MALICIOUS

Classifications: Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe**
ID	#6775961
MD5	25a54e24e9126fba91ccb92143136e9f
SHA1	27e0e9a39d77a59374b79d31e150ad50a5c622c9
SHA256	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc
File Size	69.50 KB
Report Created	2023-01-24 22:30 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 139 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies Windows automatic backups	2	-
	• (Process #4) cmd.exe deletes Windows volume shadow copies. • (Process #16) cmd.exe deletes Windows volume shadow copies.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 80 files by appending the extension ".id[8443a5af-2250].[wewillhelpyou@qq.com].adage".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Privilege Escalation	Creates elevated child process	1	-
	• (Process #10) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates (process #14) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe with elevated privileges.			
1/5	Mutex	Creates mutex	9	-
	• (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF00". • (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF01". • (Process #2) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF00". • (Process #10) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF01". • (Process #10) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF00". • (Process #12) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF01". • (Process #11) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF01". • (Process #13) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF01". • (Process #14) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates mutex with name "Global\22508443A5AF01".			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe starts (process #2) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe with a hidden window. • (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe starts (process #3) cmd.exe with a hidden window. • (Process #14) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe starts (process #15) cmd.exe with a hidden window.			
1/5	Persistence	Installs system startup script or application	10	-

Score	Category	Operation	Count	Classification
	• (Process #2) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup via registry. • (Process #2) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\users\keecfmwgj\appdata\roaming\microso... ...ndows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder. • (Process #2) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\programdata\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder. • (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup via registry. • (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\users\keecfmwgj\appdata\roaming\microso... ...ndows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder. • (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\programdata\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder. • (Process #14) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\users\keecfmwgj\appdata\roaming\micros... ...ndows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder. • (Process #14) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\programdata\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder. • (Process #10) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\users\keecfmwgj\appdata\roaming\micros... ...ndows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder. • (Process #10) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe adds "c:\programdata\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe" to Windows startup folder.		
1/5	Obfuscation	Reads from memory of another process	4	-
	• (Process #3) cmd.exe reads from (process #5) netsh.exe. • (Process #4) cmd.exe reads from (process #6) vssadmin.exe. • (Process #15) cmd.exe reads from (process #17) netsh.exe. • (Process #16) cmd.exe reads from (process #18) vssadmin.exe.			
1/5	Discovery	Enumerates running processes	3	-
	• (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe enumerates running processes. • (Process #10) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe enumerates running processes. • (Process #14) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe enumerates running processes.			
1/5	Hide Tracks	Changes folder appearance	3	-
	• (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe changes the appearance of folder "\\?\C:\$Recycle.Bin\S-1-5-21-4219442223-4223814209-3835049652-1000". • (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe changes the appearance of folder "\\?\C:\Program Files\Common Files\Microsoft Shared\Stationery". • (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe changes the appearance of folder "\\?\C:\Program Files".			
1/5	User Data Modification	Uses encryption API	1	-
	• (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe uses above average number of encryption APIs.			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\EycKgld_ulVGhuCKmRk2.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-delete.avi".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\FlickAnimation.avi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\FlickAnimation.avi".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwruklm.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwruklm.dat".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwruksh.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwruksh.dat".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwrusalm.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwrusalm.dat".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwrusash.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwrusash.dat".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\o9nleU.bmp.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Common Files\PXzWVbDzjHOIV50.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Performance\Title_Page.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Performance\Title_Page.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Performance\Title_Page_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Performance\Title_Page_PAL.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainBackground.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainBackground.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainBackground_PAL.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToNotesBackground.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToNotesBackground.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToNotesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToNotesBackground_PAL.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToScenesBackground.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToScenesBackground.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToScenesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToScenesBackground_PAL.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsNotesBackground.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsNotesBackground.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsNotesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsNotesBackground_PAL.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsScenesBackground.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsScenesBackground.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsScenesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsScenesBackground_PAL.wmv".
- (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe modifies "\\?\C:\Program Files\Java\jre1.8.0_171\bin\server\Xusage.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage".

Score	Category	Operation	Count	Classification
1/5	System Modification	Creates an unusually large number of files	1	-

• (Process #1) 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe creates an above average number of files.

Mitre ATT&CK Matrix

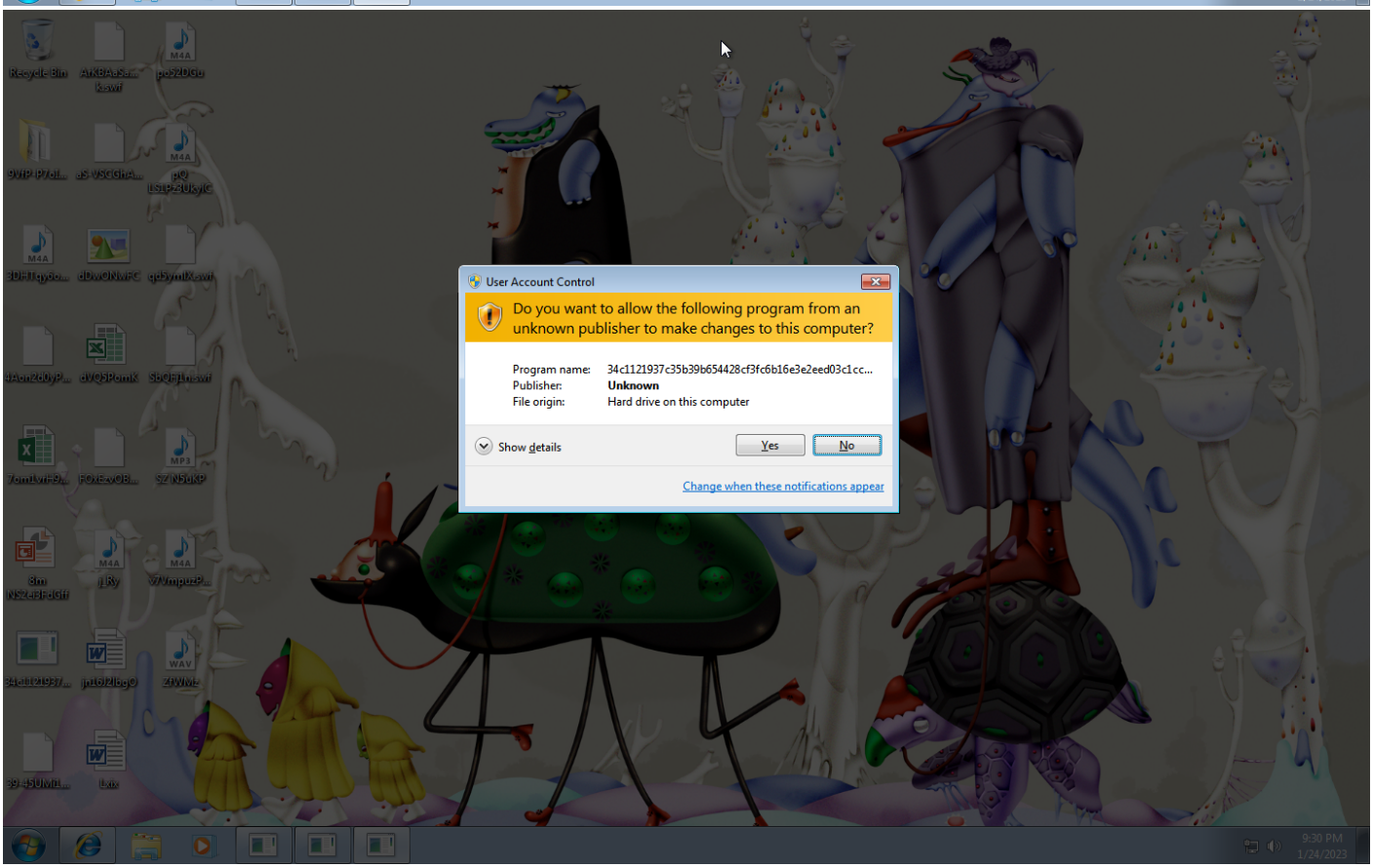
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window		#T1057 Process Discovery					#T1490 Inhibit System Recovery
				#T1112 Modify Registry							#T1486 Data Encrypted for Impact
				#T1036 Masquerading							

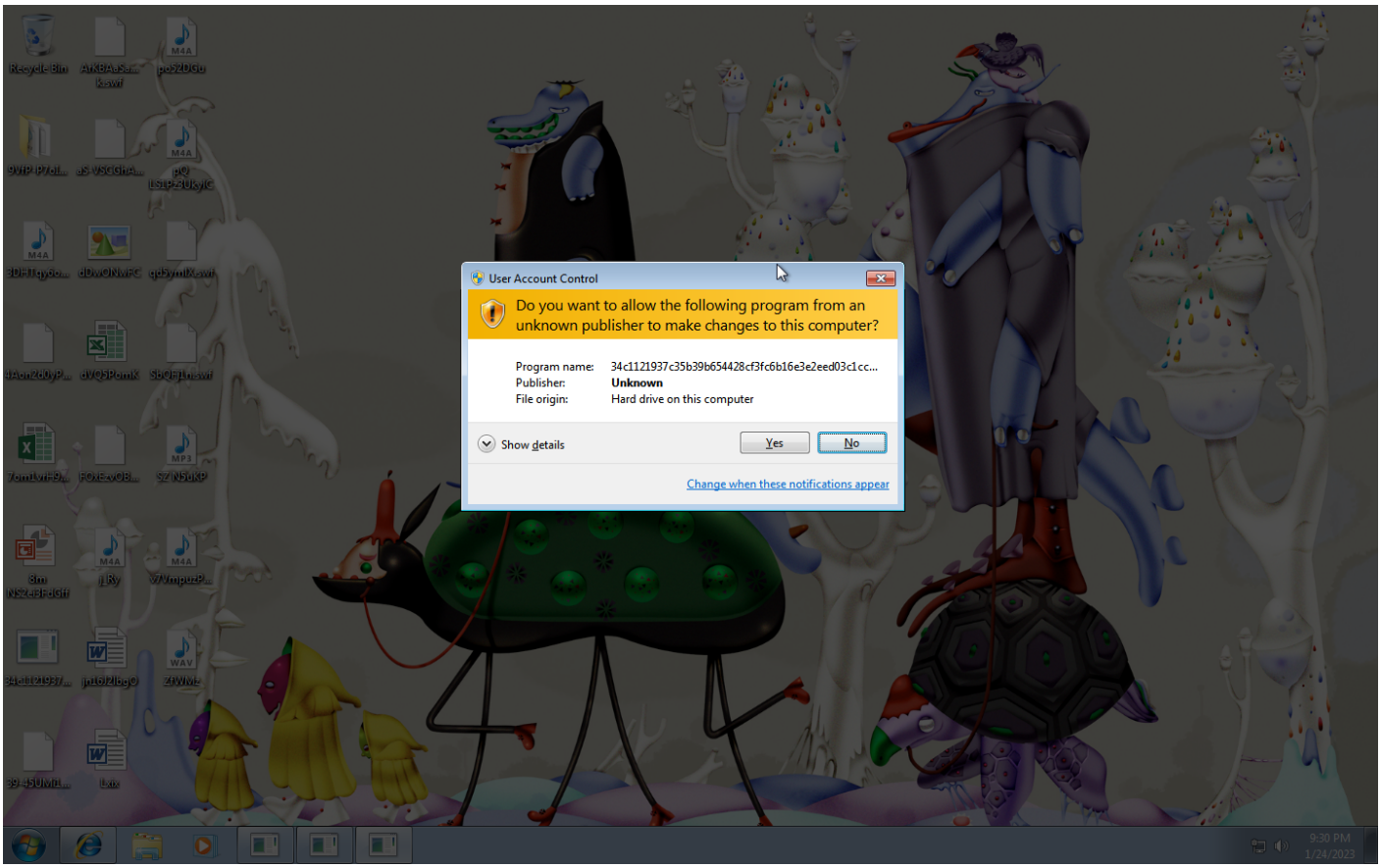
Sample Information

ID	#6775961
MD5	25a54e24e9126fba91ccb92143136e9f
SHA1	27e0e9a39d77a59374b79d31e150ad50a5c622c9
SHA256	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc
SSDeep	1536:BkGB8nHbKUvryElSpi8jCZGcqDKIKnr8dM4CWYi:BFBMHRvrAjCZmKcnr89CW
ImpHash	e6984e72559f94ba7deb365bcd2bee8a
File Name	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
File Size	69.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-01-24 22:30 (UTC+1)
Analysis Duration	00:02:11
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	16
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1cc...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

519.76 KB total sent

430.81 KB total received

1 ports 445

1 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

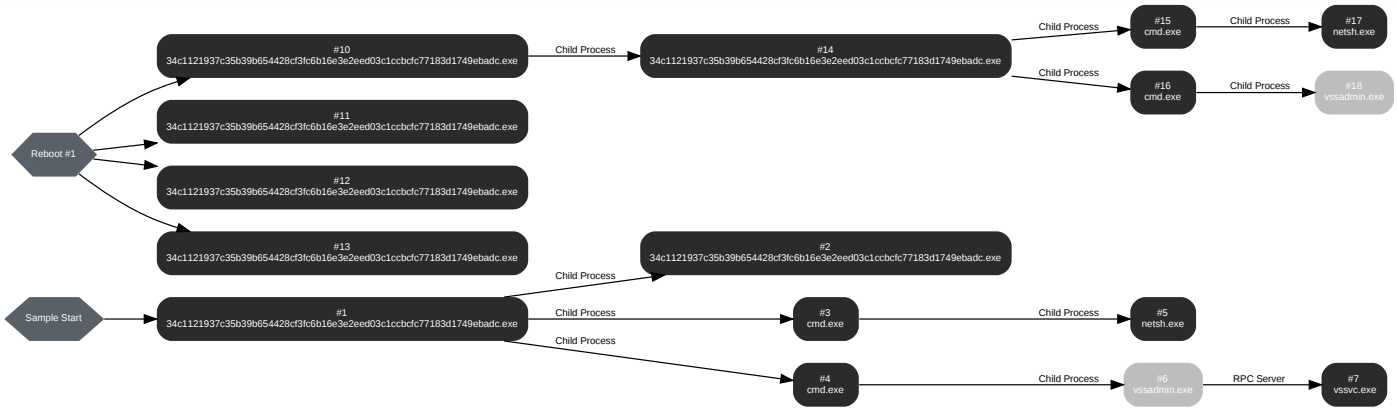
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 31475, Reason: Analysis Target
Unmonitor End Time	End Time: 69334, Reason: Terminated
Monitor duration	37.86s
Return Code	1073807364
PID	3776
Parent PID	1888
Bitness	32 Bit

Dropped Files (104)

File Name	File Size	SHA256	YARA Match
\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.35 KB	b7a8fae07c9db3f385e88c34fe2c1e5c99e47bfc78a5178b49afcfe3d950f147	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_MoveDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	418 bytes	faa06e5d54ade372d58f6124c58f3c96f5993b2b86143adb967ddd306db6edc6	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.88 KB	4b489bdc6de785675c5de881b274f0a79f6ff91f723c0fd465cbded065c0d3ab	✖
\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File A.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	386 bytes	91e305b0cf2c439856477dedf2e654e18302a09eb83cd1095482b495ba92e190	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	328.67 KB	c6e5e1b3bb59a4a375a8dcf259e7aa98957cd022ec7d2b9490870b25f6c23d3f	✖
\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.24 KB	4b1fe95d4a945584b91947e5404ea649c05ce747a04724b97547dc50e0b53b4c	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\jvm.hprof.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	4.38 KB	c0e557ac122fc280c15ea419a5ec39bfca130ec82dab89333361638c9f3b06b2	✖
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	3100.27 KB	dd54e255683302bbaf575e6e5df809f547668b395397eca40ea56594f6a5a429	✖
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.27 KB	f2d0a1f96864d2c3db5d64e6a0b26bdd9faadbba7328acba3facc77715631d58	✖
\\?\C:\Program Files\Java\jre1.8.0_171\Welcome.html.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.17 KB	9704a2f80f5ee74cbc3dba73e3005fc6ff3bd9a9d3d34f3746878ea41a63433a	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_LinkDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	434 bytes	3f5bf377d258907a41bab80257934baa88950924e8215b820630c2f3959eb540	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\osetup.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	10240.00 KB	46280bc5468ffca4e61aa1be4da69141c578511400357489b6a2ba2db1728cdd	✖
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.67 KB	200143c5b806f1c6f0e24b77a6cf6e5423001453e5e8ae12d8621268a0e47c16	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	593.94 KB	b3aa2c60c78f5e7782cc385490dc49a4d501c650fbc19ac4f2f1300dc540d8b5	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File B.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	386 bytes	8eebfdfc86ef7e6ea21ef3312de5aad87414fbc64b9587dba2673bff2c8c9a70	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_CopyNoDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	434 bytes	65cd37e81b5cdaf50039ec8d708c8455225ad5d5949385adec6fdc1234ee3d14	✖
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.11 KB	66e00a3ef790eaa85342a88723be1a97fe69f5d0840a8cf70b1d4b4b94004de2	✖
\\?\C:\Program Files\Java\jre1.8.0_171\bin\server\Xusage.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.63 KB	c52fa973be5ec3a8553f54b5687cfea43be5e57b8fd089ea23d2bbdf9b7870e7	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_LinkNoDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	434 bytes	8c294b7edf043ee719edcc3796f363aea2d431ee1c2db09b54260c45280b3122	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	5.39 KB	e109cb56dd1d27cce7a3eba04f2dceefa15d85b0aff7d350d8923b47c4c1e471	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	4620.27 KB	969ce0c61bc817e6340d1f09366df5dcf9d100e9e4d01b24ba5913f6755df918	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	10240.00 KB	8cf828796a32d97c7c89c3fe989ca8ee51c6e6e8a2a7d0a6970dd29591b1ab68	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	198.41 KB	b2de199ea42e748adf21cba5060c27c38354bf73d71026dc109d8895774d4022	✖
\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.85 KB	1a221cbbe81e313392f6179e374008312d876a4b24a33a6d7c2bef066ce582da	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.36 KB	423cd9178b1a64a79659ea8cb44bf4410e9afd536b288882d63b3e5f6c2421ab	✖
\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.30 KB	00c0cbcdd53d6f664bb4d4bd82e9fa00fa4fbb1f983446732ce4a4e1a614a1e5	✖
\\?\C:\Program Files\Common Files\PXzWVbDzjHOIV50.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	38.96 KB	b0e2fe1014a47060ccb6fb5648e64725f2a3f518db2b414f19e62eed22a0ace0	✖
\\?\C:\Program Files\Common Files\EycKgld_uIVGhuCKmRk2.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	74.00 KB	37d3bb622e177537945073aecc12c01dc9b8098845f2e36e2e845e8818e361cf	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	27.38 KB	04357036f0c7fe413596b36afc90414b15ae5de789fe172bd8c6dc9f569c8e1b	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.27 KB	598cd6fa7925a6a0b50ff55ee9ab462f2560d074a6f241104d4e9b74da62a51a	✖
\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.64 KB	88576a3518367cfe0bb52a6609d8863150b5c866655cd88d8a07f0aea5f3a430	✖
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	3.30 KB	7cdac29a27b8b5d014727520173989f1cef40b679b61551ccafa329ec7ff62ac	✖
\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	7.22 KB	5b30f94205b5d2ce385d811d0ac134db3cec79ed5837b443b53880c2383fba3d	✖
\\?\C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	898 bytes	3e068024d49151d033734780cb37154ef43da5b5b0eb1b4d5975a5029f496c41	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash_11@2x-lic.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	12.22 KB	9e267237ed9a3de1225df641bfcd1283fcd9b5f9330032e0ee180a0c0cd1e254	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_CopyDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	434 bytes	574c72b06272e104b9c9f5f9192236ccb5a47cddbd3359250b0cbb0cafc06cbd	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files\Java\jre1.8.0_171\THIRDPARTYLICENSEREADME.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	142.05 KB	a0995ccaed3749a4daff0fe9ea46dad23c27c37e0c9030633bd609fd70754807	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	14.50 KB	d23f64cbb8803d08857f440bb18486596ef1a21e544cd35e55f4ecd1ee114b8a	✖
\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote-PipelineConfig.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	802 bytes	fe294895381070bb769018225f5c9d98f33507790169a293cd39c1cc0ac12f57	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	6.17 KB	f012df0a617b7761749fb8613163767b2e6f64d94f57edd3e4d98ee8d4b41483	✖
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.27 KB	b339ee96d06d171334cb31b18563908fdbcddeb728054c82e28c1d8ce7008aa4	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	5.13 KB	2f95187bc3f10d4fa81f4466e05efb8d924e9853a78451c9c944f948d0054c6d	✖
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.44 KB	19c6bd387b0e8df89c71b0042c65b8a22ae645d8d09aec7c4157179300d59913	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\PidGenX.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1244.83 KB	98f25ad5ee9366d79329a9eb7719dbf332f1f308468da271aa21b0803a3da634	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	16.96 KB	3e67fb43acca040c086a2043d0e7e39c754328e6f7abf6cdc199b34afef83324	✖
c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excellr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	6402.59 KB	7e1aa5b82e4aad599ad98614d84faa5ad7b9b0526932cfe8d4e6bca7634cf882	✖
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.88 KB	55a526535b994f6845c0060bd98e6e57eba4e80d88835a98cab21fc7d5c3c8c7	✖
\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.02 KB	8aefc19745867e40400b31c9158b5127e3a6f118227f409b4528bed57633fc44	✖
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	3532.27 KB	e010fd78c4574ad2407d481514ae8df71942b9867f04318cd0ea90373a5913b9	✖
\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.77 KB	bd83274c1333cabadadc21d38823837354d4c50cd12c0880b96a54c8243316b0	✖
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.77 KB	32ffa3bc06afa71b041b22d224d825111132e4ea7612e16c5d3c4025a2bbf012	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.88 KB	8d31c79a5a20ac24edab811d2fad0ecedc52d52d74de1e0dbd285e06b3ed088a	✖
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.27 KB	be30d31e89e62c93d898c670ac25633e29ab658d8763112d100bb9ba6e6c4960	✖
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	6930.48 KB	a4a78fb5ce3b6a786442bc61ab958d0778eb3ae87d1403ad1f184efe16e83e86	✖
\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote-manifest.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	642 bytes	cc3375b5cdfc720d0d97a88666f90f1411b7662bde58cfe73d30d83789c9871c	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash_11-lic.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	7.88 KB	e1592a2466b975ea73fb400cbf72345ed8bdda4123b945ba82a4c75e508aa45e	✖
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	3100.27 KB	f895e08eb029e4008023d4ff13f110d83615fd7e7913a868609b0012773cae58	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files\Common Files\o9nleU.bmp.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	52.55 KB	bbeabdf761a88156583ff5651cd7cc09cb3d0829e13cc05ac576e40fc78b17b7	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	10240.00 KB	48d13089b65ebdc84e807301e9348b6515bd869b0630e1a39e79611382d59a7f	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\invalid32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	418 bytes	baa68efb0528b2eaaf44893da2d3b1c8ed0bacbf9a02a9731615716d84a3ff6c	✖
c:\programdata\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	69.50 KB	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.02 KB	7bc3187d55841c9e1a344c0936554fe8ba2f1eded4a12f7d90c92f09cdf646b5	✖
\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.96 KB	233ae0e8cb87222b8585c10241c7e151326cd8cceb7ee1c8b72318f47d3939d9	✖
\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	354 bytes	5f82ac871321ef483998b64858193760028723ef6a8afd379264f82b4c97fd0f	✖
\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentfallback.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	3.60 KB	bfc45d379fac92436e1579ca080690eb4a3a937bf6ef4528f4cdfe583d1af853	✖
\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentlogon.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	3.52 KB	873a4b751f9b0b144f0ffa7decc07b4f002731f636574f8d522ec85b9393e2ef	✖
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\branding.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	328.67 KB	fbaa24f5e36427d11ca1b7f7c1d71faac3efa04c022a527e21923b2e241fbae5	✖
\\?\C:\$Recycle.Bin\S-1-5-21-4219442223-4223814209-3835049652-1000\desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	386 bytes	644ca55cb7b7202cadf248168abad91e68cd60c18d9f432135ca3136693d0d87	✖
\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.42 KB	df88ffdd3e6207766ebb7f1451eab377740a669dfc5a64adda882ab708fc9587	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	231.44 KB	ffc7259bfe8b0a1b1ec11a3a937cddf44a5a5aa88e354b74993a0a2774c4ee98	✖
\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.35 KB	2fde5aec58d7d1897417187d716a6da8f24129b8073a0984b3320d9681dee867	✖
\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.44 KB	e2b5943591f004ed5005a71cd408f87513ec61defb864f1b0decf3ef1acb6659	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.77 KB	3e2a6d33ff41ccc130df47557402ca8eb668520d691e50f62856ee4a3c191252	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	10240.00 KB	e3e89647dc4546e34658bd88b63120981094fca3f5d2c500457a0338cd725100	✖
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlklr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	4683.47 KB	0a1d5a29f3981a871953b033e3473bff634be681ecc164781132f853f3ef8a68	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.88 KB	1ba1c1cb33b46cb86eef4e3df6c5f0ce84c5762d639917496abed4cb15e81906	✖
\\?\C:\Program Files\Java\jre1.8.0_171\README.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	290 bytes	9209d9e5095c11e3835bddac9fef25bf40dd4b8b27b32f5e7846458da74bb9a3	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_MoveNoDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	434 bytes	819c557c9f1a2ec7bef2d02868ae20eeb691d3cdb58264240383375ab90a7577	✖
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	6976.77 KB	ed68d37598af56da6c0d5d9c189c992827a0c20597d726faf99e65f094d30204	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	4246.42 KB	16ef8452d4ab4f1b0db4d8dc1b012f6386d5544b3c96752897a99ac8b16f4ca9	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.25 KB	bf31b1f506432631c6c1dd8015d32490a2adb64a438100e1d167578a923e633f	✖
\\?\C:\BOOTSECT.BAK.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	8.25 KB	f473241d06d855f78ae00a9bb01cb4fc67e26fc50c4666024158aebd19090aa7	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	10240.00 KB	8992d8b629a865b71e526769575825b65d9916dbcff6ba49486807bfc81ed7c2	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash@2x.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	15.16 KB	08727d69fb4766cb427d59f72f94f81110501f598fc6c167262337fd59b544e6	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.00 KB	26edfe7d02b84614f44595bf613855a6e16690939b1325867b0567a4585f916b	✖
\\?\C:\Boot\BOOTSTAT.DAT.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	64.25 KB	8af420b9c9480fdbf171ac634a2c533b82d7d31f4dfb7460ccd13ccc103f2b2a	✖
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.66 KB	9875d80db7e8b6273085bf3c43b9e85656f6993eafbc7aa7e72181316000258a	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	3120.27 KB	0519b124cc1c3bfa328aafd3ee4c0c4aa4fecaa4954fd23e7d62bc6c641f5375	✖
\\?\C:\Program Files\Java\jre1.8.0_171\THIRDPARTYLICENSEREADME-JAVAFX.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	104.56 KB	b045d7b8290a087c4b73527ef02504f8844010c105a815542eaea2f5305d8864	✖
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	2.00 KB	6c38b5445cfcf6ab4bb1e93b35a31e60411f8d2cfa6bd6389f36db7b9b58cb88	✖
\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	4.02 KB	aa0289930eda6afe811ff93b3202c7f2a179760377a1c511f896787cbf6a325e	✖
\\?\C:\Program Files\Microsoft Office\Office16\Mso Example Setup File A.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	354 bytes	c5819ce4fb64823f4aa440779400a2d7e7d8b16ba996f419ec0671f602e569a0	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\setup.chm.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	81.10 KB	072b0bbac42ed2f4b0b1ba8a2bd77f1ddd37030b80b638360cbded24a363c5b7	✖
\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.89 KB	67928ce83fdafa37358cc98f68c616cb84bef4a145fdae16712fe877ca85a11e	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\ffjcext.zip.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	14.06 KB	b3b8c740e85948ed72c3e2c432b5157bf17e7ca502b3f2917e2dd66358a2149b	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	576.96 KB	060d8a86eeeb2c0c5ddf49c041dfb8cb26a0429f02dbdb36cb3ec40f30535d63	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	8.63 KB	7be5574931eca408e8180a2d9bf6dadc6e3f01735caef942400ed1555f481b22	✖
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.99 KB	4c8484acfc006a6eaee38621189974b88c915b9229a87f1bea242b270400d5b7	✖
\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	3.02 KB	e7a2411b3fe068ec329c4eb5f30c3914e32aae7bb0a4d18808b0d0df00101062	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	8.53 KB	47a7270b14887720e4ec5dfdb4920c98eebc47131cbbdeaeee36e2b614262772	✖
\\?\C:\Program Files\desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	418 bytes	5cab509a3a56bff787d1607de4a574c54fcfb37cdae192d2ff1e9224dddd76f	✖

File Name	File Size	SHA256	YARA Match
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	3116.25 KB	da4ca6480830d96cb672eacb228cc8ceb52039be3844d28be9606b41a7d71b2c	✖
\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	1.67 KB	1a5c08265ee9592cf0666e7be3c5a86e4ef6fb1b277359b48220e932f2386799	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\tzdb.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	103.69 KB	c72b3ec91975c111461028d99f45d6af10984c948d30e2e8137d272b35d591f5	✖

Host Behavior

Type	Count
System	62
Module	37
File	6211
Environment	1
-	365
Mutex	41
Process	1243
Registry	20
-	6
-	10

Process #2: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 36311, Reason: Child Process
Unmonitor End Time	End Time: 68919, Reason: Terminated
Monitor duration	32.61s
Return Code	1073807364
PID	3800
Parent PID	3776
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	69.50 KB	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	32
Module	28
File	1362
Environment	1
-	133
Mutex	28
Registry	19
-	8
-	4

Process #3: cmd.exe

ID	3
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\system32\cmd.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 41204, Reason: Child Process
Unmonitor End Time	End Time: 68806, Reason: Terminated
Monitor duration	27.60s
Return Code	1073807364
PID	3876
Parent PID	3776
Bitness	64 Bit

Host Behavior

Type	Count
Module	3
File	120
Environment	5
Process	2
-	1

Process #4: cmd.exe

ID	4
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\system32\cmd.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 41212, Reason: Child Process
Unmonitor End Time	End Time: 68950, Reason: Terminated
Monitor duration	27.74s
Return Code	1073807364
PID	3884
Parent PID	3776
Bitness	64 Bit

Host Behavior

Type	Count
Module	3
File	98
Environment	5
Process	2
-	1

Process #5: netsh.exe

ID	5
File Name	c:\windows\system32\netsh.exe
Command Line	netsh advfirewall set currentprofile state off
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 41985, Reason: Child Process
Unmonitor End Time	End Time: 68773, Reason: Terminated
Monitor duration	26.79s
Return Code	1073807364
PID	3924
Parent PID	3876
Bitness	64 Bit

Host Behavior

Type	Count
System	18
Module	49
Registry	23

Process #6: vssadmin.exe

ID	6
File Name	c:\windows\system32\vssadmin.exe
Command Line	vssadmin delete shadows /all /quiet
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 41997, Reason: Child Process
Unmonitor End Time	End Time: 68948, Reason: Terminated
Monitor duration	26.95s
Return Code	1073807364
PID	3932
Parent PID	3884
Bitness	64 Bit

Process #7: vssvc.exe

ID	7
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: 44878, Reason: RPC Server
Unmonitor End Time	End Time: 163477, Reason: Terminated by timeout
Monitor duration	118.60s
Return Code	Unknown
PID	3956
Parent PID	3932
Bitness	64 Bit

Host Behavior

Type	Count
System	3

Process #10: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe

ID	10
File Name	c:\users\keecfmwgj\appdata\local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 131665, Reason: Autostart
Unmonitor End Time	End Time: 163477, Reason: Terminated by timeout
Monitor duration	31.81s
Return Code	Unknown
PID	1876
Parent PID	1788
Bitness	32 Bit

Host Behavior

Type	Count
System	47
Module	33
File	821
Environment	1
-	178
Mutex	56
Process	33
Registry	16
-	8
-	4

Process #11: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe

ID	11
File Name	c:\users\keecfmwgj\appdata\local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 131776, Reason: Autostart
Unmonitor End Time	End Time: 133598, Reason: Terminated
Monitor duration	1.82s
Return Code	0
PID	1884
Parent PID	1788
Bitness	32 Bit

Host Behavior

Type	Count
System	5
Module	8
File	3
Environment	1
-	7
Mutex	4

Process #12: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe

ID	12
File Name	c:\programdata\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
Command Line	"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 131816, Reason: Autostart
Unmonitor End Time	End Time: 133243, Reason: Terminated
Monitor duration	1.43s
Return Code	0
PID	1896
Parent PID	1788
Bitness	32 Bit

Host Behavior

Type	Count
System	5
Module	8
File	3
Environment	1
-	7
Mutex	4

Process #13: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe

ID	13
File Name	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 131857, Reason: Autostart
Unmonitor End Time	End Time: 133430, Reason: Terminated
Monitor duration	1.57s
Return Code	0
PID	1904
Parent PID	1788
Bitness	32 Bit

Host Behavior

Type	Count
System	5
Module	8
File	3
Environment	1
-	7
Mutex	4

Process #14: 34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe

ID	14
File Name	c:\users\keecfmwgj\appdata\local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 138172, Reason: Child Process
Unmonitor End Time	End Time: 163477, Reason: Terminated by timeout
Monitor duration	25.30s
Return Code	Unknown
PID	1896
Parent PID	1876
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\Cultures\OFFICE.ODF.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\Cultures\OFFICE.ODF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\DataModel\Cartridges\orcl7.xsl.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	61
Module	28
File	8088
Environment	1
-	359
Mutex	23
Registry	16
-	6
Process	818
-	10

Process #15: cmd.exe

ID	15
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\system32\cmd.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 138646, Reason: Child Process
Unmonitor End Time	End Time: 163477, Reason: Terminated by timeout
Monitor duration	24.83s
Return Code	Unknown
PID	768
Parent PID	1896
Bitness	64 Bit

Host Behavior

Type	Count
Module	3
File	116
Environment	5
Process	2
-	1

Process #16: cmd.exe

ID	16
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\system32\cmd.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 138677, Reason: Child Process
Unmonitor End Time	End Time: 163477, Reason: Terminated by timeout
Monitor duration	24.80s
Return Code	Unknown
PID	820
Parent PID	1896
Bitness	64 Bit

Host Behavior

Type	Count
Module	3
File	94
Environment	5
Process	2
-	1

Process #17: netsh.exe

ID	17
File Name	c:\windows\system32\netsh.exe
Command Line	netsh advfirewall set currentprofile state off
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 139281, Reason: Child Process
Unmonitor End Time	End Time: 163477, Reason: Terminated by timeout
Monitor duration	24.20s
Return Code	Unknown
PID	1784
Parent PID	768
Bitness	64 Bit

Host Behavior

Type	Count
System	17
Module	46
Registry	23

Process #18: vssadmin.exe

ID	18
File Name	c:\windows\system32\vssadmin.exe
Command Line	vssadmin delete shadows /all /quiet
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 139309, Reason: Child Process
Unmonitor End Time	End Time: 163477, Reason: Terminated by timeout
Monitor duration	24.17s
Return Code	Unknown
PID	1804
Parent PID	820
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc	C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe, c:\programdata\microsoft\wi... ...AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	Sample File	69.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
b7a8fae07c9db3f385e88c34fe2c1e5c99e47bfc78a5178b49afcfe3d950f147	\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-000000FF1CE}-C\GrooveMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.35 KB	application/octet-stream	Access, Create, Write	CLEAN
faa06e5d54ade372d58f6124c58f3c96f5993b2b86143adb967ddd306db6edc6	\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_MoveDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	418 bytes	application/octet-stream	Access, Create, Write	CLEAN
4b489bdc6de785675c5de881b274f0a79f6ff91f723c0fd465cbded065c0d3ab	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PublisherMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.88 KB	application/octet-stream	Access, Create, Write	CLEAN
91e305b0cf2c439856477ded f2e654e18302a09eb83cd1095482b495ba92e190	\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File A.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	386 bytes	application/octet-stream	Access, Create, Write	CLEAN
c6e5e1b3bb59a4a375a8dcf259e7aa98957cd022ec7d2b9490870b25f6c23d3f	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-000000FF1CE}-C\branding.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	328.67 KB	application/octet-stream	Access, Create, Write	CLEAN
4b1fe95d4a945584b91947e5404ea649c05ce747a04724b97547dc50e0b53b4c	\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.24 KB	application/octet-stream	Access, Create, Write	CLEAN
c0e557ac122fc280c15ea419a5ec39bfca130ec82dab89333361638c9f3b06b2	\\?\C:\Program Files\Java\jre1.8.0_171\lib\jvm.hprof.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	4.38 KB	application/octet-stream	Access, Create, Write	CLEAN
dd54e255683302bbaf575e6e5df809f547668b395397eca40ea56594f6a5a429	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\PowerPointMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\powerpointmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	3100.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f2d0a1f96864d2c3db5d64e6a0b26bdd9faadbba7328acba3facc77715631d58	\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-000000FF1CE}-C\Office64MUISet.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.27 KB	application/octet-stream	Access, Create, Write	CLEAN
9704a2f80f5ee74cbc3dba73e3005fc6ff3bd9a9d3d34f3746878ea41a63433a	\\?\C:\Program Files\Java\jre1.8.0_171\Welcome.html.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.17 KB	application/octet-stream	Access, Create, Write	CLEAN
3f5bf377d258907a41bab80257934baa88950924e8215b820630c2f3959eb540	\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_LinkDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	434 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
46280bc5468ffca4e61aa1be4da69141c57851140035748 9b6a2ba2db1728cdd	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\osetup.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\osetup.dll.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
200143c5b806f1c6f0e24b77a6cf6e5423001453e5e8ae12d8621268a0e47c16	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.67 KB	application/octet-stream	Access, Create, Write	CLEAN
b3aa2c60c78f5e7782cc385490dc49a4d501c650fbc19ac4f2f1300dc540d8b5	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	593.94 KB	application/octet-stream	Access, Create, Write	CLEAN
8eebfdfc86ef7e6ea21ef3312de5aad87414fbc64b9587dba2673bff2c8c9a70	\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File B.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	386 bytes	application/octet-stream	Access, Create, Write	CLEAN
65cd37e81b5cdaf50039ec8d708c8455225ad5d5949385adec6fdc1234ee3d14	\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_CopyNoDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	434 bytes	application/octet-stream	Access, Create, Write	CLEAN
66e00a3ef790eaa85342a88723be1a97fe69f5d0840a8cf70b1d4b4b94004de2	\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.11 KB	application/octet-stream	Access, Create, Write	CLEAN
c52fa973be5ec3a8553f54b5687cfea43be5e57b8fd089ea23d2bbdf9b7870e7	\\?\C:\Program Files\Java\jre1.8.0_171\bin\server\Xusage.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.63 KB	application/octet-stream	Access, Create, Write	CLEAN
8c294b7edf043ee719edcc3796f363aea2d431ee1c2db09b54260c45280b3122	\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_LinkNoDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	434 bytes	application/octet-stream	Access, Create, Write	CLEAN
e109cb56dd1d27cce7a3eba04f2dceefa15d85b0aff7d350d8923b47c4c1e471	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	5.39 KB	application/octet-stream	Access, Create, Write	CLEAN
969ce0c61bc817e6340d1f09366df5dcf9d100e9e4d01b24ba5913f6755df918	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\office64ww.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	4620.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
8cf828796a32d97c7c89c3fe989ca8ee51c6e6e8a2a7d0a6970dd29591b1ab68	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propsww.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b2de199ea42e748adf21cba5060c27c38354bf73d71026dc109d8895774d4022	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	198.41 KB	application/octet-stream	Access, Create, Write	CLEAN
1a221cbbe81e313392f6179e374008312d876a4b24a33a6d7c2bef066ce582da	\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.85 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
423cd9178b1a64a79659ea8cb44bf4410e9afd536b288882d63b3e5f6c2421ab	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.36 KB	application/octet-stream	Access, Create, Write	CLEAN
00c0cbcdd53d6f664bb4d4bd82e9fa00fa4fbb1f983446732ce4a4e1a614a1e5	\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-000000FF1CE}-C\WordMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.30 KB	application/octet-stream	Access, Create, Write	CLEAN
b0e2fe1014a47060ccb6fb5648e64725f2a3f518db2b414f19e62eed22a0ace0	\\?\C:\Program Files\Common Files\PXzWVbDzjHOIV50.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	38.96 KB	application/octet-stream	Access, Create, Write	CLEAN
37d3bb622e177537945073aecc12c01dc9b8098845f2e36e2e845e8818e361cf	\\?\C:\Program Files\Common Files\EycKgld_ulVGhuCKmRk2.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	74.00 KB	application/octet-stream	Access, Create, Write	CLEAN
04357036f0c7fe413596b36afc90414b15ae5de789fe172bd8c6dc9f569c8e1b	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	27.38 KB	application/octet-stream	Access, Create, Write	CLEAN
598cd6fa7925a6a0b50ff55ee9ab462f2560d074a6f241104d4e9b74da62a51a	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-000000FF1CE}-C\OfficeMUISet.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.27 KB	application/octet-stream	Access, Create, Write	CLEAN
88576a3518367cfe0bb52a6609d8863150b5c866655cd88d8a07f0aea5f3a430	\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.64 KB	application/octet-stream	Access, Create, Write	CLEAN
7cdac29a27b8b5d014727520173989f1cef40b679b61551ccafa329ec7ff62ac	\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	3.30 KB	application/octet-stream	Access, Create, Write	CLEAN
5b30f94205b5d2ce385d811d0ac134db3cec79ed5837b443b53880c2383fba3d	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	7.22 KB	application/octet-stream	Access, Create, Write	CLEAN
3e068024d49151d033734780cb37154ef43da5b5b0eb1b4d5975a5029f496c41	\\?\C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	898 bytes	application/octet-stream	Access, Create, Write	CLEAN
9e267237ed9a3de1225df641bfcd1283fcd9b5f9330032e0ee180a0c0cd1e254	\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash_11@2x-lic.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	12.22 KB	application/octet-stream	Access, Create	CLEAN
574c72b06272e104b9c9f5f9192236ccb5a47cddbd3359250b0cbb0cafc06cbd	\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_CopyDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	434 bytes	application/octet-stream	Access, Create, Write	CLEAN
a0995ccaed3749a4daff0fe9ea46dad23c27c37e0c9030633bd609fd70754807	\\?\C:\Program Files\Java\jre1.8.0_171\THIRDPARTYLICENSEREADME.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	142.05 KB	application/octet-stream	Access, Create, Write	CLEAN
d23f64cbb8803d08857f440bb18486596ef1a21e544cd35e55f4ecd1ee114b8a	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-000000FF1CE}-C\pss10r.chm.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	14.50 KB	application/octet-stream	Access, Create, Write	CLEAN
fe294895381070bb769018225f5c9d98f33507790169a293cd39c1cc0ac12f57	\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote-PipelineConfig.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	802 bytes	application/octet-stream	Access, Create, Write	CLEAN
f012df0a617b7761749fb8613163767b2e6f64d94f57edd3e4d98ee8d4b41483	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	6.17 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b339ee96d06d171334cb31b18563908fdbcddeb728054c82e28c1d8ce7008aa4	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.27 KB	application/octet-stream	Access, Create, Write	CLEAN
2f95187bc3f10d4fa81f4466e05efb8d924e9853a78451c9c944f948d0054c6d	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	5.13 KB	application/octet-stream	Access, Create, Write	CLEAN
19c6bd387b0e8df89c71b0042c65b8a22ae645d8d09aec7c4157179300d59913	\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.44 KB	application/octet-stream	Access, Create, Write	CLEAN
98f25ad5ee9366d79329a9eb7719dbf332f1f308468da271aa21b0803a3da634	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\PidGenX.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1244.83 KB	application/octet-stream	Access, Create, Write	CLEAN
3e67fb43acca040c086a2043d0e7e39c754328e6f7abf6cdc199b34afef83324	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	16.96 KB	application/octet-stream	Access, Create, Write	CLEAN
7e1aa5b82e4aad599ad98614d84faa5ad7b9b0526932cfe8d4e6bca7634cf882	c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excellr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage, \\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	6402.59 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
55a526535b994f6845c0060bd98e6e57eba4e80d88835a98cab21fc7d5c3c8c7	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.88 KB	application/octet-stream	Access, Create, Write	CLEAN
8aefc19745867e40400b31c9158b5127e3a6f118227f409b4528bed57633fc44	\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.02 KB	application/octet-stream	Access, Create, Write	CLEAN
e010fd78c4574ad2407d481514ae8df71942b9867f04318cd0ea90373a5913b9	c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage, \\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	3532.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
bd83274c1333cabadadc21d38823837354d4c50cd12c0880b96a54c8243316b0	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.77 KB	application/octet-stream	Access, Create, Write	CLEAN
32ffa3bc06afa71b041b22d224d825111132e4ea7612e16c5d3c4025a2bbf012	\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.77 KB	application/octet-stream	Access, Create, Write	CLEAN
8d31c79a5a20ac24edab811d2fad0ecedc52d52d74de1e0dbd285e06b3ed088a	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.88 KB	application/octet-stream	Access, Create, Write	CLEAN
be30d31e89e62c93d898c670ac25633e29ab658d8763112d100bb9ba6e6c4960	\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.27 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a4a78fb5ce3b6a786442bc61ab958d0778eb3ae87d1403ad1f184efe16e83e86	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\pptlr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	6930.48 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
cc3375b5cdfc720d0d97a88666f90f1411b7662bde58cfe73d30d83789c9871c	\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote-manifest.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	642 bytes	application/octet-stream	Access, Create, Write	CLEAN
e1592a2466b975ea73fb400cbf72345ed8bdda4123b945ba82a4c75e508aa45e	\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash_11-lic.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	7.88 KB	application/octet-stream	Access, Create, Write	CLEAN
f895e08eb029e4008023d4ff13f110d83615fd7e7913a868609b0012773cae58	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excelmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	3100.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
bbeabdf761a88156583ff5651cd7cc09cb3d0829e13cc05ac576e40fc78b17b7	\\?\C:\Program Files\Common Files\o9nleU.bmp.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	52.55 KB	application/octet-stream	Access, Create, Write	CLEAN
48d13089b65ebdc84e807301e9348b6515bd869b0630e1a39e79611382d59a7f	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propsww2.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
baa68efb0528b2eaaf44893da2d3b1c8ed0bacbf9a02a9731615716d84a3ff6c	\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\invalid32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	418 bytes	application/octet-stream	Access, Create, Write	CLEAN
7bc3187d55841c9e1a344c0936554fe8ba2f1eded4a12f7d90c92f09cdf646b5	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.02 KB	application/octet-stream	Access, Create, Write	CLEAN
233ae0e8cb87222b8585c10241c7e151326cd8cceb7ee1c8b72318f47d3939d9	\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.96 KB	application/octet-stream	Access, Create, Write	CLEAN
5f82ac871321ef483998b6485819376002872 3ef6a8afd379264f82b4c97fd0f	\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	354 bytes	application/octet-stream	Access, Create, Write	CLEAN
bfc45d379fac92436e1579ca080690eb4a3a937bf6ef4528f4cdfe583d1af853	\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentfallback.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	3.60 KB	application/octet-stream	Access, Create, Write	CLEAN
873a4b751f9b0b144f0ffa7decc07b4f002731f636574f8d522ec85b9393e2ef	\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentlogon.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	3.52 KB	application/octet-stream	Access, Create, Write	CLEAN
fbaa24f5e36427d11ca1b7f7c1d71faac3efa04c022a527e21923b2e241fbae5	\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\branding.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	328.67 KB	application/octet-stream	Access, Create, Write	CLEAN
644ca55cb7b7202cadf248168abad91e68cd60c18d9f432135ca3136693d0d87	\\?\C:\$Recycle.Bin\S-1-5-21-4219442223-4223814209-3835049652-1000\desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	386 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
df88ffdd3e6207766ebb7f1451eab377740a669dfc5a64adda882ab708fc9587	\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.42 KB	application/octet-stream	Access, Create, Write	CLEAN
ffc7259bfe8b0a1b1ec11a3a937cddf44a5a5aa88e354b74993a0a2774c4ee98	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	231.44 KB	application/octet-stream	Access, Create, Write	CLEAN
2fde5aec58d7d1897417187d716a6da8f24129b8073a0984b3320d9681dee867	\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.35 KB	application/octet-stream	Access, Create, Write	CLEAN
e2b5943591f004ed5005a71cd408f87513ec61defb864f1b0decf3ef1acb6659	\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.44 KB	application/octet-stream	Access, Create, Write	CLEAN
3e2a6d33ff41ccc130df47557402ca8eb668520d691e50f62856ee4a3c191252	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.77 KB	application/octet-stream	Access, Create, Write	CLEAN
e3e89647dc4546e34658bd88b63120981094fca3f5d2c500457a0338cd725100	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\owow64ww.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
0a1d5a29f3981a871953b033e3473bff634be681ecc164781132f853f3ef8a68	c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlklr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage, \\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	4683.47 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
1ba1c1cb33b46cb86eef4e3df6c5f0ce84c5762d639917496abed4cb15e81906	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.88 KB	application/octet-stream	Access, Create, Write	CLEAN
9209d9e5095c11e3835bddac9fef25bf40dd4b8b27b32f5e7846458da74bb9a3	\\?\C:\Program Files\Java\jre1.8.0_171\README.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	290 bytes	application/octet-stream	Access, Create, Write	CLEAN
819c557c9f1a2ec7bef2d02868ae20eeb691d3cdb58264240383375ab90a7577	\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_MoveNoDrop32x32.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	434 bytes	application/octet-stream	Access, Create, Write	CLEAN
ed68d37598af56da6c0d5d9c189c992827a0c20597d726faf99e65f094d30204	c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage, \\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	6976.77 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
16ef8452d4ab4f1b0db4d8dc1b012f6386d5544b3c96752897a99ac8b16f4ca9	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	4246.42 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
bf31b1f506432631c6c1dd8015d32490a2adb64a438100e1d167578a923e633f	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.25 KB	application/octet-stream	Access, Create, Write	CLEAN
f473241d06d855f78ae00a9bb01cb4fc67e26fc50c4666024158aebd19090aa7	\\?\C:\BOOTSECT.BAK.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	8.25 KB	application/octet-stream	Access, Create, Write	CLEAN
8992d8b629a865b71e526769575825b65d9916dbcff6ba49486807bfc81ed7c2	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\proplusww.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
08727d69fb4766cb427d59f72f94f81110501f598fc6c167262337fd59b544e6	\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash@2x.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	15.16 KB	application/octet-stream	Access, Create, Write	CLEAN
26edfe7d02b84614f44595bf613855a6e16690939b1325867b0567a4585f916b	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.00 KB	application/octet-stream	Access, Create, Write	CLEAN
8af420b9c9480fdbf171ac634a2c533b82d7d31f4dfb7460ccd13ccc103f2b2a	\\?\C:\Boot\BOOTSTAT.DAT.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	64.25 KB	application/octet-stream	Access, Create, Write	CLEAN
9875d80db7e8b6273085bf3c43b9e85656f6993eafbc7aa7e72181316000258a	\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.66 KB	application/octet-stream	Access, Create, Write	CLEAN
0519b124cc1c3bfa328aafd3ee4c0c4aa4fecaa4954fd23e7d62bc6c641f5375	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage, c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publishermui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Dropped File	3120.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b045d7b8290a087c4b73527ef02504f8844010c105a815542eaea2f5305d8864	\\?\C:\Program Files\Java\jre1.8.0_171\THIRDPARTYLICENSEREADME-JAVAFX.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	104.56 KB	application/octet-stream	Access, Create, Write	CLEAN
6c38b5445cfcf6ab4bb1e93b35a31e60411f8d2cfa6bd6389f36db7b9b58cb88	\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	2.00 KB	application/octet-stream	Access, Create, Write	CLEAN
aa0289930eda6afe811ff93b3202c7f2a179760377a1c511f896787cbf6a325e	\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	4.02 KB	application/octet-stream	Access, Create, Write	CLEAN
c5819ce4fb64823f4aa440779400a2d7e7d8b16ba996f419ec0671f602e569a0	\\?\C:\Program Files\Microsoft Office\Office16\Mso Example Setup File A.txt.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	354 bytes	application/octet-stream	Access, Create, Write	CLEAN
072b0bbac42ed2f4b0b1ba8a2bd77f1ddd37030b80b638360cbded24a363c5b7	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\setup.chm.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	81.10 KB	application/octet-stream	Access, Create, Write	CLEAN
67928ce83fdafa37358cc98f68c616cb84bef4a145fdae16712fe877ca85a11e	\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.89 KB	application/octet-stream	Access, Create, Write	CLEAN
b3b8c740e85948ed72c3e2c432b5157bf17e7ca502b3f2917e2dd66358a2149b	\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\ffjcext.zip.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	14.06 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
060d8a86eeeb2c0c5ddf49c041dfb8cb26a0429f02dbdb36cb3ec40f30535d63	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	576.96 KB	application/octet-stream	Access, Create, Write	CLEAN
7be5574931eca408e8180a2d9bf6dadc6e3f01735caef942400ed1555f481b22	\\?\C:\Program Files\Java\jre1.8.0_171\lib\deploy\splash.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	8.63 KB	application/octet-stream	Access, Create, Write	CLEAN
4c8484acfc006a6eaee38621189974b88c915b9229a87f1bea242b270400d5b7	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.99 KB	application/octet-stream	Access, Create, Write	CLEAN
e7a2411b3fe068ec329c4eb5f30c3914e32aae7bb0a4d18808b0d0df00101062	\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	3.02 KB	application/octet-stream	Access, Create, Write	CLEAN
47a7270b14887720e4ec5dfdb4920c98eebc47131cbbdeaeee36e2b614262772	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	8.53 KB	application/octet-stream	Access, Create, Write	CLEAN
5cab509a3a56bff787d1607de4a574c54fcfb37cdae192d2ff1e9224ddedd76f	\\?\C:\Program Files\desktop.ini.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	418 bytes	application/octet-stream	Access, Create, Write	CLEAN
da4ca6480830d96cb672eacb228cc8ceb52039be3844d28be9606b41a7d71b2c	c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage, \\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	3116.25 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
1a5c08265ee9592cf0666e7be3c5a86e4ef6fb1b277359b48220e932f2386799	\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	1.67 KB	application/octet-stream	Access, Create, Write	CLEAN
c72b3ec91975c111461028d99f45d6af10984c948d30e2e8137d272b35d591f5	\\?\C:\Program Files\Java\jre1.8.0_171\lib\tzdb.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Dropped File	103.69 KB	application/octet-stream	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\office16\csi.dll.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPOBJS.DLL.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsScenesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\acclr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\OmdProject.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\Cultures\OFFICE.ODF.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwrusalm.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\Pipeline.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlklr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovemui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Performance\Title_Page_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\Fonts\jpn_boot.ttf.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\inkobj.dll.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\program files\windows nt\tabletextservice\tabletextservicesimplifiedquanpin.txt.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\Mso40Uiwin32client.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsNotesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppsvc.exe.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\dvd maker\dvdmaker.exe.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files\common files\microsoft shared\ink\hwrusash.dat.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\boot\fonts\chs_boot.ttf.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\Mso30win32client.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\hwruksh.dat.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\msocache\all users\{90160000-012b-0409-0000-0000000ff1ce}-c\lyncmui.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\dvd maker\shared\dvdstyles\sports\sportsmaintonotesbackground.wmv.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\micaut.dll.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excellr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\CMigrate.exe.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToScenesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\office16\1033\ado210.chm.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\dvd maker\shared\dvdstyles\performance\title_page.wmv.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\osetup.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\programdata\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files\dvd maker\shared\dvdstyles\sports\sportsmaintoscenesbackground.wmv.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files\common files\microsoft shared\filters\visfilt.dll.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\windows nt\tabletextservice\tabletextservicesimplifiedzhengma.txt.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\dvd maker\shared\dvdstyles\sports\sportsnotesbackground.wmv.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\FlickAnimation.avi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	Accessed File, Sample File	Access	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\Mso99Lwin32client.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\Fonts\cht_boot.ttf.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\Filters\offfiltx.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\OmdBase.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officemui.msi.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\hwrukm.dat.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\mraut.dll.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppcext.dll.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.es\proof.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onotelr.cab.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.msi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\dvd maker\shared\dvdstyles\sports\sportsscenesbackground.wmv.id[8443a5af-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainToNotesBackground_PAL.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\OFFICE16\Mso20win32client.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\Fonts\kor_boot.ttf.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsMainBackground.wmv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
\\?\C:\Program Files\DVD Maker\PipeTran.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Delete, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\tabskb.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\38.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\System\msadc\msadcf.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows NT\TableTextService\TableTextServiceYi.txt	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\SpecialOccasion\NavigationUp_SelectionSubpicture.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\SlideShow.Gadget\images\prev_rest.png	Accessed File	Access, Write	CLEAN
\\?\C:\Program Files\Common Files\System\msadc\en-US\msadcfr.dll.mui.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Currency.Gadget\images\add_over.png	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\System\msadc\msdarem.dll	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\Microsoft Shared\Stationery\To_Do_List.emf.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\highlight.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Travel\passport_mask_right.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\Microsoft Shared\MSInfo\msinfo32.exe.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\nl-NL\tipresx.dll.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.xml	Accessed File	Access, Delete, Read	CLEAN
\\?\C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\DataModel\Cartridges\orcl7.xsl	Accessed File	Access, Read	CLEAN
\\?\UNC\192.168.0.1\documents\ydACID.jpg	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\circle_glass_Thumbnail.bmp.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\m2U2YIUMt.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Clock.Gadget\images\diner_settings.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\3.png	Accessed File	Access	CLEAN
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\C:\Program Files\Common Files\Microsoft Shared\Stationery\Stars.htm.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\HueCycle\1047x576black.png	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\Microsoft Shared\VSTO\vstoee90.tlb	Accessed File	Access, Delete, Read	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\9.png	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\RSSFeeds.Gadget\images\rssLogo.gif.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\SlideShow.Gadget\images\pause_hov.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\AhwQOJysH9.jpg	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\undocked_black_moon-new_partly-cloudy.png	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\fUgAWuSkZ3EbpCZ5Rvs.gif	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\RSSFeeds.Gadget\logo.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\docked_black_few-showers.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\ResizingPanels\bandwidth.png	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\RSSFeeds.Gadget\images\buttonDown_On.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Travel\travel.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\5.png	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Sports\SportsNotesBackground_PAL.wmv	Accessed File	Access, Create, Delete, Write	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\en-US\join.avi	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\System\ado\msadox.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\undocked_gray_thunderstorm.png	Accessed File	Access	CLEAN
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab	Accessed File	Access, Delete, Read	CLEAN
\\?\UNC\192.168.0.1\documents\B2EjwcG.xls	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\AhsbCQy.csv.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Travel\btn-next-static.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Java\jre1.8.0_171\Welcome.html	Accessed File	Access, Delete, Read	CLEAN
\\?\UNC\192.168.0.1\documents\d9y1S5e4eLHUosqR.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images\39.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\en-US\boxed-correct.avi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\SpecialOccasion\SpecialNavigationUp_ButtonGraphic.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Java\jre1.8.0_171\bin\dcpr.dll	Accessed File	Access, Delete, Read	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\circleround_glass.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\Pbnq0tEevfYiPYev3.flv	Accessed File	Access	CLEAN
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File, Dropped File	Access, Create, Write	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Vignette\whiteband.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\VQa7D2fVvyShxsM.xlsx	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\rSvaTPcyuRZ.avi.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Common Files\Microsoft Shared\ink\he-IL\tipresx.dll.mui	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Pets\Pets_btn-previous-static.png.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\C:\Program Files\Java\jre1.8.0_171\bin\api-ms-win-crt-environment-l1-1-0.dll.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access, Create, Write	CLEAN
\\?\UNC\192.168.0.1\documents\2XXFjQNQ26X8Wc.swf.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\qWCrNc.m4a.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN
\\?\UNC\192.168.0.1\documents\nXMaDbExzV3GNxn.rtf.id[8443A5AF-2250].[wewillhelpyou@qq.com].adage	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Windows Sidebar\Gadgets\RSSFeeds.Gadget\images\rssLogo.gif	Accessed File	Access	CLEAN
\\?\C:\Program Files\DVD Maker\Shared\DvdStyles\Vignette\vignettemask25.png	Accessed File	Access	CLEAN

Reduced dataset

Mutex

Name	Operations	Parent Process Name	Verdict
Global\22508443A5AF00	access, delete	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
Global\22508443A5AF01	access, delete	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup	access, read	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Common Startup	access, read	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh	access	netsh.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	access	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc	access, write	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	access	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Common Startup	access, read	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc	access, write	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	access	34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	CLEAN

Process

Process Name	Commandline	Verdict
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	"C:\Users\kEecfMwgj\Desktop\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"	MALICIOUS
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	"C:\Users\kEecfMwgj\Desktop\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"	MALICIOUS
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	"C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"	MALICIOUS
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	"C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"	MALICIOUS
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"	MALICIOUS
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	"C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"	MALICIOUS
34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe	"C:\Users\kEecfMwgj\AppData\Local\34c1121937c35b39b654428cf3fc6b16e3e2eed03c1ccbcfc77183d1749ebadc.exe"	MALICIOUS

Process Name	Commandline	Verdict
cmd.exe	"C:\Windows\system32\cmd.exe"	SUSPICIOUS
cmd.exe	"C:\Windows\system32\cmd.exe"	SUSPICIOUS
netsh.exe	netsh advfirewall set currentprofile state off	CLEAN
vssadmin.exe	vssadmin delete shadows /all /quiet	CLEAN
cmd.exe	"C:\Windows\system32\cmd.exe"	CLEAN
netsh.exe	netsh advfirewall set currentprofile state off	CLEAN
vssadmin.exe	vssadmin delete shadows /all /quiet	CLEAN
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN
cmd.exe	"C:\Windows\system32\cmd.exe"	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.7.1
Dynamic Engine Version	4.7.1 / 11/21/2022 04:40
Static Engine Version	4.7.1.0 / 2022-11-21 03:00:41
AV Exceptions Version	4.7.2.20 / 2022-12-15 11:43:19
Link Detonation Heuristics Version	4.7.2.20 / 2022-12-15 11:43:19
Smart Memory Dumping Rules Version	4.7.2.20 / 2022-12-15 11:43:19
Config Extractors Version	4.7.2.22 / 2023-01-05 11:05:11
Signature Trust Store Version	4.7.2.21 / 2023-01-03 15:44:56
VMRay Threat Identifiers Version	4.7.2.23 / 2023-01-07 18:36:42
YARA Built-in Ruleset Version	4.7.2.21

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
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	8.0.1710.11

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