MALICIOUS

Classifications: Ransomware | Spyware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe**
ID	#3765083
MD5	b8018958476178596817f734894ff64c
SHA1	e1cae0d2a320a2756ae1ee5d37bfe803b39853fa
SHA256	672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1
File Size	472.50 KB
Report Created	2022-03-08 16:19 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 193 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 725 files by appending the extension ".cuba".			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: The Bat!, AbleFTP, Windows Mail, git, Internet Explorer / Edge.			
4/5	Reputation	Known malicious file	2	-
	• The sample itself is a known malicious file. • Reputation analysis labels file "C:\!!FAQ for Decryption!!.txt" as "Mal/Generic-S".			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe tries to read sensitive data of ftp application "AbleFTP" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive mail data	2	-
	• (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe tries to read sensitive data of mail application "Windows Mail" by file. • (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe tries to read sensitive data of mail application "The Bat!" by file.			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\lcl0t-.gif".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\lcl0t-.gif.cuba".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.cuba".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i640.hash".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i640.hash.cuba".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i641033.hash".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i641033.hash.cuba".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.cuba".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.cuba".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\ar-sa\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\bg-bg\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\cs-cz\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\da-dk\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\de-de\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\el-gr\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\es-es\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\et-ee\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fi-fi\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fr-fr\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\main\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\numbers\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\web\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\he-il\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\hr-hr\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\hu-hu\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\hwrcustomization\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\it-it\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\ja-jp\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\ko-kr\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\lt-lt\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\lv-lv\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\nb-no\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\nl-nl\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\pl-pl\!!faq for decryption!!.txt".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe modifies "c:\program files\common files\microsoft shared\ink\pt-br\!!faq for decryption!!.txt".

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Changes folder appearance	75	-

- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\program files\common files\microsoft shared\stationery".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\program files".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\program files (x86)\common files\microsoft shared\stationery".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\program files (x86)".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\ringtones".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\accessibility".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\system tools".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\tablet pc".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\accessories\windows powershell".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\administrative tools".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\games".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\maintenance".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\all users\microsoft\windows\start menu\programs\startup".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\1nbur4hr".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\6asvn7j7".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\d68g7bij".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\feeds cache\kqmhsvkd".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\burn\burn".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\history".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows\history\history.ie5".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows mail\stationery".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\libraries".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\recent".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\sendto".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessories\accessibility".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessories".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessories\system tools".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\administrative tools".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\maintenance".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\startup".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\contacts".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\desktop".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\documents".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\downloads".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\favorites".
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe changes the appearance of folder "c:\users\default\favorites\links".

Score	Category	Operation	Count	Classification
1/5	Persistence	Installs system startup script or application	6	-

- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe adds "c:\users\all users\microsoft\windows\start menu\programs\startup\!!faq for decryption!!.txt" to Windows startup folder.
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe adds "c:\users\all users\microsoft\windows\start menu\programs\startup\desktop.ini.cuba" to Windows startup folder.
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe adds "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\startup\!!faq for decryption!!.txt" to Windows startup folder.
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe adds "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\startup\desktop.ini.cuba" to Windows startup folder.
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe adds "c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\startup\!!faq for decryption!!.txt" to Windows startup folder.
- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe adds "c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\startup\desktop.ini.cuba" to Windows startup folder.

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

- (Process #1) 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe resolves 40 API functions by name.

Mitre ATT&CK Matrix

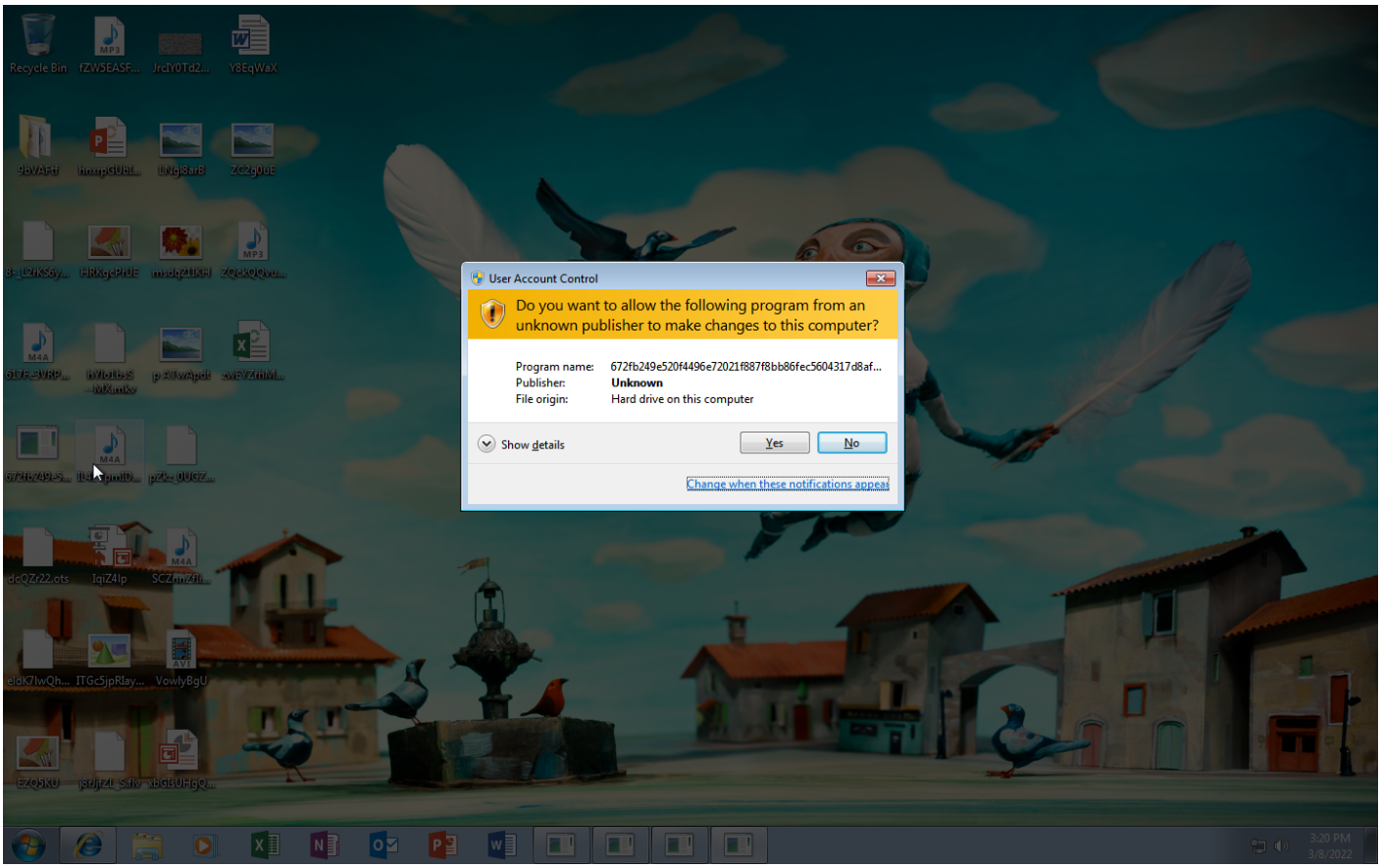
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1036 Masquerading	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119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

Sample Information

ID	#3765083
MD5	b8018958476178596817f734894ff64c
SHA1	e1cae0d2a320a2756ae1ee5d37bfe803b39853fa
SHA256	672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1
SSDeep	12288:nZqE25BWr6q6zNPrSyg8A7YNpQH/vRoV:nZqEGBdqirVxCY4HnRU
ImpHash	d9dc90dd06110fc79f0b74983e7fb09d
File Name	672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe
File Size	472.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-03-08 16:19 (UTC+1)
Analysis Duration	00:01:35
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	1
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: 672fb249e520f4496e72021f887f8bb86fec5604317d8af...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

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

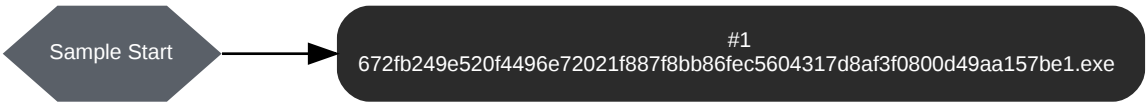
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 46281, Reason: Analysis Target
Unmonitor End Time	End Time: 142532, Reason: Terminated by Timeout
Monitor duration	96.25s
Return Code	Unknown
PID	3840
Parent PID	1928
Bitness	32 Bit

Dropped Files (104)

File Name	File Size	SHA256	YARA Match
C:\!!FAQ for Decryption!!.txt	371 bytes	36b34162ae4c570c441bfb09c81fe04d23cf752bc7a488de45d16961b7a4ba58	✗
C:\program files\common files\lcl0t-.gif	48.54 KB	725215934615864a339da52c471d3a59ec72c57f36a6e389d95326d9cfed07b9	✗
C:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml	5.04 KB	fa339e3dda5855c1affb7bc1a0c45f120219ce1d28c09689221b72a094fcc39c	✗
C:\program files\common files\microsoft shared\clicktorun\i640.hash	1.10 KB	ab51ba0dbdf5e2505c1bf494981d5348a0ee08d8124d5465e8340e7cd3c0d6d5	✗
C:\program files\common files\microsoft shared\clicktorun\i641033.hash	1.10 KB	47540f2d77a351813e18d29f3f39c2843d7c6da5eb182d4ea125b4627b0c78c8	✗
C:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml	5.67 KB	45bc6e00342de41c3470d478c0cd9987128556384c8eb156e5f73bb46dcd75b2	✗
C:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml	5.35 KB	6d65b64503fd83244ecfe948a3cfe7c9c1e309bb2441488a7a241a7b2eee954a	✗
C:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppobjs-spp-plugin-manifest-signed.xrm-ms	10.18 KB	ec00958de5cd5b5124941bd1224e6b6c714d03f7dbe613d2e82a894d5831d3a3	✗
C:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppwmi.mof	47.95 KB	0a3ab4af117961c4bc867ee1286ee59b975accbb45f8e494cc06bd15c1c2b509	✗
C:\program files\common files\microsoft shared\stationery\desktop.ini	1.63 KB	9cf370a508a1a040c5ed263516e815771f08832f53f62b6bc1ff715e3f06d564	✗
C:\program files\common files\n94j0b1q.jpg	65.36 KB	421cef89814f9a0eebd26f117bf3a833c00a9e56e424994eaa57c898b3aa4698	✗
C:\program files\common files\uxvb6tnruw.bmp	12.50 KB	ccb041fe02bde7248cc037272bf3e912be75f8d5f5b0094fc610961501d9052b	✗
C:\program files\desktop.ini	1.17 KB	a5525c7ecc0de611a2e72949aad658bf806356231f741672a24d7683a6f3df0d	✗
C:\program files\internet explorer\signup\install.ins	1.45 KB	bd4ca842a622f7dde309e719e4c714b938755d81d7bdadeaa5f89dce645c1a95	✗
C:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.targets	5.62 KB	85dcc930c6fcfe7b127115ea57e95e4437ce38e226d4f36f4767cfbce1f965f8	✗
C:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.visualbasic.targets	6.06 KB	6c560480596281720b28e65e161307f75b286353d91cb2c2f0494dc5a2937bcb	✗
C:\program files\reference assemblies\microsoft\framework\v3.0\redistlist\frameworklist.xml	7.96 KB	1b2b29f0080e5a16bf1bdf988fd7ae8b25a1908458c19aa2e6b4c107cf9a6d3e	✗
C:\program files\reference assemblies\microsoft\framework\v3.0\winfxlist.xml	3.52 KB	76909e52a55b4a18fc4ea99032ebc5692c2484dab09d131be1530b5bbb535fee	✗

File Name	File Size	SHA256	YARA Match
C:\program files\windows sidebar\settings.ini	1.08 KB	1d3fcb3f39f7af8e6313fd4f051e1fa9c7cb4652e2beb5164198780bd4201dfe	✗
C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.format.ps1xml	17.09 KB	3d4e0ebb2271f113c9f5ac8bea00383d243be3a99deec487092698a0de6902b6	✗
C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.psd1	3.24 KB	2db4e7f44507f5f96351a099bb0aa7966d91f509e9d3c4f01c4b230f1dd0d85c	✗
C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packageproviderfunctions.psm1	11.40 KB	8786dbc313abb52b4c55176e8aff23878cc86cb94abc16e86408d1757626ffb7	✗
C:\program files\windowspowershell\modules\powershellget\1.0.0.1\en-us\psget.resource.psd1	74.59 KB	7b554cab2b81ccb010510c5a612eb0c2a03bf509cf72ec2658ed2b073c55ac97	✗
C:\program files\windowspowershell\modules\powershellget\1.0.0.1\powershellget.psd1	5.22 KB	1bf8d441261b194ce6b30d814eb4932a9924c542d6a5fb7433c118b1c8d0d915	✗
C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.format.ps1xml	9.06 KB	18ce9fd1d899b601e6ac09c71851d6e66e14f236695dbe600952bb4e41ad649f	✗
C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.resource.psd1	78.26 KB	c2fc2590e8c890310005877fe068ef60656716345e11d78deae6491463bb4966	✗
C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psmodule.psm1	563.67 KB	9a82ba8fa54cdeb2a8d4ccd84e83d78d287ccd9175cc8fe10b60706b5457cdef	✗
C:\program files (x86)\common files\designer\msaddndr.olb	16.61 KB	346e0b63c5850b023e0c2524fa5f7f8245cd909b7168040ebe3463c899c850b0	✗
C:\users\keecfmwgj\appdata\roaming\microsoft\word\startup\!!FAQ for Decryption!!.txt	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\program files (x86)\common files\microsoft shared\office16\office setup controller\pkeyconfig-office.xrm-ms	577.68 KB	de836d1bcf0b4eff8ece81c514d97178327bc40648536f4fa02cd56f98544431	✗
C:\program files (x86)\common files\microsoft shared\stationery\desktop.ini	1.63 KB	e1a4f6b07cb66e80c9131d9581d6a1e8bc7873d12d5831350148db3181f63da3	✗
C:\program files (x86)\common files\microsoft shared\vsta\appinfodocument\addins.store	10.43 KB	aff8c7535bcde8c4b692e36bc2237d4ed7c89a79ddafb9e1df75dc4a7561269b	✗
C:\program files (x86)\common files\microsoft shared\vsta\pipeline.v10.0\pipelinesegments.store	128.44 KB	023e8260e5cf0034e47dc9b18a865c325245de4bab7fbcf1839bf90f5c7d45da	✗
C:\program files (x86)\common files\microsoft shared\vsta\vstofiles.cat	89.94 KB	36688f3c93ecd0e56da3b3766a784c377e86f8f333ccbb3705133667 22c6babb	✗
C:\program files (x86)\common files\microsoft shared\vsto\actionspane3.xsd	1.13 KB	24967d460039578df6937f2a9f60f402cb55adbac04c931dd7280fdd9a621420	✗
C:\program files (x86)\common files\microsoft shared\vsto\vstoee100.tlb	17.15 KB	79cdbe99aa18e3539c12c28d92f402c6c834ccea34d215f19f23970627ef00da	✗
C:\program files (x86)\common files\microsoft shared\vsto\vstoee90.tlb	22.14 KB	793e2d0333dc5d5cc30f477058fbf53cf01eeae609dbd7244db61aaf84af44cf	✗
C:\program files (x86)\desktop.ini	1.17 KB	45c528e0a53b1e9714b5f399dce5bc3db594b0960eb5c58d2acd68518c647e61	✗
C:\program files (x86)\internet explorer\signup\install.ins	1.45 KB	491de445c2c943fd5fff88dbf997ed78624fd470cd275f3ee7b6e852306fba3a	✗
C:\program files (x86)\microsoft.net\redistlist\assemblylist_4_client.xml	16.35 KB	5ecff5f9a8628cd14054f6be1f89d1d1eb5a47b194d7c00396ce8df754691b7e	✗
C:\program files (x86)\microsoft.net\redistlist\assemblylist_4_extended.xml	9.03 KB	d259c6b40cce002d6d878280cfc73bf5c97e412671ab6573b3b406d7dc2f2d1d	✗
C:\program files (x86)\msbuild\microsoft\windows workflow foundation\v3.0\workflow.targets	5.62 KB	401b12bf141485ead1d6aad315ca921c42bdd25294e0b231df356c8e0f1b55c6	✗
C:\program files (x86)\msbuild\microsoft\windows workflow foundation\v3.0\workflow.visualbasic.targets	6.06 KB	75a02539cab0a4c6dd9de69744e5e56bef49a87552b075705fe49866a63ba1cd	✗
C:\program files (x86)\reference assemblies\microsoft\framework\v3.0\redistlist\frameworklist.xml	6.55 KB	02c8f444c4c148cd276e2c9c40d2557d8b757f55c48fdddd9a5e7ae348d054cf	✗

File Name	File Size	SHA256	YARA Match
C:\program files (x86)\reference assemblies\microsoft\framework\v3.0\winfxlist.xml	3.52 KB	786e8497fcc8be68533454b88a811c4a0170cbef516723221a9686c6ec5f4169	✗
C:\program files (x86)\windows sidebar\settings.ini	1.08 KB	57134596fc4840d0bfd1896877b07e415003bf2dde32431caf82135e201098ee	✗
C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.format.ps1xml	17.09 KB	4f9f9523e6f08f00dcd83c4eb33d6dc3440cd82490056d2649000beff1661f09	✗
C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.psd1	3.24 KB	ce62b4cec6826b2a3f977101f43eaf591602592be6fd320ac72264f8c8ab3c80	✗
C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packageproviderfunctions.psm1	11.40 KB	01e9b775cdee876bac3c7091d2df8f6474cf87e07a736ce0a1866bda6d44e7b4	✗
C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\en-us\psget.resource.psd1	74.59 KB	f8c874633176cbab75c91a42c6e12bdfad4ea56c484778e048706239e4b4402b	✗
C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\powershellget.psd1	5.22 KB	dfc11fe224c1bba531de057f0ceb83ef68ef72aab1d2b8443080d98c1411d968	✗
C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psget.format.ps1xml	9.06 KB	c7a510c648ec48d9273b16662640deb290b5e19423e921b9dc2c436851687452	✗
C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psget.resource.psd1	78.26 KB	bbe162ef778005d79ee17b3ba0ca61ff72511d30de6b1ab9ca04670a019e67e2	✗
C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psmodule.psm1	563.67 KB	4b83656aa7dc7f28aa530c3b76fba35bf515f48489ee91ffc51b96494a73f208	✗
-	12.78 KB	9931fe1fcd2c046c207c1deada4240b268f41de10a25589ed733c706d6c39f2f	✗
-	218.50 KB	b9495a9726b9e57fc523a9ecef5ca0176ec254981adea8e2c17f4c82ee6319ef	✗
-	202.48 KB	15d5d9716d231e17d8f4d5df0223c15795af7aeefaac6b5cb1b0c6f596a3f354	✗
-	488.78 KB	34623495e664bf1ebd5c78d2988796936a8ab21669b467f551a2c818409294af	✗
-	15.32 KB	c271b5e1066889d89c43c0d452cc03ef0b76392a9f7506dc137b993267d30097	✗
-	1.00 KB	78d54d107c1bbd6a43e3362144c20ce303c3523726f20486ea12c91553f6033d	✗
-	853.77 KB	bbacc1dbc419a84a90cd948015a0af72e6cac7ebec403fa2724c2c6840cfcbac	✗
-	2.93 KB	806c1b95f7c46dcebdce2936e55944381238bae67d86ac0c5060bde0f0091776	✗
-	2.35 KB	ad71f6df064fd63dfa065e290cdae17f7f397414fbb68eac2d9b387be59c7dff	✗
-	22.85 KB	ee2d901b29d4132bcc3a63f542c4c8ce4829c339a9491e926c1d4eb71270ecc6	✗
-	1.10 KB	f12e0db3de540e832fa65189ffb4f72d7648d3736f3c58c45e126dfc2e03c434	✗
-	865.46 KB	521057a9c3633d63ff6255375092fb46e77421cc1f542301d9ad2f2c179a8999	✗
-	21.53 KB	888d509b4f130633657c6104d2894dfc7401bf4fc93db5974f94c51da94c8e2c	✗
-	1.10 KB	924486ae97c963f6ebaf437afac9d67c90d9eba0916c82efdabd91044e957495	✗
-	3630.45 KB	54f6592be3606edea2c3433263135c47459805cdb2d68805e4db48b28ebf1da0	✗
-	1.60 KB	9c0b12852dae83e841950342705ae67207fe12b7d8ecd200a5de643323375743	✗

File Name	File Size	SHA256	YARA Match
-	4819.01 KB	62754e2c26093b69fed1b760c61d5a29cb0ff34b77d17b2f6afac6fde2ca9584	✗
-	1.60 KB	77dc45b59b2a402ea20424c5e3d1ca8f06e4aaa3b12f8f5e3b0077128b1a7cf2	✗
-	3025.26 KB	7a768c911f9e08dfab8c8f38a02bfd659a0a073b1a6bdcb58546facc546f0e1c	✗
-	276.53 KB	d858d3fe165c1dda7337749dcc85153218b70e95477a57d640f8bcb372af536f	✗
-	38.88 KB	404eb33fded46d8cb5fb45e0ee22e7f24dc53d4efb837e94133027b10fab8f68	✗
-	57.07 KB	de8e8bccfd2559f681ea13667876fb46c22af8d5d91a54ee8ae32821480bcf33	✗
-	2.99 KB	82a4824675b26fc4f7aa54555983d7389ec58e4c949560501ef09b9be21153c8	✗
-	17.26 KB	366b7836fa80aa991230aa48d21f34084d13d8256457d498ba7adb07d49617b6	✗
-	10.58 KB	16d5852bce39628dbe21eec6313b6d0f2f78c48140f47fb4bb410c15d6fe9187	✗
-	233.30 KB	cbe62c3d3941e889b25b92833ab5c3b1d0749b62d2fecdb2c662d21a33d5ee5c	✗
-	35.20 KB	0b03a61e39d3eca72b4b82cb3080578c27a1cfd83d759efdd5412d8fdec96a8b	✗
-	36.76 KB	cd7ff67ad6fbb413b4b9bfe98bebe2859c0d199567cf7c7d1ff8756d4accfc33	✗
-	6.99 KB	c14eac01de8ff23469ee086fc7e6550f8f41d69d4f90a68a9490104e107c6d82	✗
-	88.46 KB	888493670841c4c4b4702f8d91532134662253acda96d475fa9109342c4ed92c	✗
-	23.78 KB	019c4e7c4a042ef8a28848583d0ab499cf76d686ec40d114dcb63e843afcb293	✗
-	22.44 KB	feadb8bad767f4e35e561a857cf34c1fa842afd1be9c18a56bf0e27d5234017d	✗
-	2.99 KB	e240a236f6e06519809c898cfbe5ea8a6717aa858421c5164eed1cc0483aa57a	✗
-	105.38 KB	31b4c74282ec3845623a86d47ebb00b2ccf7206bad38280f0fcfd02bdbf92bf9	✗
-	2746.82 KB	74e422c61807d2b99c8551df45b2f2cd1b039eb9b344cf5f9f896d07b3d7517c	✗
-	10240.00 KB	f724af1bc3325d26ff26b1fbb25ea718a1ceac9afaf8b93addc28f503cdf25a5	✗
-	10240.00 KB	b10b561fa53dcad4f8346f3d4d764841a1ec801db683c9c2ab3e5aa9fb2f3d95	✗
-	5089.92 KB	9ecebb04e6adb22fdc8ac15076040a20abcdaa73db015b0512812400f92ee3dd	✗
-	5665.29 KB	bf5b5b6dc76fd38cfcde6453062c6ef3936b89df5374c152cf6b7e2cbc5f3edf	✗
-	5501.25 KB	f1eafcc020518f96baf4dc7a90011664b56c014aa92c319625eec06e6a014d97	✗
-	5458.28 KB	a882b2fb55c47f9078f835b46e3c1fa41dfc6305190bbcb52a1c1787ee767597	✗
-	5034.02 KB	ea8ff2b3ea80003adb6055255d73fd06b78664225a24c25f831d931380636bf3	✗
-	4818.28 KB	06fe60f9080bc0a07318dfd79d789be573796baac518e16671099931fc2418a2	✗
C:\users\default\appdata\local\microsoft\windows mail\backup\new\windowsmail.msmessagestore	2073.00 KB	43643d78420f6aea28603cb94cdec7bd81121cc528c1d53c8298f18a26926b9f	✗
C:\users\default\appdata\local\microsoft\windows mail\windowsmail.msmessagestore	2065.00 KB	4b3b548746cb98e4f5ff91dd19805b3044c1b84e6e32b6afcc9d80000a770da6	✗

File Name	File Size	SHA256	YARA Match
C:\users\keecfmwgj\appdata\local\microsoft\media player\sync playlists\en-us\00010c6e\03_music_rated_at_4_or_5_stars.wpl	2.24 KB	53d039416d22a51357bd8f050f38673c3241adc457f1bab8013ff862e6a3188b	✗
C:\users\keecfmwgj\appdata\local\microsoft\onedrive\17.3.4604.0120\pt-pt\filesync.localizedresources.dll.mui	76.66 KB	259b239402eaf9c7db3771069c323022ce4e70b9ab7d126d46fcaec7d4968298	✗
C:\users\keecfmwgj\appdata\local\microsoft\windows mail\backup\new\windowsmail.msmessagestore	2073.00 KB	96e3455913a04103445637e380fcfb313f5dd25ff2e6bfe42bc329b8f4ba31d4	✗
C:\users\keecfmwgj\appdata\local\microsoft\windows mail\windowsmail.msmessagestore	2065.00 KB	05709736aff4af770675940046c5c69cd577f08e33a9c809aebc9d4be83fd6e7	✗
C:\users\keecfmwgj\appdata\roaming\microsoft\document building blocks\1033\16\built-in building blocks.dotx	3620.19 KB	a888d30db4fa9eb6f9e3f2ae4a1f7b949888bc362e522fd56b52db82b4e67df6	✗

Host Behavior

Type	Count
System	6
Module	68
File	8384
Environment	1
-	11

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1	C:\Users\kEecfMwgj\Desktop\672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe	Sample File	472.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
36b34162ae4c570c441bfb09c81fe04d23cf752bc7a488de45d16961b7a4ba58	C:\program files\windows sidebar\gadgets\clock.gadget\!!FAQ for Decryption!!.txt, C:\program files\dvd maker\shared\dvdstyles\rect... ...edistlist\!!FAQ for Decryption!!.txt, C:\program files\windows sidebar\gadgets\weather.gadget\en-us\css\!!FAQ for Decryption!!.txt	Dropped File	371 bytes	text/plain	Access, Create, Write	MALICIOUS
7252159346158 64a339da52c471d3a59ec72c57f36a6e389d95326d9cfed07b9	C:\program files\common files\lcl0t-.gif.cuba, C:\program files\common files\lcl0t-.gif	Modified File	48.54 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
fa339e3dda5855c1affb7bc1a0c45f120219ce1d28c09689221b72a094fcc39c	C:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.cuba, C:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml	Modified File	5.04 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
ab51ba0dbdf5e2505c1bf494981d5348a0ee08d8124d5465e8340e7cd3c0d6d5	C:\program files\common files\microsoft shared\clicktorun\i640.hash.cuba, C:\program files\common files\microsoft shared\clicktorun\i640.hash	Modified File	1.10 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
47540f2d77a351813e18d29f3f39c2843d7c6da5eb182d4ea125b4627b0c78c8	C:\program files\common files\microsoft shared\clicktorun\i641033.hash.cuba, C:\program files\common files\microsoft shared\clicktorun\i641033.hash	Modified File	1.10 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
45bc6e00342de41c3470d478c0cd9987128556384c8eb156e5f73bb46dcd75b2	C:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml, C:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.cuba	Modified File	5.67 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
6d65b64503fd83244ecfe948a3cfe7c9c1e309bb2441488a7a241a7b2eee954a	C:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.cuba, C:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml	Modified File	5.35 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
ec00958de5cd5b5124941bd1224e6b6c714d03f7dbe613d2e82a894d5831d3a3	C:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppobjs-spp-plugin-manifest-signed.xrm-ms, C:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppobjs-spp-plugin-manifest-signed.xrm-ms.cuba	Modified File	10.18 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
0a3ab4af117961c4bc867ee1286ee59b975accbb45f8e494cc06bd15c1c2b509	C:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppwmi.mof.cuba, C:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppwmi.mof	Modified File	47.95 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
9cf370a508a1a040c5ed263516e815771f08832f53f62b6bc1ff715e3f06d564	C:\program files\common files\microsoft shared\stationery\desktop.ini.cuba, C:\program files\common files\microsoft shared\stationery\desktop.ini	Modified File	1.63 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
421cef89814f9a0eebd26f117bf3a833c00a9e56e424994eaa57c898b3aa4698	C:\program files\common files\n94j0b1q.jpg, C:\program files\common files\n94j0b1q.jpg.cuba	Modified File	65.36 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
ccb041fe02bde7248cc037272bf3e912be75f8d5f5b0094fc610961501d9052b	C:\program files\common files\uxvb6tnruw.bmp.cuba, C:\program files\common files\uxvb6tnruw.bmp	Modified File	12.50 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a5525c7ecc0de611a2e72949aad658bf806356231f741672a24d7683a6f3df0d	C:\program files\desktop.ini.cuba, C:\program files\desktop.ini	Modified File	1.17 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
bd4ca842a622f7dde309e719e4c714b938755d81d7bdadeaa5f89dce645c1a95	C:\program files\internet explorer\signup\install.ins.cuba, C:\program files\internet explorer\signup\install.ins	Modified File	1.45 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
85dcc930c6fcfe7b127115ea57e95e4437ce38e226d4f36f4767cfbce1f965f8	C:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.targets, C:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.targets.cuba	Modified File	5.62 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
6c560480596281720b28e65e161307f75b286353d91cb2c2f0494dc5a2937bcb	C:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.visualbasic.targets.cuba, C:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.visualbasic.targets	Modified File	6.06 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
1b2b29f0080e5a16bf1bdf988fd7ae8b25a1908458c19aa2e6b4c107cf9a6d3e	C:\program files\reference assemblies\microsoft\framework\v3.0\redistlist\frameworklist.xml.cuba, C:\program files\reference assemblies\microsoft\framework\v3.0\redistlist\frameworklist.xml	Modified File	7.96 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
76909e52a55b4a18fc4ea99032ebc5692c2484dab09d131be1530b5bbb535fee	C:\program files\reference assemblies\microsoft\framework\v3.0\winfxlist.xml, C:\program files\reference assemblies\microsoft\framework\v3.0\winfxlist.xml.cuba	Modified File	3.52 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
1d3fcb3f39f7af8e6313fd4f051e1fa9c7cb4652e2beb5164198780bd4201dfe	C:\program files\windows sidebar\settings.ini, C:\program files\windows sidebar\settings.ini.cuba	Modified File	1.08 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
3d4e0ebb2271f113c9f5ac8bea00383d243be3a99deec487092698a0de6902b6	C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.format.ps1xml, C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.format.ps1xml.cuba	Modified File	17.09 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
2db4e7f44507f5f96351a099bb0aa7966d91f509e9d3c4f01c4b230f1dd0d85c	C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.psd1, C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.psd1.cuba	Modified File	3.24 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
8786dbc313abb52b4c55176e8aff23878cc86cb94abc16e86408d1757626ffb7	C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packageproviderfunctions.psm1, C:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packageproviderfunctions.psm1.cuba	Modified File	11.40 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
7b554cab2b81ccb010510c5a612eb0c2a03bf509cf72ec2658ed2b073c55ac97	C:\program files\windowspowershell\modules\powershellget\1.0.0.1\en-us\psget.resource.psd1, C:\program files\windowspowershell\modules\powershellget\1.0.0.1\en-us\psget.resource.psd1.cuba	Modified File	74.59 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
1bf8d441261b194ce6b30d814eb4932a9924c542d6a5fb7433c118b1c8d0d915	C:\program files\windowspowershell\modules\powershellget\1.0.0.1\powershellget.psd1.cuba, C:\program files\windowspowershell\modules\powershellget\1.0.0.1\powershellget.psd1	Modified File	5.22 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
18ce9fd1d899b601e6ac09c71851d6e66e14f236695dbe600952bb4e41ad649f	C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.format.ps1xml, C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.format.ps1xml.cuba	Modified File	9.06 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c2fc2590e8c890310005877fe068ef60656716345e11d78deae6491463bb4966	C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.resource.psd1, C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.resource.psd1.cuba	Modified File	78.26 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
9a82ba8fa54cdeb2a8d4ccd84e83d78d287ccd9175cc8fe10b60706b5457cdef	C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psmodule.psm1.cuba, C:\program files\windowspowershell\modules\powershellget\1.0.0.1\psmodule.psm1	Modified File	563.67 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
346e0b63c5850b023e0c2524fa5f7f8245cd909b7168040ebe3463c899c850b0	C:\program files (x86)\common files\designer\msaddndr.olb.cuba, C:\program files (x86)\common files\designer\msaddndr.olb	Modified File	16.61 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
de836d1bcf0b4eff8ece81c514d97178327bc40648536f4fa02cd56f98544431	C:\program files (x86)\common files\microsoft shared\office16\office setup controller\pkeyconfig-office.xrm-ms, C:\program files (x86)\common files\microsoft shared\office16\office setup controller\pkeyconfig-office.xrm-ms.cuba	Modified File	577.68 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
e1a4f6b07cb66e80c9131d9581d6a1e8bc7873d12d5831350148db3181f63da3	C:\program files (x86)\common files\microsoft shared\stationery\desktop.ini.cuba, C:\program files (x86)\common files\microsoft shared\stationery\desktop.ini	Modified File	1.63 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
aff8c7535bcde8c4b692e36bc2237d4ed7c89a79ddafb9e1df75dc4a7561269b	C:\program files (x86)\common files\microsoft shared\vsta\appinfodocument\addins.store, C:\program files (x86)\common files\microsoft shared\vsta\appinfodocument\addins.store.cuba	Modified File	10.43 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
023e8260e5cf0034e47dc9b18a865c325245de4bab7fbcf1839bf90f5c7d45da	C:\program files (x86)\common files\microsoft shared\vsta\pipeline.v10.0\pipelinesegments.store, C:\program files (x86)\common files\microsoft shared\vsta\pipeline.v10.0\pipelinesegments.store.cuba	Modified File	128.44 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
36688f3c93ecd0e56da3b3766a784c377e86f8f333ccbb370513366722c6babb	C:\program files (x86)\common files\microsoft shared\vsta\vstofiles.cat.cuba, C:\program files (x86)\common files\microsoft shared\vsta\vstofiles.cat	Modified File	89.94 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
24967d460039578df6937f2a9f60f402cb55adbac04c931dd7280fdd9a621420	C:\program files (x86)\common files\microsoft shared\vsto\actionspane3.xsd.cuba, C:\program files (x86)\common files\microsoft shared\vsto\actionspane3.xsd	Modified File	1.13 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
79cdbe99aa18e3539c12c28d92f402c6c834ccea34d215f19f23970627ef00da	C:\program files (x86)\common files\microsoft shared\vsto\vstoee100.tlb.cuba, C:\program files (x86)\common files\microsoft shared\vsto\vstoee100.tlb	Modified File	17.15 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
793e2d0333dc5d5cc30f477058fbf53cf01eeae609dbd7244db61aaf84af44cf	C:\program files (x86)\common files\microsoft shared\vsto\vstoee90.tlb, C:\program files (x86)\common files\microsoft shared\vsto\vstoee90.tlb.cuba	Modified File	22.14 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
45c528e0a53b1e9714b5f399dce5bc3db594b0960eb5c58d2acd68518c647e61	C:\program files (x86)\desktop.ini.cuba, C:\program files (x86)\desktop.ini	Modified File	1.17 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
491de445c2c943fd5fff88dbf997ed78624fd470cd275f3ee7b6e852306fba3a	C:\program files (x86)\internet explorer\signup\install.ins.cuba, C:\program files (x86)\internet explorer\signup\install.ins	Modified File	1.45 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
5ecff5f9a8628cd14054f6be1f89d1d1eb5a47b194d7c00396ce8df754691b7e	C:\program files (x86)\microsoft.net\redistlist\assemblylist_4_client.xml.cuba, C:\program files (x86)\microsoft.net\redistlist\assemblylist_4_client.xml	Modified File	16.35 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d259c6b40cce002d6d878280cfc73bf5c97e412671ab6573b3b406d7dc2f2d1d	C:\program files (x86)\microsoft.net\redistlist\assemblylist_4_extended.xml, C:\program files (x86)\microsoft.net\redistlist\assemblylist_4_extended.xml.cuba	Modified File	9.03 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
401b12bf141485ead1d6aad315ca921c42bdd25294e0b231df356c8e0f1b55c6	C:\program files (x86)\msbuild\microsoft\windows workflow foundation\v3.0\workflow.targets.cuba, C:\program files (x86)\msbuild\microsoft\windows workflow foundation\v3.0\workflow.targets	Modified File	5.62 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
75a02539cab0a4c6dd9de69744e5e56bef49a87552b075705fe49866a63ba1cd	C:\program files (x86)\msbuild\microsoft\windows workflow foundation\v3.0\workflow.visualbasic.targets.cuba, C:\program files (x86)\msbuild\microsoft\windows workflow foundation\v3.0\workflow.visualbasic.targets	Modified File	6.06 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
02c8f444c4c148cd276e2c9c40d2557d8b757f55c48fdddd9a5e7ae348d054cf	C:\program files (x86)\reference assemblies\microsoft\framework\v3.0\redistlist\frameworklist.xml, C:\program files (x86)\reference assemblies\microsoft\framework\v3.0\redistlist\frameworklist.xml.cuba	Modified File	6.55 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
786e8497fcc8be68533454b88a811c4a0170cbef516723221a9686c6ec5f4169	C:\program files (x86)\reference assemblies\microsoft\framework\v3.0\winfxlist.xml.cuba, C:\program files (x86)\reference assemblies\microsoft\framework\v3.0\winfxlist.xml	Modified File	3.52 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
57134596fc4840d0bfd1896877b07e415003bf2dde32431caf82135e201098ee	C:\program files (x86)\windows sidebar\settings.ini.cuba, C:\program files (x86)\windows sidebar\settings.ini	Modified File	1.08 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
4f9f9523e6f08f00dcd83c4eb33d6dc3440cd82490056d2649000beff1661f09	C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.format.ps1xml.cuba, C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.format.ps1xml	Modified File	17.09 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
ce62b4cec6826b2a3f977101f43eaf591602592be6fd320ac72264f8c8ab3c80	C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.psd1.cuba, C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.psd1	Modified File	3.24 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
01e9b775cdee876bac3c7091d2df8f6474cf87e07a736ce0a1866bda6d44e7b4	C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packageproviderfunctions.psm1.cuba, C:\program files (x86)\windowspowershell\modules\packagemanagement\1.0.0.1\packageproviderfunctions.psm1	Modified File	11.40 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
f8c874633176cbab75c91a42c6e12bdfad4ea56c484778e048706239e4b4402b	C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\en-us\psget.resource.psd1.cuba, C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\en-us\psget.resource.psd1	Modified File	74.59 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
dfc11fe224c1bba531de057f0ceb83ef68ef72aab1d2b8443080d98c1411d968	C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\powershellget.psd1, C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\powershellget.psd1.cuba	Modified File	5.22 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
c7a510c648ec48d9273b16662640deb290b5e19423e921b9dc2c436851687452	C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psget.format.ps1xml.cuba, C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psget.format.ps1xml	Modified File	9.06 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
bbe162ef778005d79ee17b3ba0ca61ff72511d30de6b1ab9ca04670a019e67e2	C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psget.resource.psd1.cuba, C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psget.resource.psd1	Modified File	78.26 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
4b83656aa7dc7f28aa530c3b76fba35bf515f48489ee91ffc51b96494a73f208	C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psmodule.psm1.cuba, C:\program files (x86)\windowspowershell\modules\powershellget\1.0.0.1\psmodule.psm1	Modified File	563.67 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
9931fe1fcd2c046c207c1deada4240b268f41de10a25589ed733c706d6c39f2f	C:\users\all users\microsoft\assistance\client\1.0\en-us\help_cvalidator.h1d.cuba, C:\users\all users\microsoft\assistance\client\1.0\en-us\help_cvalidator.h1d	Modified File	12.78 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
b9495a9726b9e57fc523a9ecef5ca0176ec254981adea8e2c17f4c82ee6319ef	C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mkwd_assetid.h1w.cuba, C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mkwd_assetid.h1w	Modified File	218.50 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
15d5d9716d231e17d8f4d5df0223c15795af7aeefaac6b5cb1b0c6f596a3f354	C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mkwd_bestbet.h1w.cuba, C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mkwd_bestbet.h1w	Modified File	202.48 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
34623495e664bf1ebd5c78d2988796936a8ab21669b467f551a2c818409294af	C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mtoc_help.h1h, C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mtoc_help.h1h.cuba	Modified File	488.78 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
c271b5e1066889d89c43c0d452cc03ef0b76392a9f7506dc137b993267d30097	C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mvalidator.h1d, C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mvalidator.h1d.cuba	Modified File	15.32 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
78d54d107c1bbd6a43e3362144c20ce303c3523726f20486ea12c91553f6033d	C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mvalidator.lck, C:\users\all users\microsoft\assistance\client\1.0\en-us\help_mvalidator.lck.cuba	Modified File	1.00 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
bbacc1dbc419a84a90cd948015a0af72e6cac7ebec403fa2724c2c6840cfcbac	C:\users\all users\microsoft\assistance\client\1.0\en-us\help{9daa54e8-cd95-4107-8e7f-ba3f24732d95}.h1q, C:\users\all users\microsoft\assistance\client\1.0\en-us\help{9daa54e8-cd95-4107-8e7f-ba3f24732d95}.h1q.cuba	Modified File	853.77 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
806c1b95f7c46dcebdce2936e55944381238bae67d86ac0c5060bde0f0091776	C:\users\all users\microsoft\clicktorun\deploymentconfig.0.xml.cuba, C:\users\all users\microsoft\clicktorun\deploymentconfig.0.xml	Modified File	2.93 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
ad71f6df064fd63dfa065e290cdae17f7f397414fbb68eac2d9b387be59c7dff	C:\users\all users\microsoft\clicktorun\deploymentconfig.2.xml.cuba, C:\users\all users\microsoft\clicktorun\deploymentconfig.2.xml	Modified File	2.35 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
ee2d901b29d4132bcc3a63f542c4c8ce4829c339a9491e926c1d4eb71270ecc6	C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\masterdescriptor.en-us.xml.cuba, C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\masterdescriptor.en-us.xml	Modified File	22.85 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
f12e0db3de540e832fa65189ffb4f72d7648d3736f3c58c45e126dfc2e03c434	C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\s321033.hash.cuba, C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\s321033.hash	Modified File	1.10 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
521057a9c3633d63ff6255375092fb46e77421cc1f542301d9ad2f2c179a8999	C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\stream.x86.en-us.man.dat.cuba, C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\en-us.16\stream.x86.en-us.man.dat	Modified File	865.46 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
888d509b4f130633657c6104d2894dfc7401bf4fc93db5974f94c51da94c8e2c	C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\masterdescriptor.x-none.xml, C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\masterdescriptor.x-none.xml.cuba	Modified File	21.53 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
924486ae97c963f6ebaf437afac9d67c90d9eba0916c82efdabd91044e957495	C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\s320.hash.cuba, C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\s320.hash	Modified File	1.10 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
54f6592be3606edea2c3433263135c47459805cdb2d68805e4db48b28ebf1da0	C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\stream.x86.x-none.man.dat.cuba, C:\users\all users\microsoft\clicktorun\e728f99d-05d1-4020-9ece-6de2ec414166\x-none.16\stream.x86.x-none.man.dat	Modified File	3630.45 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
9c0b12852dae83e841950342705ae67207fe12b7d8ecd200a5de643323375743	C:\users\all users\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b1... ...ta\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\deploymentconfiguration.xml.cuba	Modified File	1.60 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
62754e2c26093b69fed1b760c61d5a29cb0ff34b77d17b2f6afac6fde2ca9584	C:\users\all users\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b1... ...torun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\manifest.xml.cuba	Modified File	4819.01 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
77dc45b59b2a402ea20424c5e3d1ca8f06e4aaa3b12f8f5e3b0077128b1a7cf2	C:\users\all users\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b1... ...atalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\userdeploymentconfiguration.xml.cuba	Modified File	1.60 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
7a768c911f9e08dfab8c8f38a02bfd659a0a073b1a6bdcb58546facc546f0e1c	C:\users\all users\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b1... ...ktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\usermanifest.xml	Modified File	3025.26 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
d858d3fe165c1dda7337749dcc85153218b70e95477a57d640f8bcb372af536f	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\airspace.etw.man.cuba, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\airspace.etw.man	Modified File	276.53 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
404eb33fded46d8cb5fb45e0ee22e7f24dc53d4efb837e94133027b10fab8f68	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.access.access.x-none.msi.16.x-none.xml.... ... C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.access.access.x-none.msi.16.x-none.xml	Modified File	38.88 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
de8e8bccfd2559f681ea13667876fb46c22af8d5d91a54ee8ae32821480bcf33	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmui.msi.16.en-us.xml.cuba, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmui.msi.16.en-us.xml	Modified File	57.07 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
82a4824675b26fc4f7aa54555983d7389ec58e4c949560501ef09b9be21153c8	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmuiset.msi.16.en-us.xml.cuba, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmuiset.msi.16.en-us.xml	Modified File	2.99 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
366b7836fa80aa991230aa48d21f34084d13d8256457d498ba7adb07d49617b6	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcf.dcf.x-none.msi.16.x-none.xml.cuba, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcf.dcf.x-none.msi.16.x-none.xml	Modified File	17.26 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
16d5852bce39628dbe21eec6313b6d0f2f78c48140f47fb4bb410c15d6fe9187	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcfmui.msi.16.en-us.xml.cuba, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcfmui.msi.16.en-us.xml	Modified File	10.58 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
cbe62c3d3941e889b25b92833ab5c3b1d0749b62d2fecdb2c662d21a33d5ee5c	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excel.excel.x-none.msi.16.x-none.xml, C... ...\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excel.excel.x-none.msi.16.x-none.xml.cuba	Modified File	233.30 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
0b03a61e39d3eca72b4b82cb3080578c27a1cfd83d759efdd5412d8fdec96a8b	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excelmui.msi.16.en-us.xml.cuba, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excelmui.msi.16.en-us.xml	Modified File	35.20 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
cd7ff67ad6fbb413b4b9bfe98bebe2859c0d199567cf7c7d1ff8756d4accfc33	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groove.groove.x-none.msi.16.x-none.xml.... ... C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groove.groove.x-none.msi.16.x-none.xml	Modified File	36.76 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
c14eac01de8ff23469ee086fc7e6550f8f41d69d4f90a68a9490104e107c6d82	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groovemui.msi.16.en-us.xml, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groovemui.msi.16.en-us.xml.cuba	Modified File	6.99 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
888493670841c4c4b4702f8d91532134662253acda96d475fa9109342c4ed92c	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lync.lync.x-none.msi.16.x-none.xml.cuba, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lync.lync.x-none.msi.16.x-none.xml	Modified File	88.46 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
019c4e7c4a042ef8a28848583d0ab499cf76d686ec40d114dcb63e843afcb293	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lyncmui.msi.16.en-us.xml, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lyncmui.msi.16.en-us.xml.cuba	Modified File	23.78 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
feadb8bad767f4e35e561a857cf34c1fa842afd1be9c18a56bf0e27d5234017d	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64mui.msi.16.en-us.xml, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64mui.msi.16.en-us.xml.cuba	Modified File	22.44 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
e240a236f6e06519809c898cfbe5ea8a6717aa858421c5164eed1cc0483aa57a	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64muiset.msi.16.en-us.xml, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64muiset.msi.16.en-us.xml.cuba	Modified File	2.99 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
31b4c74282ec3845623a86d47ebb00b2ccf7206bad38280f0fcfd02bdbf92bf9	C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.officemui.msi.16.en-us.xml, C:\users\all users\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.officemui.msi.16.en-us.xml.cuba	Modified File	105.38 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
74e422c61807d2b99c8551df45b2f2cd1b039eb9b344cf5f9f896d07b3d7517c	C:\users\all users\microsoft\officesoftwareprotectionplatform\tokens.dat.cuba, C:\users\all users\microsoft\officesoftwareprotectionplatform\tokens.dat	Modified File	2746.82 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
f724af1bc3325d26ff26b1fbb25ea718a1ceac9afaf8b93addc28f503cdf25a5	C:\users\all users\microsoft\search\data\applications\windows\windows.edb.cuba, C:\users\all users\microsoft\search\data\applications\windows\windows.edb	Modified File	10240.00 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
b10b561fa53dcad4f8346f3d4d764841a1ec801db683c9c2ab3e5aa9fb2f3d95	C:\users\all users\microsoft\windows defender\definition updates\{d2b0b133-42ed-44d3-809a-46ebb62ba863}\mpasbase.vdm, C:\users\all users\microsoft\windows defender\definition updates\{d2b0b133-42ed-44d3-809a-46ebb62ba863}\mpasbase.vdm.cuba	Modified File	10240.00 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
9ecebb04e6adb22fdc8ac15076040a20abcdaa73db015b0512812400f92ee3dd	C:\users\all users\package cache\{0fa68574-690b-4b00-89aa-b28946231449}\v14.25.28508\packages\vcruntimeadditional_x86\cab1.cab, C:\users\all users\package cache\{0fa68574-690b-4b00-89aa-b28946231449}\v14.25.28508\packages\vcruntimeadditional_x86\cab1.cab.cuba	Modified File	5089.92 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
bf5b5b6dc76fd38cfcde6453062c6ef3936b89df5374c152cf6b7e2cbc5f3edf	C:\users\all users\package cache\{37b8f9c7-03fb-3253-8781-2517c99d7c00}\v11.0.61030\packages\vcruntimeadditional_amd64\cab1.cab.cuba, C:\users\all users\package cache\{37b8f9c7-03fb-3253-8781-2517c99d7c00}\v11.0.61030\packages\vcruntimeadditional_amd64\cab1.cab	Modified File	5665.29 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
f1eafcc020518f96baf4dc7a90011664b56c014aa92c319625eec06e6a014d97	C:\users\all users\package cache\{7d0b74c2-c3f8-4af1-940f-cd79ab4b2dce}\v14.25.28508\packages\vcruntimeadditional_amd64\cab1.cab.cu... ...a, C:\users\all users\package cache\{7d0b74c2-c3f8-4af1-940f-cd79ab4b2dce}\v14.25.28508\packages\vcruntimeadditional_amd64\cab1.cab	Modified File	5501.25 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a882b2fb55c47f9078f835b46e3c1fa41dfc6305190bbcb52a1c1787ee767597	C:\users\all users\package cache\{929fbd26-9020-399b-9a7a-751d61f0b942}v12.0.21005\packages\vcruntimeadditional_amd64\cab1.cab.cuba, C:\users\all users\package cache\{929fbd26-9020-399b-9a7a-751d61f0b942}v12.0.21005\packages\vcruntimeadditional_amd64\cab1.cab	Modified File	5458.28 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
ea8ff2b3ea80003adb6055255d73fd06b78664225a24c25f831d931380636bf3	C:\users\all users\package cache\{b175520c-86a2-35a7-8619-86dc379688b9}v11.0.61030\packages\vcruntimeadditional_x86\cab1.cab, C:\users\all users\package cache\{b175520c-86a2-35a7-8619-86dc379688b9}v11.0.61030\packages\vcruntimeadditional_x86\cab1.cab.cuba	Modified File	5034.02 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
06fe60f9080bc0a07318dfd79d789be573796baac518e16671099931fc2418a2	C:\users\all users\package cache\{f8cfeb22-a2e7-3971-9eda-4b11edefc185}v12.0.21005\packages\vcruntimeadditional_x86\cab1.cab.cuba, C:\users\all users\package cache\{f8cfeb22-a2e7-3971-9eda-4b11edefc185}v12.0.21005\packages\vcruntimeadditional_x86\cab1.cab	Modified File	4818.28 KB	application/octet-stream	Delete, Access, Create, Write	CLEAN
43643d78420f6aea28603cb94cdec7bd81121cc528c1d53c8298f18a26926b9f	C:\users\default\appdata\local\microsoft\windows mail\backup\new\windowsmail.msmessagestore.cuba, C:\users\default\appdata\local\microsoft\windows mail\backup\new\windowsmail.msmessagestore	Modified File	2073.00 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
4b3b548746cb98e4f5ff91dd19805b3044c1b84e6e32b6afcc9d80000a770da6	C:\users\default\appdata\local\microsoft\windows mail\windowsmail.msmessagestore, C:\users\default\appdata\local\microsoft\windows mail\windowsmail.msmessagestore.cuba	Modified File	2065.00 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
53d039416d22a51357bd8f050f38673c3241adc457f1bab8013ff862e6a3188b	C:\users\keecfmwgj\appdata\local\microsoft\media player\sync playlists\en-us\00010c6e\03_music_rated_at_4_or_5_stars.wpl, C:\users\keecfmwgj\appdata\local\microsoft\media player\sync playlists\en-us\00010c6e\03_music_rated_at_4_or_5_stars.wpl.cuba	Modified File	2.24 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
259b239402eaf9c7db3771069c323022ce4e70b9ab7d126d46fcaec7d4968298	C:\users\keecfmwgj\appdata\local\microsoft\onedrive\17.3.4604.0120\pt-pt\filesync.localizedresources.dll.mui.cuba, C:\users\keecfmwgj\appdata\local\microsoft\onedrive\17.3.4604.0120\pt-pt\filesync.localizedresources.dll.mui	Modified File	76.66 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
96e3455913a04103445637e380fcfb313f5dd25ff2e6bfe42bc329b8f4ba31d4	C:\users\keecfmwgj\appdata\local\microsoft\windows mail\backup\new\windowsmail.msmessagestore.cuba, C:\users\keecfmwgj\appdata\local\microsoft\windows mail\backup\new\windowsmail.msmessagestore	Modified File	2073.00 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN
057097364aff4af770675940046c5c69cd577f08e33a9c809aebc9d4be83fd6e7	C:\users\keecfmwgj\appdata\local\microsoft\windows mail\windowsmail.msmessagestore.cuba, C:\users\keecfmwgj\appdata\local\microsoft\windows mail\windowsmail.msmessagestore	Modified File	2065.00 KB	application/octet-stream	Create, Read, Write, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a888d30db4fa9eb6f9e3f2ae4a1f7b949888bc362e522fd56b52db82b4e67df6	C:\users\keecfmwgj\appdata\roaming\microsoft\document building blocks\1033\16\built-in building blocks.dotx.cuba, C:\users\keecfmwgj\appdata\roaming\microsoft\document building blocks\1033\16\built-in building blocks.dotx	Modified File	3620.19 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Create, Read, Write, Delete, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe	Sample File	Access	CLEAN
C:\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\bootmgr	Accessed File	Access	CLEAN
C:\bootsect.bak	Accessed File	Access	CLEAN
C:\perflogs\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\perflogs\admin\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\lcl0t-.gif	Modified File	Access, Write, Delete, Read	CLEAN
C:\program files\common files\lcl0t-.gif.cuba	Modified File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\clicktorun\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml	Modified File	Access, Write, Delete, Read	CLEAN
C:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.cuba	Modified File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\clicktorun\i640.hash	Modified File	Access, Write, Delete, Read	CLEAN
C:\program files\common files\microsoft shared\clicktorun\i640.hash.cuba	Modified File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\clicktorun\i641033.hash	Modified File	Access, Write, Delete, Read	CLEAN
C:\program files\common files\microsoft shared\clicktorun\i641033.hash.cuba	Modified File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml	Modified File	Access, Write, Delete, Read	CLEAN
C:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.cuba	Modified File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml	Modified File	Access, Write, Delete, Read	CLEAN
C:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.cuba	Modified File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\alphabet.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ar-sa\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\ar-sa\tipresx.dll.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\program files\common files\microsoft shared\ink\bg-bg\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\bg-bg\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\content.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\cs-cz\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\cs-cz\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\da-dk\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\da-dk\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\de-de\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\de-de\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\el-gr\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\el-gr\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\boxed-correct.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\boxed-delete.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\boxed-join.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\boxed-split.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\correct.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\delete.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\flicklearningwizard.exe.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\inkobj.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\inkwatson.exe.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\inputpersonalization.exe.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\ipseventlogmsg.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\ipsmigrationplugin.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\join.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\micaut.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\mip.exe.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\mshwlatin.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\rtscom.dll.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\program files\common files\microsoft shared\ink\en-us\shapecollector.exe.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\split.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\tabskb.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\tipband.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\tipres.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\en-us\tiptsf.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\es-es\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\es-es\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\et-ee\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\et-ee\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fi-fi\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fi-fi\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\flickanimation.avi	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fr-fr\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fr-fr\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad\auxbase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\ea.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\keypadbase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\kor-kor.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\keypad.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\base.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\basealtgr_rtl.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_altgr.xml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_ca.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_heb.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_jpn.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_kor.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_rtl.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\ja-jp.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\ko-kr.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-changjei.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-dayi.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-phonetic.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\main.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\numbers\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\numbers\numbase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\numbers.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\oskmenubase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred\oskpredbase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\ea-sym.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\ja-jp-sym.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\symbase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\symbols.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\web\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\program files\common files\microsoft shared\ink\fsdefinitions\web\webbase.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\fsdefinitions\web.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\he-il\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\he-il\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hr-hr\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\hr-hr\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hu-hu\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\hu-hu\tipresx.dll.mui	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwrcommonlm.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwrcustomization\!!FAQ for Decryption!!.txt	Dropped File	Access, Create, Write	CLEAN
C:\program files\common files\microsoft shared\ink\hwrenalm.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwrenclm.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwrlatinlm.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwruklm.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwruksh.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwrusalm.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\hwrusash.dat	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipscat.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipschs.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipscht.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipscsy.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsdan.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsdeu.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsen.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsesp.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsfin.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsfra.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipshrv.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsita.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsjpn.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipskor.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsnld.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsnor.xml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\program files\common files\microsoft shared\ink\ipsplk.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsptb.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsptg.xml	Accessed File	Access	CLEAN
C:\program files\common files\microsoft shared\ink\ipsrom.xml	Accessed File	Access	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe	"C:\Users\kEecfMwgj\Desktop\672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1.exe"	MALICIOUS

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	4.4.1.7 / 2021-12-15 19:11:26
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	4.4.1.14 / 2022-03-06 13:15:30
YARA Built-in Ruleset Version	4.4.1.13

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