MALICIOUS

Classifications: Spyware, Ransomware

Threat Names: Maze, ChaCha, Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe**
ID	#3219556
MD5	248c960c1ae54103dea5bfae924f28e2
SHA1	504ce8efee0f7f8329c09c6d045a21c795a84b42
SHA256	3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363
File Size	453.50 KB
Report Created	2022-01-02 14:03 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (21 rules, 132 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies Windows automatic backups	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe deletes Windows volume shadow copies.			
5/5	YARA	Malicious content matched by YARA rules	100	Ransomware

- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Boot\BOOTSTAT.DAT".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\MSNBC News~.feed-ms".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-ms".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Feeds Cache\index.dat".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.bak".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\01_Music_auto_rated_at_5_stars.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\02_Music_added_in_the_last_month.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\03_Music_rated_at_4_or_5_stars.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\04_Music_played_in_the_last_month.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\05_Pictures_taken_in_the_last_month.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\06_Pictures_rated_4_or_5_stars.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\07_TV_recorded_in_the_last_week.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\08_Video_rated_at_4_or_5_stars.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\09_Music_played_the_most.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\10_All_Music.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\11_All_Pictures.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\12_All_Video.wpl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TM.blf".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000001.regtrans-ms".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000002.regtrans-ms".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{1CD43F3B-668B-4CA8-B816-34F74122EC0F}.oeaccount".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{AF0DB737-2EF9-4633-BF5E-1A6761ED1577}.oeaccount".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\edb00001.log".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.MSMessageStore".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.pat".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.chk".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.log".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb00001.log".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00001.jrs".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00002.jrs".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\oeold.xml".
- Rule "MazeEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.htm".

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Encrypts content of user files	1	Ransomware
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe encrypts the content of multiple user files.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Internet Explorer / Edge, Windows Mail, git, The Bat!, Total Commander.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
3/5	Hide Tracks	Hides data in extended file attributes	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe sets extended file attributes for "c:\programdata\foo.db" to possibly hide the file.			
3/5	System Modification	Modifies certificate store	5	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe deletes a certificate from the local certificate list "my" by file. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe deletes a certificate from the local revocation list "my" by file. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe deletes a certificate from the local certificate trust list "my" by file. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe deletes all certificate entries for the local list "my" by file. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe deletes all certificate entries for the local list "olvrr9ld.dat" by file.			
2/5	Discovery	Executes WMI query	3	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe executes WMI query: Select * From AntiVirusPr. • (Process #5) wmic.exe executes WMI query: SELECT * FROM Win32_ShadowCopy. • (Process #10) wmic.exe executes WMI query: SELECT * FROM Win32_ShadowCopy.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe has a thread which sleeps more than 5 minutes.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive mail data	2	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe tries to read sensitive data of mail application "Windows Mail" by file. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	System Modification	Changes the desktop wallpaper	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe sets the desktop wallpaper to the file "c:\users\keecfmwgj\appdata\local\temp\123456789.bmp".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe enumerates running processes.			

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe creates mutex with name "ae780a138443a5af".			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe starts (process #5) wmic.exe with a hidden window. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe starts (process #10) wmic.exe with a hidden window.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #5) wmic.exe enables process privilege "". • (Process #10) wmic.exe enables process privilege "".			
1/5	Persistence	Installs system startup script or application	4	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe adds "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\startup\olvrr9ld.dat" to Windows startup folder. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe adds "c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\startup\decrypt-files.html" to Windows startup folder. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe adds "c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\startup\olvrr9ld.dat" to Windows startup folder. • (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe adds "c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\startup\decrypt-files.html" to Windows startup folder.			
1/5	Obfuscation	Overwrites code	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe overwrites code to possibly hide behavior.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe resolves 54 API functions by name.			

Mitre ATT&CK Matrix

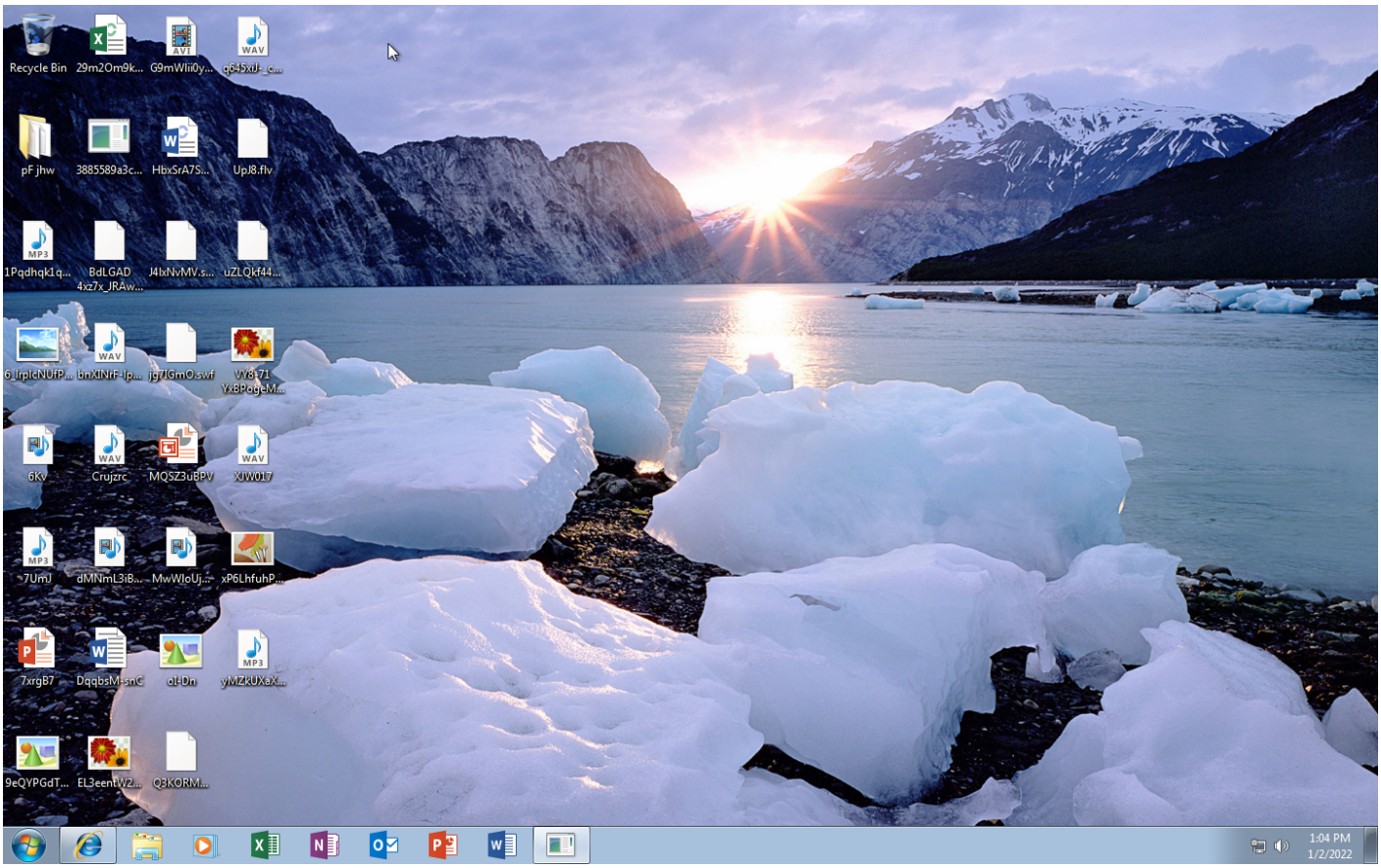
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#T1057 Process Discovery		#T1119 Automated Collection			#T1491 Defacement
				#T1045 Software Packing		#T1083 File and Directory Discovery		#T1005 Data from Local System			#T1486 Data Encrypted for Impact
											#T1490 Inhibit System Recovery

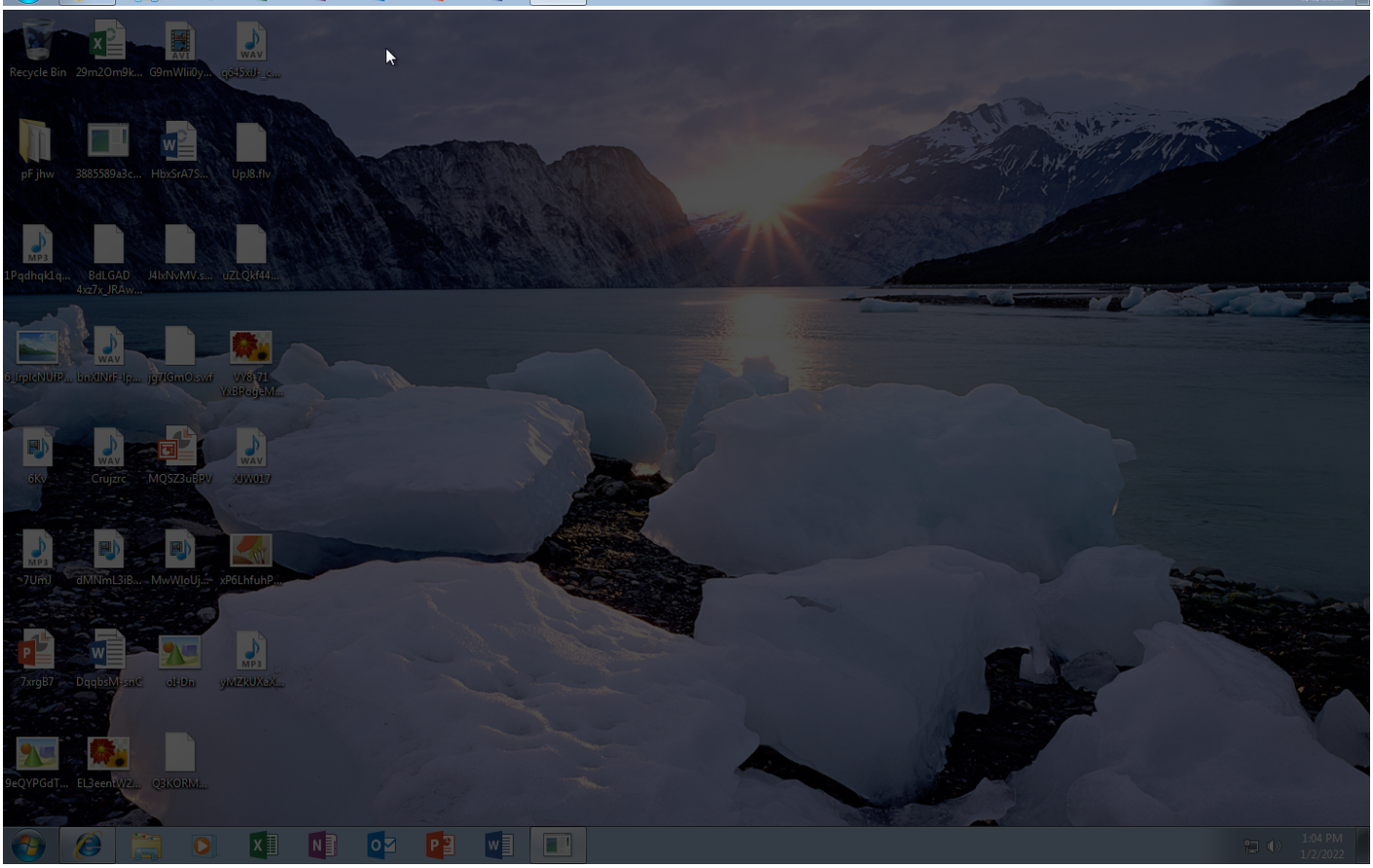
Sample Information

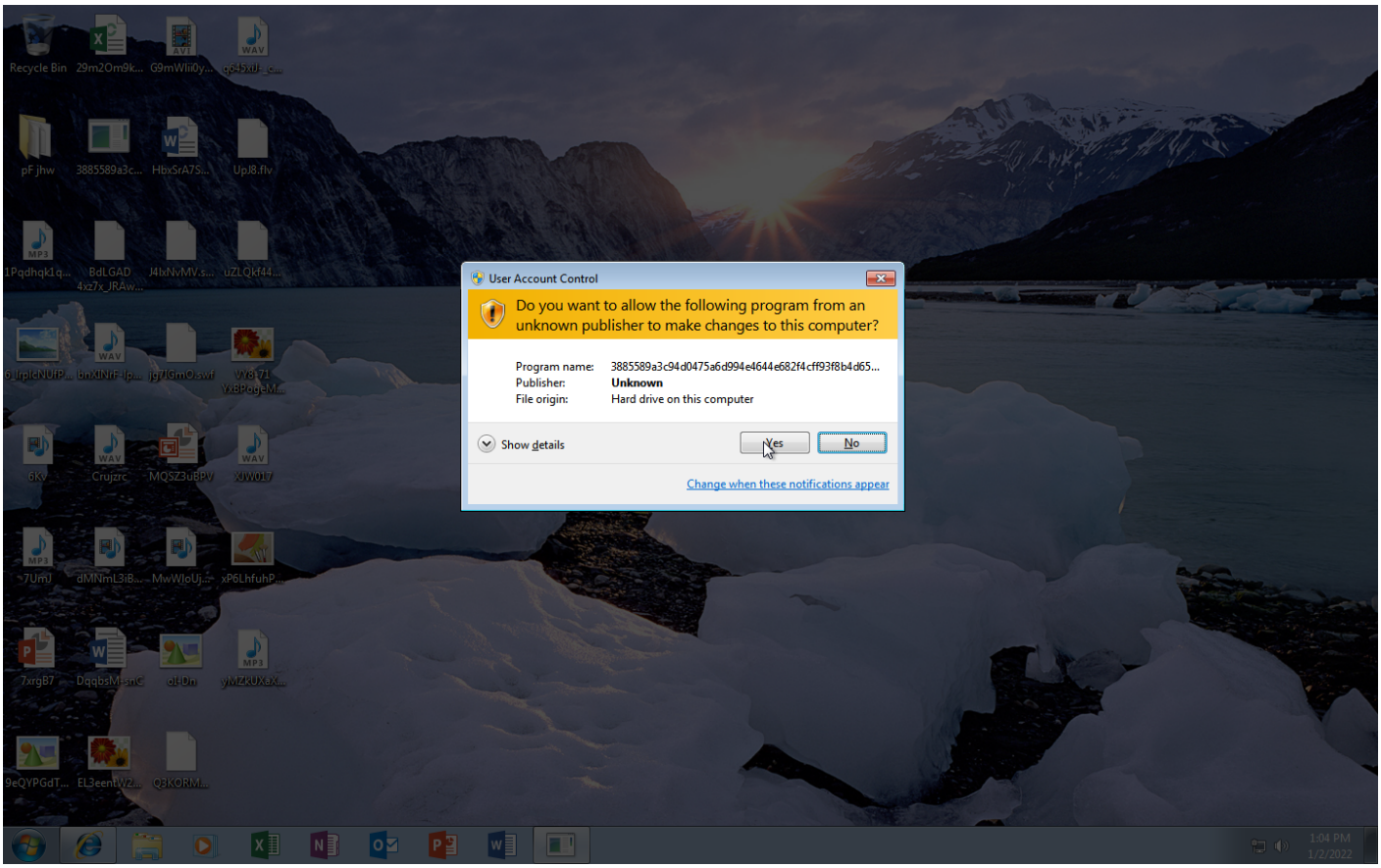
ID	#3219556
MD5	248c960c1ae54103dea5bfae924f28e2
SHA1	504ce8efee0f7f8329c09c6d045a21c795a84b42
SHA256	3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363
SSDeep	6144:/P2vVfY9RbTrI5Tm6oUAcEtKY/e8ImceEoAE77OvaHhdRwc9/P2wdAn7gJRKKRqX:aVw9prIVpb3F8ltQIBwc9/P2l7gT6
ImpHash	fed6080d5570a9033baa7765bc13e05e
File Name	3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe
File Size	453.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

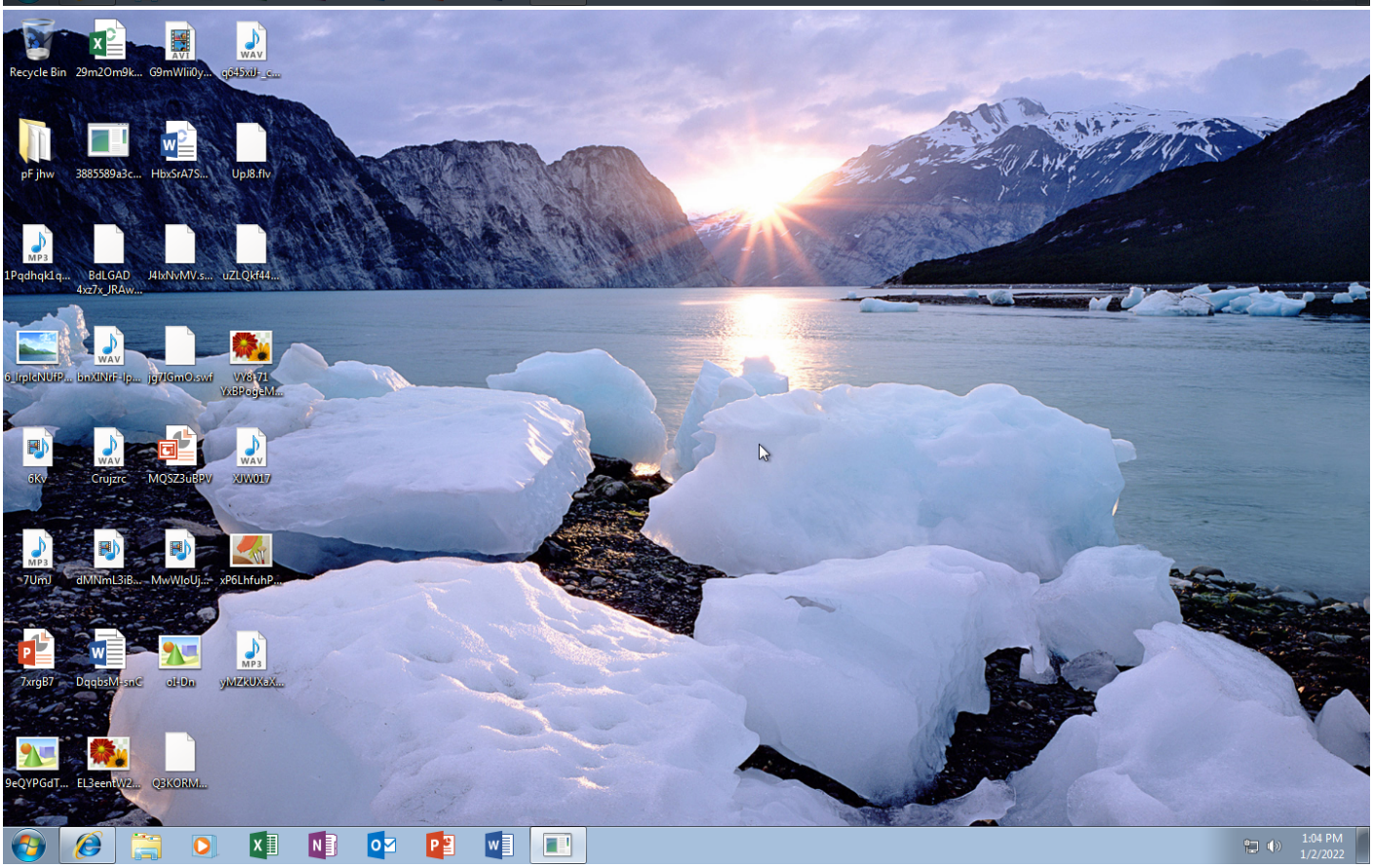
Analysis Information

Creation Time	2022-01-02 14:03 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	6
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	105


Recycle Bin
29m2Om9k...
G9mWlii0y...
q645xU-_c...
pF jhw
3885589a3c...
HbxSrA7S...
UpJ8.flv
1Pqdhqk1q...
BdLGAD
4xz7x_JRAw...
J4lxNvMV.s...
uZLQkf44...
6_IrplcNUfP...
bnXlNrF-Ip...
jgr1GmO.swf
VY8-71
YxBPogeM...
6Kv
Crujzrc
MQSZ3uBPV
XlW017
7UmJ
dMNmL3iB...
MwWloUj...
xP6LhfuhP...
7xrgB7
DqqbsM-snC
dLDn
yMZKUxeX...
9eQYPGdT...
EL3eentV2...
Q3KORM...
1:04 PM
1/2/2022







Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

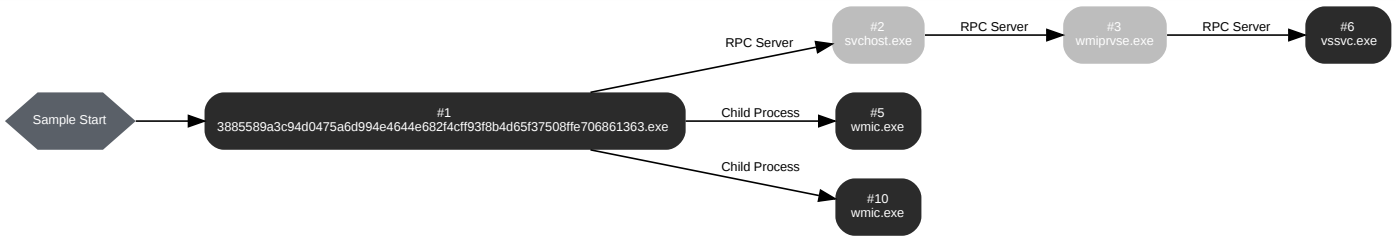
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 43143, Reason: Analysis Target
Unmonitor End Time	End Time: 283582, Reason: Terminated by Timeout
Monitor duration	240.44s
Return Code	Unknown
PID	3672
Parent PID	912
Bitness	32 Bit

Dropped Files (122)

File Name	File Size	SHA256	YARA Match
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies\\olvrr9ld.dat	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✕
C:\\DECRYPT-FILES.html	6.41 KB	2cd0c3207ade26fbd3245ade2886f4a6cd104f98252d0c0b7de752a3d8d4a352	✕
C:\Boot\BOOTSTAT.DAT	64.26 KB	768b6ee1f7ba11f257739a82ea4ccd40daca09deb830abf71a3eb560330a8b76	✕
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi	3096.26 KB	057850506a0c547f6837ab1a03ce13b1e2894574f07865579466d0ce90d889fd	✕
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\Winre.wim	10240.00 KB	4b1a3c3a3b5308af1c865f2e08eec33713195e2f0d25002d514260cf9606e608	✕
C:\Users\Default\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms	6.76 KB	cf4fb5a69a6a4fb87b7cf7413ca613469637396fbb1ecfea0d164880a6bebd20	✕
C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms	28.26 KB	31c5718463b7f5b6a51087757c6589c86a2fc411a2bc3ee1d775846bb5302ee5	✕
C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms	28.26 KB	db7a87e2bd59fe5b1b486d9cbcfdf197b22be5032133382e65d111f6bbbad490	✕
C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\MSNBC News~.feed-ms	28.26 KB	4d1529279d206df5087cf20e1d6a51c09771eaa264e57a247127abff40efcab5	✕
C:\Users\Default\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-ms	28.26 KB	37ce5a25fed59ab383237a5ab968db80b22eae2afe61b737bf846329c490356d	✕
C:\Users\Default\AppData\Local\Microsoft\Feeds Cache\index.dat	32.26 KB	cfac9241532a85cb2c58d41d592950690f6875dba06f2d303218877d28bc5173	✕
C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.bak	12.17 KB	8e7a5f0474aba5cddd910a308b50bd0190135334663c8bf0de0aa3a906b24d34	✕
C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	12.17 KB	013395aff92f0deb0408c61d12bb92ba4e9ad2cded9719f104625ec05b985ffa	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb	1044.26 KB	de250144bdc91402242b8ea112741a7c21f97ceea54e9788a27c6a6a0cc34760	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb	68.36 KB	7d030fbcddbe816480bbef37aba16ba2aeee96b37628f372e5e97a9e3921c771	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\01_Music_auto_rated_at_5_stars.wpl	1.28 KB	e5b94687021d057f83446bafc9a3761a9529d22dd74b502c72c3b2c89d494b91	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\02_Music_added_in_the_last_month.wpl	1.51 KB	a8d952aacff90fb7c26a4dcea472e37aca00413d533674658565459 11e5faef3	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\03_Music_rated_at_4_or_5_stars.wpl	1.50 KB	a2de71b4b1b8b5b37c926be0086d8c087fc3fa1f4a5c6cb5f8be08f117ccd7ab	✕

File Name	File Size	SHA256	YARA Match
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\04_Music_played_in_the_last_month.wpl	1.51 KB	ddaac17dc26b03e50f2d67eb137543350eaf7d6446e91c51f90bb8a5249bbe3c	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\05_Pictures_taken_in_the_last_month.wpl	1.04 KB	f0c9d531ae8e5dbd32abe48116b4856c1f04210b9e4cbdc2b945526e254f66ae	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\06_Pictures_rated_4_or_5_stars.wpl	1.02 KB	dee83e885e176365a583ffa7d9a21bff336059b75628d6b9e7b3a611d3d6f9fc	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\07_TV_recorded_in_the_last_week.wpl	1.27 KB	c0bb45bd666dba7ef96a03bf6711a08a93d4f6ba591814ce352c83d54f486e12	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\08_Video_rated_at_4_or_5_stars.wpl	1.25 KB	810e8028ec7344174fce6d02d0eeebe1485c1cd5c2b1debd503eeeacbfb9a892	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\09_Music_played_the_most.wpl	1.26 KB	f20a6e3d88c07f482faa857e74c7f5a6093f1004eb3004a89c00e3b510e4b247	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\10_All_Music.wpl	1.30 KB	137c36b7dfc77f6a5e30f5f0e2e7d32a82f613d1cbe3e13961d96d777245b476	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\11_All_Pictures.wpl	849 bytes	9a7584c002303744b15f9c5f79160aa5228a1423461963fd1709c96b33c9011d	✕
C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\12_All_Video.wpl	1.31 KB	9d3600a7115d001bf2b88599a701d609654a08bbd41d02be58397286d6d46564	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	40.26 KB	2c847cfdad49638a3aae38d9aa5f29899f9e7a1542a886cb84dddf2ad49cd87c	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	16.26 KB	325ac52d97f8254f3744d20a938594982818332d5871b55c5758b6a2cb77413f	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db	288 bytes	b8fa4e77fefbfac96a49df26a39f0f1aa6dc5fce39a6fbe5949e9b024dbb9c44	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	1024.26 KB	b6d95fa2aec1061668c4d10ff2af6dec785fb724f9e573b6b9b262e6dc57f287	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db	288 bytes	8cc155f186444227cd17ee657c3f452c7667bce23cc311908718e4c09cc8c9d5	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db	288 bytes	40225296f2202a8f5b1ba66959978407357508ca382bcf9a0183d4a47f665e36	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	3.44 KB	c78c3fb31df71ea7846bb81a510852509f01581bfa5da39228a5f36d1927593c	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db	288 bytes	ce079259933c88172e40ca571a8ad60f220d32af16950e472d7014a9d30392e9	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	16.26 KB	db78b302b7d602b654c5deaffa82ec908975b60413fa1d6e0b86626794950470	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat	32.26 KB	e757e4d3fc660af1f8185278202d4c3270cada23b354c11582485a4c4beefc12	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat	256.26 KB	9210430a6c0350a3788482ffab7641c1b36acd8e3a0bc87b7698c303c54454a2	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1	45.26 KB	a9f683887fd8d3427a8e301b891cba38472240db23f311eb6926796e0883d89c	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TM.blf	64.26 KB	b3f47ef41d00304b3b20a629ea69c6d989b85229e39db820b4b25501dffb9658	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000001.regtrans-ms	512.26 KB	de0f85c3f3b78f3b145987e6b5c8ed36193da3bf2c3ef67717fc86b81f4305de	✕
C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000002.regtrans-ms	512.26 KB	ad1be52d6e62da02262b98d5a920267e7d818df8ff6f3cc57821f2bde78010dd	✕

File Name	File Size	SHA256	YARA Match
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{047EF9CE-9C1F-4250-9CA7-D206DB8B643C}.oeaccount	1.73 KB	87ae850ae061c4f1fbc1b6bbbfe2bc647da3e2bf1c4bb3ba3e651a522d49fc0b	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{1CD43F3B-668B-4CA8-B816-34F74122EC0F}.oeaccount	936 bytes	3577ff5e91fea601e917303f0d555a1a61c69da85a6757b8b36d74e108634ce1	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{AF0DB737-2EF9-4633-BF5E-1A6761ED1577}.oeaccount	1.95 KB	371b59ad6a0714faf3eca9c6b6e01e0a19578cf4f4b2df7995f9e677b51c77a0	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\edb00001.log	2048.26 KB	0b2fdc7bbdd5a508a7e334d85fbb28da5f28f1e338d8b2b3524aa03716a6c48d	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.MSMessageStore	2072.26 KB	5502984fb8b79cf46a76abaf031d9ea2bfaecc5216f4425d27bb3976a114a788	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.pat	16.26 KB	776dcacc9f282d3a428086bbea5ed30a34f889cdfb12dfab04005683ee38f137	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.chk	8.26 KB	fdaaf42312b7a898586cb4b3b87b8c61a925c9446668e7d578d5385ffd7ddf0c	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.log	2048.26 KB	baaed3b65ec1c3b310131b77fe764d4a0649deb2a253eba912397792f42879b5	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb00001.log	2048.26 KB	a165f95755f23f88161eb64ec113ff4e699d8ca94b0a6c2bde7f28d47b0f99f8	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00001.jrs	2048.26 KB	ea1d7c9bfdd3160aca28e8dd91d3bb18e778fef7ae23051a8ab4a8bdf92c7202	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00002.jrs	2048.26 KB	a102fa85a62786b3c9123b9d02f879eb2b399ff0163b4a91447743af5f1dd8f4	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\oeold.xml	524 bytes	dfd710f3182299a621692d1e9c5ed8dc75490f05434c3302d99c110d11c501fc	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.htm	519 bytes	ab9b6a4741160b1e6b3a4b8aa1f123c7f5035b905f99d7f8f3fac0c7279a4321	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.jpg	1.31 KB	1706fb4062063128433855df60068cec66af0388324a1809ba5d6d98d5b195e4	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.htm	495 bytes	8c66942e3dff70be6583f89362eba379b508a29209c2803cc6538246757c4fcb	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.jpg	23.57 KB	5986e3c1fc37459c159484d1905be2511161e96b4afa57f3e2623620f122842a	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Green Bubbles.htm	501 bytes	97454ce7cd52b74cd559ad30d3a92109ccdf5ef5840f7c6f505cd18e572667c3	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\GreenBubbles.jpg	6.51 KB	87640782aacb92bb5d966c5d41dc8e56e6c5f59e6f2fd8edcc31d7feb8bc9400	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Hand Prints.htm	499 bytes	aafcecb6212328a5a67c792c77394619e9e52fcd1e82dcb0b8842c4f26059237	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\HandPrints.jpg	4.38 KB	0b3d634b193d18375be2d38cbf4697aa1a8524aacefa5495dd296a9f19a93046	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Orange Circles.htm	501 bytes	0a784d4ad102f063dcd5d58e6a9b3270ec7e0e8bd0d152162c8ef402e33e7129	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\OrangeCircles.jpg	6.49 KB	287c2925e479d4065dcc61932ce169daf29ffced4c12df72aac0f7b66d57aa54	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.htm	496 bytes	7768c1ca7d46b43c738403e7cb1b967a8036f06638ee5c2c68036a33c265c3a4	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.jpg	5.25 KB	4968b14f841adfd10c7557f13d22818fbd9f5faef87d8c742724c52386a9ad05	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.htm	497 bytes	bd3a377d9aa768153c77c20c4800a9b87c483282b003ec7bc9720354bf2cd7e4	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.jpg	2.13 KB	4205a37406adff9c21bf5c6379eee1b052d00eaed2622a24357bee355fd250fe	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Shades of Blue.htm	501 bytes	54a84d303880a1ddaff893e6c050563b51888e8f75087b30c65148d662bc5e25	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\ShadesOfBlue.jpg	4.88 KB	6b512cd9eb6d5938db4a042170e99bad80cb38b2c835371c150f2caf7a204d1a	✕

File Name	File Size	SHA256	YARA Match
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Soft Blue.htm	496 bytes	04cd20f6f0d00406b7a2a9548c4674d9bb4a6ce70e2fedcbc45191a7cd8424ab	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\SoftBlue.jpg	10.58 KB	216e7dec5c11531d61f17643c73a4aca204afbf8731447e00611a1444372ba92	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.htm	494 bytes	8c94d5af70552195c98b0c8d7ec149bb602e4d3a29671fab9c39490c486c7a75	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.jpg	7.59 KB	dfefaef1e22e975b4870232a40224d02f8f96c09b65e27b9901095074a84d6f1	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore	2064.26 KB	262a0edd658035682f706462fc670ca5d4f49bb6050513bea0e9d9a14a888bc1	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat	16.26 KB	40f546b8048d7c6642a7136aebe5c909adfed469287c678f3044b255b44e1476	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.DTD	762 bytes	0be33970ac7b4c9dd35a3179daf793d0f00f3edb0c81aaee6059c5a686ac3b52	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.XML	10.21 KB	f35680e69bc5295bd92bf54a567a1d7fb33db2b7bfc9a272d8c7b32fb047211b	✕
C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar\Settings.ini	348 bytes	9eaeeb7fce04fe31b22bc2f02a2269eeead84ee1183707d25161d34bd3748ae4	✕
C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9	816 bytes	c45d85048b42070f32bfb9c9188c818ee22cf268838ea3b6f9b625e5f6c879ca	✕
C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9	524 bytes	4daf7f9a9662321dc4fdf5a5ef70f3f9e2a569e055b1cefde786e1555f32c5d3	✕
C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015	568 bytes	d58ae48e9253fbc156fd7bab505424cddd8a65896fc95616825ba1e065d538f3	✕
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk	554 bytes	f64828307aec04ac843282f19d2c2cb6942e7c6b852ce8b8c5cbbea9d533f713	✕
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk	1.67 KB	c5196da2f37cba7f7d089b27e2d112a9f597572a5019de08c306bed4d517d876	✕
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk	1.46 KB	828e0c70c620bc659fc4b7d8f0631eeb42de832e672cc2c7bf324fc37688f8ad	✕
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk	1.77 KB	bffa58c8da0c8c54a38dc57aa1eaba877bfbf152489813f9e6d36b43a0aa0c04	✕
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk	536 bytes	c330f06284914ffc060c8cc1f932b446c6c86251694dccbebe145a279bafef23	✕
C:\Users\Default\AppData\Roaming\Microsoft\Protect\CREDHIST	288 bytes	a9234facd98b1851a54ff99ca5164087f88d9a1f86fa6fbefc56eb5254996d53	✕
C:\Users\Default\AppData\Roaming\Microsoft\Protect\S-1-5-21-3111613574-2524581245-2586426736-500\be5b4fbd-cb99-45f5-9462-5f896dd3a6b9	732 bytes	437a70e7ca5e5965b5e29f92cdb28528aba58ed23983ebddf4e6041dd6449f7b	✕
C:\Users\Default\AppData\Roaming\Microsoft\Protect\S-1-5-21-3111613574-2524581245-2586426736-500\Preferred	288 bytes	36634978a43442a9a9056e248e0ccb48fcb5f8c4201bccc2a3c8d8be1c37d896	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	16.26 KB	b43a12c663bc805bc1f7e044c6d5c5778d16501799b87b6998fa40679604662b	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat	240.26 KB	c4d158925bafc105907774d8d73aa0a4795d9a1c5416a518763fb33671b9b349	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	3.76 KB	b9f89119f795511fd559db900f37bbabd670806b32df893bf14044b08fd74e27	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	3.72 KB	daa957bd6fa3db8168e3bfe6ba79885a48babfc5f54ad0feec8b9de0e6e6f512	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	3.75 KB	3ac6b0e8a2008dbd28c9be551b95b0d4a30d2655a9771fad8e112c878c077ab7	✕

File Name	File Size	SHA256	YARA Match
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	3.73 KB	a4c2a67c3af807f67f1f78360c3f13b7185abd5fa31fa36b980a14ff29174f42	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms	5.76 KB	46d2055e812adcc7f353b18b985bed33232aa56a424fb0924c4e27d348f7113d	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.customDestinations-ms	288 bytes	7c915df4e40c3bcec789a085c33a3089cbcb4aed46d6f1c60dd570a385b54b5f	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-ms	15.28 KB	5b6982f480dae6914570326746c6f3ade1507d55b94abb334caa2cc477c068d0	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7e4dca80246863e3.customDestinations-ms	288 bytes	74a8892e970a34475ba710d91ce1152d079395948f8eec917326c505b1b18eaf	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget	267 bytes	52326a13843533056ff361af90adac077806e60df8a52e4438e00ea015dec630	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink	271 bytes	c60575c918ede1d123b7251c08b5e3d2393ff17f8c5551a9e881fe3edc04a1e5	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk	1.47 KB	a794dc63bd59c21497498bdf868e7758f99b72d47efafa6a2a784366fe9f28e8	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail	268 bytes	b1caebd84f7dc6b3bbbc98ed25a5dfd028f8cf6fc36db105ce99a39ad68300b8	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Ease of Access.lnk	1.58 KB	ccf9b09dd7018832f50491f873ec2a77a9761d1d16d3b9c0bbcb6201335cb899	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Magnify.lnk	1.49 KB	e83524bcb206d0379a636b9c11a2bf3a9cbc668739bf4454d65641f0210f3996	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk	1.49 KB	7de5e78604303cad48278c1351daefc6803daa2c9701608cd971f44530df13e4	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk	1.48 KB	8411155bf6e35e09b8cf6ccacaefdbe750b2f6b1a374c72503710a35287304b0	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Command Prompt.lnk	1.51 KB	b0f0c9ef8073be77e9ed7091fa3240c46ff100342ac7ce2b5124e540b3d02a16	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk	1.53 KB	2897d23ea26bf17dc94dd837b9e9f2d246629530f8d87785dbb46c3549852af4	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Run.lnk	526 bytes	857a33fb8816d4fc10bb50ea1eabbb64c01f6f466f36db9cb265244d21b2d6db	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.lnk	526 bytes	b2539862c6d8e4f7d20aabaee8065b526701b0aa505ef2a3a5aa8841f6571116	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Control Panel.lnk	526 bytes	2b05bdc5d2748eff46a09eb466db8e8eb3af78b235c2c4755d2392bb3e81dbe7	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Internet Explorer (No Add-ons).lnk	1.72 KB	c4e2850c2a81c0602d4431d9a16fd448c1233e269fbd9d269e9a4f7ab93345ce	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Private Character Editor.lnk	1.53 KB	11cfc005bc82789f5b4bffc0ec54ac1889de4edbecf45fd109bb293d71870f71	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Explorer.lnk	1.46 KB	6745f99e32ecf3500663d0263d806d948dd6a8bf30c2cca27a4605133866a684	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer (64-bit).lnk	1.64 KB	a1a3887c510d71fe409a7e33093113f40eff0c6b87496a6257c44ed5f06bc807	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk	1.67 KB	4fc616485617452f926a63280d222ea1733d1e2aaf2cbc5b77e5fb13c85545e5	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Help.lnk	526 bytes	0817f17ad64137398dfb461d0f04b1a7e4d8d09a48e826199eb3182ccba57c9a	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Microsoft OneDrive.lnk	2.32 KB	d4fe66b70af1fc45006785cdcd3335c23721f4eb0ce2cd4d5cc393d9fb92a7c0	✕
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg	622.57 KB	0b73e0120eb1d9035acbbac011502f0ed5f4f17111913534b6ebb45d1c09becd	✕

File Name	File Size	SHA256	YARA Match
C:\Users\Default\Contacts\Administrator.contact	67.04 KB	dbf84af259734e57aa05f6352429222fa8690da86773ba655dc5ffc0d430714c	✕

Host Behavior

Type	Count
System	2943
Module	2935
File	7127
Environment	1
Process	100
User	1
COM	5
-	1
Mutex	1
Window	1

Process #2: svchost.exe

ID	2
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: 63072, Reason: RPC Server
Unmonitor End Time	End Time: 283582, Reason: Terminated by Timeout
Monitor duration	220.51s
Return Code	Unknown
PID	864
Parent PID	456
Bitness	64 Bit

Process #3: wmiprvse.exe

ID	3
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63072, Reason: RPC Server
Unmonitor End Time	End Time: 283582, Reason: Terminated by Timeout
Monitor duration	220.51s
Return Code	Unknown
PID	3132
Parent PID	584
Bitness	64 Bit

Process #5: wmic.exe

ID	5
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	"C:\wg\..\Windows\svt\n\..\..\system32\rkqf\wbt\i\..\..\..\wbem\y\lb\po\..\..\..\wmic.exe" shadowcopy delete
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83764, Reason: Child Process
Unmonitor End Time	End Time: 163688, Reason: Terminated
Monitor duration	79.92s
Return Code	0
PID	3736
Parent PID	3672
Bitness	64 Bit

Host Behavior

Type	Count
System	7
Module	3
COM	2
Registry	5
File	49
-	1

Process #6: vssvc.exe

ID	6
File Name	c:\windows\system32\vssvc.exe
Command Line	C:\Windows\system32\vssvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 88976, Reason: RPC Server
Unmonitor End Time	End Time: 283582, Reason: Terminated by Timeout
Monitor duration	194.61s
Return Code	Unknown
PID	3796
Parent PID	456
Bitness	64 Bit

Host Behavior

Type	Count
System	3

Process #10: wmic.exe

ID	10
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	"C:\xtlrq\..\Windows\c\q\..\..\system32\aorg\gujy\..\..\wbem\ydo\yjkto\..\..\wmic.exe" shadowcopy delete
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 213182, Reason: Child Process
Unmonitor End Time	End Time: 216735, Reason: Terminated
Monitor duration	3.55s
Return Code	0
PID	3176
Parent PID	3672
Bitness	64 Bit

Host Behavior

Type	Count
System	7
Module	3
COM	2
Registry	5
File	2
-	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
768b6ee1f7ba11f257739a82ea4ccd40daca09deb830abf71a3eb560330a8b76	C:\Boot\BOOTSTAT.DAT.8QpXV, C:\Boot\BOOTSTAT.DAT	Modified File	64.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
057850506a0c547f6837ab1a03ce13b1e2894574f07865579466d0ce90d889fd	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi.iM3sh, C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi	Modified File	3096.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
cf4fb5a69a6a4fb87b7cf7413ca613469637396fbb1ecfea0d164880a6bebd20	C:\Users\Default\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms.0ot79, C:\Users\Default\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms	Modified File	6.76 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
31c5718463b7f5b6a51087757c6589c86a2fc411a2bc3ee1d775846bb5302ee5	C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms.8fld, C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms	Modified File	28.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
db7a87e2bd59fe5b1b486d9cbcfdf197b22be5032133382e65d111f6bbbad490	C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms.q4ALte, C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms	Modified File	28.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
4d1529279d206df5087cf20e1d6a51c09771eaa264e57a247127abff40efcab5	C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\MSNBC News~.feed-ms, C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\MSNBC News~.feed-ms.DMEyT	Modified File	28.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
37ce5a25fed59ab383237a5ab968db80b22eae2afe61b737bf846329c490356d	C:\Users\Default\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-ms, C:\Users\Default\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-ms.MHQL2H	Modified File	28.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
cfac9241532a85cb2c58d41d592950690f6875dba06f2d303218877d28bc5173	C:\Users\Default\AppData\Local\Microsoft\Feeds Cache\index.dat.Zfti, C:\Users\Default\AppData\Local\Microsoft\Feeds Cache\index.dat	Modified File	32.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
8e7a5f0474aba5cddd910a308b50bd0190135334663c8bf0de0aa3a906b24d34	C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.bak, C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.bak.ZUtDrB3	Modified File	12.17 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
013395aff92f0deb0408c61d12bb92ba4e9ad2cded9719f104625ec05b985ffa	C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt, C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.bkZF	Modified File	12.17 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
de250144bdc91402242b8ea112741a7c21f97ceea54e9788a27c6a6a0cc34760	C:\Users\Default\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb, C:\Users\Default\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb.sTzFJC	Modified File	1044.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7d030fbcddbe816480bbef37aba16ba2aeee96b37628f372e5e97a9e3921c771	C:\Users\Default\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb.3ywf, C:\Users\Default\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb	Modified File	68.36 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
e5b94687021d057f83446bafc9a3761a9529d22dd74b502c72c3b2c89d494b91	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\01_Music_auto_rated_at_5_stars.wpl.W62nYJK, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\01_Music_auto_rated_at_5_stars.wpl	Modified File	1.28 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
a8d952aacff90fb7c26a4dcea472e37aca00413d53367465856545911e5faef3	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\02_Music_added_in_the_last_month.wpl.mqcoX5, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\02_Music_added_in_the_last_month.wpl	Modified File	1.51 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
a2de71b4b1b8b5b37c926be0086d8c087fc3fa1f4a5c6cb5f8be08f117ccd7ab	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\03_Music_rated_at_4_or_5_stars.wpl, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\03_Music_rated_at_4_or_5_stars.wpl.Z55jRG	Modified File	1.50 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
ddaac17dc26b03e50f2d67eb137543350eaf7d6446e91c51f90bb8a5249bbe3c	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\04_Music_played_in_the_last_month.wpl, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\04_Music_played_in_the_last_month.wpl.L1Gnk	Modified File	1.51 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
f0c9d531ae8e5dbd32abe48116b4856c1f04210b9e4cbdc2b945526e254f66ae	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\05_Pictures_taken_in_the_last_month.wpl.n0Pkr6q, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\05_Pictures_taken_in_the_last_month.wpl	Modified File	1.04 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
dee83e885e176365a583ffa7d9a21bff336059b75628d6b9e7b3a611d3d6f9fc	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\06_Pictures_rated_4_or_5_stars.wpl.SMe5QqU, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\06_Pictures_rated_4_or_5_stars.wpl	Modified File	1.02 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
c0bb45bd666dba7ef96a03bf6711a08a93d4f6ba591814ce352c83d54f486e12	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\07_TV_recorded_in_the_last_week.wpl, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\07_TV_recorded_in_the_last_week.wpl.aWDJI	Modified File	1.27 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
810e8028ec7344174fce6d02d0eeebe1485c1cd5c2b1debd503eeeacbfb9a892	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\08_Video_rated_at_4_or_5_stars.wpl.T1slk, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\08_Video_rated_at_4_or_5_stars.wpl	Modified File	1.25 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f20a6e3d88c07f482faa857e74c7f5a6093f1004eb3004a89c00e3b510e4b247	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\09_Music_played_the_most.wpl, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\09_Music_played_the_most.wpl.R5GO	Modified File	1.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
137c36b7dfc77f6a5e30f5f0e2e7d32a82f613d1cbe3e13961d96d777245b476	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\10_All_Music.wpl, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\10_All_Music.wpl.OIXNDJR	Modified File	1.30 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
9a7584c002303744b15f9c5f79160aa5228a1423461963fd1709c96b33c9011d	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\11_All_Pictures.wpl, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\11_All_Pictures.wpl.kMfs	Modified File	849 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
9d3600a7115d001bf2b88599a701d609654a08bbd41d02be58397286d6d46564	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\12_All_Video.wpl.P5qdJAn, C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\12_All_Video.wpl	Modified File	1.31 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
2c847cfdad49638a3aae38d9aa5f29899f9e7a1542a886cb84dddf2ad49cd87c	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl.c4rtaO, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	Modified File	40.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
325ac52d97f8254f3744d20a938594982818332d5871b55c5758b6a2cb77413f	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl.AHUWV6Z, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	Modified File	16.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
b6d95fa2aec1061668c4d10ff2af6dec785fb724f9e573b6b9b262e6dc57f287	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db.VVef	Modified File	1024.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
c78c3fb31df71ea7846bb81a510852509f01581bfa5da3928a5f36d1927593c	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db.4aFgzcs, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	Modified File	3.44 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
db78b302b7d602b654c5deaffa82ec908975b60413fa1d6e0b86626794950470	C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat, C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat.X30Y	Modified File	16.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
e757e4d3fc660af1f8185278202d4c3270cada23b354c11582485a4c4beefc12	C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat.D2nwT, C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat	Modified File	32.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
9210430a6c0350a3788482ffab7641c1b36acd8e3a0bc87b7698c303c54454a2	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat, C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat.iJHZvTo	Modified File	256.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a9f683887fd8d3427a8e301b891cba38472240db23f311eb6926796e0883d89c	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1, C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1.7yg2uf8	Modified File	45.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
b3f47ef41d00304b3b20a629ea69c6d989b85229e39db820b4b25501dffb9658	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TM.blf, C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TM.blf.4JdFvBx	Modified File	64.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
de0f85c3f3b78f3b145987e6b5c8ed36193da3bf2c3ef67717fc86b81f4305de	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000000... ...ult\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000001.regtrans-ms	Modified File	512.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
ad1be52d6e62da02262b98d5a920267e7d818df8ff6f3cc57821f2bde78010dd	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000000... ...ppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000002.regtrans-ms.OdnT	Modified File	512.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
3577ff5e91fea601e917303f0d555a1a61c69da85a6757b8b36d74e108634ce1	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{1CD43F3B-668B-4CA8-B816-34F74122EC0F}.oeaccount, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{1CD43F3B-668B-4CA8-B816-34F74122EC0F}.oeaccount.bTfq	Modified File	936 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
371b59ad6a0714faf3eca9c6b6e01e0a19578cf4f4b2df7995f9e677b51c77a0	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{AF0DB737-2EF9-4633-BF5E-1A6761ED1577}.oeaccount.HPqYEbs, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{AF0DB737-2EF9-4633-BF5E-1A6761ED1577}.oeaccount	Modified File	1.95 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
0b2fdc7bbdd5a508a7e334d85fbb28da5f28f1e338d8b2b3524aa03716a6c48d	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\edb00001.log.qhvDx5, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\edb00001.log	Modified File	2048.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
5502984fb8b79cf46a76abaf031d9ea2bfaecc5216f4425d27bb3976a114a788	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.MSMessageStore, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.MSMessageStore.sttnqT	Modified File	2072.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
776dcacc9f282d3a428086bbea5ed30a34f889cdfb12dfab04005683ee38f137	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.pat.Bq7VQU, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.pat	Modified File	16.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
fdaaf42312b7a898586cb4b3b87b8c61a925c9446668e7d578d5385ffd7ddf0c	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.chk, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.chk.omY5ph	Modified File	8.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
baaed3b65ec1c3b310131b77fe764d4a0649deb2a253eba912397792f42879b5	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.log.DXVDekp, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.log	Modified File	2048.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
a165f95755f23f88161eb64ec113ff4e699d8ca94b0a6c2bde7f28d47b0f99f8	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb00001.log, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb00001.log.ixxkMTz	Modified File	2048.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
ea1d7c9bfdd3160aca28e8dd91d3bb18e778fef7ae23051a8ab4a8bdf92c7202	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00001.jrs.Pbz3, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00001.jrs	Modified File	2048.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
a102fa85a62786b3c9123b9d02f879eb2b399ff0163b4a91447743af5f1dd8f4	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00002.jrs.dvZ4uP, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00002.jrs	Modified File	2048.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
dfd710f3182299a621692d1e9c5ed8dc75490f05434c3302d99c110d11c501fc	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\oeold.xml.edNkytX, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\oeold.xml	Modified File	524 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
ab9b6a4741160b1e6b3a4b8aa1f123c7f5035b905f99d7f8f3fac0c7279a4321	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.htm.FAQzzh, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.htm	Modified File	519 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
1706fb406206312843385 5df60068cec66af0388324a1809ba5d6d98d5b195e4	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.jpg.5HfB, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.jpg	Modified File	1.31 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
8c66942e3dff70be6583f89362eba379b508a29209c2803cc6538246757c4fcb	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.htm, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.htm.8006e	Modified File	495 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
5986e3c1fc37459c159484d1905be2511161e96b4afa57f3e2623620f122842a	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.jpg, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.jpg.3ZJI9Uz	Modified File	23.57 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
97454ce7cd52b74cd559ad30d3a92109ccdf5ef5840f7c6f505cd18e572667c3	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Green Bubbles.htm, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Green Bubbles.htm.ZAV7	Modified File	501 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
87640782aacb92bb5d966c5d41dc8e56e6c5f59e6f2fd8edcc31d7feb8bc9400	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\GreenBubbles.jpg.oUaQu, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\GreenBubbles.jpg	Modified File	6.51 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
aafcecb6212328a5a67c792c77394619e9e52fcd1e82dcb0b8842c4f26059237	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Hand Prints.htm, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Hand Prints.htm.9vjzy3	Modified File	499 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0b3d634b193d18375be2d38cbf4697aa1a8524aacefa5495dd296a9f19a93046	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\HandPrints.jpg.4i76wWf, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\HandPrints.jpg	Modified File	4.38 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
0a784d4ad102f063dcd5d58e6a9b3270ec7e0e8bd0d152162c8ef402e33e7129	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Orange Circles.htm.Z8eN, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Orange Circles.htm	Modified File	501 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
287c2925e479d4065dcc61932ce169daf29ffced4c12df72aac0f7b66d57aa54	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\OrangeCircles.jpg.YrMMWEW, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\OrangeCircles.jpg	Modified File	6.49 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
7768c1ca7d46b43c738403e7cb1b967a8036f06638ee5c2c68036a33c265c3a4	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.htm, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.htm.LeUtCae	Modified File	496 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
4968b14f841adfd10c7557f13d22818fbd9f5faef87d8c742724c52386a9ad05	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.jpg.FeWFobi, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.jpg	Modified File	5.25 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
bd3a377d9aa768153c77c20c4800a9b87c483282b003ec7bc9720354bf2cd7e4	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.htm.dGI3Z, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.htm	Modified File	497 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
4205a37406adff9c21bf5c6379eee1b052d00eaed2622a24357bee355fd250fe	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.jpg, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.jpg.W7qCcu7	Modified File	2.13 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
54a84d303880a1ddaff893e6c050563b51888e8f75087b30c65148d662bc5e25	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Shades of Blue.htm.GmfqskO, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Shades of Blue.htm	Modified File	501 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
6b512cd9eb6d5938db4a042170e99bad80cb38b2c835371c150f2caf7a204d1a	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\ShadesOfBlue.jpg.UPuwR, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\ShadesOfBlue.jpg	Modified File	4.88 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
04cd20f6f0d00406b7a2a9548c4674d9bb4a6ce70e2fedcbc45191a7cd8424ab	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Soft Blue.htm.mTTYux, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Soft Blue.htm	Modified File	496 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
216e7dec5c11531d61f17643c73a4aca204afbf8731447e00611a1444372ba92	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\SoftBlue.jpg.AFm537Y, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\SoftBlue.jpg	Modified File	10.58 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8c94d5af70552195c98b0c8d7ec149bb602e4d3a29671fab9c39490c486c7a75	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.htm, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.htm.kuDpsGS	Modified File	494 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
dfefaef1e22e975b4870232a40224d02f8f96c09b65e27b9901095074a84d6f1	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.jpg.FhLOwdh, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.jpg	Modified File	7.59 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
262a0edd658035682f706462fc670ca5d4f49bb6050513bea0e9d9a14a888bc1	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore.ZtcsMS, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore	Modified File	2064.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
40f546b8048d7c6642a7136aebe5c909adfed469287c678f3044b255b44e1476	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat.HzeBkau	Modified File	16.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
0be33970ac7b4c9dd35a3179daf793d0f00f3edb0c81aaee6059c5a686ac3b52	C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.DTD, C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.DTD.KDM6A	Modified File	762 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
f35680e69bc5295bd92bf54a567a1d7fb33db2b7bfc9a272d8c7b32fb047211b	C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.XML.75NIdK, C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.XML	Modified File	10.21 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
c45d85048b42070f32bfb9c9188c818ee22cf268838ea3b6f9b625e5f6c879ca	C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9, C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9.qS2B	Modified File	816 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
4daf7f9a9662321dc4fdf5a5ef70f3f9e2a569e055b1cefde786e1555f32c5d3	C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9.2zZtu, C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9	Modified File	524 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
d58ae48e9253fbc156fd7bab505424cddd8a65896fc95616825ba1e065d538f3	C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015.ASfWLt, C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015	Modified File	568 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
f64828307aec04ac843282f19d2c2cb6942e7c6b852ce8b8c5cbbea9d533f713	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk.E5uq	Modified File	554 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c5196da2f37cba7f7d089b27e2d112a9f597572a5019de08c306bed4d517d876	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk.IoEXV, C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk	Modified File	1.67 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
828e0c70c620bc659fc4b7d8f0631eeb42de832e672cc2c7bf324fc37688f8ad	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk.O5WFn7O	Modified File	1.46 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
bffa58c8da0c8c54a38dc57aa1eaba877bfbf152489813f9e6d36b43a0aa0c04	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk.kd6q, C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk	Modified File	1.77 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
c330f06284914ffc060c8cc1f932b446c6c86251694dccbebe145a279bafef23	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk.mYrV, C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk	Modified File	536 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
437a70e7ca5e5965b5e29f92cdb28528aba58ed23983ebddf4e6041dd6449f7b	C:\Users\Default\AppData\Roaming\Microsoft\Protect\S-1-5-21-3111613574-2524581245-2586426736-500\be5b4fbd-cb99-45f5-9462-5f896dd3a... ...fault\AppData\Roaming\Microsoft\Protect\S-1-5-21-3111613574-2524581245-2586426736-500\be5b4fbd-cb99-45f5-9462-5f896dd3a6b9.U4HBKWc	Modified File	732 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
b43a12c663bc805bc1f7e044c6d5c5778d16501799b87b6998fa40679604662b	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies\index.dat, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies\index.dat.EYDBJ	Modified File	16.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
c4d158925bafc105907774d8d73aa0a4795d9a1c5416a518763fb33671b9b349	C:\Users\Default\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat, C:\Users\Default\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat.64ivOp7	Modified File	240.26 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
b9f89119f795511fd559db900f37bbabd670806b32df893bf14044b08fd74e27	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms.oht06CE, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	Modified File	3.76 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
daa957bd6fa3db8168e3bfe6ba79885a48babfc5f54ad0feec8b9de0e6e6f512	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms.Xs73cBH, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	Modified File	3.72 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
3ac6b0e8a2008dbd28c9be551b95b0d4a30d2655a9771fad8e112c878c077ab7	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms.8GFiG9C, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	Modified File	3.75 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a4c2a67c3af807f67f1f78360c3f13b7185abd5fa31fa36b980a14ff29174f42	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms.ejfbV, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	Modified File	3.73 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
46d2055e812adcc7f353b18b985bed33232aa56a424fb0924c4e27d348f7113d	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms.Nhhh	Modified File	5.76 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
5b6982f480dae6914570326746c6f3ade1507d55b94abb334caa2cc477c068d0	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-ms, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-ms.pRc5	Modified File	15.28 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
a794dc63bd59c21497498bdf868e7758f99b72d47efafa6a2a784366fe9f28e8	C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk.TVf8MK, C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk	Modified File	1.47 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
ccf9b09dd7018832f50491f873ec2a77a9761d1d16d3b9c0bbcb6201335cb899	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Ease of Access.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Ease of Access.lnk.RCWups	Modified File	1.58 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
7de5e78604303cad48278c1351daefc6803daa2c9701608cd971f44530df13e4	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk.C1giP, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk	Modified File	1.49 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
8411155bf6e35e09b8cf6ccacaefdbe750b2f6b1a374c72503710a35287304b0	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk.TpKTdS	Modified File	1.48 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
b0f0c9ef8073be77e9ed7091fa3240c46ff100342ac7ce2b5124e540b3d02a16	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Command Prompt.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Command Prompt.lnk.UJCI	Modified File	1.51 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
2897d23ea26bf17dc94dd837b9e9f2d246629530f8d87785dbb46c3549852af4	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk.P0IHZ	Modified File	1.53 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
857a33fb8816d4fc10bb50ea1eabbb64c01f6f466f36db9cb265244d21b2d6db	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Run.lnk.oDF5, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Run.lnk	Modified File	526 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b2539862c6d8e4f7d20aabaee8065b526701b0aa505ef2a3a5aa8841f6571116	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.lnk.lrwm	Modified File	526 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
2b05bdc5d2748eff46a09eb466db8e8eb3af78b235c2c4755d2392bb3e81dbe7	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Control Panel.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Control Panel.lnk.uJuat1l	Modified File	526 bytes	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
c4e2850c2a81c0602d4431d9a16fd448c1233e269fbd9d269e9a4f7ab93345ce	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Internet Explorer (No Add-ons).lnk... ...\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Internet Explorer (No Add-ons).lnk.zoBQnOn	Modified File	1.72 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
11cfc005bc82789f5b4bffc0ec54ac1889de4edbecf45fd109bb293d71870f71	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Private Character Editor.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Private Character Editor.lnk.avpJ	Modified File	1.53 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
6745f99e32ecf3500663d0263d806d948dd6a8bf30c2cca27a4605133866a684	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Explorer.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Explorer.lnk.vb28C	Modified File	1.46 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
a1a3887c510d71fe409a7e33093113f40eff0c6b87496a6257c44ed5f06bc807	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer (64-bit).lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer (64-bit).lnk.kiwPKeJ	Modified File	1.64 KB	application/octet-stream	Create, Delete, Access, Write	MALICIOUS
3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363	C:\Users\kEecfMwgj\Desktop\3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe	Sample File	453.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
4fc616485617452f926a63280d222ea1733d1e2aaf2cbc5b77e5fb13c85545e5	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk.q4w7x	Modified File	1.67 KB	application/octet-stream	Create, Delete, Access, Write	CLEAN
0817f17ad64137398dfb461d0f04b1a7e4d8d09a48e826199eb3182ccba57c9a	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Help.lnk.uUALWCY, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Help.lnk	Modified File	526 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
d4fe66b70af1fc45006785cdcd3335c23721f4eb0ce2cd4d5cc393d9fb92a7c0	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Microsoft OneDrive.lnk.NPcw9B, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Microsoft OneDrive.lnk	Modified File	2.32 KB	application/octet-stream	Create, Delete, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0b73e0120eb1d9035acbbac011502f0ed5f4f17111913534b6ebb45d1c09becd	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg.YTrS, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg	Modified File	622.57 KB	application/octet-stream	Create, Delete, Access, Write	CLEAN
dbf84af259734e57aa05f6352429222fa8690da86773ba655dc5ffc0d430714c	C:\Users\Default\Contacts\Administrator.contact.ELCT, C:\Users\Default\Contacts\Administrator.contact	Modified File	67.04 KB	application/octet-stream	Create, Delete, Access, Write	CLEAN
4b1a3c3a3b5308af1c865f2e08eec33713195e2f0d25002d514260cf9606e608	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\Winre.wim, C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\Winre.wim.Z40cRh	Modified File	10240.00 KB	application/octet-stream	Delete, Create, Access, Read, Write	CLEAN
b8fa4e77fefbfac96a49df26a39f0f1aa6dc5fce39a6fbe5949e9b024dbb9c44	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db.vXzEfE	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
8cc155f186444227cd17ee657c3f452c7667bce23cc311908718e4c09cc8c9d5	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db.U7l9k, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
40225296f2202a8f5b1ba66959978407357508ca382bcf9a0183d4a47f665e36	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db.PhtuPDv, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
ce079259933c88172e40ca571a8ad60f220d32af16950e472d7014a9d30392e9	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db, C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db.QRQv	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
87ae850ae061c4f1fbc1b6bbbfe2bc647da3e2bf1c4bb3ba3e651a522d49fc0b	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{047EF9CE-9C1F-4250-9CA7-D206DB8B643C}.oeaccount, C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{047EF9CE-9C1F-4250-9CA7-D206DB8B643C}.oeaccount.NcGhQ9	Modified File	1.73 KB	application/octet-stream	Create, Delete, Access, Write	CLEAN
9eaeeb7fce04fe31b22bc2f02a2269eeead84ee1183707d25161d34bd3748ae4	C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar\Settings.ini.L0SIF, C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar\Settings.ini	Modified File	348 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
a9234facd98b1851a54ff99ca5164087f88d9a1f86fa6fbefc56eb5254996d53	C:\Users\Default\AppData\Roaming\Microsoft\Protect\CREDHIST, C:\Users\Default\AppData\Roaming\Microsoft\Protect\CREDHIST.I88ji	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
36634978a43442a9a9056e248e0ccb48fcb5f8c4201bccc2a3c8d8be1c37d896	C:\Users\Default\AppData\Roaming\Microsoft\Protect\S-1-5-21-3111613574-2524581245-2586426736-500\Preferred, C:\Users\Default\AppData\Roaming\Microsoft\Protect\S-1-5-21-3111613574-2524581245-2586426736-500\Preferred.hHHaz	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7c915df4e40c3bcec789a085c33a3089cbcb4aed46d6f1c60dd570a385b54b5f	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.customDestinations-ms.4scwLK, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.customDestinations-ms	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
74a8892e970a34475ba710d91ce1152d079395948f8eec917326c505b1b18eaf	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7e4dca80246863e3.customDestinations-ms, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7e4dca80246863e3.customDestinations-ms.HViwp	Modified File	288 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
52326a13843533056ff361af90adac077806e60df8a52e4438e00ea015dec630	C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget.Lu5pEQ, C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget	Modified File	267 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
c60575c918ede1d123b7251c08b5e3d2393ff17f8c5551a9e881fe3edc04a1e5	C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink, C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Desktop (create shortcut).DeskLink.p1SC	Modified File	271 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
b1caebd84f7dc6b3bbbc98ed25a5dfd028f8cf6fc36db105ce99a39ad68300b8	C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail.ZtKx9tM, C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail	Modified File	268 bytes	application/octet-stream	Create, Delete, Access, Write	CLEAN
e83524bcb206d0379a636b9c11a2bf3a9cbc668739bf4454d65641f0210f3996	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Magnify.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Magnify.lnk.Onl3	Modified File	1.49 KB	application/x-dosexec	Create, Delete, Access, Write	CLEAN
2cd0c3207ade26fbd3245ade2886f4a6cd104f98252d0c0b7de752a3d8d4a352	C:\Users\Default\AppData\LocalLow\\DECRYPT-FILES.html, C:\Boot\zh-CN\\DECRYPT-FILES.html, C:\Users\Default\AppData\Roaming\Microso... ...\Windows Mail\Backup\\DECRYPT-FILES.html, C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5\\DECRYPT-FILES.html	Dropped File	6.41 KB	text/html	Write, Access, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe	Sample File	Access	CLEAN
C:\ProgramData\foo.db	Accessed File	Access, Create	CLEAN
C:\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\$Recycle.Bin\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\$Recycle.Bin\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\$Recycle.Bin\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\$Recycle.Bin\S-1-5-21-4219442223-4223814209-3835049652-1000\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN

File Name	Category	Operations	Verdict
C:\$Recycle.Bin\S-1-5-21-4219442223-4223814209-3835049652-1000\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\$Recycle.Bin\S-1-5-21-4219442223-4223814209-3835049652-1000\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\BCD	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG1	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG2	Accessed File	Access	CLEAN
C:\Boot\BOOTSTAT.DAT	Modified File	Delete, Access, Write	CLEAN
C:\Boot\BOOTSTAT.DAT.8QpXV	Modified File	Write, Access, Create	CLEAN
C:\Boot\cs-CZ\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\cs-CZ\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\cs-CZ\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\cs-CZ\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\da-DK\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\da-DK\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\da-DK\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\da-DK\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\de-DE\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\de-DE\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\de-DE\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\de-DE\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\el-GR\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\el-GR\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\el-GR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\el-GR\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\en-US\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\en-US\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\en-US\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\en-US\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\en-US\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\es-ES\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\es-ES\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\es-ES\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\es-ES\olvrr9ld.dat	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\fi-FI\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\fi-FI\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\fi-FI\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fi-FI\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\Fonts\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\Fonts\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\Fonts\chs_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\cht_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\jpn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\kor_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\Fonts\wgl4_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\fr-FR\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\fr-FR\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\fr-FR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fr-FR\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\hu-HU\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\hu-HU\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\hu-HU\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\hu-HU\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\it-IT\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\it-IT\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\it-IT\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\it-IT\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\ja-JP\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\ja-JP\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\ja-JP\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ja-JP\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\ko-KR\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\ko-KR\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\ko-KR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ko-KR\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\memtest.exe	Accessed File	Access	CLEAN
C:\Boot\nb-NO\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\nb-NO\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\nb-NO\bootmgr.exe.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\nb-NO\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\nl-NL\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\nl-NL\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\nl-NL\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\nl-NL\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\pl-PL\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\pl-PL\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\pl-PL\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pl-PL\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\pt-BR\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\pt-BR\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\pt-BR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pt-BR\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\pt-PT\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\pt-PT\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\pt-PT\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\pt-PT\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\ru-RU\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\ru-RU\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\ru-RU\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ru-RU\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\sv-SE\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\sv-SE\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\sv-SE\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\sv-SE\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\tr-TR\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\tr-TR\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\tr-TR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\tr-TR\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\zh-CN\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\zh-CN\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\zh-CN\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\zh-CN\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\zh-HK\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\zh-HK\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\zh-HK\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\zh-HK\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Boot\zh-TW\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Boot\zh-TW\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Boot\zh-TW\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\zh-TW\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\bootmgr	Accessed File	Access	CLEAN
C:\Documents and Settings\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Documents and Settings\\DECRYPT-FILES.html	Accessed File	Write, Access, Create	CLEAN
C:\hiberfil.sys	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\XSL-Mappings.xml	Accessed File	Access	CLEAN
C:\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\pagefile.sys	Accessed File	Access	CLEAN
C:\PerfLogs\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\PerfLogs\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\PerfLogs\Admin\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\PerfLogs\Admin\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\PerfLogs\Admin\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\PerfLogs\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Recovery\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Recovery\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi	Modified File	Delete, Access, Write	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi.iM3sh	Modified File	Write, Access, Create	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\Winre.wim	Modified File	Read, Delete, Access, Write	CLEAN
C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\Winre.wim.Z40cRh	Modified File	Write, Access, Create	CLEAN
C:\Recovery\olvrr9ld.dat	Accessed File	Access	CLEAN
C:\System Volume Information\\olvrr9ld.dat	Accessed File	Access, Create	CLEAN
C:\System Volume Information\\DECRYPT-FILES.html	Accessed File	Access, Create	CLEAN
C:\Users\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Users\\DECRYPT-FILES.html	Dropped File	Access, Create	CLEAN
C:\Users\Default\\olvrr9ld.dat	Accessed File	Write, Access, Create	CLEAN
C:\Users\Default\\DECRYPT-FILES.html	Dropped File	Write, Access, Create	CLEAN

Reduced dataset

Mutex

Name	Operations	Parent Process Name	Verdict
ae780a138443a5af	access	3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	read, access	wmic.exe	CLEAN

Process

Process Name	Commandline	Verdict
3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe	"C:\Users\kEecfMwgj\Desktop\3885589a3c94d0475a6d994e4644e682f4cff93f8b4d65f37508ffe706861363.exe"	MALICIOUS
wmic.exe	"C:\wg\..\Windows\svt\n\..\..\system32\rkqf\wbt\i\..\..\..\wbem\y\lb\po\..\..\..\wmic.exe" shadowcopy delete	SUSPICIOUS
wmic.exe	"C:\xtlrq\..\Windows\c\q\..\..\system32\aorg\gujy\..\..\wbem\ydo\yjkto\..\..\wmic.exe" shadowcopy delete	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN

YARA / AV

YARA (105)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Boot\BOOTSTAT.DAT	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Recovery\d327d5c2-7147-11eb-9862-d731c5aaa7a9\boot.sdi	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\MSNBC News~.feed-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Feeds Cache\index.dat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.bak	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\CurrentDatabase_372.wmdb	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\01_Music_auto_rated_at_5_stars.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\02_Music_added_in_the_last_month.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\03_Music_rated_at_4_or_5_stars.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\04_Music_played_in_the_last_month.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\05_Pictures_taken_in_the_last_month.wpl	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\06_Pictures_rated_4_or_5_stars.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\07_TV_recorded_in_the_last_week.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\08_Video_rated_at_4_or_5_stars.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\09_Music_played_the_most.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\10_All_Music.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\11_All_Pictures.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00010C6E\12_All_Video.wpl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog.etl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\ExplorerStartupLog_RunOnce.etl	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TM.blf	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000001.regtrans-ms	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows\UsrClass.dat{0f6d7aa7-f51a-11df-ae0e-001d09f21116}.TMContainer00000000000000000002.regtrans-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{1CD43F3B-668B-4CA8-B816-34F74122EC0F}.oeaccount	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\account{AF0DB737-2EF9-4633-BF5E-1A6761ED1577}.oeaccount	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\edb00001.log	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.MSMessageStore	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Backup\new\WindowsMail.pat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.chk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb.log	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edb00001.log	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00001.jrs	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\edbres00002.jrs	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\oeold.xml	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Green Bubbles.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\GreenBubbles.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Hand Prints.htm	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\HandPrints.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Orange Circles.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\OrangeCircles.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Shades of Blue.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\ShadesOfBlue.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Soft Blue.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\SoftBlue.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.htm	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.jpg	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.DTD	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Local\Microsoft\Windows Media\12.0\WMSDKNS.XML	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Protect\S-1-5-21-3111613574-2524581245-2586426736-500\be5b4fbd-cb99-45f5-9462-5f896dd3a6b9	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-ms	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Ease of Access.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Command Prompt.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Run.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Control Panel.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Internet Explorer (No Add-ons).lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Private Character Editor.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Explorer.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer (64-bit).lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Help.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Microsoft OneDrive.lnk	Ransomware	5/5
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	MazeEncryptedFile	File encrypted by Maze Ransomware	Dropped File	C:\Users\Default\Contacts\Administrator.contact	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	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

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