MALICIOUS

Classifications: Injector | Spyware | Ransomware

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe**
ID	#4174583
MD5	2f21af3173d0ee0960961105945f4fe6
SHA1	6bff623bb8b365575971c7051cca859953a90f7d
SHA256	a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844
File Size	96.00 KB
Report Created	2022-04-23 08:16 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 89 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #2) cvtres.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 1069 files by appending the extension ".ozq0".			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: git, Internet Explorer / Edge, Windows Mail.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe modifies memory of (process #2) cvtres.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe alters context of (process #2) cvtres.exe.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #2) cvtres.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #2) cvtres.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) cvtres.exe tries to read sensitive data of mail application "Windows Mail" by file.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe starts (process #2) cvtres.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe reads from (process #2) cvtres.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Hide Tracks	Changes folder appearance	74	-

• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\ringtones".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\accessibility".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\system tools".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\tablet pc".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\windows powershell".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\administrative tools".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\games".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\maintenance".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\startup".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\1nbur4hr".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\6asvn7j7".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\d68g7bij".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\kqmhsvkd".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\burn\burn".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\history".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\history\history.ie5".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\temporary internet files\content.ie5".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\temporary internet files\content.ie5\mm5o9xqs".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\temporary internet files\content.ie5\pmmr5k9k".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\temporary internet files\content.ie5\rijuql1c".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\temporary internet files".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows mail\stationery".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\libraries".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\recent".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\sendto".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessories\accessibility".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessories".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessories\system tools".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\administrative tools".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\maintenance".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\startup".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\contacts".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\desktop".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\documents".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\downloads".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\favorites".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\favorites\links".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\links".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\music".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\pictures".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\saved games".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\searches".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\default\videos".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\feeds cache\1nbur4hr".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\feeds cache\6asvn7j7".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\feeds cache\d68g7bij".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\feeds cache".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\feeds cache\kqmhsvkd".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\windows\burn\burn".
• (Process #2) cvtres.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\windows\burn\burn1".

Score	Category	Operation	Count	Classification
1/5	Persistence	Installs system startup script or application	2	-
	• (Process #2) cvtres.exe adds "c:\users\all users\microsoft\windows\start menu\programs\startup\desktop.ini.ozq0" to Windows startup folder. • (Process #2) cvtres.exe adds "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\startup\desktop.ini.ozq0" to Windows startup folder.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) cvtres.exe resolves 168 API functions by name.			

Mitre ATT&CK Matrix

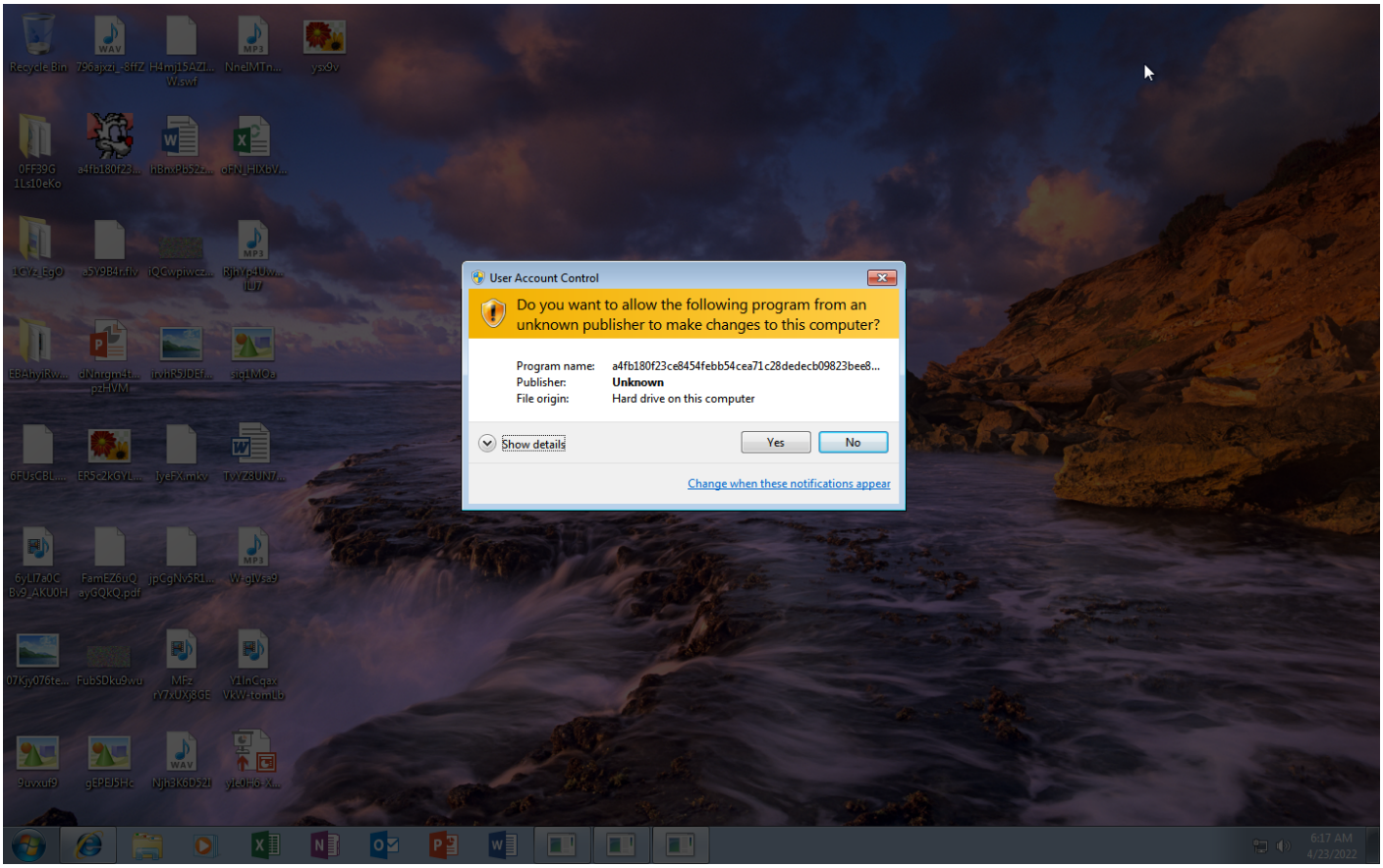
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
				#T1045 Software Packing				#T1005 Data from Local System			
				#T1036 Masquerading							

Sample Information

ID	#4174583
MD5	2f21af3173d0ee0960961105945f4fe6
SHA1	6bff623bb8b365575971c7051cca859953a90f7d
SHA256	a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844
SSDeep	1536:c/mzjPBTMLJqiUdE2tjyTyyyyyyF8ylyyRGYyyyyyyyyyyyyyyyyyyDmX99dHdnt:c/mzNsJqVC/9xllKwZPyitBmc1yY
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe
File Size	96.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-04-23 08:16 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: a4fb180f23ce8454febb54cea71c28dedecb09823bee8...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Small Spend Similar

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

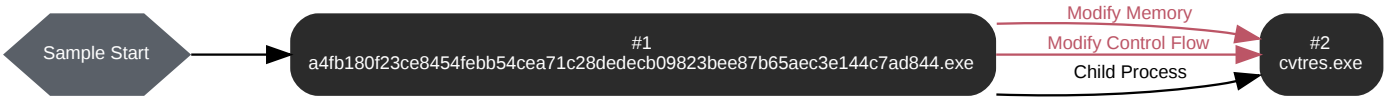
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 51498, Reason: Analysis Target
Unmonitor End Time	End Time: 75720, Reason: Terminated
Monitor duration	24.22s
Return Code	0
PID	3756
Parent PID	1928
Bitness	32 Bit

Host Behavior

Type	Count
Module	32
System	5
File	2
Process	1
-	3
-	7

Process #2: cvtres.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v2.0.50727\cvtres.exe
Command Line	C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 72492, Reason: Child Process
Unmonitor End Time	End Time: 291643, Reason: Terminated by Timeout
Monitor duration	219.15s
Return Code	Unknown
PID	3812
Parent PID	3756
Bitness	32 Bit

Injection Information (5)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe	0xeb0	0x400000(4194304)	0x1000	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe	0xeb0	0x417000(4288512)	0x9a00	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe	0xeb0	0x421000(4329472)	0xe00	✓	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe	0xeb0	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe	0xeb0 / 0xee8		-	✓	1

Dropped Files (317)

File Name	File Size	SHA256	YARA Match
-	11.80 KB	6cae2b44e0989d2f7e3940b9a0457c77169f9064278295aa708d6c982dabeb3f	✗
-	217.50 KB	7141a8d8fb880c016d57c17090a44c857e6d08e91b6a38567e5922c004a4044a	✗
-	201.48 KB	6b88ea27eb17038324ad1d53fb3d0a71b3ddc68fbca35f38fd6e648ccf876f84	✗
-	487.78 KB	293e92af0dff9a0631ccd41817d889914efbfe5bfa5e5b320b81b032a367a0ee	✗
-	14.33 KB	09dcf799070cbd0ccb313434a333eef2de056e3b6bd541723757aa3e91120520	✗
-	16 bytes	3ffdc4c0b99ccf12ff72193fd88703e0856072ad52d09ee60e3effec38b6688e	✗
-	852.78 KB	9d7471c2960c549f7ad820b0006be7e33a3dbb4da4973bfbb3256dfb6ebc91a5	✗
-	1.94 KB	df6ee410303ad933f72d1e98326c576569933d7dbc555f7fe2741f46ded37ddb	✗

File Name	File Size	SHA256	YARA Match
-	1.36 KB	aa171428e2a5325202f4b628897899c59418ce836872ce7d080dddde661e1e5e	✗
-	21.86 KB	a75c582379eb42d569e03ffcc586f076b250ec43814706687432d1ff79992d76	✗
-	112 bytes	88d62a1aed83e66d120f06e48655406f64c12285f7e89eb85a02def3342de90b	✗
-	864.47 KB	044acffabb306f067df0f179c317e7b9913addec287c28f6096cee387bb2edb3	✗
-	20.55 KB	7ec9782c87a8232cf63be95efc7f2bf2eee0f16d7d4834c83bbaec8d1b578cfd	✗
-	112 bytes	4df5b2dbd6a73550e4718efe2816399b2cb2f806170f4b051d68f003e580b774	✗
-	3629.45 KB	48a53b233669ac34e2597dd71e48c9b08c331e1eaa2ec4c8549a6e47b714faae	✗
-	624 bytes	603023e96ef388e08fa0ab4500d44943588c7372c8f2843d46b396a21f930927	✗
-	4818.02 KB	617d8586da7ce0b4eae04b237c0bf1dd2fd3152cc938c1539716cf2df31b4cc2	✗
-	624 bytes	c636270ba1beb3e4daca80490a4c4112725803aa4f011ed796b56fb75ca55b72	✗
-	3024.27 KB	2624b77220c433f253d2af304c796d5746ba08233046db510f03315b62c0aa9d	✗
-	275.55 KB	e37ba368cbb3f245d44cee6a202b2b1ea4a0f5b82b2d159a9535e9eeb191393e	✗
-	37.89 KB	c1a76009f89b41682c7f813de9f9158ed59ba895544c6edf6be4f3c0b7e53295	✗
-	56.08 KB	8944c4bff7a505e74fb3cab0beafe29f893447cd05a940470e8893e3a39ac63b	✗
-	2.00 KB	d5b2df956c860a4902213cc0a33bac44f5a7d32349ea95ada1fa0d8923a57e9d	✗
-	16.27 KB	d9d72a09268da08e44753e2ebfce36082703d49a50ad5c56fa6139e4ea49b193	✗
-	9.59 KB	b28c62b78259a9e78046ed89f8acbf9ba6cd701d4abd905fc5aae8809c9f76fd	✗
-	232.31 KB	6bd2b71adbc24376fb4324c0913f4d4822fa5bbb43c88762debb6f96fdebe9bc	✗
-	34.22 KB	8b7c57a633aea70b1a0701ddbccf8ccba03bd4eee0de53d912eddc177cd61c02	✗
-	35.77 KB	4ee35a080aab7ebf7a123bad465e104ca1a4b382f0a650d6a4c538c6d162231f	✗
-	6.00 KB	424ac0049e097d68d5e67adcb3164bdb86ba42aba25822bee723aff63fb4ef0d	✗
-	87.47 KB	fd2aea4496294dc13f517ab95ccc9e89a9fd822decfdc60ca43f1c1d5ad54b66	✗
-	22.80 KB	61691df5d44c7ff93c60c9dfc2c2ebc066359b380638923eb0d4415ba8db6762	✗
-	21.45 KB	f46d6e450ea7beb450fc9cb08937adbc0aca794880e7a771c01b68131ffc60bb	✗
-	2.00 KB	706ceac0577142972363fb7a5ebf743b39ada60a0f628e6069f7763f9b49fe5a	✗
-	261.20 KB	505502a51e4ed19e24fdc3301b775893042cd17e7c4ff0ac4a18654ea9ab2906	✗
-	104.39 KB	dc77fb2c961f46edfb516b79fd95376c98227ee70a349a2391c0494cfe6f40db	✗
-	2.00 KB	b57116266284167fd48f49a4701c75d358a043a54c8894b6f75076f1d2b2a1db	✗
-	93.70 KB	59c942f196e76d3ddbb300a0ff0c31fba1f027824e73860911959536414c52cd	✗

File Name	File Size	SHA256	YARA Match
-	18.53 KB	b5ba8ea7b1075518852b0995f903449fee50344783aabe3b026c15b5d54a366c	✗
-	1.48 KB	ebb264329890c98b56a897663035df279e54cbfb7cf20bf3f0217ccfc0a48db3	✗
-	10.78 KB	2996680e1ff41ebdf5cd1bc102e6ddcf4a0f0206adafbc05793e6daf55ba8701	✗
-	2.25 KB	014d455bd04184d2502e611552e3acd3907b10cdef40c90b9cba8ac71e468fde	✗
-	9.66 KB	62004ca4fc442607e1f025590a4db0f03428e82e5f3569c9c8fbec8c36d02bcc	✗
-	91.16 KB	ee6f069e347bb9ae20b1a0d40ff4c355ac7591630b74695c35b27f948211bb3e	✗
-	94.20 KB	cecac506cb90d016efe05315a0877a27aa4cf0912372ffc58a562cced015a3d1	✗
-	695.23 KB	9f1ce0fafada2644732222de661b60299231c1558a62ae5643a8db37e396a6f2	✗
-	100.38 KB	4812935755458906d8e530b7e312f3a91519e1961b326c8c76a4fc286af5b6b7	✗
-	26.08 KB	609882fcf42b12e2925556153b8be1a15c93c0998acd4e12b85903f7ec24d78c	✗
-	24.86 KB	900ac6108a121c5ff2dc90298dea2ac41fba95804397daedb4836c01a96f42b5	✗
-	23.92 KB	2b8677b7f91cc9665c4e63f76fd4a75d42a743823850cbb0cd1f8bdb518a90bc	✗
-	23.92 KB	5484b8d47ff3aa1c7a5fb925e0422730e6a3fc9e68eb2f021bf58838b9b91416	✗
-	2.00 KB	05d82c99b68b0ddc8f6ce90ea2e2fbfd47e409e50580dcf80dbeb4c51cac434b	✗
-	75.36 KB	75ac382f8b4e1529aec890388f20292b37b37eeac0e17fbaaacb9ba848cd4dc9	✗
-	13.77 KB	6b384cdec581d1a4653d415125443fb87814f689191bdf4dc37e0979b46f1b3f	✗
-	683.06 KB	5cb7f7e100c1b8c2a8a3c99ac5d6441f4ecacdab8d2b2ed2a4a25818c3653efc	✗
-	84.64 KB	72da6629f6372f61918cdee778f880b50b0de614037fabca0210775e3c01afbf	✗
-	76.03 KB	69e4de5622c0a1fd650a2a83cd37aa0febc584343445fe4c704a892d262d7713	✗
-	839.62 KB	abcc28bfd03feb486a57586360740d60b029b11f4f2ea92a202ab4ad19761293	✗
-	3.25 KB	8ec22653478fcaf3d928787e020fdea506f35f497095786a054ea09b3e7ea4ae	✗
-	3.19 KB	f92fa60cde90c5ffd6a338f440c2a765a878e946f3dccb3b0f3444bebc49be1b	✗
-	110.05 KB	7d14873baec24b48135e47680c9f80b3de342f727103a3052636a7bf075f2502	✗
-	623.47 KB	0a688b5d036cf005b29e4ac848f577863a33b8cbadf8e1b82e2cd0011707552b	✗
-	126.72 KB	c52b8f6df91f544340e00103234f916c6a6669a64946d64909ea5840b468ab9b	✗
-	2.86 KB	c4ae6edeea3aedf32f4cbbb14bbbe96f53ee8e12af7ca39143a7e7db744c5ae8	✗
-	43.45 KB	a88d9f0e7e63391c8b0c12149b489bf185d65127d065184d004d771840fbb1d7	✗
-	28.20 KB	e2532114a369dd2a3b72300bfdbdbd19ba5697433193d593e829d30a75f54976	✗
-	38.47 KB	62366db0453624a083a8feecfac77936d8980d36b50425e9bcbcf4d84347298b	✗

File Name	File Size	SHA256	YARA Match
-	126.72 KB	d434a0e7647c2f15d822670af98d62eefe5d6b88bfc18eb89d275028746e3450	✗
-	1.86 KB	7c809e2b75e2f0858f7dff54434b5b87909ace3f9120551f2983671877f1dad0	✗
-	28.20 KB	78a858dacae6b6d2e4654d07f603d49b1be89a66020c6988edc22cd2e37dc191	✗
-	1.31 KB	6fc8e6ed1e4a1dc01de782549fc64c0f0ac975b13576e4985df5c213fc8cf32d	✗
-	52.17 KB	0c5c90e9834fba973e89273dc85a55644ccf5c7fea6b420a3ca379d45f019129	✗
-	28.73 KB	61c981204df895f35787eb3beff837269d8c772e553d74a24d596aee8245a63c	✗
-	81.61 KB	e0c6e70eea4d1fbf6f4f37492a52fc992519c3b72f9caa98e416c0d6c5056a55	✗
-	1.31 KB	dc43e4c794de758c49fa2367c1be8ad5ccd805ada9a6b9153a9cf012270af9e3	✗
-	50.67 KB	5bf939b73fba249e798cdb00802188757382 80aaf58833b6a98b2180ec713a14	✗
-	66.09 KB	68d9a59ddb3bcaf472fc8a1fee71c9caa9d8faf16b4e5de82ac7a813dee60de5	✗
-	48.08 KB	8be4a368e7ec2c73304af53e83e3d1dc8d7067e8591692a1cfe9fe7f74d9e02c	✗
-	13.12 KB	2e15e493f019342e8b71688d7ca418868a0190f132cb1e5d3617829e137e1d21	✗
-	110.50 KB	b0706b4d15bec96700a24f19d9d195954d6d06503bed038185faf23807286aae	✗
-	1.48 KB	b21320bf2803f29063629a4a6f60b9629d145eddf3cdda8020a229c70fa4fd9b	✗
-	52.17 KB	1ab871387870649168982b0bc3faed12b14ec8c3a6b261b6d101aefa8fe1599f	✗
-	56.95 KB	023a8de4ff38286efc20cf8c232049be027e8152973df050e7396a0787e1c8ca	✗
-	58.94 KB	ec900381d1c865b4202cb7ce878263cd8b32a5d225867a5da4237b215485499c	✗
-	56.00 KB	97ebc628f13b0f9f3637f65d2bc0992a9e7e0f738bcd6dca2fddcc766ff1771e	✗
-	59.12 KB	82bd76fb9bed208dbf69824e9b001066b8f4e060f092abce51c722ceac9fecdb	✗
-	65.59 KB	024539346e29f8d39fa1edf425c93058f239f9fcd1d16117fae53e1edb7f41e1	✗
-	62.20 KB	5b6b0abb48479903c55c796552d57991c20e354feafce8953e221360445e6d4a	✗
-	11.11 KB	3072e65ca05447fad482e97bd5d936d76db63af59a2b0667746385ea11bc2411	✗
-	15.27 KB	43471baa2bd5166c398a6a1e6395eb34d70a6977a866c7090f3202f00e267f05	✗
-	248.27 KB	eca6f967f32b1915070b2bf3239858ecd37c76ddaf4d274d9a535be711dbf16e	✗
-	14.62 KB	d893cd678bd81221ceebc0c2453241a04bf7252d56eb29f97bf246dc650225e6b	✗
-	14.62 KB	bda638bc7845c9179add3fa482eb4cd0b47b2fd531c3a35868a08c508908a11b	✗
-	89.36 KB	e30ed1d15696230b5a3f9b409137f0872ac342203a4af093908334a102900a66	✗
-	2745.83 KB	bfc64305a956dab622bfc2dcf8e4df3a9a2603c95fb12f02f1ef253900eb6d4d	✗
-	320 bytes	ba59304af0a1fa1029421aefeba215ee58f59c15ee95831d80bf2064b6e29706	✗

File Name	File Size	SHA256	YARA Match
-	560 bytes	94d62274d6b7dc1bebe7f281fc68b2fefcb21e1e5dc468b6c9a390e5ccc0454b	✗
-	8.02 KB	9009558717ac87a591a838c9e8070ba965aaa33aab3f948c23e51080113de56f	✗
-	1024.02 KB	23978bce6a7bdf214953488086101dd86d1b55ad2e819c50630cb7deabc19a2f	✗
-	1024.02 KB	a3caeb39e63fda20632d65618a256a9f3e80f013a45cc42b79319af3be9765cd	✗
-	1024.02 KB	308cf23771e975a2718daeabcfb1f7e4d30b15b29474bf44a2afb0f0b53ca6c6	✗
-	256 bytes	e84a4fe9eb332107cc9003128f2e35d4ada575c2514c11e556477c0c308389f7	✗
-	16 bytes	6a152a739485bdd612c7aefe62defe6a1af1b6edb3225de05269e3fef2a2ec58	✗
-	16 bytes	32af5a79a280873372d7bd4938b0d4c7a769d0de0ba6bf6477ebae2418565563	✗
-	256 bytes	337666d008b5c19c74b8b343e0d525c1fd044a5a5b35a00eb67670f6a7951166	✗
-	16 bytes	4d20934edbc12acc4b25e874c224ca9dfca45afe813d5cd75b832c7df6a1f1fb	✗
-	16 bytes	d57595067599d0a43b052b23703a4ee2e83f11038644bb590b0ef5e7bcd32e7e	✗
-	256 bytes	72fa0ebda8adf2ed9fc43c6a830245d8c464a8bc6e98859ead2534055178d45c	✗
-	16 bytes	c08239e60c749f129693332264d59cd819dd778576065863ec56c46809ecb941	✗
-	16 bytes	d9c22f34809eb02fad7fd045d32159295a8237c3d92272f4a7a46aec6de0c800	✗
-	256 bytes	a3682d70f211dfbbf9c93eb3c9b5d873f0c26451069b126316ad4f27f12e808b	✗
-	64.02 KB	9b5c3180fbfc6e6f68ed21b491e545d57c458cf012a20cf4529fd193e9344c58	✗
-	64.02 KB	2b8f1d09fe3b1d3cc32b6b604573985f2515a5f4415dc0d1b52fac99507dd842	✗
-	16 bytes	83410128f7f17c0ecfc9be810036cbc5cf31d34b2392133a53cf0b1a8ad1f14f	✗
-	256 bytes	34a970d1b45876468cd7ed651d8f148db9d24b911cda42e8bce26a131e36fefd	✗
-	64.02 KB	c711060fa8e19fb84424c72b1cd07101f2522cad4c53d2c5e207a082f501e72c	✗
-	64.02 KB	14a93a8d0ed4f64958716146e4561791f43af88176bce362125ddb86dc00c401	✗
-	256 bytes	349bd43f7473f1f8fbefe38052681bf60e661257d785142db3480320e55b1794	✗
-	64.02 KB	688f9fa86a29ca304c48676a76da9c0e2f9268c2a65bf8c1fbdfc7afded2c03d	✗
-	64.02 KB	00344935b50fecb72c9db1a9409e219be3c29bda6bc71fa166a9f6830e34caf0	✗
-	10240.00 KB	c3caed90909a2b8ba9e0d682fb95271c42b2fa14e33205699b0fa3f00c035385	✗
-	48.06 KB	885b57f6ee1fbde91902eb341406b2bf0eae46c9c089b3f7c418debe83168cca	✗
-	48.06 KB	ff3ccddfda28c0ff940b9d1f478f64279d8210c3af8a38a963f039f5c398a33f	✗
-	48.06 KB	4cf0f86a9a2d372302bba1a8af8256be87733892fb7a09dc4b960f4aa6842b31	✗
-	47.69 KB	28be4f4f230d0fb774a58966efce86002fc8b6f68989fe0cefa6697475ae5150	✗

File Name	File Size	SHA256	YARA Match
-	48.06 KB	699279b69169cd9aa873365a279f11513fe20d8133ce1bddbc0036d01a3a61af	✗
-	48.06 KB	20caf2ba679c59c713ec79836afdf963a5a360755e32b5ca37e5e6329ecf224d	✗
-	48.06 KB	e4faf036e6b28b003f844626785af2757b6946a6cbcabf9aee1e734c40f07928	✗
-	48.06 KB	551ab80f92a917d780de43e956436542e0b141495e517b32c963c644ecf1718b	✗
-	48.06 KB	ac92c81e87e19fb90f647a788f4ce46db7bce5ef6250952770f51b8f827a0a02	✗
-	48.06 KB	1e1d43ef8a7790a9cc8be1459d1dc75bf9e7dd5785cbc8fee133a2b3b04c4b12	✗
-	48.06 KB	e3a724a2ce5d48fa576425621eef25e771b4bc783edc03b0b614a4a923047b2a	✗
-	48.06 KB	bd7133be16ab2ea270b21b5139c5a72fe05c1059040bdd03869c6dfafaff1f62	✗
-	48.06 KB	036873ad3e5a350331e71253fc058c7230a240286046427cb19a0caa95ea6f43	✗
-	48.06 KB	c3c66cbc782dceb42385721f54747d4b5331e95275553b98f4e6a01c11599b53	✗
-	48.06 KB	50e4653af9fd6ac612aedab0bb05e58ba268b28cf2df5029453567b07eb475d5	✗
-	48.06 KB	ff89e18608bb0b7b462d0c0d2421f840a1d38e9df346d89ef38e13393259604c	✗
-	48.06 KB	7b386c1ea8275dc4d4a249129d3cc0ac14bd16e62594be075a4a0d6e0b275804	✗
-	48.06 KB	72a35d87f394919517f4e652fde1b6169bddac253c36612568b0c7c4f20d44db	✗
-	48.06 KB	13568398ae982f68f452d83b9ed49264b154bd04abb600f067f5b1db5d22503b	✗
-	48.06 KB	3c44464d8191a121cf02c16416b742dcc30e2f67650ed72a7f541178fe2957ba	✗
-	48.06 KB	15bd4c3b4d95f115a9107e026508ece05c9c1812f87a5c2406c3b5043a614ac0	✗
-	48.06 KB	9ebe38749e2beb218a8be7d235b62721723ff5fc98fc7e4c3e7c911b3b9c3fc3	✗
-	48.06 KB	6f9bc18e916d4838d38280af3eb0ba759c4a44828fd99b60a7f6bee1dbdddd96a	✗
-	48.06 KB	e315384697ee1a18b36ae77c13356acb5ba08e01f40827c8331e920c2ad8f98d	✗
-	48.06 KB	d63d020d9f0c41ce9197bc6f6314780b01483da249a34bc54aeb24f5b1fccd7a	✗
-	48.06 KB	5400064e85a9a0f42baaceddd95bda0196af3fc539bdea1ee1e563cd1b8d3fd6	✗
-	48.06 KB	8304603c18de5269ff78bdd6798319d31629216691f97e35e604842e02414387	✗
-	48.06 KB	717e6e9730efbc2a6e6948ed3053185c325cdf2ef49d23883200460af74dcc7f	✗
-	48.06 KB	a8f8d52575cfea7b878ccccdf74c5933928c6ae5a89ead376e0c99ba9659b7f11	✗
-	48.06 KB	497aa4df1a8b4590a84f917fceb069c6f618e8ba3697c94cf29b6ae8e418520a	✗

Reduced dataset

Host Behavior

Type	Count
Module	203

Type	Count
Registry	2
Keyboard	1
System	5
Window	3
File	11685

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844	C:\Users\kEecfMwgj\Desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe	Sample File	96.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
6cae2b44e0989d2f7e3940b9a0457c77169f9064278295aa708d6c982dabeb3f	c:\programdata\microsoft\assistance\client\1.0\en-us\help_cvalidator.h1d.ozq0	Dropped File	11.80 KB	application/octet-stream	-	CLEAN
7141a8d8fb880c016d57c17090a44c857e6d08e91b6a38567e5922c004a4044a	c:\programdata\microsoft\assistance\client\1.0\en-us\help_mkwd_assetid.h1w.ozq0	Dropped File	217.50 KB	application/octet-stream	-	CLEAN
6b88ea27eb17038324ad1d53fb3d0a71b3ddc68fbca35f38fd6e648ccf876f84	c:\programdata\microsoft\assistance\client\1.0\en-us\help_mkwd_bestbet.h1w.ozq0	Dropped File	201.48 KB	application/octet-stream	-	CLEAN
293e92af0dff9a0631ccd41817d889914efbfe5bfa5e5b320b81b032a367a0ee	c:\programdata\microsoft\assistance\client\1.0\en-us\help_mtoc_help.h1h.ozq0	Dropped File	487.78 KB	application/octet-stream	-	CLEAN
09dcf799070cbd0ccb313434a333eef2de056e3b6bd543723757aa3e91120520	c:\programdata\microsoft\assistance\client\1.0\en-us\help_mvalidator.h1d.ozq0	Dropped File	14.33 KB	application/octet-stream	-	CLEAN
3ffdc4c0b99ccf12ff72193fd88703e0856072ad52d09ee60e3effec38b6688e	c:\programdata\microsoft\assistance\client\1.0\en-us\help_mvalidator.lck.ozq0	Dropped File	16 bytes	application/octet-stream	-	CLEAN
9d7471c2960c549f7ad820b0006be7e33a3dbb4da4973bfbb3256dfb6ebc91a5	c:\programdata\microsoft\assistance\client\1.0\en-us\help{9daa54e8-cd95-4107-8e7f-ba3f24732d95}.h1q.ozq0	Dropped File	852.78 KB	application/octet-stream	-	CLEAN
df6ee410303ad933f72d1e98326c576569933d7dbc555f7fe2741f46ded37ddb	c:\programdata\microsoft\clicktorun\deploymentconfig.0.xml.ozq0	Dropped File	1.94 KB	application/octet-stream	-	CLEAN
aa171428e2a5325202f4b628897899c59418ce836872ce7d080dddde661e1e5e	c:\programdata\microsoft\clicktorun\deploymentconfig.2.xml.ozq0	Dropped File	1.36 KB	application/octet-stream	-	CLEAN
a75c582379eb42d569e03ffcc586f076b250ec43814706687432d1ff79992d76	c:\programdata\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\masterdescriptor.en-us.xml.ozq0	Dropped File	21.86 KB	application/octet-stream	-	CLEAN
88d62a1aed83e66d120f06e48655406f64c12285f7e89eb85a02def3342de90b	c:\programdata\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\s321033.hash.ozq0	Dropped File	112 bytes	application/octet-stream	-	CLEAN
044acffabb306f067df0f179c317e7b9913addec287c28f6096cee387bb2edb3	c:\programdata\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\stream.x86.en-us.man.dat.ozq0	Dropped File	864.47 KB	application/octet-stream	-	CLEAN
7ec9782c87a8232cf63be95efc7f2bf2eee0f16d7d4834c83bbaec8d1b578cfd	c:\programdata\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\masterdescriptor.x-none.xml.ozq0	Dropped File	20.55 KB	application/octet-stream	-	CLEAN
4df5b2dbd6a73550e4718efe2816399b2cb2f806170f4b051d68f003e580b774	c:\programdata\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\s320.hash.ozq0	Dropped File	112 bytes	application/octet-stream	-	CLEAN
48a53b233669ac34e2597dd71e48c9b08c331e1eaa2ec4c8549a6e47b714faae	c:\programdata\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\stream.x86.x-none.man.dat.ozq0	Dropped File	3629.45 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
603023e96ef388e08fa0ab4500d44943588c7372c8f2843d46b396a21f930927	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\deploymentconfiguration.xml.ozq0	Dropped File	624 bytes	application/octet-stream	-	CLEAN
617d8586da7ce0b4eae04b237c0bf1dd2fd3152cc938c1539716cf2df31b4cc2	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\manifest.xml.ozq0	Dropped File	4818.02 KB	application/octet-stream	-	CLEAN
c636270ba1beb3e4daca80490a4c4112725803aa4f011ed796b56fb75ca55b72	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\userdeploymentconfiguration.xml.ozq0	Dropped File	624 bytes	application/octet-stream	-	CLEAN
2624b77220c433f253d2af304c796d5746ba08233046db510f03315b62c0aa9d	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\usermanifest.xml.ozq0	Dropped File	3024.27 KB	application/octet-stream	-	CLEAN
e37ba368cbb3f245d44cee6a202b2b1ea4a0f5b82b2d159a9535e9eeb191393e	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\airspace.etw.man.ozq0	Dropped File	275.55 KB	application/octet-stream	-	CLEAN
c1a76009f89b41682c7f813de9f9158ed59ba895544c6edf6be4f3c0b7e53295	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.access.access.x-none.msi.16.x-none.xml.ozq0	Dropped File	37.89 KB	application/octet-stream	-	CLEAN
8944c4bff7a505e74fb3cab0beafe29f893447cd05a940470e8893e3a39ac63b	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmui.msi.16.en-us.xml.ozq0	Dropped File	56.08 KB	application/octet-stream	-	CLEAN
d5b2df956c860a4902213cc0a33bac44f5a7d32349ea95ada1fa0d8923a57e9d	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmuiset.msi.16.en-us.xml.ozq0	Dropped File	2.00 KB	application/octet-stream	-	CLEAN
d9d72a09268da08e44753e2ebfce36082703d49a50ad5c56fa6139e4ea49b193	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcf.dcf.x-none.msi.16.x-none.xml.ozq0	Dropped File	16.27 KB	application/octet-stream	-	CLEAN
b28c62b78259a9e78046ed89f8acbf9ba6cd701d4abd905fc5aae8809c9f76fd	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcfmui.msi.16.en-us.xml.ozq0	Dropped File	9.59 KB	application/octet-stream	-	CLEAN
6bd2b71adbc24376fb4324c0913f4d4822fa5bbb43c88762debb6f96fdebe9bc	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excel.excel.x-none.msi.16.x-none.xml.ozq0	Dropped File	232.31 KB	application/octet-stream	-	CLEAN
8b7c57a633aea70b1a0701ddbccf8ccba03bd4eee0de53d912eddc177cd61c02	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excelmui.msi.16.en-us.xml.ozq0	Dropped File	34.22 KB	application/octet-stream	-	CLEAN
4ee35a080aab7ebf7a123bad465e104ca1a4b382f0a650d6a4c538c6d162231f	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groove.groove.x-none.msi.16.x-none.xml.ozq0	Dropped File	35.77 KB	application/octet-stream	-	CLEAN
424ac0049e097d68d5e67adcb3164bdb86ba42aba25822bee723aff63fb4ef0d	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groovemui.msi.16.en-us.xml.ozq0	Dropped File	6.00 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fd2aea4496294dc13f517ab95ccc9e89a9fd822decfdc60ca43f1c1d5ad54b66	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lync.lync.x-none.msi.16.x-none.xml.ozq0	Dropped File	87.47 KB	application/octet-stream	-	CLEAN
61691df5d44c7ff93c60c9dfc2c2ebc066359b380638923eb0d4415ba8db6762	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lyncmui.msi.16.en-us.xml.ozq0	Dropped File	22.80 KB	application/octet-stream	-	CLEAN
f46d6e450ea7beb450fc9cb08937adbc0aca794880e7a771c01b68131ffc60bb	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64mui.msi.16.en-us.xml.ozq0	Dropped File	21.45 KB	application/octet-stream	-	CLEAN
706ceac0577142972363fb7a5ebf743b39ada60a0f628e6069f7763f9b49fe5a	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64muiset.msi.16.en-us.xml.ozq0	Dropped File	2.00 KB	application/octet-stream	-	CLEAN
505502a51e4ed19e24fdc3301b775893042cd17e7c4ff0ac4a18654ea9ab2906	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64ww.msi.16.x-none.xml.ozq0	Dropped File	261.20 KB	application/octet-stream	-	CLEAN
dc77fb2c961f46edfb516b79fd95376c98227ee70a349a2391c0494cfe6f40db	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.officemui.msi.16.en-us.xml.ozq0	Dropped File	104.39 KB	application/octet-stream	-	CLEAN
b57116266284167fd48f49a4701c75d358a043a54c8894b6f75076f1d2b2a1db	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.officemuiset.msi.16.en-us.xml.ozq0	Dropped File	2.00 KB	application/octet-stream	-	CLEAN
59c942f196e76d3ddbb300a0ff0c31fba1f027824e73860911959536414c52cd	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.onenote.onenote.x-none.msi.16.x-none.xml.ozq0	Dropped File	93.70 KB	application/octet-stream	-	CLEAN
b5ba8ea7b1075518852b0995f903449fee50344783aabe3b026c15b5d54a366c	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.onenotemui.msi.16.en-us.xml.ozq0	Dropped File	18.53 KB	application/octet-stream	-	CLEAN
ebb264329890c98b56a897663035df279e54cbfb7cf20bf3f0217ccfc0a48db3	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osm.osm.x-none.msi.16.x-none.xml.ozq0	Dropped File	1.48 KB	application/octet-stream	-	CLEAN
2996680e1ff41ebdf5cd1bc102e6ddcf4a0f0206adafbc05793e6daf55ba8701	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osmmui.msi.16.en-us.xml.ozq0	Dropped File	10.78 KB	application/octet-stream	-	CLEAN
014d455bd04184d2502e611552e3acd3907b10cdef40c90b9cba8ac71e468fde	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osmux.osmux.x-none.msi.16.x-none.xml.ozq0	Dropped File	2.25 KB	application/octet-stream	-	CLEAN
62004ca4fc442607e1f025590a4db0f03428e82e5f3569c9c8fbec8c36d02bcc	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osmuxmui.msi.16.en-us.xml.ozq0	Dropped File	9.66 KB	application/octet-stream	-	CLEAN
ee6f069e347bb9ae20b1a0d40ff4c355ac7591630b74695c35b27f948211bb3e	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.outlook.outlook.x-none.msi.16.x-none.xml.ozq0	Dropped File	91.16 KB	application/octet-stream	-	CLEAN
cecac506cb90d016efe05315a0877a27aa4cf0912372ffc58a562cced015a3d1	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.outlookmui.msi.16.en-us.xml.ozq0	Dropped File	94.20 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9f1ce0fafada2644732222de661b60299231c1558a62ae5643a8db37e396a6f2	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.powerpivot.powerpivot.x-none.msi.16.x-none.xml.ozq0	Dropped File	695.23 KB	application/octet-stream	-	CLEAN
48129357554589 06d8e530b7e312f3a91519e1961b326c8c76a4fc286af5b6b7	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.powerpoint.powerpoint.x-none.msi.16.x-none.xml.ozq0	Dropped File	100.38 KB	application/octet-stream	-	CLEAN
609882fcf42b12e2925556153b8be1a15c93c0998acd4e12b85903f7ec24d78c	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.powerpointmui.msi.16.en-us.xml.ozq0	Dropped File	26.08 KB	application/octet-stream	-	CLEAN
900ac6108a121c5ff2dc90298dea2ac41fba95804397daedb4836c01a96f42b5	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proof.culture.msi.16.en-us.xml.ozq0	Dropped File	24.86 KB	application/octet-stream	-	CLEAN
2b8677b7f91cc9665c4e63f76fd4a75d42a743823850cbb0cd1f8bdb518a90bc	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proof.culture.msi.16.es-es.xml.ozq0	Dropped File	23.92 KB	application/octet-stream	-	CLEAN
5484b8d47ff3aa1c7a5fb925e0422730e6a3fc9e68eb2f021bf58838b9b91416	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proof.culture.msi.16.fr-fr.xml.ozq0	Dropped File	23.92 KB	application/octet-stream	-	CLEAN
05d82c99b68b0ddc8f6ce90ea2e2fbfd47e409e50580dcf80dbeb4c51cac434b	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proofing.msi.16.en-us.xml.ozq0	Dropped File	2.00 KB	application/octet-stream	-	CLEAN
75ac382f8b4e1529aec890388f20292b37b37eeac0e17fbaacb9ba848cd4dc9	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.publisher.publisher.x-none.msi.16.x-none.xml.ozq0	Dropped File	75.36 KB	application/octet-stream	-	CLEAN
6b384cdec581d1a4653d415125443fb87814f689191bdf4dc37e0979b46f1b3f	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.publishermui.msi.16.en-us.xml.ozq0	Dropped File	13.77 KB	application/octet-stream	-	CLEAN
5cb7f7e100c1b8c2a8a3c99ac5d6441f4ecacdab8d2b2ed2a4a25818c3653efc	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.shared.office.x-none.msi.16.x-none.xml.ozq0	Dropped File	683.06 KB	application/octet-stream	-	CLEAN
72da6629f6372f61918cdee778f880b50b0de614037fabca0210775e3c01afbf	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.word.word.x-none.msi.16.x-none.xml.ozq0	Dropped File	84.64 KB	application/octet-stream	-	CLEAN
69e4de5622c0a1fd650a2a83cd37aa0febc584343445fe4c704a892d262d7713	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.wordmui.msi.16.en-us.xml.ozq0	Dropped File	76.03 KB	application/octet-stream	-	CLEAN
abcc28bfd03feb486a57586360740d60b029b11f4f2ea92a202ab4ad19761293	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\integrator.exe.ozq0	Dropped File	839.62 KB	application/octet-stream	-	CLEAN
8ec22653478fcaf3d928787e020fdea506f35f497095786a054ea09b3e7ea4ae	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\microsoft_office_officetelemetryagentfallback2016.xml.ozq0	Dropped File	3.25 KB	application/octet-stream	-	CLEAN
f92fa60cde90c5ffd6a338f440c2a765a878e946f3dccb3b0f3444bebc49be1b	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\microsoft_office_officetelemetryagentlogon2016.xml.ozq0	Dropped File	3.19 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7d14873baec24b48135e47680c9f80b3de342f727103a3052636a7bf075f2502	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\msoutilstat.etw.man.ozq0	Dropped File	110.05 KB	application/octet-stream	-	CLEAN
0a688b5d036cf005b29e4ac848f577863a33b8cbadf8e1b82e2cd0011707552b	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\wordetw.man.ozq0	Dropped File	623.47 KB	application/octet-stream	-	CLEAN
c52b8f6df91f544340e00103234f916c6a6669a64946d64909ea5840b468ab9b	c:\programdata\microsoft\devicestage\device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png.ozq0	Dropped File	126.72 KB	application/octet-stream	-	CLEAN
c4ae6edeea3aedf32f4cbbb14bbbe96f53ee8e12af7ca39143a7e7db744c5ae8	c:\programdata\microsoft\devicestage\device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\behavior.xml.ozq0	Dropped File	2.86 KB	application/octet-stream	-	CLEAN
a88d9f0e7e63391c8b0c12149b489bf185d65127d065184d004d771840fbb1d7	c:\programdata\microsoft\devicestage\device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png.ozq0	Dropped File	43.45 KB	application/octet-stream	-	CLEAN
e2532114a369dd2a3b72300bfdbdbd19ba5697433193d593e829d30a75f54976	c:\programdata\microsoft\devicestage\device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png.ozq0	Dropped File	28.20 KB	application/octet-stream	-	CLEAN
62366db0453624a083a8feecfac77936d8980d36b50425e9bcbcf4d84347298b	c:\programdata\microsoft\devicestage\device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png.ozq0	Dropped File	38.47 KB	application/octet-stream	-	CLEAN
d434a0e7647c2f15d822670af98d62eefe5d6b88bfc18eb89d275028746e3450	c:\programdata\microsoft\devicestage\device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png.ozq0	Dropped File	126.72 KB	application/octet-stream	-	CLEAN
7c809e2b75e2f0858f7dff54434b5b87909ace3f9120551f2983671877f1dad0	c:\programdata\microsoft\devicestage\device\{8702d817-5aad-4674-9ef3-4d3decd87120}\behavior.xml.ozq0	Dropped File	1.86 KB	application/octet-stream	-	CLEAN
78a858dacae6b6d2e4654d07f603d49b1be89a66020c6988edc22cd2e37dc191	c:\programdata\microsoft\devicestage\device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png.ozq0	Dropped File	28.20 KB	application/octet-stream	-	CLEAN
6fc8e6ed1e4a1dc01de782549fc64c0f0ac975b13576e4985df5c213fc8cf32d	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-us\resource.xml.ozq0	Dropped File	1.31 KB	application/octet-stream	-	CLEAN
0c5c90e9834fba973e89273dc85a55644ccf5c7fea6b420a3ca379d45f019129	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\folder.ico.ozq0	Dropped File	52.17 KB	application/octet-stream	-	CLEAN
61c981204df895f35787eb3beff837269d8c772e553d74a24d596aee8245a63c	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\netfol.ico.ozq0	Dropped File	28.73 KB	application/octet-stream	-	CLEAN
e0c6e70eea4d1fbf6f4f37492a52fc992519c3b72f9caa98e416c0d6c5056a55	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\pictures.ico.ozq0	Dropped File	81.61 KB	application/octet-stream	-	CLEAN
dc43e4c794de758c49fa2367c1be8ad5ccd805ada9a6b9153a9cf012270af9e3	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\resource.xml.ozq0	Dropped File	1.31 KB	application/octet-stream	-	CLEAN
5bf939b73fba249e798cdb0080218875738280aaf58833b6a98b2180ec713a14	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\ringtones.ico.ozq0	Dropped File	50.67 KB	application/octet-stream	-	CLEAN
68d9a59ddb3bcaf472fc8a1fee71c9caa9d8faf16b4e5de82ac7a813dee60de5	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\settings.ico.ozq0	Dropped File	66.09 KB	application/octet-stream	-	CLEAN
8be4a368e7ec2c73304af53e83e3d1dc8d7067e8591692a1cfe9fe7f74d9e02c	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\sync.ico.ozq0	Dropped File	48.08 KB	application/octet-stream	-	CLEAN
2e15e493f019342e8b71688d7ca418868a0190f132cb1e5d3617829e137e1d21	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\tasks.xml.ozq0	Dropped File	13.12 KB	application/octet-stream	-	CLEAN
b0706b4d15bec96700a24f19d9d195954d6d06503bed038185faf23807286aae	c:\programdata\microsoft\devicestage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\wmp.ico.ozq0	Dropped File	110.50 KB	application/octet-stream	-	CLEAN
b21320bf2803f29063629a4a6f60b9629d145eddf3cdda8020a229c70fa4fd9b	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\en-us\resource.xml.ozq0	Dropped File	1.48 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1ab8713878706491689 82b0bc3faed12b14ec8c3a6b261b6d101aefa8fe1599f	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\folder.ico.ozq0	Dropped File	52.17 KB	application/octet-stream	-	CLEAN
023a8de4ff38286efc20cf8c232049be027e8152973df050e7396a0787e1c8ca	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\print_pref.ico.ozq0	Dropped File	56.95 KB	application/octet-stream	-	CLEAN
ec900381d1c865b4202cb7ce878263cd8b32a5d225867a5da4237b215485499c	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\print_property.ico.ozq0	Dropped File	58.94 KB	application/octet-stream	-	CLEAN
97ebc628f13b0f9f3637f65d2bc0992a9e7e0f738bcd6dca2fddcc766ff1771e	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\print_queue.ico.ozq0	Dropped File	56.00 KB	application/octet-stream	-	CLEAN
82bd76fb9bed208dbf69824e9b001066b8f4e060f092abce51c722ceac9fecdb	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\scan_.ico.ozq0	Dropped File	59.12 KB	application/octet-stream	-	CLEAN
024539346e29f8d39fa1edf425c93058f239f9fcd1d16117fae53e1edb7f41e1	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\scan_property.ico.ozq0	Dropped File	65.59 KB	application/octet-stream	-	CLEAN
5b6b0abb48479903c55c796552d57991c20e354feafce8953e221360445e6d4a	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\scan_settings.ico.ozq0	Dropped File	62.20 KB	application/octet-stream	-	CLEAN
3072e65ca05447fad482e97bd5d936d76db63af59a2b0667746385ea11bc2411	c:\programdata\microsoft\devicestage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\tasks.xml.ozq0	Dropped File	11.11 KB	application/octet-stream	-	CLEAN
43471baa2bd5166c398a6a1e6395eb34d70a6977a866c7090f3202f00e267f05	c:\programdata\microsoft\identitycrl\ppcrlconfig.dll.ozq0	Dropped File	15.27 KB	application/octet-stream	-	CLEAN
eca6f967f32b1915070b2bf3239858ecd37c76ddaf4d274d9a535be711dbf16e	c:\programdata\microsoft\identitycrl\ppcrlui.dll.ozq0	Dropped File	248.27 KB	application/octet-stream	-	CLEAN
d893cd678bd81221ceebc0c2453241a04bf7252d56eb29f97bf246dc65025e6b	c:\programdata\microsoft\mf\active.grl.ozq0	Dropped File	14.62 KB	application/octet-stream	-	CLEAN
bda638bc7845c9179add3fa482eb4cd0b47b2fd531c3a35868a08c508908a11b	c:\programdata\microsoft\mf\pending.grl.ozq0	Dropped File	14.62 KB	application/octet-stream	-	CLEAN
e30ed1d15696230b5a3f9b409137f0872ac342203a4af093908334a102900a66	c:\programdata\microsoft\officesoftwareprotectionplatform\cache\cache.dat.ozq0	Dropped File	89.36 KB	application/octet-stream	-	CLEAN
bfc64305a956dab622bfc2dcf8e4df3a9a2603c95fb12f02f1ef253900eb6d4d	c:\programdata\microsoft\officesoftwareprotectionplatform\tokens.dat.ozq0	Dropped File	2745.83 KB	application/octet-stream	-	CLEAN
ba59304af0a1fa1029421aefeba215ee58f59c15ee95831d80bf2064b6e29706	c:\programdata\microsoft\search\data\applications\windows\gatherlogs\systemindex\systemindex.1.crwl.ozq0	Dropped File	320 bytes	application/octet-stream	-	CLEAN
94d62274d6b7dc1bebe7f281fc68b2fefcb21e1e5dc468b6c9a390e5ccc0454b	c:\programdata\microsoft\search\data\applications\windows\gatherlogs\systemindex\systemindex.1.gthr.ozq0	Dropped File	560 bytes	application/octet-stream	-	CLEAN
9009558717ac87a591a838c9e8070ba965aaa33aab3f948c23e51080113de56f	c:\programdata\microsoft\search\data\applications\windows\mss.chk.ozq0	Dropped File	8.02 KB	application/octet-stream	-	CLEAN
23978bce6a7bdf214953488086101dd86d1b55ad2e819c50630cb7deabc19a2f	c:\programdata\microsoft\search\data\applications\windows\mss.log.ozq0	Dropped File	1024.02 KB	application/octet-stream	-	CLEAN
a3caeb39e63fda20632d65618a256a9f3e80f013a45cc42b79319af3be9765cd	c:\programdata\microsoft\search\data\applications\windows\mssres00001.jrs.ozq0	Dropped File	1024.02 KB	application/octet-stream	-	CLEAN
308cf23771e975a2718daeabcfb1f7e4d30b15b29474bf44a2afb0f0b53ca6c6	c:\programdata\microsoft\search\data\applications\windows\mssres00002.jrs.ozq0	Dropped File	1024.02 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e84a4fe9eb332107cc9003128f2e35d4ada575c2514c11e556477c0c308389f7	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciab0001.000.ozq0	Dropped File	256 bytes	application/octet-stream	-	CLEAN
6a152a739485bdd612c7aefe62defe6a1af1b6edb3225de05269e3fef2a2ec58	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciab0001.001.ozq0	Dropped File	16 bytes	text/plain	-	CLEAN
32af5a79a280873372d7bd4938b0d4c7a769d0de0ba6bf6477ebae2418565563	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciab0001.002.ozq0	Dropped File	16 bytes	application/octet-stream	-	CLEAN
337666d008b5c19c74b8b343e0d525c1fd044a5a5b35a00eb67670f6a7951166	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciab0002.000.ozq0	Dropped File	256 bytes	application/octet-stream	-	CLEAN
4d20934edbc12acc4b25e874c224ca9dfca45afe813d5cd75b832c7df6a1f1fb	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciab0002.001.ozq0	Dropped File	16 bytes	text/plain	-	CLEAN
d57595067599d0a43b052b23703a4ee2e83f11038644bb590b0ef5e7bcd32e7e	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciab0002.002.ozq0	Dropped File	16 bytes	application/octet-stream	-	CLEAN
72fa0ebda8adf2ed9fc43c6a830245d8c464a8bc6e98859ead2534055178d45c	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciad0001.000.ozq0	Dropped File	256 bytes	application/octet-stream	-	CLEAN
c08239e60c749f129693332264d59cd819dd778576065863ec56c46809ecb941	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciad0001.001.ozq0	Dropped File	16 bytes	application/octet-stream	-	CLEAN
d9c22f34809eb02fad7fd045d32159295a8237c3d92272f4a7a46aec6de0c800	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\ciad0001.002.ozq0	Dropped File	16 bytes	application/octet-stream	-	CLEAN
a3682d70f211dfbbf9c93eb3c9b5d873f0c26451069b126316ad4f27f12e808b	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\index.000.ozq0	Dropped File	256 bytes	application/octet-stream	-	CLEAN
9b5c3180fbfc6e6f68ed21b491e545d57c458cf012a20cf4529fd193e9344c58	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\index.001.ozq0	Dropped File	64.02 KB	application/octet-stream	-	CLEAN
2b8f1d09fe3b1d3cc32b6b604573985f2515a5f4415dc0d1b52fac99507dd842	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\index.002.ozq0	Dropped File	64.02 KB	application/octet-stream	-	CLEAN
83410128f7f17c0ecfc9be810036cbc5cf31d34b2392133a53cf0b1a8ad1f14f	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\indexer\cifiles\settings.dia.ozq0	Dropped File	16 bytes	application/octet-stream	-	CLEAN
34a970d1b45876468cd7ed651d8f148db9d24b911cda42e8bce26a131e36fefd	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\propmap\cipt0000.000.ozq0	Dropped File	256 bytes	application/octet-stream	-	CLEAN
c711060fa8e19fb84424c72b1cd07101f2522cad4c53d2c5e207a082f501e72c	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\propmap\cipt0000.001.ozq0	Dropped File	64.02 KB	application/octet-stream	-	CLEAN
14a93a8d0ed4f64958716146e4561791f43af88176bce362125ddb86dc00c401	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\propmap\cipt0000.002.ozq0	Dropped File	64.02 KB	application/octet-stream	-	CLEAN
349bd43f7473f1f8fbefe38052681bf60e661257d785142db3480320e55b1794	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\secstore\cist0000.000.ozq0	Dropped File	256 bytes	application/octet-stream	-	CLEAN
688f9fa86a29ca304c48676a76da9c0e2f9268c2a65bf8c1fbdfc7afded2c03d	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\secstore\cist0000.001.ozq0	Dropped File	64.02 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
00344935b50fecb72c9db1a9409e219be3c29bda6bc71fa166a9f6830e34caf0	c:\programdata\microsoft\search\data\applications\windows\projects\systemindex\secstore\cist0000.002.ozq0	Dropped File	64.02 KB	application/octet-stream	-	CLEAN
c3caed90909a2b8ba9e0d682fb95271c42b2fa14e33205699b0fa3f00c035385	c:\programdata\microsoft\search\data\applications\windows\windows.edb.ozq0	Dropped File	10240.00 KB	application/octet-stream	-	CLEAN
885b57f6ee1fbde91902eb341406b2bf0eae46c9c089b3f7c418debe83168cca	c:\programdata\microsoft\user account pictures\default pictures\usertile10.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
ff3ccddfda28c0ff940b9d1f478f64279d8210c3af8a38a963f039f5c398a33f	c:\programdata\microsoft\user account pictures\default pictures\usertile11.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
4cf0f86a9a2d372302bba1a8af8256be87733892fb7a09dc4b960f4aa6842b31	c:\programdata\microsoft\user account pictures\default pictures\usertile12.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
28be4f4f230d0fb774a58966efce86002fc8b6f68989fe0cefa6697475ae5150	c:\programdata\microsoft\user account pictures\default pictures\usertile13.bmp.ozq0	Dropped File	47.69 KB	application/octet-stream	-	CLEAN
699279b69169cd9aa873365a279f11513fe20d8133ce1bddbc0036d01a3a61af	c:\programdata\microsoft\user account pictures\default pictures\usertile14.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
20caf2ba679c59c713ec79836afdf963a5a360755e32b5ca37e5e6329ecf224d	c:\programdata\microsoft\user account pictures\default pictures\usertile15.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
e4faf036e6b28b003f844626785af2757b6946a6cbcabf9aee1e734c40f07928	c:\programdata\microsoft\user account pictures\default pictures\usertile16.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
551ab80f92a917d780de43e956436542e0b141495e517b32c963c644ecf1718b	c:\programdata\microsoft\user account pictures\default pictures\usertile17.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
ac92c81e87e19fb90f647a788f4ce46db7bce5ef6250952770f51b8f827a0a02	c:\programdata\microsoft\user account pictures\default pictures\usertile18.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
1e1d43ef8a7790a9cc8be1459d1dc75bf9e7dd5785cbc8fee133a2b3b04c4b12	c:\programdata\microsoft\user account pictures\default pictures\usertile19.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
e3a724a2ce5d48fa576425621eef25e771b4bc783edc03b0b614a4a923047b2a	c:\programdata\microsoft\user account pictures\default pictures\usertile20.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
bd7133be16ab2ea270b21b5139c5a72fe05c1059040bdd03869c6dfafaff1f62	c:\programdata\microsoft\user account pictures\default pictures\usertile21.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
036873ad3e5a350331e71253fc058c7230a240286046427cb19a0caa95ea6f43	c:\programdata\microsoft\user account pictures\default pictures\usertile22.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
c3c66cbc782dceb42385721f54747d4b5331e95275553b98f4e6a01c11599b53	c:\programdata\microsoft\user account pictures\default pictures\usertile23.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
50e4653af9fd6ac612aedab0bb05e58ba268b28cf2df5029453567b07eb475d5	c:\programdata\microsoft\user account pictures\default pictures\usertile24.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
ff89e18608bb0b7b462d0c0d2421f840a1d38e9df346d89ef38e13393259604c	c:\programdata\microsoft\user account pictures\default pictures\usertile25.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
7b386c1ea8275dc4d4a249129d3cc0ac14bd16e62594be075a4a0d6e0b275804	c:\programdata\microsoft\user account pictures\default pictures\usertile26.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
72a35d87f394919517f4e652fde1b6169bddac253c36612568b0c7c4f20d44db	c:\programdata\microsoft\user account pictures\default pictures\usertile27.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
13568398ae982f68f452d83b9ed49264b154bd04abb600f067f5b1db5d22503b	c:\programdata\microsoft\user account pictures\default pictures\usertile28.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
3c44464d8191a121cf02c16416b742dcc30e2f67650ed72a7f541178fe2957ba	c:\programdata\microsoft\user account pictures\default pictures\usertile29.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
15bd4c3b4d95f115a9107e026508ece05c9c1812f87a5c2406c3b5043a614ac0	c:\programdata\microsoft\user account pictures\default pictures\usertile30.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
9ebe38749e2beb218a8be7d235b62721723ff5fc98fc7e4c3e7c911b3b9c3fc3	c:\programdata\microsoft\user account pictures\default pictures\usertile31.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
6f9bc18e916d4838d38280af3eb0ba759c4a44828fd99b60a7f6bee1dbddd96a	c:\programdata\microsoft\user account pictures\default pictures\usertile32.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
e315384697ee1a18b36ae77c13356acb5ba08e01f40827c8331e920c2ad8f98d	c:\programdata\microsoft\user account pictures\default pictures\usertile33.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
d63d020d9f0c41ce9197bc6f6314780b01483da249a34bc54aeb24f5b1fccd7a	c:\programdata\microsoft\user account pictures\default pictures\usertile34.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
5400064e85a9a0f42baaceddd95bda0196af3fc539bdea1ee1e563cd1b8d3fd6	c:\programdata\microsoft\user account pictures\default pictures\usertile35.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
8304603c18de5269ff78bdd6798319d31629216691f97e35e604842e02414387	c:\programdata\microsoft\user account pictures\default pictures\usertile36.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
717e6e9730efbc2a6e6948ed3053185c325cdf2ef49d23883200460af74dcc7f	c:\programdata\microsoft\user account pictures\default pictures\usertile37.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN
a8f8d52575cfea7b878cccdf74c5933928c6ae5a89ead376e0c99ba9659b7f11	c:\programdata\microsoft\user account pictures\default pictures\usertile38.bmp.ozq0	Dropped File	48.06 KB	application/octet-stream	-	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
System Paging File	Accessed File	Access	CLEAN
C:\Program Files (x86)	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe	Accessed File	Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_CValidator.H1D	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_CValidator.H1D.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MKWD_AssetId.H1W	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MKWD_AssetId.H1W.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MKWD_BestBet.H1W	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MKWD_BestBet.H1W.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MTOC_help.H1H	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MTOC_help.H1H.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MValidator.H1D	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MValidator.H1D.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MValidator.Lck	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help_MValidator.Lck.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help{9DAA54E8-CD95-4107-8E7F-BA3F24732D95}.H1Q	Accessed File	Delete, Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\Help{9DAA54E8-CD95-4107-8E7F-BA3F24732D95}.H1Q.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\DeploymentConfig.0.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\DeploymentConfig.0.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\DeploymentConfig.2.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\DeploymentConfig.2.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\MasterDescriptor.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\MasterDescriptor.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\s321033.hash	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\s321033.hash.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\stream.x86.en-us.man.dat	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\stream.x86.en-us.man.dat.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\MasterDescriptor.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\MasterDescriptor.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\s320.hash	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\s320.hash.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\stream.x86.x-none.man.dat	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\stream.x86.x-none.man.dat.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\DeploymentConfiguration.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\DeploymentConfiguration.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\Manifest.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\Manifest.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserDeploymentConfiguration.xml	Accessed File	Delete, Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserDeploymentConfiguration.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserManifest.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserManifest.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\AirSpace.Etw.man	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\AirSpace.Etw.man.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Access.Access.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Access.Access.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmuiset.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmuiset.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.DCF.DCF.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.DCF.DCF.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.dcfmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.dcfmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Excel.Excel.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Excel.Excel.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.excelmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.excelmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Groove.Groove.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Groove.Groove.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.groovemui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.groovemui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Lync.Lync.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Lync.Lync.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.lyncmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.lyncmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64mui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64mui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64muiset.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64muiset.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64ww.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64ww.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemuiset.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemuiset.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OneNote.OneNote.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OneNote.OneNote.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.onenotemui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.onenotemui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSM.OSM.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSM.OSM.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSMUX.OSMUX.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSMUX.OSMUX.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmuxmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmuxmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Outlook.Outlook.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Outlook.Outlook.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.outlookmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.outlookmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPivot.PowerPivot.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPivot.PowerPivot.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPoint.PowerPoint.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPoint.PowerPoint.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.powerpointmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.powerpointmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.es-es.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.es-es.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.fr-fr.xml	Accessed File	Delete, Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.fr-fr.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.proofing.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.proofing.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Publisher.Publisher.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Publisher.Publisher.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.publishermui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.publishermui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.shared.Office.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.shared.Office.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Word.Word.x-none.msi.16.x-none.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Word.Word.x-none.msi.16.x-none.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.wordmui.msi.16.en-us.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.wordmui.msi.16.en-us.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\integrator.exe	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\integrator.exe.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentFallBack2016.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentFallBack2016.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentLogOn2016.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentLogOn2016.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\msoutilstat.etw.man	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\msoutilstat.etw.man.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man	Accessed File	Delete, Read, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\behavior.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\behavior.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\behavior.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\behavior.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-US\resource.xml	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-US\resource.xml.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\folder.ico	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\folder.ico.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\netfol.ico	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\netfol.ico.ozq0	Accessed File	Create, Write, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\pictures.ico	Accessed File	Delete, Read, Access	CLEAN
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\pictures.ico.ozq0	Accessed File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\resource.xml	Accessed File	Delete, Read, Access	CLEAN

Reduced dataset

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	cvtres.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	cvtres.exe	CLEAN

Process

Process Name	Commandline	Verdict
a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe	"C:\Users\kEecfMwgj\Desktop\a4fb180f23ce8454febb54cea71c28dedecb09823bee87b65aec3e144c7ad844.exe"	MALICIOUS
cvtres.exe	C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe	SUSPICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.19 / 2022-03-31 10:55:59
YARA Built-in Ruleset Version	4.4.1.19

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

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