MALICIOUS

Classifications: -

Threat Names: LockBit

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe**
ID	#4784413
MD5	889328e2cf5f5d74531b9b0a25c1871c
SHA1	d14a6e699a1f0805bd1248c80c2dc9dfccf0f403
SHA256	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f
File Size	101.50 KB
Report Created	2022-06-30 16:27 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (14 rules, 116 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies Windows automatic backups	2	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe deletes Windows volume shadow copies. • (Process #2) cmd.exe deletes Windows volume shadow copies.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 100 files by appending the extension ".lockbit".			
5/5	YARA	Malicious content matched by YARA rules	2	Ransomware
	• Rule "LockBit" from ruleset "Ransomware" has matched on the function strings for (process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe. • Rule "LockBit" from ruleset "Ransomware" has matched on a memory dump for (process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	System Modification	Disables a Windows system tool	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe disables startup repair by executing ""C:\Window... ...it /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet".			
3/5	Discovery	Reads SMB connection information	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe collects information on network shares at "Z:".			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe tries to read sensitive data of ftp application "AbleFTP" by file.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe creates mutex with name "Global\{BEF590BE-11A6-442A-A85B-656C1081E04C}".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe adds ""C"" to Windows startup via registry.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe enumerates running processes.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe starts (process #2) cmd.exe with a hidden window. • (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe starts Anonymous Process with a hidden window.			
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
	• (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe hides 1280 bytes in "HKEY_CURRENT_USER\SOFTWARE\LockBit\full".			

Score	Category	Operation	Count	Classification
1/5	System Modification	Modifies application directory	100	-

- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\44-vnbkTRNEu.gif.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\C2RHeartbeatConfig.xml.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\i640.hash.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\i641033.hash.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeUpdateSchedule.xml.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\ServiceWatcherSchedule.xml.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\Alphabet.xml.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\ar-SA\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\bg-BG\tipresx.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\bg-BG\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\Content.xml.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\tipresx.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\da-DK\tipresx.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\da-DK\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\de-DE\tipresx.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\de-DE\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\el-GR\tipresx.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\el-GR\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-correct.avi.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\Restore-My-Files.txt".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-delete.avi.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-join.avi.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-split.avi.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\correct.avi.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\delete.avi.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\FlickLearningWizard.exe.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InkObj.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InkWatson.exe.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InputPersonalization.exe.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\IPSEventLogMsg.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\IpsMigrationPlugin.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\join.avi.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\micaut.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "\??\C:\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\mshwLatin.dll.mui.lockbit".
- (Process #1) 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe modifies "C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\rtscom.dll.mui.lockbit".

Mitre ATT&CK Matrix

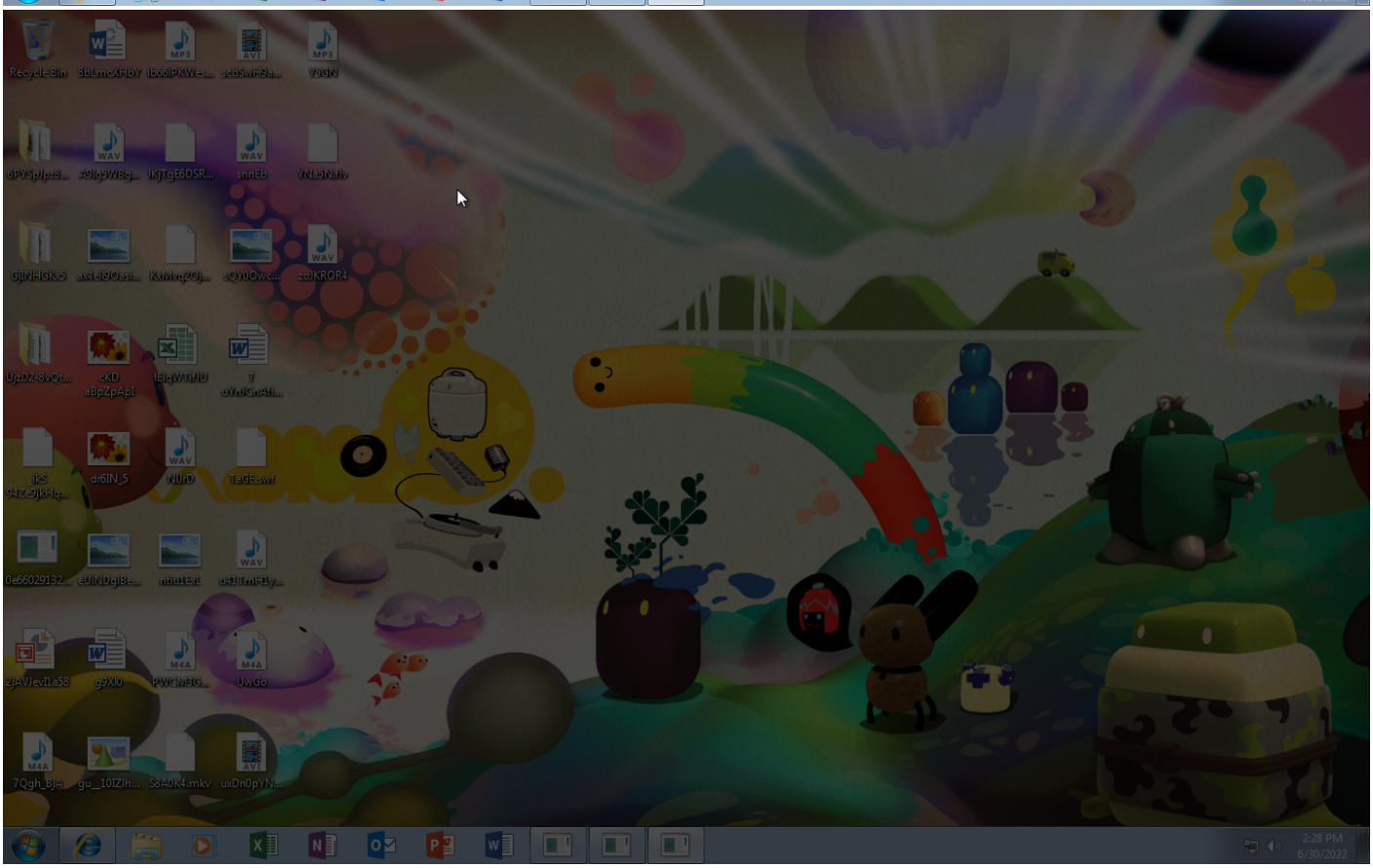
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry	#T1081 Credentials in Files	#T1057 Process Discovery		#T1119 Automated Collection			#T1490 Inhibit System Recovery
				#T1143 Hidden Window		#T1016 System Network Configuration Discovery		#T1005 Data from Local System			#T1486 Data Encrypted for Impact
						#T1049 System Network Connections Discovery					
						#T1135 Network Share Discovery					
						#T1083 File and Directory Discovery					

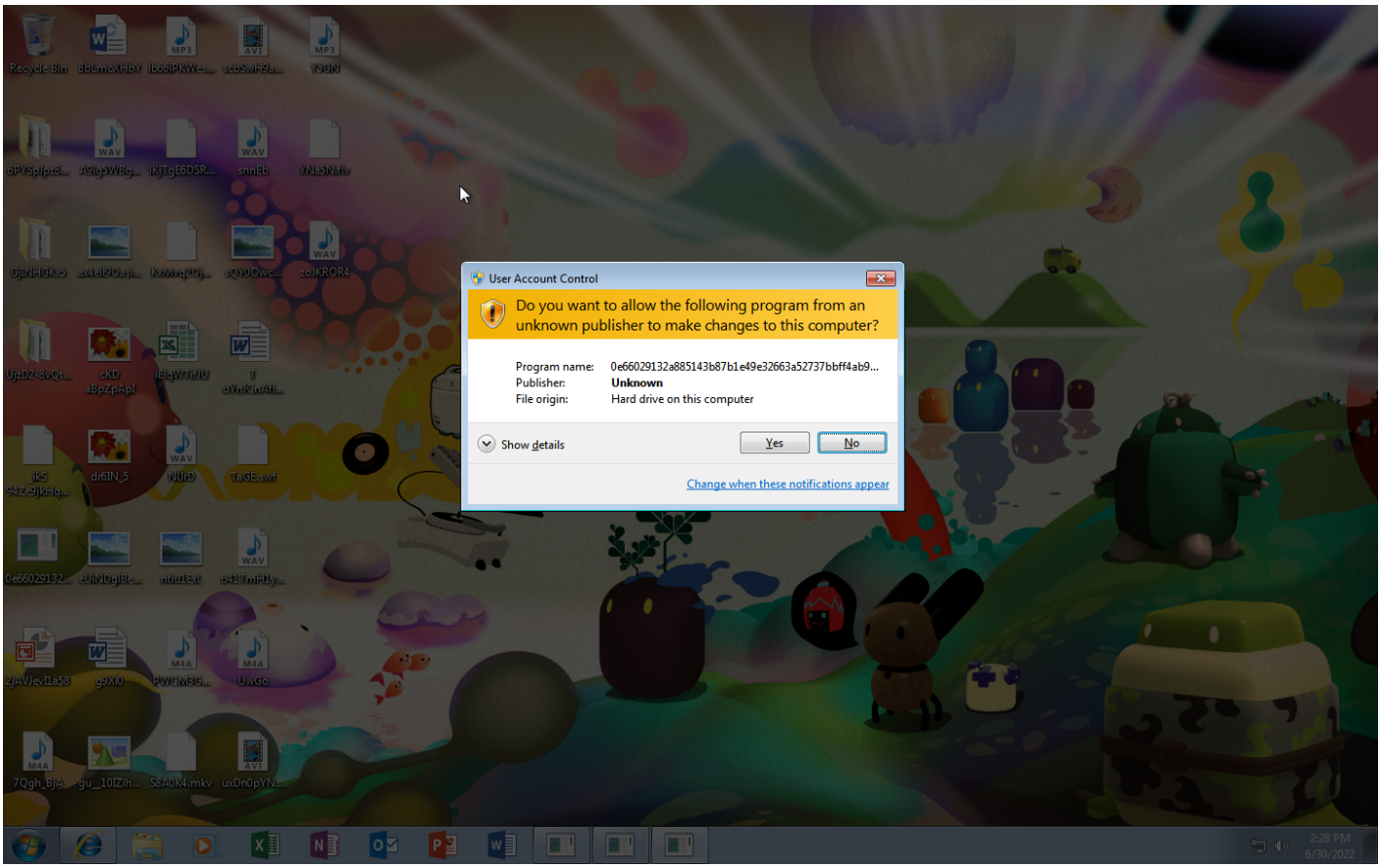
Sample Information

ID	#4784413
MD5	889328e2cf5f5d74531b9b0a25c1871c
SHA1	d14a6e699a1f0805bd1248c80c2dc9dfccf0f403
SHA256	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f
SSDeep	3072:AmD1tmtnnhf1j6VTAjIF66yRru77xHLbMqqD/txX6T:AyHWnn7WTWIF66yY8qqD/txqT
ImpHash	2430c4d884e6b7c075f835fdb6a6475c
File Name	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe
File Size	101.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-06-30 16:27 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	22
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	2





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

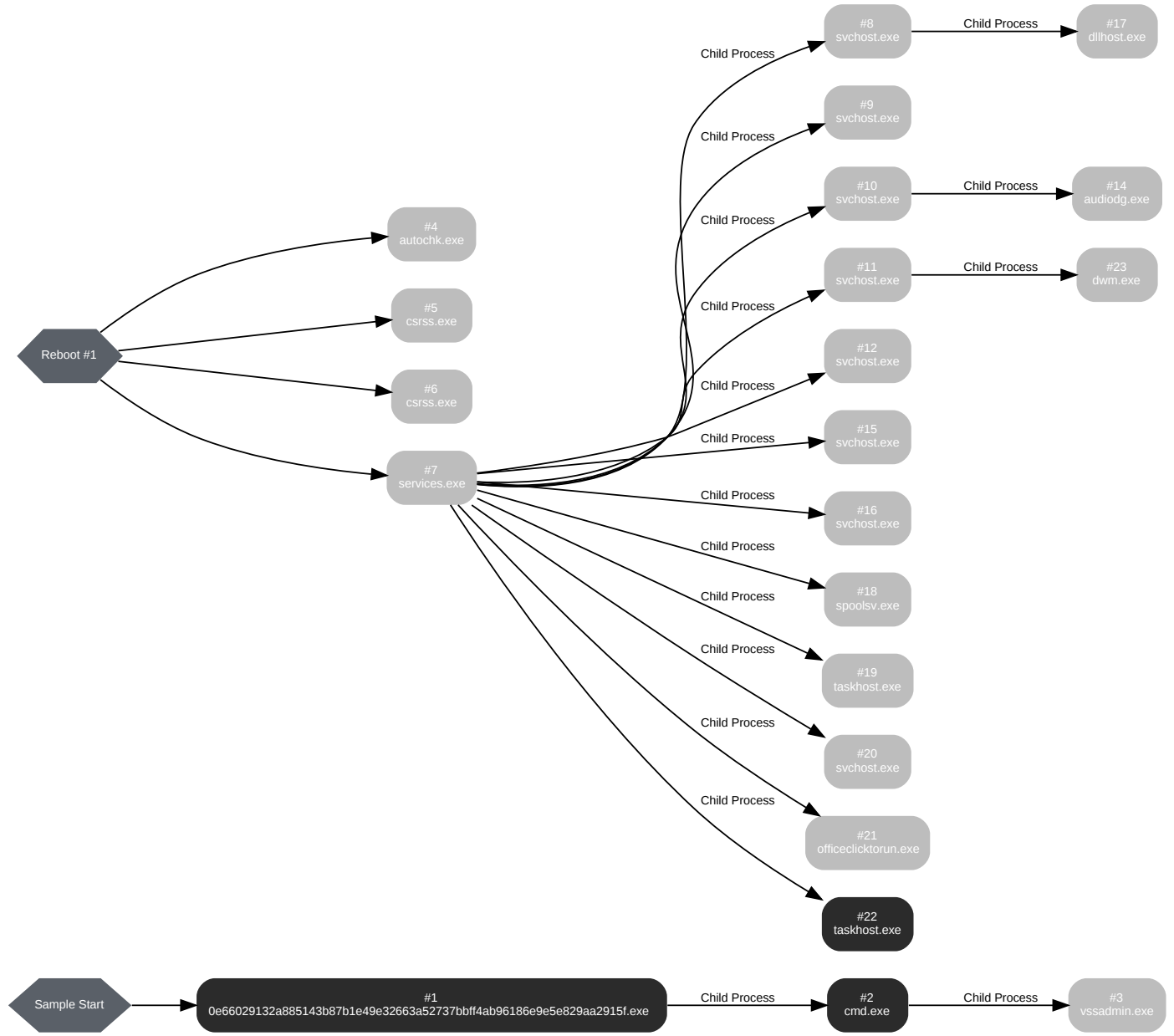
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 44052, Reason: Analysis Target
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	240.05s
Return Code	Unknown
PID	3940
Parent PID	1928
Bitness	32 Bit

Dropped Files (102)

File Name	File Size	SHA256	YARA Match
c:\program files\common files\microsoft shared\ink\en-us\join.avi.lockbit	218.52 KB	716bcafb2c66a66034f0f53b1122fc1faea285c61555a0e8d37f31a5ec4713ba	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\web.xml.lockbit	1.72 KB	9e965cb63540087b4834ee1027054e85d3c8ab822c22bf491ea0e3491e25c099	✖
c:\program files\common files\microsoft shared\ink\alphabet.xml.lockbit	774.65 KB	e37fdb873c8290d629629f02ed949606f8392a470e5e963125cacb1a634e88dc	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrenalm.dat.lockbit	731.28 KB	eae14390cebb2eeb05da088a90157a56071b90094153959ad56058a087de0a9a	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\tipresx.dll.mui.lockbit	5.02 KB	d8163ee1b2346855929ca5e2c9dfa5cdd875eac83dbca88c7446211937280490	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main.xml.lockbit	39.11 KB	d94ca372bed98d3ae531fbe1a83abe91717a5a3435e68c3d87f76c5f000fbf6c	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-changjei.xml.lockbit	11.09 KB	b7b8b7584372e5223003d20d9085b402ec77109019c675a2eeabaedbbc19e127	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipRes.dll.mui.lockbit	33.52 KB	116c3debb350ae3ab5caa7ab3be34749f922980c97679d3497cb9cca2680d358	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ipscsy.xml.lockbit	4.02 KB	5d09cab7302a19cc68a99df5221d902ab261a657e9875033be0ecec5fe2adf24	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fi-FI\tipresx.dll.mui.lockbit	5.02 KB	d827ca4d7b0da5bf2869d40dfb659e48295127a786d6ffc4819434f2e4b78705	✖
c:\program files\common files\microsoft shared\ink\en-us\correct.avi.lockbit	194.02 KB	f61d9e70394152bd49eb5d3d86efe9f18a63a1014ebfbd099379d73c2631f90f	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu.xml.lockbit	1.73 KB	a688d2f64e56196387e260282985d80b17c41321e29cd81eadf3dedb5d6e65ae	✖
c:\program files\common files\microsoft shared\ink\en-us\boxed-delete.avi.lockbit	32.52 KB	ff9a2e45351716baefba7e85b4d015a4408a31fd6d94c88178905006cf8784d8	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui.lockbit	5.02 KB	1783951e6b096e03aa1e302caf54084e053f772480ed7f3a95f0b607f623e989	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml.lockbit	2.92 KB	2322d473ad5f68712d24a70b7b28c701392c49ec9441d8c5e7ef39484f4b9a3f	✖
c:\program files\common files\microsoft shared\ink\en-us\ipseventlogmsg.dll.mui.lockbit	23.52 KB	f1c78a3c0eadf79fc5eb48608d3d842d4840d6de57d8a1ab138dafe8da91fbce	✖
c:\program files\common files\44-vnbktrneu.gif.lockbit	78.44 KB	344d37ede376887ba1f501fa360e01f578ee5d3cb481a1db1e9c814411b77b37	✖
c:\program files\common files\microsoft shared\ink\ipsesp.xml.lockbit	4.47 KB	fa5c5989856ec1c3c646e091f469d1e57e3642fa25426a378ec867183e546a72	✖

File Name	File Size	SHA256	YARA Match
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\delete.avi.lockbit	220.52 KB	14021076f9eeb9681d2e2e585136d761b5c7ca143e9e8a1060c166e972f588b4	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\rtscom.dll.mui.lockbit	4.02 KB	583fddd5dfa24a9959df1ffd0761c935c236ef85d6696b7e9d78677377a77697	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\numbers\numbase.xml.lockbit	2.72 KB	3d398f1bbfee8c4b89b625cdda8cd0ba11c7448dad43cdeb5754dba0005e6566	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_kor.xml.lockbit	2.00 KB	6993afbdd4c716f0d1e1cfbec0eb35cc8c4bd9a41e0f5750ffbdc3dd25980152	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols\ja-jp-sym.xml.lockbit	2.25 KB	7ee74ad46c0b81246c899575936dd945f11168124db8042392466f88558d25b2	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\hu-HU\Restore-My-Files.txt	929 bytes	177d51941e2085a69987af5ef7dc168694fab25cbeda0ac2b793cb3e67d5dd8c	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\tabskb.dll.mui.lockbit	4.52 KB	17ba56f48000aec9332ee8bdf3bd95187faf9066c0b40ce10be6ae21c2aad331	✖
c:\program files\common files\microsoft shared\clicktorun\i640.hash.lockbit	1.62 KB	b88dc3712345d6e1c61170a49e9ea97f24805c62c4640847154d8d26eeca26bb	✖
c:\program files\common files\microsoft shared\ink\en-us\tipband.dll.mui.lockbit	4.52 KB	e99019308c1f8dc80e416dda6e5d712e21a16eae15607028213c7bca45015e93	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrenclm.dat.lockbit	798.08 KB	ab2793f22aa67281e865fd779f4b272bf60d11b457b14db021bef25a89717e6d	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\bg-BG\tipresx.dll.mui.lockbit	5.52 KB	328dc24e58838a2287e76a4c21192ca7769bb7bf6be4d9b83b5beccc9bf09e70	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_ca.xml.lockbit	4.61 KB	894de7e5f1b4b05f96c13fb6d83c11908ad2e645dd72c5d349de8a881fc532af	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\el-GR\tipresx.dll.mui.lockbit	5.52 KB	5afef6eebc19e7c7e3621d9e7ce7054f10ab2410988c1f5c7983b91983790a37	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base.xml.lockbit	4.59 KB	7af02dd0e30b7d4b6781622f7e5c0d4698e537971ab8ace3004bed1c813e758d	✖
c:\program files\common files\microsoft shared\ink\hwruklm.dat.lockbit	2983.92 KB	74439f7b997b671c7127a993e84ae58f51c15d5e77b77f8883eed0775d58f6be	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ipscht.xml.lockbit	3.91 KB	187071538f09bfd94e0a500ea631dc97cf5bc093c686cc65d40ab90a57385474	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_altgr.xml.lockbit	4.61 KB	430dea8972661266a5408f77e363305d23d8065174f6df2588374662d72ec842	✖
c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.lockbit	6.19 KB	0414ac37585d5b4b70aaa80bb96d7751a2bddd1a76d5224c0808727f3976905f	✖
c:\program files\common files\microsoft shared\ink\hwruksh.dat.lockbit	2177.27 KB	a7e7145d2f8dd1284924debaaa06c20d290b2b3c0e55ab7cfdf3f386bec25d24	✖
c:\program files\common files\microsoft shared\ink\en-us\micaut.dll.mui.lockbit	10.02 KB	ee88100174afc061d8ca7ee83a54ffc2a350105ed16b6e97142f8d4f920bd0f1	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui.lockbit	5.52 KB	e669ad36c8a0fa44b615cd84dbb9ac76eafee441c6e6c4c073cea09afe1578db	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\ko-kr.xml.lockbit	16.27 KB	f0e2c5e36798ea02f51d5e2de2c58c0ab7d9b26c4af9c4fd4912c3b2128596a8	✖
c:\program files\common files\microsoft shared\ink\hu-hu\tipresx.dll.mui.lockbit	5.02 KB	d7e55b75eb0ca283562a7ef9883c41dcbf7b604205062b9772454b66d54ad4e6	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui.lockbit	11.52 KB	8fedd8ad67b29928b46e7e089513af839456a2b6ff69810a2b77706312db102f	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-phonetic.xml.lockbit	12.22 KB	cce525b3986c829b3ef500af425866c707a391417a8c1afbd2bce330c39a83b1	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\split.avi.lockbit	191.02 KB	84b59f0ce95e68832d5fa87fa6f1cf74bc9417839b22469a1d846a8702898046	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-split.avi.lockbit	63.02 KB	2aade3d0f04183244fb2747d908f179d5ef6e9b9af3956c0fde13edc0065c8ab	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsen.xml.lockbit	4.05 KB	a6edc65824644329e6e75a0dfee0bc50624ec6501877007276119022235 4e123	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web\webbase.xml.lockbit	2.66 KB	c7d76d8bf1d03518ae76316989c26b34c00527df220a57038ffe54bc28dd2a60	✖

File Name	File Size	SHA256	YARA Match
C:\\Program Files\Common Files\Microsoft Shared\ink\ipscat.xml.lockbit	4.05 KB	0d69e634ea24fb8ccd2dd2bd14a650efe156b3a002990f4563e23990df6eba78	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred\oskpredbase.xml.lockbit	2.42 KB	0041110e24481a211186bbf1cc593a2782ba424b5d78c0d8bf9c9f1fc9ae6f07	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\symbase.xml.lockbit	4.22 KB	b23bfd1cedb8568d7ffb3c7c076c3d89a5d30bc3d53a80fbce639fd04cda0323	✖
c:\program files\common files\microsoft shared\ink\en-us\tipresx.dll.mui.lockbit	5.02 KB	68c024ebb99d94c79ccebc58a4cac4cfc93d58c641bcccc3f852b9271c84563a	✖
c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.lockbit	5.88 KB	5fc0698756a34c6a8f4b6b79e4a8fafd914e772e510bb3e7e8ce61bed23a9ed3	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipTsf.dll.mui.lockbit	4.52 KB	464a53a27a21ca3fcfcfd5a0df34bf7485f2399db1c66a755696129b1221dbe3	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_jpn.xml.lockbit	2.31 KB	90f04406813c795ca904c11a13f8067777900892bf32cafa88035cd161a55034	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\basealtgr_rtl.xml.lockbit	1.77 KB	aa09a9dbe015a1a93fab9382ba2ee717ff64340fb71d60bc3e105bd66c4747d2	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_rtl.xml.lockbit	2.12 KB	459ecfcc63921133deffbed9258b2dedfe2c2147488859e9f0c43eb85ec167e3	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsdan.xml.lockbit	3.98 KB	5ef79e638448d68c41f71d68b54bc09e0da9a3a873eba748daa1f50aca689e27	✖
c:\program files\common files\microsoft shared\ink\de-de\tipresx.dll.mui.lockbit	5.52 KB	f8bea6dc41c9ccb7ddfc691b4f4f40dcbc0d7e82f383dac1d22538a2c8f79cf6	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\numbers.xml.lockbit	1.73 KB	b847b4fc8deda4679b2ffe3504d1467d489da486084d0a4826cf24dfe071c9f8	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\oskmenubase.xml.lockbit	1.98 KB	e050d405b6e9ceb3008c8943f9c64ba44de1eba94fbd44d864719b26d7834c38	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\et-EE\tipresx.dll.mui.lockbit	5.52 KB	9204fefbaf6e62a62bbf118f47e321f2074875b57ad2536ffdec70787787d310	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\keypadbase.xml.lockbit	2.61 KB	e835b781d2331fca8493b11e462b183fba28c13e39962e535066004f7ef5b73a	✖
c:\program files\common files\microsoft shared\ink\flickanimation.avi.lockbit	1564.39 KB	cce93243fe1ecccf9fe1e9adb51ce376a7c5f5791b17aeefa51fd9e95e33237e	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrlatinlm.dat.lockbit	1076.09 KB	cfcd61fb6e01ac119e120ffaa6446d02de0d39d1e7825b9633f67924f16534ca	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad.xml.lockbit	2.23 KB	55f4b086ebb9d22e926e69152ce57e7f18556a07663aa4aad0b0288391f76670	✖
c:\program files\common files\microsoft shared\ink\fr-fr\tipresx.dll.mui.lockbit	5.52 KB	e81bc2595d349fcecc447baccf91732c957894d459503aa0a071a87cb3e064e0	✖
c:\program files\common files\microsoft shared\ink\en-us\boxed-correct.avi.lockbit	89.02 KB	8b7b8b4839014de48937664a94c92879ec0dd037ef0fef8b2a48d24cbefdfee6	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad.xml.lockbit	1.73 KB	d0db0b2592e06268bba860d0fea1156d8eb4b5d6afee27ccafefdb931236b1a8	✖
C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\i641033.hash.lockbit	1.62 KB	41758cb9458d4c69496d57ddc6bf5d061bd8f32093774e8ebca749768519c567	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_heb.xml.lockbit	2.25 KB	b4b84a8e7333f3adb0f7c9748481396862f06b963b01e222b607f600c6f31b8c	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\da-DK\tipresx.dll.mui.lockbit	5.02 KB	f597411834957efb1543b16cd45de304f489fb95fb7d8810641e7a217d30e0f0	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ipschs.xml.lockbit	3.92 KB	47afb4bd9a06ebf073899dd8fe7416ef9b7dd9d77e3c8c84c64a73806cd3867b	✖
c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.lockbit	5.56 KB	bec7a30c02a3a6af7eec94b88e168e011bc16ccfc6c7e27b31fafa51ef4e4e00	✖
c:\program files\common files\microsoft shared\ink\ipsfra.xml.lockbit	4.09 KB	010d2279c4ef47316641a802ec93c14d6e284230614f7fc13a7abc93c942058f	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InkWatson.exe.mui.lockbit	10.52 KB	06a0d475056d67826618623ca3d16f403e66ce324225e82db99dcf54dc6d2e37	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred.xml.lockbit	1.73 KB	25cfa20995eca6f34942f2c8d3106970163d221a73afad87764d2732f79b37f2	✖

File Name	File Size	SHA256	YARA Match
c:\program files\common files\microsoft shared\ink\ipsfin.xml.lockbit	4.12 KB	ca5dda5dd53179e1d8efce6bd22574e77febc049ebf0a04573a82d3269db95d7	✖
c:\program files\common files\microsoft shared\ink\en-us\mshwlatin.dll.mui.lockbit	4.02 KB	c22163481fb87c84bd7a7c05f4798eb0e5d6c6216073ce5f2ffe35a76091aab8	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\kor-kor.xml.lockbit	1.91 KB	947865f3d39a2d9589a9a423796d14c3b425ceba33b3a400cd06a1141f7aa6c5	✖
c:\program files\common files\microsoft shared\ink\en-us\ipsmigrationplugin.dll.mui.lockbit	4.02 KB	9e436403b25f9fa297ddc623e05eb5d6fcbcab79da6a5e19cec0ae73d0d6863b	✖
c:\program files\common files\microsoft shared\ink\en-us\inputpersonalization.exe.mui.lockbit	4.02 KB	a32b189630479af819da78600a2754f7cd6c15e5d43e27303bc6313c7fc1b451	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-dayi.xml.lockbit	12.33 KB	f21f8f948c7755f5bcec6b033a8ffa74407b2bfe83fd643b9ac8b1d55a1d3026	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\ea-sym.xml.lockbit	2.25 KB	d5da7276c02eb7645b9fa2c8915d538f3f4824e0394c9b938ab5b91932e228fa	✖
c:\program files\common files\microsoft shared\ink\en-us\shapecollector.exe.mui.lockbit	44.02 KB	a2ab56f308734dd1627a87ac76ec612d973dde49a6fd930f6be2dd932e9a80aa	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\ja-jp.xml.lockbit	17.75 KB	392e91173904c9867b531bb86aff31acdd5db59daf724b4c008220312460a8c1	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrusash.dat.lockbit	4025.72 KB	42c622e07173484ed9b52a3c6229b1f363481ac02f3cbace879515b805a339b5	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols.xml.lockbit	2.09 KB	9f8a55d127dda6337a9f6ee4bed61dcda14c21371d66adc9decba497d191f661	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrcommonlm.dat.lockbit	47.05 KB	100f8564c80c388c13edda48d46ff2f545c8a3a2e4730b99c784b6fe47833cb2	✖
c:\program files\common files\microsoft shared\ink\hr-hr\tipresx.dll.mui.lockbit	5.52 KB	f809b5e7b9dbc9049bf689cbd6ad861b71489c0bc93f1144a0e0ea355b13fe1c	✖
c:\program files\common files\microsoft shared\ink\en-us\inkobj.dll.mui.lockbit	6.02 KB	00036a9256e15b1ff6d4853c87d865a7602ff4af47a1179fc793e26a62cff854	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-join.avi.lockbit	34.02 KB	776f7ec1e9b025eaafd0a0bc2e1cb0167604a44f882c3a0f15a3155426d484ec	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsdeu.xml.lockbit	4.08 KB	95a0f7048806cae844b32e64e637fc162796fa397983c3db3518e8aac1ca2db0	✖
c:\program files\common files\microsoft shared\ink\en-us\flicklearningwizard.exe.mui.lockbit	10.02 KB	7b8727d57e2bae19b4fedf15c2a6ed056e6e0245cf6a54dd400ad8513a4b16bd	✖
c:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad.xml.lockbit	1.73 KB	4d3571c4a363a9afcd08c1c9e0f342d4b0565c632ed88cf48ffe4485c288def8	✖
c:\program files\common files\microsoft shared\ink\he-il\tipresx.dll.mui.lockbit	5.02 KB	c7e9725e691f76da715ee495a82686161c0d210f278de4bf198ff10d3aa98556	✖
c:\program files\common files\microsoft shared\ink\hwrusalm.dat.lockbit	3122.31 KB	f6c70487a935d519482a1ca2e3ea7d39c61e3594834b67102009ca9180b4ba6b	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\Content.xml.lockbit	27.94 KB	aeab27c925b596d7030801c318230f034a70bb0c5a829dcedfbf438b79874682	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad\auxbase.xml.lockbit	2.92 KB	036e3b6f50095fdd7e8cda42ba932a1bae124d5c0c956f8ee39988d75706f10b	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\ea.xml.lockbit	1.89 KB	16c54cd441716efffb1928226ec3a3d1e047a873f3ef591182e35cc4b67a5c75	✖
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsita.xml.lockbit	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files\common files\microsoft shared\ink\ipshrv.xml.lockbit	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
File	1282
-	8

Type	Count
Module	476
Process	549
System	141
-	47
Registry	8
Window	1
User	1
Mutex	2

Process #2: cmd.exe

ID	2
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 75667, Reason: Child Process
Unmonitor End Time	End Time: 94709, Reason: Terminated
Monitor duration	19.04s
Return Code	1073807364
PID	4044
Parent PID	3940
Bitness	64 Bit

Host Behavior

Type	Count
Environment	4
File	5
Module	1
Process	1

Process #3: vssadmin.exe

ID	3
File Name	c:\windows\system32\vssadmin.exe
Command Line	vssadmin delete shadows /all /quiet
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81182, Reason: Child Process
Unmonitor End Time	End Time: 94693, Reason: Terminated
Monitor duration	13.51s
Return Code	1073807364
PID	4080
Parent PID	4044
Bitness	64 Bit

Process #4: autochk.exe

ID	4
File Name	c:\windows\system32\autochk.exe
Command Line	\??\C:\Windows\system32\autochk.exe *
Initial Working Directory	C:\Windows\system32
Monitor Start Time	Start Time: 149029, Reason: Autostart
Unmonitor End Time	End Time: 150549, Reason: Terminated
Monitor duration	1.52s
Return Code	0
PID	256
Parent PID	244
Bitness	64 Bit

Process #5: csrss.exe

ID	5
File Name	c:\windows\system32\csrss.exe
Command Line	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=b... ...ServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
Initial Working Directory	C:\Windows\system32
Monitor Start Time	Start Time: 153423, Reason: Autostart
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	130.68s
Return Code	Unknown
PID	312
Parent PID	304
Bitness	64 Bit

Process #6: csrss.exe

ID	6
File Name	c:\windows\system32\csrss.exe
Command Line	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=b... ...ServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
Initial Working Directory	C:\Windows\system32
Monitor Start Time	Start Time: 154823, Reason: Autostart
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	129.28s
Return Code	Unknown
PID	360
Parent PID	340
Bitness	64 Bit

Process #7: services.exe

ID	7
File Name	c:\windows\system32\services.exe
Command Line	C:\Windows\system32\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 156890, Reason: Autostart
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	127.21s
Return Code	Unknown
PID	448
Parent PID	348
Bitness	64 Bit

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 163353, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	120.75s
Return Code	Unknown
PID	556
Parent PID	448
Bitness	64 Bit

Process #9: svchost.exe

ID	9
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k RPCSS
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 169607, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	114.50s
Return Code	Unknown
PID	620
Parent PID	448
Bitness	64 Bit

Process #10: svchost.exe

ID	10
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 170419, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	113.69s
Return Code	Unknown
PID	672
Parent PID	448
Bitness	64 Bit

Process #11: svchost.exe

ID	11
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 175575, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	108.53s
Return Code	Unknown
PID	760
Parent PID	448
Bitness	64 Bit

Process #12: svchost.exe

ID	12
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 175748, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	108.36s
Return Code	Unknown
PID	784
Parent PID	448
Bitness	64 Bit

Process #14: audiodg.exe

ID	14
File Name	c:\windows\system32\audiodg.exe
Command Line	C:\Windows\system32\AUDIODG.EXE 0x2b8
Initial Working Directory	C:\Windows
Monitor Start Time	Start Time: 186660, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	97.44s
Return Code	Unknown
PID	892
Parent PID	672
Bitness	64 Bit

Process #15: svchost.exe

ID	15
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 193892, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	90.21s
Return Code	Unknown
PID	964
Parent PID	448
Bitness	64 Bit

Process #16: svchost.exe

ID	16
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k NetworkService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 199684, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	84.42s
Return Code	Unknown
PID	344
Parent PID	448
Bitness	64 Bit

Process #17: dllhost.exe

ID	17
File Name	c:\windows\system32\dllhost.exe
Command Line	C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201990, Reason: Child Process
Unmonitor End Time	End Time: 220144, Reason: Terminated
Monitor duration	18.15s
Return Code	0
PID	572
Parent PID	556
Bitness	64 Bit

Process #18: spoolsv.exe

ID	18
File Name	c:\windows\system32\spoolsv.exe
Command Line	C:\Windows\System32\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 213038, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	71.07s
Return Code	Unknown
PID	1080
Parent PID	448
Bitness	64 Bit

Process #19: taskhost.exe

ID	19
File Name	c:\windows\system32\taskhost.exe
Command Line	"taskhost.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 213960, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	70.14s
Return Code	Unknown
PID	1100
Parent PID	448
Bitness	64 Bit

Process #20: svchost.exe

ID	20
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 214520, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	69.58s
Return Code	Unknown
PID	1144
Parent PID	448
Bitness	64 Bit

Process #21: officeclicktorun.exe

ID	21
File Name	c:\program files\common files\microsoft shared\clicktorun\officeclicktorun.exe
Command Line	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 220477, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	63.63s
Return Code	Unknown
PID	1280
Parent PID	448
Bitness	64 Bit

Process #22: taskhost.exe

ID	22
File Name	c:\windows\system32\taskhost.exe
Command Line	taskhost.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 262019, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	22.09s
Return Code	Unknown
PID	1564
Parent PID	448
Bitness	64 Bit

Host Behavior

Type	Count
Registry	4
System	4

Process #23: dwm.exe

ID	23
File Name	c:\windows\system32\dwm.exe
Command Line	"C:\Windows\system32\Dwm.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 277173, Reason: Child Process
Unmonitor End Time	End Time: 284104, Reason: Terminated by timeout
Monitor duration	6.93s
Return Code	Unknown
PID	1796
Parent PID	760
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f	C:\Users\kEecfMwgj\Desktop\0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	Sample File	101.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
716bcafb2c66a66034f0f53b1122fc1faea285c61555a0e8d37f31a5ec4713ba	c:\program files\common files\microsoft shared\ink\en-us\join.avi.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\join.avi.lockbit	Dropped File	218.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
9e965cb63540087b4834ee1027054e85d3c8ab822c22bf491ea0e3491e25c099	c:\program files\common files\microsoft shared\ink\fsdefinitions\web.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web.xml.lockbit	Dropped File	1.72 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e37fdb873c8290d629629f02ed949606f8392a470e5e963125cacb1a634e88dc	c:\program files\common files\microsoft shared\ink\alphabet.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\Alphabet.xml.lockbit	Dropped File	774.65 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
eae14390cebb2eeb05da088a90157a56071b90094153959ad56058a087de0a9a	C:\\Program Files\Common Files\Microsoft Shared\ink\hwrenalm.dat.lockbit, c:\program files\common files\microsoft shared\ink\hwrenalm.dat.lockbit	Dropped File	731.28 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d8163ee1b2346855929ca5e2c9dfa5cdd875eac83dbca88c7446211937280490	C:\\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\cs-cz\tipresx.dll.mui.lockbit	Dropped File	5.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d94ca372bed98d3ae531fbe1a83abe91717a5a3435e68c3d87f76c5f000fbf6c	c:\program files\common files\microsoft shared\ink\fsdefinitions\main.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main.xml.lockbit	Dropped File	39.11 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b7b8b7584372e5223003d20d9085b402ec77109019c675a2eeabaedbbc19e127	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-changjei.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-changjei.xml.lockbit	Dropped File	11.09 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
116c3debb350ae3ab5caa7ab3be34749f922980c97679d3497cb9cca2680d358	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipRes.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\en-us\tipres.dll.mui.lockbit	Dropped File	33.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
5d09cab7302a19cc68a99df5221d902ab261a657e9875033be0ecec5fe2adf24	C:\\Program Files\Common Files\Microsoft Shared\ink\ipscsy.xml.lockbit, c:\program files\common files\microsoft shared\ink\ipscsy.xml.lockbit	Dropped File	4.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d827ca4d7b0da5bf2869d40dfb659e48295127a786d6ffc4819434f2e4b78705	C:\\Program Files\Common Files\Microsoft Shared\ink\fi-FI\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\fi-fi\tipresx.dll.mui.lockbit	Dropped File	5.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f61d9e70394152bd49eb5d3d86efe9f18a63a1014ebfbd099379d73c2631f90f	c:\program files\common files\microsoft shared\ink\en-us\correct.avi.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\correct.avi.lockbit	Dropped File	194.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a688d2f64e56196387e260282985d80b17c41321e29cd81eadf3dedb5d6e65ae	c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskmenu.xml.lockbit	Dropped File	1.73 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ff9a2e45351716baefba7e85b4d015a4408a31fd6d94c88178905006cf8784d8	c:\program files\common files\microsoft shared\ink\en-us\boxed-delete.avi.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-delete.avi.lockbit	Dropped File	32.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
1783951e6b096e03aa1e302caf54084e053f772480ed7f3a95f0b607f623e989	C:\\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\ar-sa\tipresx.dll.mui.lockbit	Dropped File	5.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
2322d473ad5f68712d24a70b7b28c701392c49ec9441d8c5e7ef39484f4b9a3f	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml.lockbit	Dropped File	2.92 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f1c78a3c0eadf79fc5eb48608d3d842d4840d6de57d8a1ab138dafe8da91fbce	c:\program files\common files\microsoft shared\ink\en-us\ipseventlogmsg.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\IPSEventLogMsg.dll.mui.lockbit	Dropped File	23.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
344d37ede376887ba1f501fa360e01f578ee5d3cb481a1db1e9c814411b77b37	c:\program files\common files\44-vnbktrneu.gif.lockbit, C:\\Program Files\Common Files\44-vnbkTRNEu.gif.lockbit	Dropped File	78.44 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
fa5c5989856ec1c3c646e091f469d1e57e3642fa25426a378ec867183e546a72	c:\program files\common files\microsoft shared\ink\ipsesp.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\ipsesp.xml.lockbit	Dropped File	4.47 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
14021076f9eeb9681d2e2e585136d761b5c7ca143e9e8a1060c166e972f588b4	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\delete.avi.lockbit, c:\program files\common files\microsoft shared\ink\en-us\delete.avi.lockbit	Dropped File	220.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
583fddd5dfa24a9959df1ffd0761c935c236ef85d6696b7e9d78677377a77697	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\rtscom.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\en-us\rtscom.dll.mui.lockbit	Dropped File	4.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
3d398f1bbfee8c4b89b625cdda8cd0ba11c7448dad43cdeb5754dba0005e6566	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\numbers\numbase.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\numbers\numbase.xml.lockbit	Dropped File	2.72 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
6993afbdd4c716f0d1e1cfbec0eb35cc8c4bd9a41e0f5750ffbdc3dd25980152	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_kor.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_kor.xml.lockbit	Dropped File	2.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
7ee74ad46c0b81246c899575936dd945f11168124db8042392466f88558d25b2	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols\ja-jp-sym.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\ja-jp-sym.xml.lockbit	Dropped File	2.25 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
177d51941e2085a69987af5ef7dc168694fab25cbeda0ac2b793cb3e67d5dd8c	C:\\Program Files\Common Files\Microsoft Shared\ink\hu-HU\Restore-My-Files.txt, C:\\Program Files\Common Files\Microsoft Shared\in... ...ared\ink\fsdefinitions\keypad\Restore-My-Files.txt, C:\\Program Files\Common Files\Microsoft Shared\ink\fi-FI\Restore-My-Files.txt	Dropped File	929 bytes	text/plain	Access, Create, Write	CLEAN
17ba56f48000aec9332ee8bdf3bd95187faf9066c0b40ce10be6ae21c2aad331	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\tabskb.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\en-us\tabskb.dll.mui.lockbit	Dropped File	4.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b88dc3712345d6e1c61170a49e9ea97f24805c62c4640847154d8d26eeca26bb	c:\program files\common files\microsoft shared\clicktorun\i640.hash.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\i640.hash.lockbit	Dropped File	1.62 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e99019308c1f8dc80e416dda6e5d712e21a16eae15607028213c7bca45015e93	c:\program files\common files\microsoft shared\ink\en-us\tipband.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipBand.dll.mui.lockbit	Dropped File	4.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ab2793f22aa67281e865fd779f4b272bf60d11b457b14db021bef25a89717e6d	C:\\Program Files\Common Files\Microsoft Shared\ink\hwrenclm.dat.lockbit, c:\program files\common files\microsoft shared\ink\hwrenclm.dat.lockbit	Dropped File	798.08 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
328dc24e58838a2287e76a4c21192ca7769bb7bf6be4d9b83b5beccc9bf09e70	C:\\Program Files\Common Files\Microsoft Shared\ink\bg-BG\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\bg-bg\tipresx.dll.mui.lockbit	Dropped File	5.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
894de7e5f1b4b05f96c13fb6d83c11908ad2e645dd72c5d349de8a881fc532af	c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_ca.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_ca.xml.lockbit	Dropped File	4.61 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
5afef6eebc19e7c7e3621d9e7ce7054f10ab2410988c1f5c7983b91983790a37	C:\\Program Files\Common Files\Microsoft Shared\ink\el-GR\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\el-gr\tipresx.dll.mui.lockbit	Dropped File	5.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
7af02dd0e30b7d4b6781622f7e5c0d4698e537971ab8ace3004bed1c813e758d	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base.xml.lockbit	Dropped File	4.59 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
74439f7b997b671c7127a993e84ae58f51c15d5e77b77f8883eed0775d58f6be	c:\program files\common files\microsoft shared\ink\hwruklm.dat.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\hwruklm.dat.lockbit	Dropped File	2983.92 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
187071538f09bfd94e0a500ea631dc97cf5bc093c686cc65d40ab90a57385474	C:\\Program Files\Common Files\Microsoft Shared\ink\ipscht.xml.lockbit, c:\program files\common files\microsoft shared\ink\ipscht.xml.lockbit	Dropped File	3.91 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
430dea8972661266a5408f77e363305d23d8065174f6df2588374662d72ec842	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_altgr.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_altgr.xml.lockbit	Dropped File	4.61 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
0414ac37585d5b4b70aaa80bb96d7751a2bddd1a76d5224c0808727f3976905f	c:\program files\common files\microsoft shared\clicktorun\officeupdatescheduler.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeUpdateSchedule.xml.lockbit	Dropped File	6.19 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a7e7145d2f8dd1284924debaaa06c20d290b2b3c0e55ab7cfdf3f386bec25d24	c:\program files\common files\microsoft shared\ink\hwruksh.dat.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\hwruksh.dat.lockbit	Dropped File	2177.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ee88100174afc061d8ca7ee83a54ffc2a350105ed16b6e97142f8d4f920bd0f1	c:\program files\common files\microsoft shared\ink\en-us\micaut.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\micaut.dll.mui.lockbit	Dropped File	10.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e669ad36c8a0fa44b615cd84dbb9ac76eafee441c6e6c4c073cea09afe1578db	C:\\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\es-es\tipresx.dll.mui.lockbit	Dropped File	5.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f0e2c5e36798ea02f51d5e2de2c58c0ab7d9b26c4af9c4fd4912c3b2128596a8	c:\program files\common files\microsoft shared\ink\fsdefinitions\main\ko-kr.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\ko-kr.xml.lockbit	Dropped File	16.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d7e55b75eb0ca283562a7ef9883c41dcbf7b604205062b9772454b66d54ad4e6	c:\program files\common files\microsoft shared\ink\hu-hu\tipresx.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\hu-HU\tipresx.dll.mui.lockbit	Dropped File	5.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
8fedd8ad67b29928b46e7e089513af839456a2b6ff69810a2b77706312db102f	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui.lockbit, c:\program files\common files\microsoft shared\ink\en-us\mip.exe.mui.lockbit	Dropped File	11.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
cce525b3986c829b3ef500af425866c707a391417a8c1afbd2bce330c39a83b1	c:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-phonetic.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-phonetic.xml.lockbit	Dropped File	12.22 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
84b59f0ce95e68832d5fa87fa6f1cf74bc9417839b22469a1d846a8702898046	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\split.avi.lockbit, c:\program files\common files\microsoft shared\ink\en-us\split.avi.lockbit	Dropped File	191.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
2aade3d0f04183244fb2747d908f179d5ef6e9b9af3956c0fde13edc0065c8ab	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-split.avi.lockbit, c:\program files\common files\microsoft shared\ink\en-us\boxed-split.avi.lockbit	Dropped File	63.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a6edc65824644329e6e75a0dfee0bc50624ec65018770072761190222354e123	C:\\Program Files\Common Files\Microsoft Shared\ink\ipsen.xml.lockbit, c:\program files\common files\microsoft shared\ink\ipsen.xml.lockbit	Dropped File	4.05 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
c7d76d8bf1d03518ae76316989c26b34c00527df220a57038ffe54bc28dd2a60	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web\webbase.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\web\webbase.xml.lockbit	Dropped File	2.66 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
0d69e634ea24fb8ccd2dd2bd14a650efe156b3a002990f4563e23990df6eba78	C:\\Program Files\Common Files\Microsoft Shared\ink\ipscat.xml.lockbit, c:\program files\common files\microsoft shared\ink\ipscat.xml.lockbit	Dropped File	4.05 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
0041110e24481a211186bbf1cc593a2782ba424b5d78c0d8bf9c9f1fc9ae6f07	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred\oskpredbase.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred\oskpredbase.xml.lockbit	Dropped File	2.42 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b23bfd1cedb8568d7ffb3c7c076c3d89a5d30bc3d53a80fbce639fd04cda0323	c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\symbase.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols\symbase.xml.lockbit	Dropped File	4.22 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
68c024ebb99d94c79ccebc58a4cac4cfc93d58c641bcccc3f852b9271c84563a	c:\program files\common files\microsoft shared\ink\en-us\tipresx.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\tipresx.dll.mui.lockbit	Dropped File	5.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5fc0698756a34c6a8f4b6b79e4a8fafd914e772e510bb3e7e8ce61bed23a9ed3	c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\ServiceWatcherSchedule.xml.lockbit	Dropped File	5.88 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
464a53a27a21ca3fcfcfd5a0df34bf7485f2399db1c66a755696129b1221dbe3	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipTsf.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\en-us\tiptsf.dll.mui.lockbit	Dropped File	4.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
90f04406813c795ca904c11a13f8067777900892bf32cafa88035cd161a55034	c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_jpn.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_jpn.xml.lockbit	Dropped File	2.31 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
aa09a9dbe015a1a93fab9382ba2ee717ff64340fb71d60bc3e105bd66c4747d2	c:\program files\common files\microsoft shared\ink\fsdefinitions\main\basealtgr_rtl.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\baseAltGr_rtl.xml.lockbit	Dropped File	1.77 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
459ecfcc63921133deffbed9258b2dedfe2c2147488859e9f0c43eb85ec167e3	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_rtl.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_rtl.xml.lockbit	Dropped File	2.12 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
5ef79e638448d68c41f71d68b54bc09e0da9a3a873eba748daa1f50aca689e27	C:\\Program Files\Common Files\Microsoft Shared\ink\ipsdan.xml.lockbit, c:\program files\common files\microsoft shared\ink\ipsdan.xml.lockbit	Dropped File	3.98 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f8bea6dc41c9ccb7ddfc691b4f4f40dcbc0d7e82f383dac1d22538a2c8f79cf6	c:\program files\common files\microsoft shared\ink\de-de\tipresx.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\de-DE\tipresx.dll.mui.lockbit	Dropped File	5.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b847b4fc8deda4679b2ffe3504d1467d489da486084d0a4826cf24dfe071c9f8	c:\program files\common files\microsoft shared\ink\fsdefinitions\numbers.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\numbers.xml.lockbit	Dropped File	1.73 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e050d405b6e9ceb3008c8943f9c64ba44de1eba94fbd44d864719b26d7834c38	c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\oskmenubase.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskmenu\oskmenubase.xml.lockbit	Dropped File	1.98 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
9204fefbaf6e62a62bbf118f47e321f2074875b57ad2536ffdec70787787d310	C:\\Program Files\Common Files\Microsoft Shared\ink\et-EE\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\et-ee\tipresx.dll.mui.lockbit	Dropped File	5.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e835b781d2331fca8493b11e462b183fba28c13e39962e535066004f7ef5b73a	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\keypadbase.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\keypadbase.xml.lockbit	Dropped File	2.61 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
cce93243fe1ecccf9fe1e9adb51ce376a7c5f5791b17aeefa51fd9e95e33237e	c:\program files\common files\microsoft shared\ink\flickanimation.avi.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\FlickAnimation.avi.lockbit	Dropped File	1564.39 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
cfcd61fb6e01ac119e120ffaa6446d02de0d39d1e7825b9633f67924f16534ca	C:\\Program Files\Common Files\Microsoft Shared\ink\hwrlatinlm.dat.lockbit, c:\program files\common files\microsoft shared\ink\hwrlatinlm.dat.lockbit	Dropped File	1076.09 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
55f4b086ebb9d22e926e69152ce57e7f18556a07663aa4aad0b0288391f76670	c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad.xml.lockbit	Dropped File	2.23 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e81bc2595d349fcecc447baccf91732c957894d459503aa0a071a87cb3e064e0	c:\program files\common files\microsoft shared\ink\fr-fr\tipresx.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fr-FR\tipresx.dll.mui.lockbit	Dropped File	5.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
8b7b8b4839014de48937664a94c92879ec0dd037ef0fef8b2a48d24cbefdfee6	c:\program files\common files\microsoft shared\ink\en-us\boxed-correct.avi.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-correct.avi.lockbit	Dropped File	89.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d0db0b2592e06268bba860d0fea1156d8eb4b5d6afee27ccafefdb931236b1a8	c:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad.xml.lockbit	Dropped File	1.73 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
41758cb9458d4c69496d57ddc6bf5d061bd8f32093774e8ebca749768519c567	C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\i641033.hash.lockbit, c:\program files\common files\microsoft shared\clicktorun\i641033.hash.lockbit	Dropped File	1.62 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b4b84a8e7333f3adb0f7c9748481396862f06b963b01e222b607f600c6f31b8c	c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_heb.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_heb.xml.lockbit	Dropped File	2.25 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f597411834957efb1543b16cd45de304f489fb95fb7d8810641e7a217d30e0f0	C:\\Program Files\Common Files\Microsoft Shared\ink\da-DK\tipresx.dll.mui.lockbit, c:\program files\common files\microsoft shared\ink\da-dk\tipresx.dll.mui.lockbit	Dropped File	5.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
47afb4bd9a06ebf073899dd8fe7416ef9b7dd9d77e3c8c84c64a73806cd3867b	C:\\Program Files\Common Files\Microsoft Shared\ink\ipschs.xml.lockbit, c:\program files\common files\microsoft shared\ink\ipschs.xml.lockbit	Dropped File	3.92 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
bec7a30c02a3a6af7eec94b88e168e011bc16ccfc6c7e27b31fafa51ef4e4e00	c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\C2RHeartbeatConfig.xml.lockbit	Dropped File	5.56 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
010d2279c4ef47316641a802ec93c14d6e284230614f7fc13a7abc93c942058f	c:\program files\common files\microsoft shared\ink\ipsfra.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\ipsfra.xml.lockbit	Dropped File	4.09 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
06a0d475056d67826618623ca3d16f403e66ce324225e82db99dcf54dc6d2e37	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InkWatson.exe.mui.lockbit, c:\program files\common files\microsoft shared\ink\en-us\inkwatson.exe.mui.lockbit	Dropped File	10.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
25cfa20995eca6f34942f2c8d3106970163d221a73afad87764d2732f79b37f2	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred.xml.lockbit	Dropped File	1.73 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ca5dda5dd53179e1d8efce6bd22574e77febc049ebf0a04573a82d3269db95d7	c:\program files\common files\microsoft shared\ink\ipsfin.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\ipsfin.xml.lockbit	Dropped File	4.12 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c22163481fb87c84bd7a7c05f4798eb0e5d6c6216073ce5f2ffe35a76091aab8	c:\program files\common files\microsoft shared\ink\en-us\mshwlatin.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\mshwLatin.dll.mui.lockbit	Dropped File	4.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
947865f3d39a2d9589a9a423796d14c3b425ceba33b3a400cd06a1141f7aa6c5	c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\kor-kor.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\kor-kor.xml.lockbit	Dropped File	1.91 KB	application/x-dosexec	Access, Create, Read, Write	CLEAN
9e436403b25f9fa297ddc623e05eb5d6fcbcab79da6a5e19cec0ae73d0d6863b	c:\program files\common files\microsoft shared\ink\en-us\ipsmigrationplugin.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\IpsMigrationPlugin.dll.mui.lockbit	Dropped File	4.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a32b189630479af819da78600a2754f7cd6c15e5d43e27303bc6313c7fc1b451	c:\program files\common files\microsoft shared\ink\en-us\inputpersonalization.exe.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InputPersonalization.exe.mui.lockbit	Dropped File	4.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f21f8f948c7755f5bcec6b033a8ffa74407b2bfe83fd643b9ac8b1d55a1d3026	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-dayi.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-dayi.xml.lockbit	Dropped File	12.33 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d5da7276c02eb7645b9fa2c8915d538f3f4824e0394c9b938ab5b91932e228fa	c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\ea-sym.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols\ea-sym.xml.lockbit	Dropped File	2.25 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a2ab56f308734dd1627a87ac76ec612d973dde49a6fd930f6be2dd932e9a80aa	c:\program files\common files\microsoft shared\ink\en-us\shapecollector.exe.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\ShapeCollector.exe.mui.lockbit	Dropped File	44.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
392e91173904c9867b531bb86aff31acdd5db59daf724b4c008220312460a8c1	c:\program files\common files\microsoft shared\ink\fsdefinitions\main\ja-jp.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\ja-jp.xml.lockbit	Dropped File	17.75 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
42c622e07173484ed9b52a3c6229b1f363481ac02f3cbace879515b805a339b5	C:\\Program Files\Common Files\Microsoft Shared\ink\hwrusash.dat.lockbit, c:\program files\common files\microsoft shared\ink\hwrusash.dat.lockbit	Dropped File	4025.72 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
9f8a55d127dda6337a9f6ee4bed61dcda14c21371d66adc9decba497d191f661	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols.xml.lockbit	Dropped File	2.09 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
100f8564c80c388c13edda48d46ff2f545c8a3a2e4730b99c784b6fe47833cb2	C:\\Program Files\Common Files\Microsoft Shared\ink\hwrcommonlm.dat.lockbit, c:\program files\common files\microsoft shared\ink\hwrcommonlm.dat.lockbit	Dropped File	47.05 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f809b5e7b9dbc9049bf689cbd6ad861b71489c0bc93f1144a0e0ea355b13fe1c	c:\program files\common files\microsoft shared\ink\hr-hr\tipresx.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\hr-HR\tipresx.dll.mui.lockbit	Dropped File	5.52 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
00036a9256e15b1ff6d4853c87d865a7602ff4af47a1179fc793e26a62cff854	c:\program files\common files\microsoft shared\ink\en-us\inkobj.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InkObj.dll.mui.lockbit	Dropped File	6.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
776f7ec1e9b025eaafd0a0bc2e1cb0167604a44f882c3a0f15a3155426d484ec	C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-join.avi.lockbit, c:\program files\common files\microsoft shared\ink\en-us\boxed-join.avi.lockbit	Dropped File	34.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
95a0f7048806cae844b32e64e637fc162796fa397983c3db3518e8aac1ca2db0	C:\\Program Files\Common Files\Microsoft Shared\ink\ipsdeu.xml.lockbit, c:\program files\common files\microsoft shared\ink\ipsdeu.xml.lockbit	Dropped File	4.08 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
7b8727d57e2bae19b4fedf15c2a6ed056e6e0245cf6a54dd400ad8513a4b16bd	c:\program files\common files\microsoft shared\ink\en-us\flicklearningwizard.exe.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\FlickLearningWizard.exe.mui.lockbit	Dropped File	10.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
4d3571c4a363a9afcd08c1c9e0f342d4b0565c632ed88cf48ffe4485c288def8	c:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad.xml.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\osknumpad.xml.lockbit	Dropped File	1.73 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
c7e9725e691f76da715ee495a82686161c0d210f278de4bf198ff10d3aa98556	c:\program files\common files\microsoft shared\ink\he-il\tipresx.dll.mui.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\he-IL\tipresx.dll.mui.lockbit	Dropped File	5.02 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f6c70487a935d519482a1ca2e3ea7d39c61e3594834b67102009ca9180b4ba6b	c:\program files\common files\microsoft shared\ink\hwrusalm.dat.lockbit, C:\\Program Files\Common Files\Microsoft Shared\ink\hwrusalm.dat.lockbit	Dropped File	3122.31 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
aeab27c925b596d7030801c318230f034a70bb0c5a829dcedfbf438b79874682	C:\\Program Files\Common Files\Microsoft Shared\ink\Content.xml.lockbit, c:\program files\common files\microsoft shared\ink\content.xml.lockbit	Dropped File	27.94 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
036e3b6f50095fdd7e8cda42ba932a1bae124d5c0c956f8ee39988d75706f10b	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad\auxbase.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad\auxbase.xml.lockbit	Dropped File	2.92 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
16c54cd441716efffb1928226ec3a3d1e047a873f3ef591182e35cc4b67a5c75	C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\ea.xml.lockbit, c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\ea.xml.lockbit	Dropped File	1.89 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\kor-kor.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\hwruklm.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrlatinlm.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_kor.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\osknumpad\osknumpadbase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\split.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\alphabet.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_ca.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\hwruksh.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrenalm.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\bg-BG\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\oskmenubase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad\auxbase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\he-il\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipsfra.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\correct.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsen.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\boxed-correct.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fi-FI\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fr-fr\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\ja-jp.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\Content.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-dayi.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\delete.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsdeu.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\et-EE\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\44-vnbktrneu.gif.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_altgr.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-split.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files\common files\microsoft shared\ink\en-us\micaut.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\numbers.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\keypadbase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\flicklearningwizard.exe.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\shapecollector.exe.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-changjei.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\el-GR\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\tabskb.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipscsy.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipschs.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\tipband.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\inputpersonalization.exe.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-join.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsita.xml.lockbit	Dropped File, Accessed File, Not Extracted	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\inkobj.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\de-de\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipshrv.xml.lockbit	Dropped File, Accessed File, Not Extracted	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\ko-kr.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_jpn.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\InkWatson.exe.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrcommonlm.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols\ja-jp-sym.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\numbers\numbase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\symbase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\rtscom.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipscat.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\ea-sym.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\ipseventlogmsg.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\i641033.hash.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\boxed-delete.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\ipsmigrationplugin.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrusash.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\hu-hu\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\hwrusalm.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred\oskpredbase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipTsf.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipsesp.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ar-SA\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipscht.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\join.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\da-DK\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web\webbase.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\web.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\base_heb.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\clicktorun\i640.hash.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\mshwlatin.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\basealtgr_rtl.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsdan.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrenclm.dat.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\flickanimation.avi.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\ea.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\hr-hr\tipresx.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipsfin.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\zh-phonetic.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_rtl.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipRes.dll.mui.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad.xml.lockbit	Dropped File, Accessed File	Access, Create, Read, Write	MALICIOUS
C:\\Program Files\Common Files\Microsoft Shared\ink\de-DE\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\ServiceWatcherSchedule.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\hwrenalm.dat	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\en-US\IpsMigrationPlugin.dll.mui	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\IPSEventLogMsg.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\zh-phonetic.xml	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\el-GR\tipresx.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\et-EE\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\hwruklm.dat	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\tabskb.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\ipscat.xml	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred\oskpredbase.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\osknumpad\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeUpdateSchedule.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\C2RHeartbeatConfig.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\es-ES\tipresx.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\TipRes.dll.mui	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\ipscsy.xml	Accessed File	Access, Delete	CLEAN

File Name	Category	Operations	Verdict
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskmenu\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\correct.avi	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\44-vnbkTRNEu.gif	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\ipsesp.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\numbers.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\keypadbase.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\ipsita.xml	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols\symbase.xml	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\hr-HR\tipresx.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\hu-HU\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad\ea.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad.xml	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\el-GR\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\auxpad\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ClickToRun\i640.hash	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\micaut.dll.mui	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\hwrcommonlm.dat	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\tipresx.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\cs-CZ\Restore-My-Files.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols\ja-jp-sym.xml	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\FlickAnimation.avi	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\de-DE\tipresx.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-delete.avi	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\en-US\rtscom.dll.mui	Accessed File	Access, Delete	CLEAN
C:\\Program Files\Common Files\Microsoft Shared\ink\ipshrv.xml	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main\base_altgr.xml	Accessed File	Access, Delete	CLEAN
\??\C:\Program Files\Common Files\Microsoft Shared\ink\en-US\InkObj.dll.mui	Accessed File	Access, Delete	CLEAN

Reduced dataset

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.88	-	-	-	CLEAN
192.168.0.139	-	-	-	CLEAN
192.168.0.199	-	-	-	CLEAN
192.168.0.217	-	-	-	CLEAN
192.168.0.189	-	-	-	CLEAN
192.168.0.71	-	-	-	CLEAN
192.168.0.180	-	-	-	CLEAN
192.168.0.178	-	-	-	CLEAN
192.168.0.219	-	-	-	CLEAN
192.168.0.77	-	-	-	CLEAN
192.168.0.136	-	-	-	CLEAN
192.168.0.140	-	-	-	CLEAN
192.168.0.241	-	-	-	CLEAN
192.168.0.218	-	-	-	CLEAN
192.168.0.112	-	-	-	CLEAN
192.168.0.86	-	-	-	CLEAN
192.168.0.73	-	-	-	CLEAN
192.168.0.67	-	-	-	CLEAN
192.168.0.63	-	-	-	CLEAN
192.168.0.102	-	-	-	CLEAN
192.168.0.215	-	-	-	CLEAN
192.168.0.133	-	-	-	CLEAN
192.168.0.196	-	-	-	CLEAN
192.168.0.250	-	-	-	CLEAN
192.168.0.216	-	-	-	CLEAN
192.168.0.228	-	-	-	CLEAN
192.168.0.243	-	-	-	CLEAN
192.168.0.121	-	-	-	CLEAN
192.168.0.222	-	-	-	CLEAN
192.168.0.107	-	-	-	CLEAN
192.168.0.124	-	-	-	CLEAN
192.168.0.160	-	-	-	CLEAN
192.168.0.207	-	-	-	CLEAN
192.168.0.126	-	-	-	CLEAN
192.168.0.221	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
192.168.0.181	-	-	-	CLEAN
192.168.0.188	-	-	-	CLEAN
192.168.0.246	-	-	-	CLEAN
192.168.0.144	-	-	-	CLEAN
192.168.0.230	-	-	-	CLEAN
192.168.0.90	-	-	-	CLEAN
192.168.0.156	-	-	-	CLEAN
192.168.0.85	-	-	-	CLEAN
192.168.0.203	-	-	-	CLEAN
192.168.0.98	-	-	-	CLEAN
192.168.0.120	-	-	-	CLEAN
192.168.0.234	-	-	-	CLEAN
192.168.0.233	-	-	-	CLEAN
192.168.0.254	-	-	-	CLEAN
192.168.0.182	-	-	-	CLEAN
192.168.0.174	-	-	-	CLEAN
192.168.0.129	-	-	-	CLEAN
192.168.0.123	-	-	-	CLEAN
192.168.0.247	-	-	-	CLEAN
192.168.0.165	-	-	-	CLEAN
192.168.0.158	-	-	-	CLEAN
192.168.0.99	-	-	-	CLEAN
192.168.0.93	-	-	-	CLEAN
192.168.0.238	-	-	-	CLEAN
192.168.0.242	-	-	-	CLEAN
192.168.0.249	-	-	-	CLEAN
192.168.0.154	-	-	-	CLEAN
192.168.0.116	-	-	-	CLEAN
192.168.0.152	-	-	-	CLEAN
192.168.0.55	-	-	-	CLEAN
192.168.0.60	-	-	-	CLEAN
192.168.0.229	-	-	-	CLEAN
192.168.0.74	-	-	-	CLEAN
192.168.0.227	-	-	-	CLEAN
192.168.0.59	-	-	-	CLEAN
192.168.0.51	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
192.168.0.150	-	-	-	CLEAN
192.168.0.110	-	-	-	CLEAN
192.168.0.192	-	-	-	CLEAN
192.168.0.212	-	-	-	CLEAN
192.168.0.105	-	-	-	CLEAN
192.168.0.76	-	-	-	CLEAN
192.168.0.251	-	-	-	CLEAN
192.168.0.95	-	-	-	CLEAN
192.168.0.201	-	-	-	CLEAN
192.168.0.72	-	-	-	CLEAN
192.168.0.89	-	-	-	CLEAN
192.168.0.96	-	-	-	CLEAN
192.168.0.200	-	-	-	CLEAN
192.168.0.91	-	-	-	CLEAN
192.168.0.64	-	-	-	CLEAN
192.168.0.145	-	-	-	CLEAN
192.168.0.141	-	-	-	CLEAN
192.168.0.177	-	-	-	CLEAN
192.168.0.183	-	-	-	CLEAN
192.168.0.149	-	-	-	CLEAN
192.168.0.151	-	-	-	CLEAN
192.168.0.130	-	-	-	CLEAN
192.168.0.125	-	-	-	CLEAN
192.168.0.82	-	-	-	CLEAN
192.168.0.78	-	-	-	CLEAN
192.168.0.220	-	-	-	CLEAN
192.168.0.169	-	-	-	CLEAN
192.168.0.211	-	-	-	CLEAN
192.168.0.66	-	-	-	CLEAN
192.168.0.194	-	-	-	CLEAN
192.168.0.87	-	-	-	CLEAN
192.168.0.127	-	-	-	CLEAN
192.168.0.61	-	-	-	CLEAN
192.168.0.153	-	-	-	CLEAN
192.168.0.206	-	-	-	CLEAN
192.168.0.166	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
192.168.0.248	-	-	-	CLEAN
192.168.0.58	-	-	-	CLEAN
192.168.0.204	-	-	-	CLEAN
192.168.0.244	-	-	-	CLEAN
192.168.0.198	-	-	-	CLEAN
192.168.0.195	-	-	-	CLEAN
192.168.0.137	-	-	-	CLEAN
192.168.0.83	-	-	-	CLEAN
192.168.0.118	-	-	-	CLEAN
192.168.0.214	-	-	-	CLEAN
192.168.0.122	-	-	-	CLEAN
192.168.0.68	-	-	-	CLEAN
192.168.0.147	-	-	-	CLEAN
192.168.0.138	-	-	-	CLEAN
192.168.0.115	-	-	-	CLEAN
192.168.0.84	-	-	-	CLEAN
192.168.0.162	-	-	-	CLEAN
192.168.0.113	-	-	-	CLEAN
192.168.0.209	-	-	-	CLEAN
192.168.0.157	-	-	-	CLEAN
192.168.0.213	-	-	-	CLEAN
192.168.0.184	-	-	-	CLEAN
192.168.0.185	-	-	-	CLEAN
192.168.0.54	-	-	-	CLEAN
192.168.0.109	-	-	-	CLEAN
192.168.0.161	-	-	-	CLEAN
192.168.0.176	-	-	-	CLEAN
192.168.0.148	-	-	-	CLEAN
192.168.0.197	-	-	-	CLEAN
192.168.0.75	-	-	-	CLEAN
192.168.0.163	-	-	-	CLEAN
192.168.0.190	-	-	-	CLEAN
192.168.0.168	-	-	-	CLEAN
192.168.0.224	-	-	-	CLEAN
192.168.0.159	-	-	-	CLEAN
192.168.0.135	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
192.168.0.101	-	-	-	CLEAN
192.168.0.232	-	-	-	CLEAN
192.168.0.92	-	-	-	CLEAN
192.168.0.97	-	-	-	CLEAN
192.168.0.191	-	-	-	CLEAN
192.168.0.50	-	-	-	CLEAN
192.168.0.175	-	-	-	CLEAN

Reduced dataset

Mutex

Name	Operations	Parent Process Name	Verdict
Global\{BEF590BE-11A6-442A-A85B-656C1081E04C}	access	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\AutoEnrollment\Debug	read, access	taskhost.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\XO1XADpO01	write, read, access	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\LockBit\Public	write, read, access	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration	access	taskhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\AutoEnrollment	create, access	taskhost.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	create, access	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\LockBit\full	write, read, access	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\LockBit	create, access	0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	CLEAN

Process

Process Name	Commandline	Verdict
0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe	"C:\Users\kEecfMwgj\Desktop\0e66029132a885143b87b1e49e32663a52737bbff4ab96186e9e5e829aa2915f.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet	SUSPICIOUS
vssadmin.exe	vssadmin delete shadows /all /quiet	CLEAN
autochk.exe	\??\C:\Windows\system32\autochk.exe *	CLEAN
csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=b... ...ServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	CLEAN
csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=b... ...ServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	CLEAN
services.exe	C:\Windows\system32\services.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	CLEAN

Process Name	Commandline	Verdict
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
audiodg.exe	C:\Windows\system32\AUDIODG.EXE 0x2b8	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService	CLEAN
dllhost.exe	C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}	CLEAN
spoolsv.exe	C:\Windows\System32\spoolsv.exe	CLEAN
taskhost.exe	"taskhost.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	CLEAN
officeclicktorun.exe	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service	CLEAN
taskhost.exe	taskhost.exe SYSTEM	CLEAN
dwm.exe	"C:\Windows\system32\Dwm.exe"	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	LockBit	LockBit Ransomware	Function Strings	-	Ransomware	5/5
Ransomware	LockBit	LockBit Ransomware	Memory Dump	-	Ransomware	5/5

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	4.5.1
Dynamic Engine Version	4.5.1 / 05/09/2022 04:24
Static Engine Version	4.5.1.0 / 2022-05-09 03:00:28
AV Exceptions Version	4.5.1.25 / 2022-04-28 14:12:58
Link Detonation Heuristics Version	4.5.1.36 / 2022-06-03 13:04:14
Smart Memory Dumping Rules Version	4.5.1.38 / 2022-06-13 09:02:33
Config Extractors Version	4.5.1.44 / 2022-06-27 08:43:44
Signature Trust Store Version	4.5.1.30 / 2022-05-16 06:57:54
VMRay Threat Identifiers Version	4.5.1.44 / 2022-06-27 08:43:44
YARA Built-in Ruleset Version	4.5.1.44

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