3.pxj	Dropped File	52.79 KB	application/octet-stream	Access, Create, Write	CLEAN
7a315839c65c68ad2dc29c0a8a19dfd9b5b57f7fc50fec4492ef9876cb60b8f9	C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.002.etl.pxj, c:\programdata\usoshared\logs\updatessessionorchestration.002.etl.pxj	Dropped File	12.26 KB	application/octet-stream	Access, Create, Write	CLEAN
88bd3193f4982743e65a79f3090392e905b9307b462dbd80a45834daf89b5886	C:\Users\RDhJ0CNFevzX\Desktop\gbfl3bOsRvBD1R.mp4.pxj, c:\users\rdhj0cnfevzx\desktop\gbfl3bosrvbd1r.mp4.pxj	Dropped File	29.98 KB	application/octet-stream	Access, Create, Write	CLEAN
ab9e41d1f3b65bdde7830679f2e5cd3293ce951bf5b5c0487da6a8445dd128c9	C:\Program Files\Common Files\microsoft shared\ClickToRun\IntegratedOffice.exe.pxj, c:\program files\common files\microsoft shared\clicktorun\integratedoffice.exe.pxj	Dropped File	1067.88 KB	application/octet-stream	Access, Create, Write	CLEAN
0683711b2f49086268b72f780d4993cee11fb5c757be398f40b6daeb77eff4b2	C:\Users\RDhJ0CNFevzX\Documents\cF4DGiix-UPJ.pptx.pxj, c:\users\rdhj0cnfevzx\documents\cf4dgiix-upj.pptx.pxj	Dropped File	64.32 KB	application/octet-stream	Access, Create, Write	CLEAN
1e208a9fce49a197d6b02cd48849514be7e29393989375b4311b16e3d343c526	C:\Users\RDhJ0CNFevzX\Desktop\rj-kMB.mkv.pxj, c:\users\rdhj0cnfevzx\desktop\rj-kmb.mkv.pxj	Dropped File	56.30 KB	application/octet-stream	Access, Create, Write	CLEAN
bb34ac591a12773b7fab42f339bca0f10ae412a5aba52b43df5f17882923be36	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\officemuiset.msi.16.en-us.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\officemuiset.msi.16.en-us.tree.dat.pxj	Dropped File	4.82 KB	application/octet-stream	Access, Create, Write	CLEAN
d8d9661f560f7d06f3da371db0d42453a8635fc33df15fb4ec2c92169533d340	C:\Users\RDhJ0CNFevzX\Pictures\WxUzKFkgu_fy5.gif.pxj, c:\users\rdhj0cnfevzx\pictures\wxuzkfkgu_fy5.gif.pxj	Dropped File	84.49 KB	application/octet-stream	Access, Create, Write	CLEAN
a7f31274d14054d18f0861a643e079f3ce2c7fef4953cc946744c990c81c6cd8	c:\users\rdhj0cnfevzx\documents\zvx04_f1i1z9rufq15x.docx.pxj, C:\Users\RDhJ0CNFevzX\Documents\zvx04_F1i1z9rUfQ15x.docx.pxj	Dropped File	76.80 KB	application/octet-stream	Access, Create, Write	CLEAN
8492415e97283b80a354d4121686293dbfc708153a6d5e45b2a0e71c34d912a0	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0015-0409-0000-0000000ff1ce.xml.pxj	Dropped File	1.76 KB	application/octet-stream	Access, Create, Write	CLEAN
06b03d96402cb5989ee94310199ca583cf81cce90318dbf8bc74e682f390d037	c:\users\rdhj0cnfevzx\documents\oitf3cbvpsy_.pptx.pxj, C:\Users\RDhJ0CNFevzX\Documents\Oitf3cBVPSY_.pptx.pxj	Dropped File	29.32 KB	application/octet-stream	Access, Create, Write	CLEAN
680ef46531c4b7f41471159f833ac4ccc2f978a31f5fe38c68b07ab52a795cd5	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00a1-0000-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml.pxj	Dropped File	54.93 KB	application/octet-stream	Access, Create, Write	CLEAN
0b2ccbd84fac7dc8a338e7b1c76c6e250e476fe3ac24e1e491779ac32821afaa	C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml.pxj, c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.pxj	Dropped File	4.93 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7f2c781168225c8930288faaeda3c8619e2e4ed07a6faf28fd49fb452245149c	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-private-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-private-l1-1-0.dll.pxj	Dropped File	69.45 KB	application/octet-stream	Access, Create, Write	CLEAN
22cc50d1267920ce97097eed1c91d79a0262ecbc42046c1e1f171a51d35de447	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0016-0409-0000-0000000ff1ce.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
9bd1ede987a4592c2c05e374184c2eda6db0d73b1a7d5150c2e38d9259d72772	c:\program files\common files\microsoft shared\clicktorun\officec2rcom.dll.pxj, C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RCom.dll.pxj	Dropped File	973.48 KB	application/octet-stream	Access, Create, Write	CLEAN
0e1136d699ff8aef4e2018d99677a3281dbaa67a2d6ff40d82daf8090d71565d	C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Office 16 Click-to-Run Localization Component.swidtag.pxj, c:\programdata\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft office 16 click-to-run localization component.swidtag.pxj	Dropped File	1.30 KB	application/octet-stream	Access, Create, Write	CLEAN
0b299980675046da48be595ddf7d9a13ed15fcd9dbcd033dee228215e056be9c	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00ba-0409-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
2ffdaf6bed85b388350f9c7a5ee73b3cf41cdce281e301145a825b3457f7cb9d	C:\Users\RDhJ0CNFevzX\Documents\ILqiypjS419b.pptx.pxj, c:\users\rdhj0cnfevzx\documents\ilqiypjs419b.pptx.pxj	Dropped File	53.73 KB	application/octet-stream	Access, Create, Write	CLEAN
167efdce92c716cebf8ba1b0c968bc40fd83237303c41c52091cedeb5c72268f	C:\Users\RDhJ0CNFevzX\Videos\9Wec6D64kyBAn0qJ_5E.avi.pxj, c:\users\rdhj0cnfevzx\videos\9wec6d64kyban0qj_5e.avi.pxj	Dropped File	56.90 KB	application/octet-stream	Access, Create, Write	CLEAN
d9682743f61d723dc56e8b5df6f5f2618f74a6ea121bcd7d310caad74ef7a602	C:\ProgramData\Package Cache\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\state.rsm.pxj, c:\programdata\package cache\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\state.rsm.pxj	Dropped File	1.04 KB	application/octet-stream	Access, Create, Write	CLEAN
6c4a2e94ecc07770924bc95b6f643c9a1960d03cc7277c2e45ea907ebc4c8ea2	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00e2-0409-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
51fc6402445797e424386aca986986f3b5fe5ede888956e0f5de85116c2610ba	C:\Users\RDhJ0CNFevzX\Music\6P6Dok-d9o.m4a.pxj, c:\users\rdhj0cnfevzx\music\6p6dok-d9o.m4a.pxj	Dropped File	27.16 KB	application/octet-stream	Access, Create, Write	CLEAN
51e7d5974cc7875f76d957402bd223f6520cac29574d26946907bc6edfe54b7e	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmuxmui.msi.16.en-us.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\osmuxmui.msi.16.en-us.tree.dat.pxj	Dropped File	9.29 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9a0fe1604b619ab1eadd79417b02d3183f34d8e4290e8457505fb733cfd29a38	C:\Users\RDhJ0CNFevzX\Desktop\uXa6yixBdTufjOde5f.jpg.pxj, c:\users\rdhj0cnfevzx\desktop\uxa6yixbdtufjode5f.jpg.pxj	Dropped File	11.82 KB	application/octet-stream	Access, Create, Write	CLEAN
7b797a81e1865d476d3d3866ffb6c098e1b37bb9b89ae37ffa180fcfa61b2e8f	c:\users\rdhj0cnfevzx\desktop\zpxp0xgs9ush4tgnr.mp4.pxj, C:\Users\RDhJ0CNFevzX\Desktop\ZPxP0xGS9USh4TGNr.mp4.pxj	Dropped File	81.51 KB	application/octet-stream	Access, Create, Write	CLEAN
bb6ec5a255a0bc2b9cff12e79461fc0294475bd5d49ea08516ffb3d72c508c21	c:\users\rdhj0cnfevzx\documents\qh--wkythvdi7yqhmto.ots.pxj, C:\Users\RDhJ0CNFevzX\Documents\QH--WkYtHVdi7yQhMto.ots.pxj	Dropped File	37.76 KB	application/octet-stream	Access, Create, Write	CLEAN
5e5b6ee31e4794791e3abf3d0b0d8c03fe1810aea7bac59ddad2dd149f18b4b1	c:\program files (x86)\internet explorer\signup\install.ins.pxj, C:\Program Files (x86)\Internet Explorer\SIGNUP\install.ins.pxj	Dropped File	728 bytes	application/octet-stream	Access, Create, Write	CLEAN
9c69f879b497b361216e92cac91cee25a41bf861b7070238800e435f8af6286f	c:\users\rdhj0cnfevzx\documents\rqq1bkjumf5k.xlsx.pxj, C:\Users\RDhJ0CNFevzX\Documents\rQq1Bkjumf5K.xlsx.pxj	Dropped File	44.82 KB	application/octet-stream	Access, Create, Write	CLEAN
b058c1e631c3ffc4adb180e78a1452003df7c755c0a1ed0eb224cbf110c2393a	C:\Users\RDhJ0CNFevzX\Desktop\3lBOIgfmZ.wav.pxj, c:\users\rdhj0cnfevzx\desktop\3iboigfmz.wav.pxj	Dropped File	59.87 KB	application/octet-stream	Access, Create, Write	CLEAN
0e4783241db9a84cacd1984604658d1f150a5a205b9f07f4ed1390c41640e314	c:\users\rdhj0cnfevzx\videos\mnt8n-etnj4iwx.mkv.pxj, C:\Users\RDhJ0CNFevzX\Videos\mNT8n-etNJ4IWX.mkv.pxj	Dropped File	12.23 KB	application/octet-stream	Access, Create, Write	CLEAN
e35519cbb6173d29ab62b878839cc174c601f417e85b40ee1c99b3c93fb77433	C:\Users\RDhJ0CNFevzX\Desktop\Y4Mcz1FsjYq4n.m4a.pxj, c:\users\rdhj0cnfevzx\desktop\y4mcz1fsjyq4n.m4a.pxj	Dropped File	45.41 KB	application/octet-stream	Access, Create, Write	CLEAN
623e11308f2ec3c3094eed69a85fb85b867f493dd9472fd70953fe69dfd87a18	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0090-0409-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
77ceb7e988752773c32f8a45e4eb1f0f53f513448f79edf4b295aa01804e3ac0	C:\Program Files\Common Files\microsoft shared\ClickToRun\vccorlib140.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\vccorlib140.dll.pxj	Dropped File	381.43 KB	application/octet-stream	Access, Create, Write	CLEAN
9055ca49408d939f7ffb0f9b96e208d4d1ff30e232741584ad82cba1eea22b21	c:\users\rdhj0cnfevzx\desktop\qtrnijjfd.avi.pxj, C:\Users\RDhJ0CNFevzX\Desktop\QtRnljJFd.avi.pxj	Dropped File	40.12 KB	application/octet-stream	Access, Create, Write	CLEAN
114730a7a507419621368edf4d2ef140b3665756e454c50b16642af5f7e151b4	c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-filesystem-l1-1-0.dll.pxj, C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-filesystem-l1-1-0.dll.pxj	Dropped File	20.45 KB	application/octet-stream	Access, Create, Write	CLEAN
733cc42d4183d9dc8f3175dc83c9a12e083c821dd635a3585bb92230fbeb3b49	c:\program files\common files\x3dqavt3.jpg.pxj, C:\Program Files\Common Files\x3dQaVt3.jpg.pxj	Dropped File	13.55 KB	application/octet-stream	Access, Create, Write	CLEAN
3c580e7b8f9c298f6bf8e92743c5ead2c70415c71c27bf8a5772d1fc1fffabbf	c:\program files (x86)\microsoft office\office16\ospp.htm.pxj, C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM.pxj	Dropped File	170.70 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9a571b1e5c269292137edb038659f4fbba12912aa8f407a433e93053a9e0c6a6	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00e1-0409-0000-0000000ff1ce.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
326a19169f1013cd3aade59b5486767f05be7085cb94539e4856dbb11726ec14	c:\program files\common files\microsoft shared\clicktorun\officec2rclient.exe.pxj, C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe.pxj	Dropped File	5828.37 KB	application/octet-stream	Access, Create, Write	CLEAN
ed13d8591854c31ef9c7f566b522b563892927ba6b4d81d831bd6b9246ff0442	C:\Users\RDhJ0CNFevzX\Music\F34KZnz.wav.pxj, c:\users\rdhj0cnfevzx\music\f34kznz.wav.pxj	Dropped File	81.91 KB	application/octet-stream	Access, Create, Write	CLEAN
13ec996e5bdd88cd105252e6f13a406faf754a7fa2d52e9c3763c3f388e0491d	c:\users\rdhj0cnfevzx\links\downloads.lnk.pxj, C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk.pxj	Dropped File	1.21 KB	application/octet-stream	Access, Create, Write	CLEAN
2a9124e850137a9f198ef7f1dfcdd766517d2996ae35cad006ce161c92c83646	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\outlookmui.msi.16.en-us.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\outlookmui.msi.16.en-us.tree.dat.pxj	Dropped File	74.98 KB	application/octet-stream	Access, Create, Write	CLEAN
06d568b87bc71ef24aceb78370ee4f27f17e38fbc4cd51138c9e8b25a5be083b	c:\program files\internet explorer\signup\install.ins.pxj, C:\Program Files\Internet Explorer\SIGNUP\install.ins.pxj	Dropped File	728 bytes	application/octet-stream	Access, Create, Write	CLEAN
7dd8dedc889275ec73f11c15a5f4f5a69ddbf45d45b8516d5fdd3854a53352cb	c:\program files (x86)\microsoft office\root\rsodwow6432\officemuiset.msi.16.en-us.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\officemuiset.msi.16.en-us.boot.tree.dat.pxj	Dropped File	2.51 KB	application/octet-stream	Access, Create, Write	CLEAN
7d1b5687c4508e5b92b5131c541f635db44dcc305da7351e1cbd2be6dfaf715a	C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVScripting.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\appvscripting.dll.pxj	Dropped File	500.48 KB	application/octet-stream	Access, Create, Write	CLEAN
340ca2ed55ccf4888ecc2ab80cf5834263c1aba1293f62611954760a4a81ab5d	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\office64mui.msi.16.en-us.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\office64mui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	6.95 KB	application/octet-stream	Access, Create, Write	CLEAN
8bfe61b33fd3fc54715c94e73f90d43fd5fa52043c98a8f5ff6790ba297dabfa	c:\programdata\usoshared\logs\updatesessionorchestration.009.etl.pxj, C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.009.etl.pxj	Dropped File	4.26 KB	application/octet-stream	Access, Create, Write	CLEAN
87ca215e5b70b15d480a4353d93380a18b11140a6c76df08a9bdf9c8ce652f7d	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00e2-0000-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml.pxj	Dropped File	3.93 KB	application/octet-stream	Access, Create, Write	CLEAN
424c776eea9e38fd4d6caa6051606cc9fe6c7272ef188b49acc12cb25278fc38	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-file-l1-2-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-core-file-l1-2-0.dll.pxj	Dropped File	18.45 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1b045f876842ed21a783387e98f7d513229ad5388539bb1948c446294d9795b8	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00ba-0000-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml.pxj	Dropped File	9.26 KB	application/octet-stream	Access, Create, Write	CLEAN
24da9e72bb85174c450534cfe28e57655c9002b5024b7a08acd4cc31d8a10cf4	c:\users\rdhj0cnfevzx\desktop\qr-r.mkv.pxj, C:\Users\RDhJ0CNFevzX\Desktop\Qr-r.mkv.pxj	Dropped File	48.54 KB	application/x-dosexec	Access, Create, Write	CLEAN
376229dd1054d0ec92fd125c0f3aed975e34ea9b82ce5023729321c545d2dddc	c:\users\rdhj0cnfevzx\videos\pklzhb14u2fpdy.mp4.pxj, C:\Users\RDhJ0CNFevzX\Videos\PklZHb14U2fpdy.mp4.pxj	Dropped File	15.20 KB	application/octet-stream	Access, Create, Write	CLEAN
939af0be23ede46bd02da70ad898de15473605ab4fbee14ee2067c2424f8f780	C:\ProgramData\Package Cache\{3c3aafc8-d898-43ec-998f-965ffdae065a}\vcredist_x64.exe.pxj, c:\programdata\package cache\{3c3aafc8-d898-43ec-998f-965ffdae065a}\vcredist_x64.exe.pxj	Dropped File	452.43 KB	application/octet-stream	Access, Create, Write	CLEAN
d90d631dc7366083afc14cf9cce702391b4d6bd9d7f5443c0278465b05652456	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0115-0409-0000-0000000ff1ce.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
950b9b259466d2af0a4d12f832ad199e8a531183d69fc270d4542b1686abacf7	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\lyncmui.msi.16.en-us.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\lyncmui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	8.90 KB	application/octet-stream	Access, Create, Write	CLEAN
16d63727793ef936755ab77beaf07331b8a0e4020c7e13f45faae29f2a569e93	c:\users\rdhj0cnfevzx\documents\h4zgddgxc.docx.pxj, C:\Users\RDhJ0CNFevzX\Documents\h4ZgddgxC.docx.pxj	Dropped File	31.15 KB	application/octet-stream	Access, Create, Write	CLEAN
5fee95d8cb77d1fadbf0b9294100e8418009455fc368f23cd74aab4e505a1823	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\powerpointmui.msi.16.en-us.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\powerpointmui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	14.68 KB	application/x-dosexec	Access, Create, Write	CLEAN
9beb3c4dc049b6ed870a863013a71ec56bab29f6461f3baf2c53cb6c592769b7	c:\users\rdhj0cnfevzx\desktop\3kw6phj1nu.mp4.pxj, C:\Users\RDhJ0CNFevzX\Desktop\3kW6pHj1NU.mp4.pxj	Dropped File	25.49 KB	application/octet-stream	Access, Create, Write	CLEAN
1a3af86e247fc4020caa9ed2aeeefd9f36eb8477499d18c04afb9aac1941674d	c:\programdata\usosharedlogs\updatessessionorchestration.003.etl.pxj, C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.003.etl.pxj	Dropped File	12.26 KB	application/octet-stream	Access, Create, Write	CLEAN
8cd9c44c35cd27b1e33496ea18ecd061fa3eed04efce58789f223062dbc76164	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001b-0000-0000-0000000ff1ce.xml.pxj	Dropped File	720.85 KB	application/octet-stream	Access, Create, Write	CLEAN
7647eb67a842883e92cf91611395d312011e055d4a41e6e4646e44ac6035688f	C:\Users\RDhJ0CNFevzX\Videos\WwNHxljnQ8Fh_KvDi.mp4.pxj, c:\users\rdhj0cnfevzx\videos\wwnhxljnq8fh_kvdi.mp4.pxj	Dropped File	85.73 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
989c17f4eaa5fdb3b02786372949b80483ac4f2ad6c9f3f7e6c897aee65d63da	c:\program files\common files\microsoft shared\clicktorun\appvisvsubsystems64.dll.pxj, C:\Program Files\Common Files\microsoft shared\ClickToRun\AppvIsvSubsystems64.dll.pxj	Dropped File	2232.43 KB	application/octet-stream	Access, Create, Write	CLEAN
e888279d08685b379ac2652222f8be552c5b3febb73d559acc2ff43f3d998d54	C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash.pxj, c:\program files\common files\microsoft shared\clicktorun\i640.hash.pxj	Dropped File	376 bytes	application/octet-stream	Access, Create, Write	CLEAN
c100b89298110b8d995d91ea2c8b5afac4a7a3f04a2bf90b6ff34d4d3f2495f0	c:\program files (x86)\microsoft office\root\rsodwow6432\excelmui.msi.16.en-us.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\excelmui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	19.66 KB	application/octet-stream	Access, Create, Write	CLEAN
e7a1ca814c5df138f5a0b5793f70bd2d568577880907896742fe719641645eec	c:\program files (x86)\microsoft office\root\rsodwow6432\outlook.x-none.msi.16.x-none.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Outlook.x-none.msi.16.x-none.tree.dat.pxj	Dropped File	581.90 KB	application/octet-stream	Access, Create, Write	CLEAN
1db85199132d60d9ea9e44794a123448c51f5f2f9fd223f631727846546fc5b3	C:\Users\RDhJ0CNFevzX\Music\56SXCIp.m4a.pxj, c:\users\rdhj0cnfevzx\music\56sxcip.m4a.pxj	Dropped File	7.10 KB	application/octet-stream	Access, Create, Write	CLEAN
4eba523461e0a72d8f96e71c8525b6af00db0334697ea81b26e36e5a308bf654	c:\program files (x86)\microsoft office\root\rsodwow6432\groove.x-none.msi.16.x-none.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Groove.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File	9.10 KB	application/octet-stream	Access, Create, Write	CLEAN
fd8da5a08158700f51bb2a538f6c7948123bd27fb4cffeb5a4b033e3be5a482b	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.common.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml.pxj	Dropped File	1951.24 KB	application/octet-stream	Access, Create, Write	CLEAN
d204ddc6fe352e2af5e948bdbf4a70d5379c29f41adfa8ff59fd31ba1a9f593e	c:\users\rdhj0cnfevzx\videos\8ooufkkqdq_ci1.flv.pxj, C:\Users\RDhJ0CNFevzX\Videos\8oOUFKKqDQ_ci1.flv.pxj	Dropped File	5.82 KB	application/octet-stream	Access, Create, Write	CLEAN
132feb293339ff720f798eed4d8cd2ec84bb80fc793ec607f4b32aa47e4a33bd	c:\users\rdhj0cnfevzx\documents\3oc5blwnmi_d.pptx.pxj, C:\Users\RDhJ0CNFevzX\Documents\3oC5blwNMI_D.pptx.pxj	Dropped File	95.32 KB	application/octet-stream	Access, Create, Write	CLEAN
ad87fac02da39735cee230bea47fa18015f2affdff2278c484fb30ea897e775d	C:\Users\RDhJ0CNFevzX\Desktop\ajdQmxaQYMm_L.bmp.pxj, c:\users\rdhj0cnfevzx\desktop\ajdqmxaqymm_l.bmp.pxj	Dropped File	22.60 KB	application/octet-stream	Access, Create, Write	CLEAN
a615a0735e6ad5b44c3deb2826cbe7c67fc8f2dc7a762474a7ce934b3a59c1c3	c:\users\rdhj0cnfevzx\documents\onljyqjpwbk.xlsx.pxj, C:\Users\RDhJ0CNFevzX\Documents\onlJyQJpwBK.xlsx.pxj	Dropped File	67.34 KB	application/octet-stream	Access, Create, Write	CLEAN
7ec90bc32c3e61338de65fcf1997f6f841193b0503d9e190950368159528dbb9	C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Office 16 Click-to-Run Licensing Component.swidtag.pxj, c:\programdata\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft office 16 click-to-run licensing component.swidtag.pxj	Dropped File	1.30 KB	application/octet-stream	Access, Create, Write	CLEAN
ee645cd56f0d4a81bcea2268396e47e2b8f94d4cbea230ed55b3db9096b2f44a	c:\program files (x86)\microsoft office\root\rsodwow6432\access.x-none.msi.16.x-none.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Access.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File	48.12 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
33f6c61bf539b270ef9d1e36aeeebf1ef6514222268bfe5017e69b536d87cc77	c:\program files (x86)\microsoft office\root\rsodwow6432\dcf.x-none.msi.16.x-none.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\DCF.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File	9.12 KB	application/octet-stream	Access, Create, Write	CLEAN
c68d3554c6a569b23067ed2b4300e2317aaa4d512133495cb6b069521f1f17a7	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\placeholder.txt.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\placeholder.txt.pxj	Dropped File	632 bytes	application/octet-stream	Access, Create, Write	CLEAN
3ec6137267020f5438f6e4ba6e2b354830fe596282e42e37830a5e5ecf69d0b4	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0015-0000-0000-0000000ff1ce.xml.pxj	Dropped File	314.84 KB	application/octet-stream	Access, Create, Write	CLEAN
abf1e6b926cd33f030664b3b95f4e878c3d7b3aaf6930205204633f6d26eba52	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-002a-0409-1000-0000000ff1ce.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
675b2c9285b7fad14aae359785632460cb863d728bc0120a9120515033ef379a	c:\users\rdhj0cnfevzx\music\zfxe-iab.wav.pxj, C:\Users\RDhJ0CNFevzX\Music\zFxE-IAB.wav.pxj	Dropped File	79.70 KB	application/octet-stream	Access, Create, Write	CLEAN
c0d1531a803d382d0dc017f596cb71bb90f8b83ed93ff11d79e6e68e6829152f	c:\program files (x86)\microsoft office\root\rsodwow6432\powerpivot.x-none.msi.16.x-none.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\PowerPivot.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File	446.79 KB	application/octet-stream	Access, Create, Write	CLEAN
4710b81c12383406581a876c6b90e9e84e23211b01830c2e29e5cc11f0fe7b3a	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\powerpointmui.msi.16.en-us.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\powerpointmui.msi.16.en-us.tree.dat.pxj	Dropped File	18.90 KB	application/octet-stream	Access, Create, Write	CLEAN
be6d7edf554a98fe7dd6c97ff581b509c882f2fef71a8d8d1c78c7a8778b44f2	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-locale-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-locale-l1-1-0.dll.pxj	Dropped File	18.95 KB	application/octet-stream	Access, Create, Write	CLEAN
8ffe3ea923d1d64311a06f91ad6cd38e83c3c8b1d25859fc073d0fc44a9d7798	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\officemui.msi.16.en-us.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\officemui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	62.91 KB	application/octet-stream	Access, Create, Write	CLEAN
2b85980d4cf404e9ef4ef217d3a5fc994af9c8d04c26c5999aa5e51bc2001ff3	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-002a-0000-1000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml.pxj	Dropped File	34.15 KB	application/octet-stream	Access, Create, Write	CLEAN
199b30a2b560fc84b1ff3bfde95136fdc2f3ab0c785617ac120c5632ccd20474	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-runtime-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-runtime-l1-1-0.dll.pxj	Dropped File	22.95 KB	application/octet-stream	Access, Create, Write	CLEAN
cf3c75cca5f31ca0749c080910563c3f3ed124649868a7800951b2f3fdb103a5	C:\Program Files\Common Files\microsoft shared\ClickToRun\ucrtbase.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\ucrtbase.dll.pxj	Dropped File	959.95 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9080e6e868550de905a0de13d90bcf3654d1d80bcf7b0f060a60f0b22b120df4	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\dcfmui.msi.16.en-us.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\dcfmui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	5.77 KB	application/octet-stream	Access, Create, Write	CLEAN
71cb187c2b1f53cef3a666d197817696467bc6de05b12ebaa7f25fd2c24da4e9	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmuxmui.msi.16.en-us.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\osmuxmui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	6.34 KB	application/octet-stream	Access, Create, Write	CLEAN
3b6e2f058e8202e1bbb16677de28ce946f0a8b62843a9d178910d50f8dd836ca	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-006e-0409-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml.pxj	Dropped File	14.48 KB	application/octet-stream	Access, Create, Write	CLEAN
ba8453f8443681bbc6faad001a840f11562ac9805663ca9565bfed76fc835524	c:\program files\microsoft office 15\clientx64\officeclicktorun.exe.pxj, C:\Program Files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe.pxj	Dropped File	1067.88 KB	application/octet-stream	Access, Create, Write	CLEAN
7f9fbbc2471efcc427d771e1e0e9d5dd5b28c99380d2a923cc29eb3bc4bdbf63	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-3101-0000-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml.pxj	Dropped File	3.55 KB	application/octet-stream	Access, Create, Write	CLEAN
0140b489f769d0e2cfd4931bb4b33115d4d8f997038f45114875f16978704a79	c:\program files (x86)\microsoft office\root\rsodwow6432\onenotemui.msi.16.en-us.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\onenotemui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	10.79 KB	application/octet-stream	Access, Create, Write	CLEAN
b9feaa41497f2051f45702fdf7e96ee93d6bc975dfa91ae6df3d602108ee918f	c:\programdata\package cache\{65e650ff-30be-469d-b63a-418d71ea1765}\vc_redist.x86.exe.pxj, C:\ProgramData\Package Cache\{65e650ff-30be-469d-b63a-418d71ea1765}\VC_redist.x86.exe.pxj	Dropped File	632.99 KB	application/octet-stream	Access, Create, Write	CLEAN
56250aacb9fdd8560cf8e6dbf1c04c3cfc89036dac1ade7992710557d1775520	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Proof.fr-fr.msi.16.fr-fr.boot.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\proof.fr-fr.msi.16.fr-fr.boot.tree.dat.pxj	Dropped File	15.96 KB	application/octet-stream	Access, Create, Write	CLEAN
0ff7eecd8dc0f928119fc76e35e4425cd3c044bd4a270ce71e753df3b4f9af8f	c:\programdata\usoshared\logs\updatessessionorchestration.010.etl.pxj, C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.010.etl.pxj	Dropped File	4.26 KB	application/octet-stream	Access, Create, Write	CLEAN
11c908f07fe393884b23f127c6a9ebba096c38b0f549ec0e4d64a717701fb1ea	c:\program files\common files\gwfgft_br_n0vy16u6.gif.pxj, C:\Program Files\Common Files\gWFgft_br_n0vY16u6.gif.pxj	Dropped File	36.57 KB	application/octet-stream	Access, Create, Write	CLEAN
5646eb6e25cc061095624d927e9a951e2b3a233b09599e36fc496bae6ceb2cf2	C:\Users\RDhJ0CNFevzX\Pictures\VZ7J2h1NNIuHd_.png.pxj, c:\users\rdhj0cnfevzx\pictures\vz7j2h1nniuhd_.png.pxj	Dropped File	72.90 KB	application/octet-stream	Access, Create, Write	CLEAN
a0a24ab1b6355ae55766d3d4a5485ac7e4273d78c86be1edd0d09c681aa14e32	C:\Users\RDhJ0CNFevzX\Documents\koDg-zIFa XRKP63Q3p2.xlsx.pxj, c:\users\rdhj0cnfevzx\documents\kodg-zifa xrkp63q3p2.xlsx.pxj	Dropped File	38.49 KB	application/octet-stream	Access, Create, Write	CLEAN
13f8c9afa23b28d465183f9d5116860d0fe6822b4ae1ae52949d3219a5ab86ef	C:\Users\RDhJ0CNFevzX\Desktop\3FSu0.gif.pxj, c:\users\rdhj0cnfevzx\desktop\3fsu0.gif.pxj	Dropped File	40.52 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
db4221beb611a56879385bb3d33e2c69892a0f2618b5f115b6115366c5135556	c:\program files (x86)\microsoft office\root\rsodwow6432\proof.es-es.msi.16.es-es.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\Proof.es-es.msi.16.es-es.boot.tree.dat.pxj	Dropped File	15.96 KB	application/octet-stream	Access, Create, Write	CLEAN
892d7fa18b8dd600e365c25f94cceb8d96372e5974b658a8cd6a2511c0cec390	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-time-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-time-l1-1-0.dll.pxj	Dropped File	20.95 KB	application/octet-stream	Access, Create, Write	CLEAN
bdcd1ba759384358ed4a4173fff530261e915dc7d966b91ae995545f67f23b8c	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-processthreads-l1-1-1.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-core-processthreads-l1-1-1.dll.pxj	Dropped File	18.95 KB	application/octet-stream	Access, Create, Write	CLEAN
96e66866caf8ebee1d155ac4e272c6c2e4667f5c2637f85869e794e26ed6374a	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-00a1-0409-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
58ca5d3a02e38c9a2d434e1f8c0d65aac8142d562fec8e3590cc778489b86995	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-001f-0409-0000-0000000ff1ce.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN
bad278ed356e2d88787226180c1d1f122e2ac55edda4719a3a5c7927c4a0309a	c:\program files (x86)\microsoft office\root\rsodwow6432\accessmuiset.msi.16.en-us.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\accessmuiset.msi.16.en-us.boot.tree.dat.pxj	Dropped File	2.51 KB	application/octet-stream	Access, Create, Write	CLEAN
f3566531825301d6c24ed72cd9c898660c5bd074dd687d25b3a771848defc7d1	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-synch-l1-2-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-core-synch-l1-2-0.dll.pxj	Dropped File	18.95 KB	application/octet-stream	Access, Create, Write	CLEAN
b1e9d20aaa2b3a110d9f30364c554a98ae6d38fb6ba2d9828ddb528fdc657874	C:\ProgramData\Package Cache\{3c3aafc8-d898-43ec-998f-965ffdae065a}\state.rsm.pxj, c:\programdata\package cache\{3c3aafc8-d898-43ec-998f-965ffdae065a}\state.rsm.pxj	Dropped File	904 bytes	application/octet-stream	Access, Create, Write	CLEAN
1369e1e14566dd4d136046a56783438bf74624edac77d8122436f544648c5395	c:\programdata\package cache\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\state.rsm.pxj, C:\ProgramData\Package Cache\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\state.rsm.pxj	Dropped File	904 bytes	application/octet-stream	Access, Create, Write	CLEAN
5ddfe4551b3dd12511f0b128a750d5ca2f4fc855f5e015eaf08285690fa6d752	C:\Users\RDhJ0CNFevzX\Documents\W9Zb9GI99.odt.pxj, c:\users\rdhj0cnfevzx\documents\w9zb9gi99.odt.pxj	Dropped File	42.51 KB	application/octet-stream	Access, Create, Write	CLEAN
48a5ba1bcb2c6fd1db2b67b481bf3ac74b4092741db200b53c2ef82760230151	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-012b-0409-0000-0000000ff1ce.xml.pxj	Dropped File	1.49 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
431f7355add6d58b7c095c45604a47c9fea31bcee597187be5e399702bbc80ae	c:\program files (x86)\microsoft office\root\rsodwow6432\osmmui.msi.16.en-us.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmmui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	2.80 KB	application/octet-stream	Access, Create, Write	CLEAN
b3b7ed8db4bf66c6325283d1d977144e9408b2aeba569a32294307f8ca9ec982	C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.004.etl.pxj, c:\programdata\usoshared\logs\updatessionorchestration.004.etl.pxj	Dropped File	12.26 KB	application/octet-stream	Access, Create, Write	CLEAN
55980d372e528b484e05fcd2c6e701406986617b070ad9348dec565cbd76c6ac	C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmmui.msi.16.en-us.tree.dat.pxj, c:\program files (x86)\microsoft office\root\rsodwow6432\osmmui.msi.16.en-us.tree.dat.pxj	Dropped File	5.18 KB	application/octet-stream	Access, Create, Write	CLEAN
19ec4b95c9da7733ef33d8fe81776cf1ad2a80107747fede26a73afa8ce6c269	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0018-0000-0000-0000000ff1ce.xml.pxj	Dropped File	453.37 KB	application/octet-stream	Access, Create, Write	CLEAN
8e12e6d2aac6c12f8b7c067053aa7e5d29afa8ece0e3b7c5821131f2f503889b	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml.pxj, c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-0016-0000-0000-0000000ff1ce.xml.pxj	Dropped File	758.16 KB	application/octet-stream	Access, Create, Write	CLEAN
9bb622c0e0221da3e715c4d6355a1cbe43e46d652b83b378dc9c9724f1f28712	c:\program files (x86)\microsoft office\packagemanifests\appxmanifestloc.en-us.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml.pxj	Dropped File	9.87 KB	application/octet-stream	Access, Create, Write	CLEAN
cfee2d4b810a7f904d6bbba64ac53bf69228259f514131532e40f7566d48ca98	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-string-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-string-l1-1-0.dll.pxj	Dropped File	24.45 KB	application/octet-stream	Access, Create, Write	CLEAN
70fb52ba3ddefc1cdd7a801fe07bdc0cad37d1aa104217ccd3f3f23592a3f49e	c:\program files (x86)\microsoft office\root\rsodwow6432\groovemui.msi.16.en-us.boot.tree.dat.pxj, C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\groovemui.msi.16.en-us.boot.tree.dat.pxj	Dropped File	3.85 KB	application/octet-stream	Access, Create, Write	CLEAN
5f68f3b005a32816ceb5dfbebd4d5fc19b4e6a2a65450a047492d25ee3c17801	c:\program files (x86)\microsoft office\office16\slerror.xml.pxj, C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML.pxj	Dropped File	35.74 KB	application/octet-stream	Access, Create, Write	CLEAN
02f63fc1bfefd2d98c19965c75dac70bf271ecff37731aa5c79bd5c2257e2138	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-environment-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-environment-l1-1-0.dll.pxj	Dropped File	18.95 KB	application/octet-stream	Access, Create, Write	CLEAN
83af66bc316c7daae3cb3045d2f8e27e03c28fb3a09021f315fe5cdae43e61d9	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-crt-conio-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-conio-l1-1-0.dll.pxj	Dropped File	19.45 KB	application/octet-stream	Access, Create, Write	CLEAN
b4febd50db795e01fb82f217d08afe0357bb717a9356c285b640ac429034a7da	c:\programdata\usoshared\logs\updatessionorchestration.005.etl.pxj, C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.005.etl.pxj	Dropped File	12.26 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
714822afe82b60f56783c0a95ba4d809377ecadeb2ec97eda44814fdaafe3fad	c:\users\rdhj0cnfevzx\desktop\10gs1e2cow2stsot.mp3.pxj, C:\Users\RDhJ0CNFevzX\Desktop\10gs1e2CoW2STsot.mp3.pxj	Dropped File	95.29 KB	application/octet-stream	Access, Create, Write	CLEAN
9a653932ef0c54276ea15e75709b1509321186a269ce40d43474ad2365cdb4c9	c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.90160000-012a-0000-0000-0000000ff1ce.xml.pxj, C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml.pxj	Dropped File	516.54 KB	application/octet-stream	Access, Create, Write	CLEAN
dba6b592d01e4762659afdb908011e6b808b4f685eb1a32ae70622d577bf8681	C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-timezone-l1-1-0.dll.pxj, c:\program files\common files\microsoft shared\clicktorun\api-ms-win-core-timezone-l1-1-0.dll.pxj	Dropped File	18.45 KB	application/octet-stream	Access, Create, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
c:\program files (x86)\microsoft office\root\clipart\pub60cor\dd01181_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\zpxp0xgs9ush4tgnr.mp4.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\j0105306.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\FIRSTRUN.EXE.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\mondor_subscription2-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\accessr_grace-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\rsod\access.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\o365smallbuspremr_subtrial4-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\rx wjjwoaxmfhzluz0.jpg.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\accessr_retail-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\O365ProPlusR_SubTrial1-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0148798.JPG.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8JonlJBbUS5BP.gif.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\proplusr_oem_perp5-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\Dur-J3pX lal45sj1RDj.mp3.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\accessvl_kms_client-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\o365homepremr_grace-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0107154.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\office16\mscss7fr.dll.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\PTXT9.DLL.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files (x86)\microsoft office\root\licenses16\o365homepremr_grace-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\o365proplusdemor_bypasstrial180-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\OneNoteR_OEM_Perp-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\integration\c2rmanifest.officemuiset.msi.16.en-us.xml.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\ProjectProR_OEM_Perp-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\office16\offrhd.dll.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\OSM.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\temp\e9tm.mkv.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\VisioProO365R_SubTrial-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Flattener\api-ms-win-crt-math-l1-1-0.dll.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\office16\msohtmed.exe.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\bp8bq8gw\r-kpysyyvwtn.wav.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\O365HomePremR_SubTrial3-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\O365HomePremR_Subscription1-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\ExcelR_Grace-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\VisioProCO365R_Subscription-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\hh02312_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Integration\C2RManifest.wordmui.msi.16.en-us.xml.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00096_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01657_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\ProjectProR_OEM_Perp-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\Microsoft.Lync.Utilities.Controls.zip.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\VisioProR_Trial-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0151047.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\bs00440_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\OneNoteVL_MAK-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\pklzhb14u2fpdy.mp4.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0174639.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\StandardR_Retail-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\hh01065_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\ag00057_.gif.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\ProjectProCO365R_SubTrial-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\fd00586_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\integration\c2rmanifest.shared.office.x-none.msi.16.x-none.xml.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\integration\windows8.1-kb2999226-x64.msu.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01545_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\programdata\usoshared\logs\updatesessionorchestration.009.etl.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\rsodwow6432\publishermui.msi.16.en-us.tree.dat.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\URLREDIR.DLL.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\IIJtewH3wwKtNi57gKeC\Oq138uzGGN8c_UVv6n.mp4.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Flattener\api-ms-win-crt-convert-l1-1-0.dll.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\zPAIqxRnRXWryau.jpg.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\bp8bq8gw\ikox4nrclc11j.jpg.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\O365ProPlusR_Subscription1-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\proplusr_oem_perp5-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01366_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\o365homepremr_subscription4-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\hh00231_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\MondoR_Retail-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\3kw 6phj1nu.mp4.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\fd02097_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0099188.JPG.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files (x86)\microsoft office\root\licenses16\visioprovl_mak-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\skypeforbusinessr_trial-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\mset7tkjp.dll.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\wordvl_kms_client-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\j0107742.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files\Common Files\microsoft shared\ClickToRun\api-ms-win-core-timezone-l1-1-0.dll.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\office16\rtmmvrhw.dll.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\O365SmallBusPremR_SubTrial4-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01160_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\in00557_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01157_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\j0152890.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\visiostdr_oem_perp-ul-phn.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\o365businessr_subscription-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\j0152622.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\clicktorun\api-ms-win-crt-utility-l1-1-0.dll.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\BD00146_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\j0152556.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\programdata\package cache\{a749d8e6-b613-3be3-8f5f-045c84eba29b} v12.0.21005\packages\vcruntimeminimum_amd64\cab1.cab.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0151067.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0152704.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\bl00265_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\o365smallbuspremr_subscription4-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\ONLNTCOMLIB.DLL.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Oajh.png.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\rsod\officemuiset.msi.16.en-us.tree.dat.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\mondor_subtrial2-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0177806.JPG.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files (x86)\microsoft office\root\flattener\appvmanifest.dll.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\rsodWoW6432\osmmui.msi.16.en-us.tree.dat.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\o365smallbuspremdemor_bypasstrial180-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\MondoR_OEM_Perp-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\ProgramData\Package Cache\{3c3aafc8-d898-43ec-998f-965ffdae065a}\state.rsm.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\j0145361.jpg.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\ed00184_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\qtrnijjfd.avi.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\4rnoj.docx.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\flattener\microsoft.tools.office.c2r.packager.dll.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\EMSMDB32.DLL.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\HH00681_.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\HomeBusinessR_Retail-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\office16\onres.dll.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\visiostdr_oem_perp-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\ProfessionalPipcR_OEM_Perp-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\projectprovl_kms_client-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\fd00459_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\j0153305.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\excelr_trial-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\rsod\word.x-none.msi.16.x-none.boot.tree.dat.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\J0171847.WMF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\onenotevl_kms_client-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\HomeBusinessPipcR_Grace-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\office16\groove.exe.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\MondoVL_MAK-ul-oob.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files (x86)\microsoft office\packagemanifests\appxmanifest.common.xml.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\MYx5l61W_4ZPF.mp4.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\o4gu.pptx.pxj	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\VisioProR_OEM_Perp-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\MSPPT.OLB.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\flattener\msvcp140.dll.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\ProPlusR_OEM_Perp-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\flattener\appvstreammap.dll.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\clipart\pub60cor\an00932_.wmf.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\wordEtw.man.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\root\licenses16\mondor_oem_perp-pl.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Integration\C2RManifest.Outlook.Outlook.x-none.msi.16.x-none.xml.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.VisualElementsManifest.xml.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Licenses16\OneNoteR_Grace-ppd.xrm-ms.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\Office16\SEQCHK10.DLL.pxj	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF.pxj	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

Reduced dataset

Mutex

Name	Operations	Parent Process Name	Verdict
XVFXGW DOUBLE SET	access	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe	CLEAN

Process

Process Name	Commandline	Verdict
9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1.exe"	MALICIOUS
vssadmin.exe	vssadmin.exe delete shadows /all /quiet	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.5.0
Dynamic Engine Version	4.5.0 / 04/22/2022 19:04
Static Engine Version	4.5.0.0 / 2022-04-22 17:45:13
AV Exceptions Version	4.5.0.2 / 2022-04-03 15:57:54
Link Detonation Heuristics Version	4.5.0.19 / 2022-04-20 05:46:11
Smart Memory Dumping Rules Version	4.5.0.2 / 2022-04-03 15:57:54
Config Extractors Version	4.5.0.14 / 2022-04-07 17:00:08
Signature Trust Store Version	4.5.0.2 / 2022-04-03 15:57:54
VMRay Threat Identifiers Version	4.5.0.24 / 2022-04-26 09:10:00
YARA Built-in Ruleset Version	4.5.0.2

Software Information

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

System Information

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

System Root	C:\Windows