MALICIOUS

Classifications: Ransomware

Threat Names: Ryuk

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe**
ID	#7097337
MD5	987336d00fdbec3bcdb95b078f7de46f
SHA1	8bbded5710280f055bf53f9e4f6c5abb596f7899
SHA256	a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e
File Size	548.30 KB
Report Created	2023-03-09 20:54 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 117 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies Windows automatic backups	3	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe deletes Windows volume shadow copies. • (Process #6) cmd.exe deletes Windows volume shadow copies. • (Process #5) cmd.exe deletes Windows volume shadow copies.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 356 files by appending the extension ".ryk".			
5/5	YARA	Malicious content matched by YARA rules	64	Ransomware

- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...n data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.013.etl.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...application data\application data\application data\application data\application data\microsoft\office\sharepointteamsite.ico.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...n Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.012.etl.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ... Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\AssetLibrary.ico.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...ication data\application data\application data\application data\application data\microsoft\windows defender\scans\mpdiag.bin.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...data\application data\application data\application data\application data\application data\microsoft help\ms.lync.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...ication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-40.png.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...n Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.004.etl.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...a\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.bk.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...plication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedScenarios\Windows.Uif.static.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...pplication Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC_BASIC.16.1033.hxn.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...ata\application data\application data\application data\application data\application data\microsoft help\ms.mspub.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...pplication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\MF\Active.GRL.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\MySharePoints.ico.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...plication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\guest.png.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...lication data\application data\application data\application data\application data\application data\microsoft help\nslist.hxl.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...ata\application data\application data\application data\application data\application data\microsoft help\ms.msouc.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...ation data\application data\application data\application data\application data\microsoft help\ms.databasecompare.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...plication Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...n Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.008.etl.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...n data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.011.etl.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...ication Data\Application Data\Application Data\Application Data\Application Data\Start Menu\Programs\Java\Visit Java.com.url.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...ication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-32.png.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...ata\application data\application data\application data\application data\application data\microsoft help\ms.graph.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...n Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.007.etl.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...n data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.006.etl.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...pplication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user.png.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...plication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\guest.bmp.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...cation Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\MySite.ico.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...n data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.014.etl.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...application data\application data\application data\application data\application data\microsoft\office\documentrepository.ico.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...a\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SETLANG.16.1033.hxn.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...ta\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.GROOVE.16.1033.hxn.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...a\application data\application data\application data\application data\application data\microsoft help\ms.onenote.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...ication Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...a\application data\application data\application data\application data\application data\microsoft help\ms.outlook.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...ation Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn.RYK".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\documents and settings\all users\appl... ...a\application data\application data\application data\application data\application data\microsoft help\ms.winword.16.1033.hxn.ryk".
- Rule "HermesRyukEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Documents and Settings\All Users\Appl... ...cation Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn.RYK".

Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	System Modification	Disables a Windows system tool	1	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe disables startup repair by executing "cmd /c "bcdedit /set {default} recoveryenabled No & bcdedit /set {default}"".			
3/5	Heuristics	Executable is signed with a revoked certificate	1	-
	• C:\Users\RDhJ0CNFevzX\Desktop\OgHBMCIPSlan.exe is signed with a certificate of PET PLUS PTY LTD that has been revoked.			
2/5	Hide Tracks	Hides files	2	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe hides the file "C:\Users\RDhJ0CNFevzX\Desktop\OgHBMCIPSlan.exe" by setting its "hidden" attribute. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe hides the file "C:\Users\RDhJ0CNFevzX\Desktop\MCbYiQSuvlan.exe" by setting its "hidden" attribute.			
2/5	Privilege Escalation	Enables critical process privilege	2	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe enables critical process privilege "SeBackupPrivilege". • (Process #27) wmic.exe enables critical process privilege "SeBackupPrivilege".			
2/5	Discovery	Collects information about services	1	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe queries information about services via API.			
1/5	Hide Tracks	Creates process with hidden window	17	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #2) oghbmcipslan.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #3) mcbyiqsuvlan.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #9) icacls.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #5) cmd.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #6) cmd.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #7) cmd.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #8) cmd.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #16) taskkill.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #19) net.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #18) taskkill.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #23) net.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #28) net.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #33) net.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #34) taskkill.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #39) taskkill.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts (process #40) taskkill.exe with a hidden window. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe starts Anonymous Process with a hidden window.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe enumerates running processes.			
1/5	User Data Modification	Uses encryption API	1	-
	• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe uses above average number of encryption APIs.			
1/5	Persistence	Installs system startup script or application	2	-

Score	Category	Operation	Count	Classification
		• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe adds "C:\Documents and Settings\All Users\Applic... ...n Data\Application Data\Application Data\Microsoft\Windows\Start Menu\Programs\StartUp\RyukReadMe.html" to Windows startup folder. • (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe adds "C:\Documents and Settings\All Users\Applic... ...n Data\Application Data\Application Data\Microsoft\Windows\Start Menu\Programs\StartUp\RyukReadMe.html" to Windows startup folder.		
1/5	Obfuscation	Reads from memory of another process	17	-
		• (Process #43) wmiprvse.exe reads from searchui.exe. • (Process #43) wmiprvse.exe reads from svchost.exe. • (Process #43) wmiprvse.exe reads from wmiadap.exe. • (Process #43) wmiprvse.exe reads from backgroundtaskhost.exe. • (Process #43) wmiprvse.exe reads from (process #44) wmiprvse.exe. • (Process #43) wmiprvse.exe reads from iexplore.exe. • (Process #43) wmiprvse.exe reads from find_course.exe. • (Process #43) wmiprvse.exe reads from serioushopelow.exe. • (Process #43) wmiprvse.exe reads from environment resource think.exe. • (Process #43) wmiprvse.exe reads from all.exe. • (Process #43) wmiprvse.exe reads from pay.exe. • (Process #43) wmiprvse.exe reads from carry million.exe. • (Process #43) wmiprvse.exe reads from focus_between.exe. • (Process #43) wmiprvse.exe reads from view-hot-other.exe. • (Process #43) wmiprvse.exe reads from decision.exe. • (Process #43) wmiprvse.exe reads from line.exe. • (Process #43) wmiprvse.exe reads from democrat could.exe.		
1/5	Obfuscation	Resolves API functions dynamically	3	-
		• (Process #1) a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe resolves 191 API functions by name. • (Process #2) oghbmcipslan.exe resolves 120 API functions by name. • (Process #3) mcbyiqsuvlan.exe resolves 120 API functions by name.		

Mitre ATT&CK Matrix

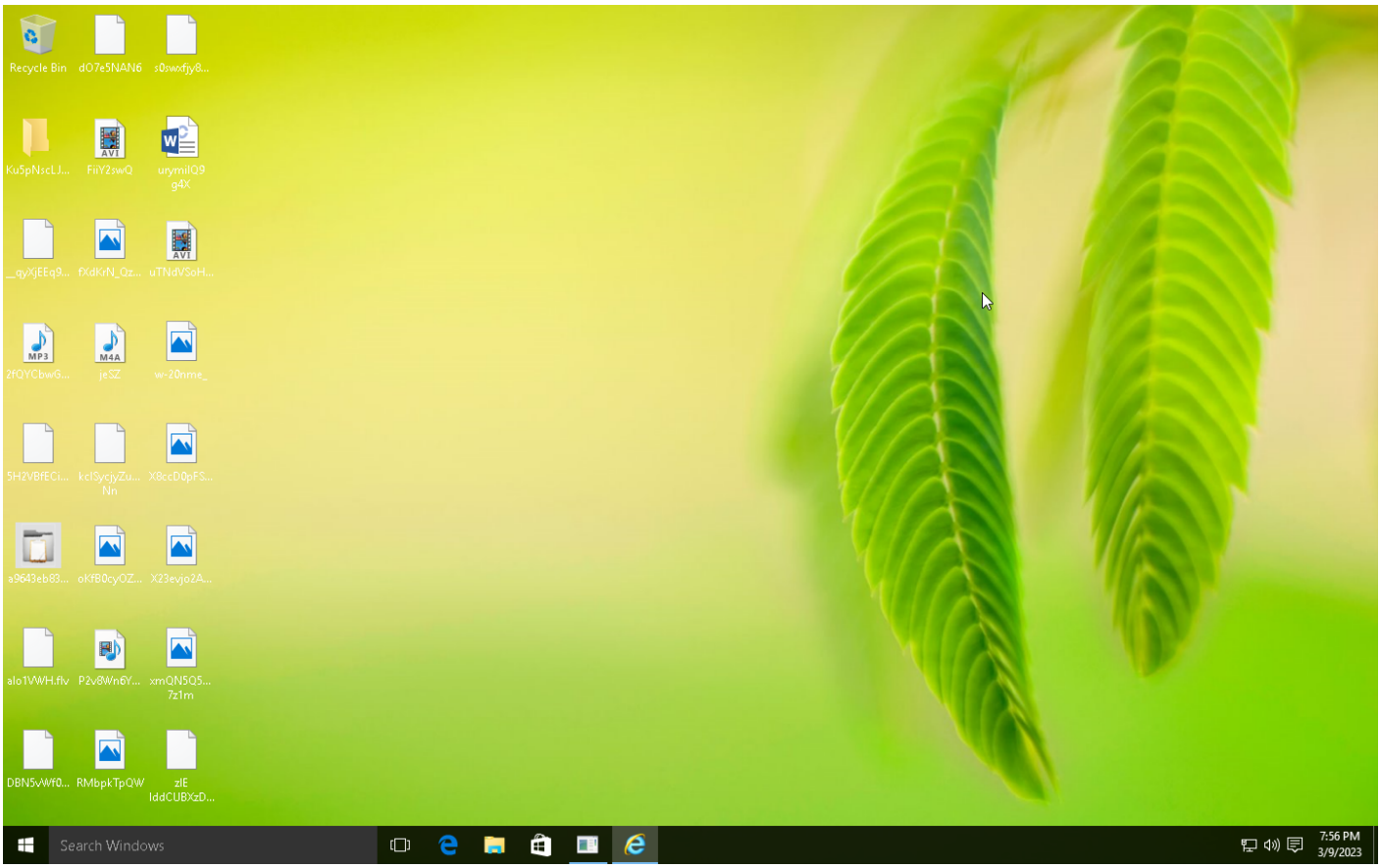
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1158 Hidden Files and Directories		#T1158 Hidden Files and Directories		#T1057 Process Discovery					#T1490 Inhibit System Recovery
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window		#T1007 System Service Discovery					#T1486 Data Encrypted for Impact
				#T1045 Software Packing							

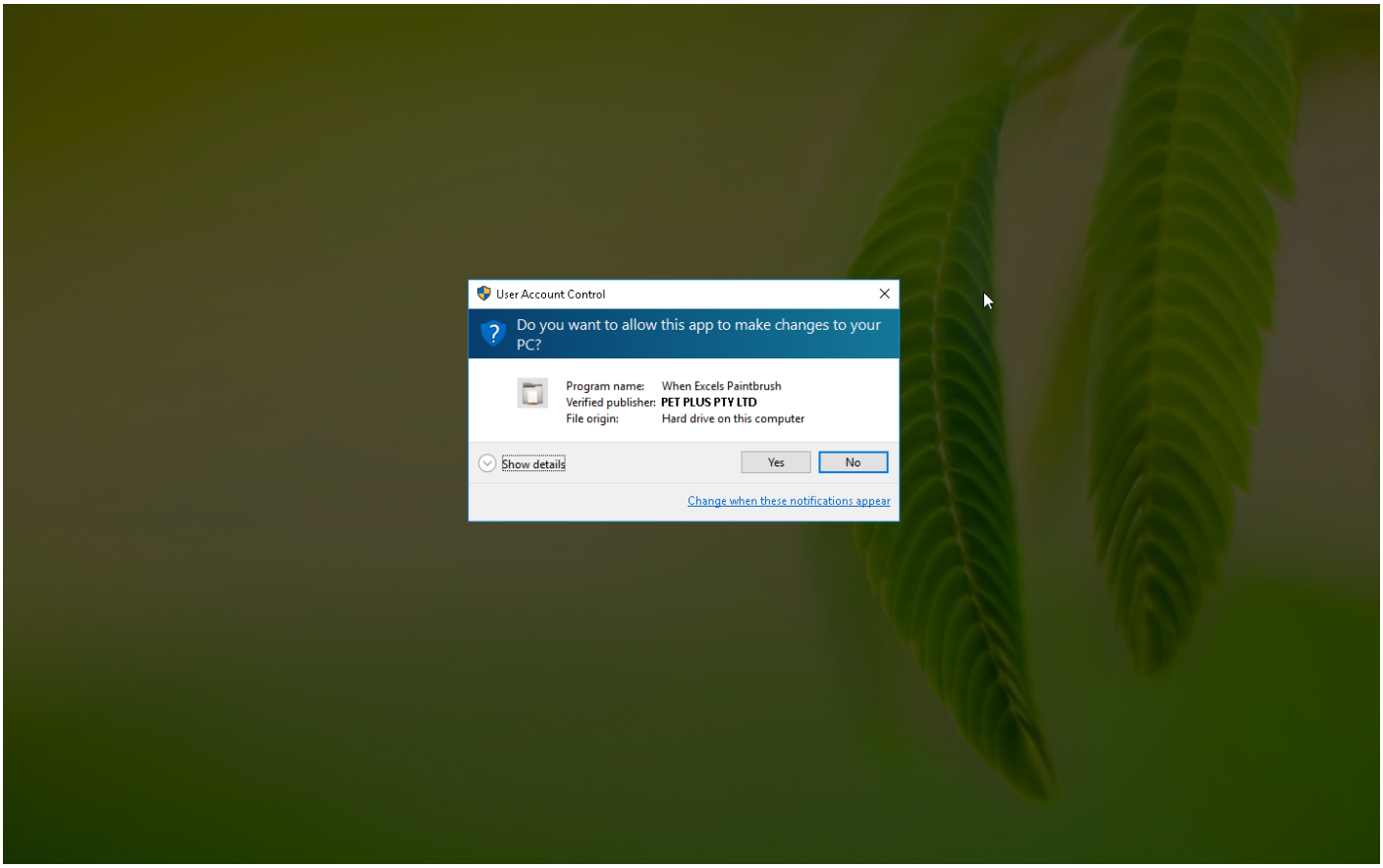
Sample Information

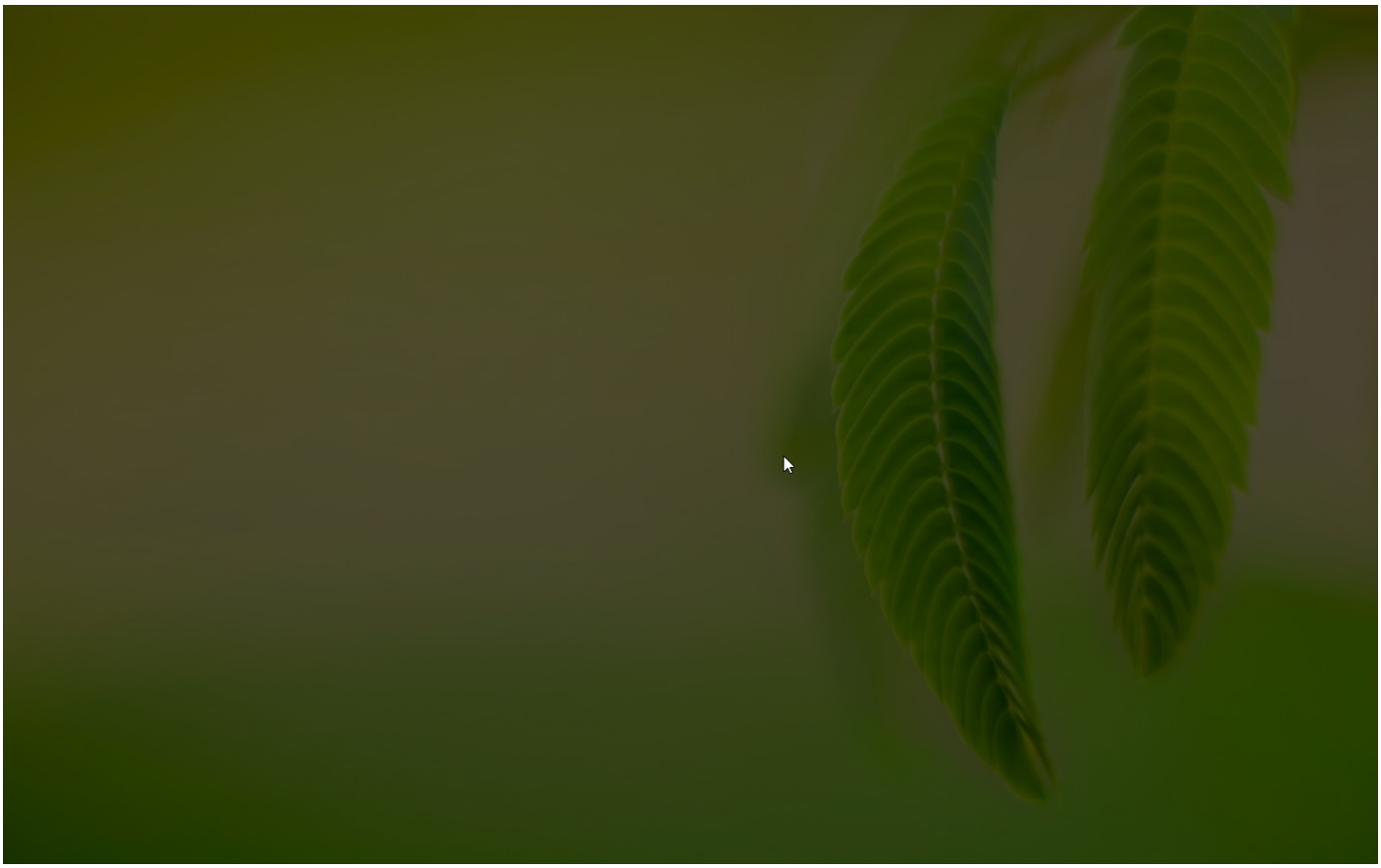
ID	#7097337
MD5	987336d00fdbec3bcdb95b078f7de46f
SHA1	8bbded5710280f055bf53f9e4f6c5abb596f7899
SHA256	a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e
SSDeep	12288:bma40rTiKNAIRhOnloZq7St7ulUr086ah2I/0xI8QTPCXOY1LEfVUF:bH4URP0lVEO0xI8CIOIIfK
ImpHash	d6a677b0acf9110e3d824cb1899dbc41
File Name	a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe
File Size	548.30 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

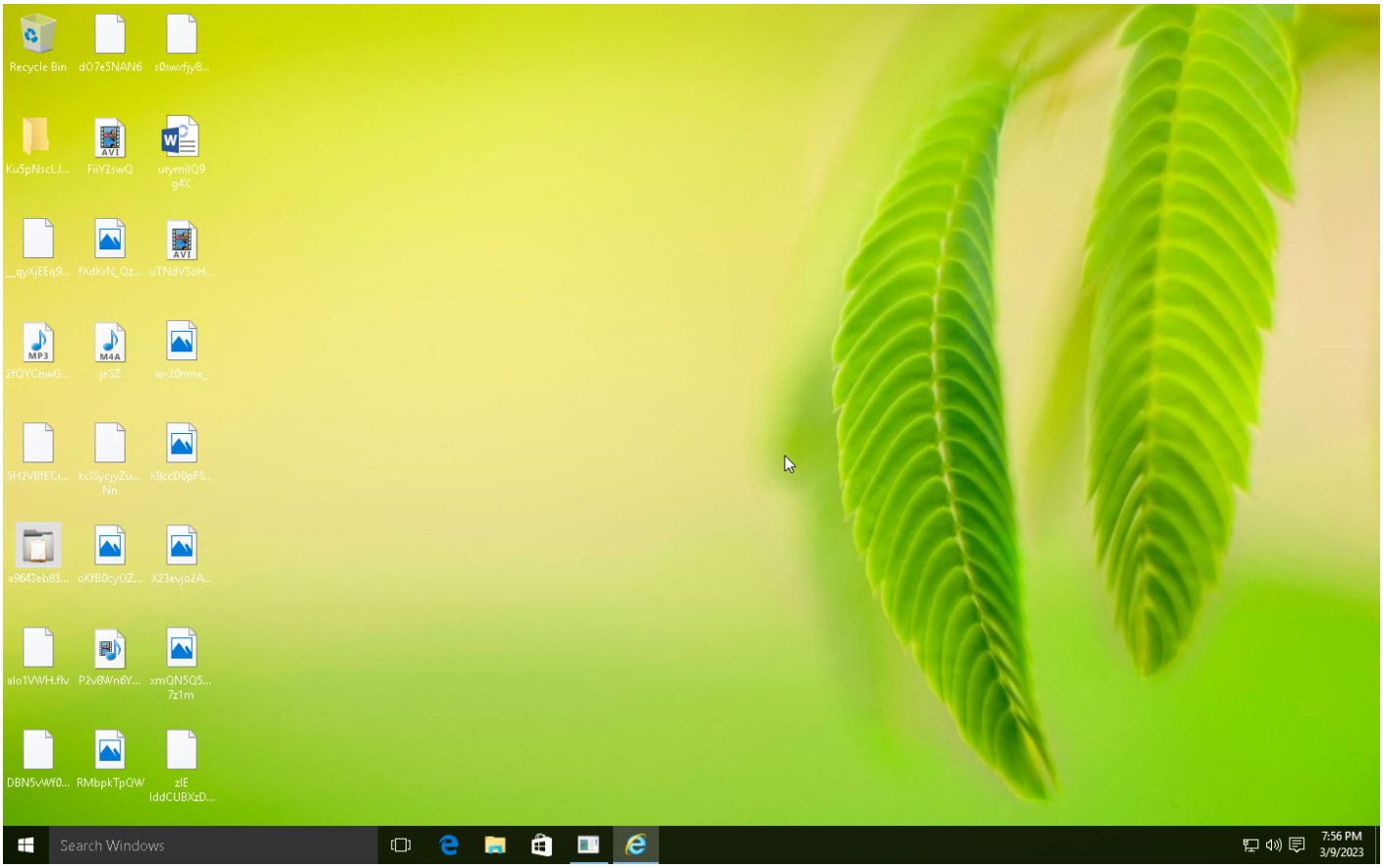
Analysis Information

Creation Time	2023-03-09 20:54 (UTC+1)
Analysis Duration	00:03:03
Termination Reason	Timeout
Number of Monitored Processes	29
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	64


Recycle Bin
Search Windows
7:56 PM
3/9/2023


User Account Control
Do you want to allow this app to make changes to your PC?
Program name: When Excels Paintbrush
Verified publisher: PET PLUS PTY LTD
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear




Recycle Bin
dO7e5NAN6
s0swxfjy8...
Ku5pNscLJ...
FriY2swQ
urymilQ9 g4X
__qyXjEEq9...
fXdKrN_Qz...
uTNdVSoH...
2fQYCbwG...
jeSZ
w-20nme_
5H2VBfECi...
kclSycjyZu... Nn
X9ccD0pFS...
a9643eb83...
oKfB0cyOZ...
X23evjo2A...
alo1VWH.flv
P2v8Wn6Y...
xmQN5Q5... 7z1m
DBN5vWf0...
RMbpkTpQW
zlE lddCUBXzD...
Search Windows
7:56 PM
3/9/2023

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

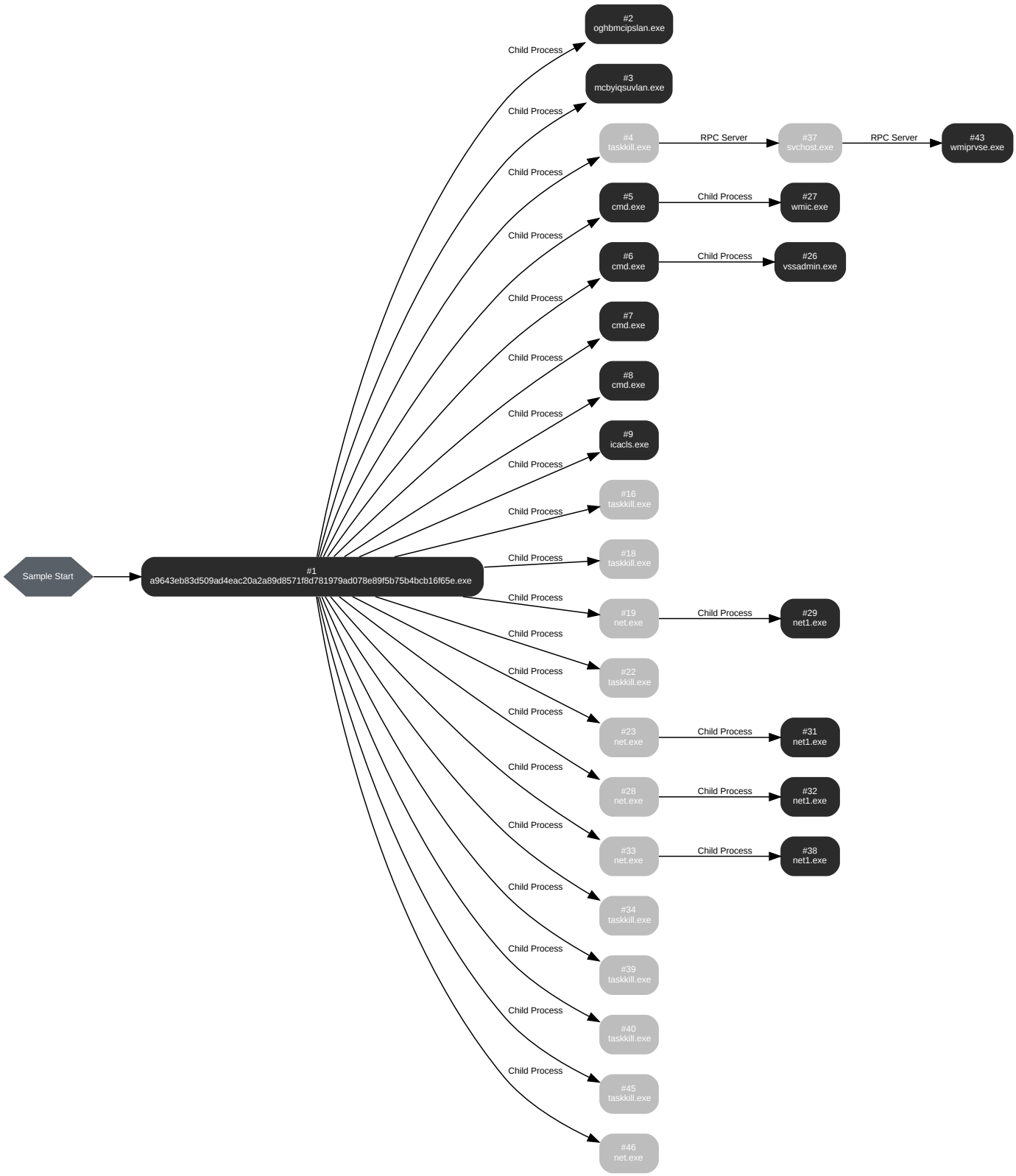
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 139664, Reason: Analysis Target
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	182.32s
Return Code	Unknown
PID	3348
Parent PID	1900
Bitness	32 Bit

Dropped Files (70)

File Name	File Size	SHA256	YARA Match
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.013.etl.ryk	4.28 KB	91a293ebea2a111dd8951f4c1d6780c3d27535c343cc75014090e95e3012846c	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\office\sharepointteamsite.ico.ryk	24.89 KB	738524dde96cb4b0e10793c9e4019dde2408b47cd92c0f5ad087ebb9a5bf51d9	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.012.etl.RYK	12.28 KB	e47e6623f7dcc689e7b3ff27d7443a38bcd989e23c9ae7defa42b3883f3aff22	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\AssetLibrary.ico.RYK	5.58 KB	a68e96d5b1f6c36954eff6edee47090003ac12eca2736abf2e1c1498b6f769ad	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\windows defender\scans\mpdiag.bin.ryk	402 bytes	9f62df03c3ea01470db38bb3e63ed4e614eaefa5fa962f2f6f41769a88a4df65	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.lync.16.1033.hxn.ryk	626 bytes	45f1ea3c7a1de2be7788332d0d0b215ba70311e9dbfa689bc138e8a3294dc8c3	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-40.png.RYK	722 bytes	b04f0c7cf88c4f9709776698cad0eaed6726fd4dc69d2f5bfedfb1c3448c9261	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.004.etl.RYK	12.28 KB	e702e7759000c0d335a54404e5b2fe82be3c85e0f92fa51548096c0d9bbd30aa	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.bk.RYK	1.67 KB	a5b9c2e079045bdc8a3f2f5a9b61713043fc2121ceecef8c4fca4a0ce7c8fb71	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedScenarios\Windows.Uif.static.RYK	2.83 KB	2de7e218c5647016541bc63d43f3959a012b976f170b6906ec94f59f20f80715	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC_BASIC.16.1033.hxn.RYK	658 bytes	3a672469aae2c351681f69319e8f4f85796914216239642ebfd0b0e592484f1f	✔

File Name	File Size	SHA256	YARA Match
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.mspub.16.1033.hxn.ryk	626 bytes	6ecb4dbcf592412cc91c55a149cfa685727f318840ca7fcfb0d380333d295f6d	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\MF\Active.GRL.RYK	14.89 KB	a5705881063c4db4be0d4316405fb380894fd380c136ccb241a344e684bcc96d	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\MySharePoints.ico.RYK	97.22 KB	9d6607247f10dbbf6e1fd4abb3cebb99f54d57e80b5c8a0cb8d75d56eee8286a	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\guest.png.RYK	5.55 KB	ee0583838757f338e22b622347f36fa2a914b02c3d114d4f4873eafdb1aaf62d	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\nslist.hxl.ryk	6.39 KB	4d240bf4e25f4a1292f6be7e81d2878e43e3d15ea64d63c66ae4a72edf3c5797	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.msouc.16.1033.hxn.ryk	626 bytes	80076b661fdca66fc588570c7b89318d85ffa6460342b47388facc6800e8853c	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.databasecompare.16.1033.hxn.ryk	706 bytes	274a2ee70dab3fdb121cd2e772455145151bb6ef69f1e894cc3c5446c4d8d312	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn.RYK	674 bytes	8377205bffb5783d5ef13a382c3f908d2dc58231194c08393d72358b4ff0c02d	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.008.etl.RYK	12.28 KB	29d5d06810cb5058d1b92edc34958a0fbfffaa0a8dc58fac7624b04f0d12a0cd	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.011.etl.ryk	8.28 KB	8e093383eafb7ae2232b22d72dbf2f4da6d3192c4a2f33939b4ed951d42e8d48	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Start Menu\Programs\Java\Visit Java.com.url.RYK	466 bytes	c000e5c49d31c18502772e174156f5ffef3bf43bedce64258dcfbcc8fdf938d8	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-32.png.RYK	690 bytes	ec1f536f7da56cdb2def008a5fa656a41c56da0e965333b3280a536539205787	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.graph.16.1033.hxn.ryk	626 bytes	9e400d222f2dedd866c64e2689d56a907fd1851ec40f52bfd030fbaa3b719dbc	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.007.etl.RYK	12.28 KB	36b44a2a7d2dd2ce9d376b9a7884f5fabc2276c44e48a09d97dbcabb3d99edcf	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.006.etl.ryk	12.28 KB	c2321e20148c0ba4f654faab4fe2d86289b90a868a2d27015ec12bca1ad2851e	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user.png.RYK	5.55 KB	ba15d3586f36bb62eb56d86149da5b87b7b338f9228a6ef3409816d3f73facb	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\guest.bmp.RYK	588.33 KB	5d0ab6959c734aeac448b074347f527ffc20e7e8c7deac6d3bb2d498673b3b26	✔
C:\Users\RDhJ0CNFevzX\Desktop\OgHBMCIPSlan.exe	548.30 KB	a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e	✖

File Name	File Size	SHA256	YARA Match
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\MySite.ico.RYK	24.89 KB	4d9fdfcbcd896f6792f729be94c6173d21d30ca9585d7c71f047a178a555087a	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.014.etl.ryk	4.28 KB	49eb6105406472317ebdc2d60171fc87fe1181383d84d08cd4f2e6b69a930a35	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\office\documentrepository.ico.ryk	24.89 KB	466408313d9776af4733ba030809464642071c85183f86531096fb620dd46d01	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SETLANG.16.1033.hxn.RYK	642 bytes	e34b5285b6cc568f77db6f73292f70360787ee9a127455a867b6f4d7faf2965a	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.GROOVE.16.1033.hxn.RYK	642 bytes	3b46002d7576c4df9ba09083baea4db777cbf2e60255e95b8437d61b60c6a0da	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.onenote.16.1033.hxn.ryk	642 bytes	a398774de5e5291af21166ff679343a8de761a2d954ba2f70fbb611334d2505e	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn.RYK	674 bytes	b83ddaa082defa65e5de6fc74a7b83e6116ed18a1c1f4baaef1172920e0d4c42	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.outlook.16.1033.hxn.ryk	642 bytes	66766a20d1cb01868051b477dae5dcd7a4af8dbb2106b44d1982d5a75654bdd1	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn.RYK	690 bytes	3d88859c0c70246453038205l9b5689f0b571a146c319c347b0fc884d82fe2aa	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.winword.16.1033.hxn.ryk	642 bytes	db88d1b85eed9a7255a807f2c2849287570202773a32520333edf1b9175f670f	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn.RYK	690 bytes	83dee63000b5ced17e617ee51e66e0ee081e680bd78720e42ac73442cb2d6087	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\clicktorun\deploymentconfig.0.xml.ryk	2.21 KB	d1fcce0e0b5a97910bfc9ead474347f804659e0d499c8a62c926fb540d3e676b	✔
-	52 bytes	a1a21799e98f97f271657ce656076f33dcb020d9370f1f2671d783cafd230294	✖
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.001.etl.RYK	16.28 KB	a6fa9a878a46687334feea32c96feee860b8879b9fb46e97b287725e3f63073a	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn.RYK	722 bytes	12a9c9f234fec7ef277a09a5b7cc2233ff5268c7f86e32d7d4c8131828a96c17	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\clicktorun\deploymentconfig.1.xml.ryk	2.21 KB	1bbeef8805086288d42ed1bfba2959835046d20c5858997c2038b2ce9227b436	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\clicktorun\deploymentconfig.2.xml.ryk	1.63 KB	aba383de58595987ad2fb01ca71d1f1f767f4ce3470226afa907ad892710e7a1	✔
C:\Boot\el-GR\RyukReadMe.html	627 bytes	9d02b65535798947514ce2d4191de4e3789036a05e8b4bdfe87bf5957de8afa3	✖
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.010.etl.RYK	12.28 KB	c24e976b80ab4f1f4bf1ed8898b41d795b6c61265cee87b72c5d9b23c88d6c0a	✔

File Name	File Size	SHA256	YARA Match
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\MF\Pending.GRL.RYK	14.89 KB	c99f43dfb9b4cd902046e9760d8d243e6144aa641682a59ac400670e3f793510	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateUx.001.etl.RYK	4.28 KB	e4c87bf294abcf8efca9f33eebde2f3f9d6f1ebb8ed475607ca2635d69b6eff9	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\SharePointPortalSite.ico.RYK	24.89 KB	bc980be8f527b75aa0e1d189f5225b932d2e0f984ada469bec53328db8364746	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.015.etl.RYK	8.28 KB	b80021103fc58db012883590e488f4abbcdb5eb1c572e367f042540c13f0517d	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\start menu\programs\java\get help.url.ryk	466 bytes	dfa875efb5856c5ac1c53c92edbeb56bce352b73b05ef19c0d54faf53e6eaa1b	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user-48.png.ryk	786 bytes	a99f27aa6a7cb4133bbab1cd8be9936f45112596425a61682f95794eb1201c7d	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user.bmp.ryk	588.33 KB	028cfcb4fbfd9cd1024174c10223f593d92a8a069e6728f5b270dc6f39618919	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.MSACCESS.16.1033.hxn.RYK	658 bytes	7dd7d944c73fbbe4a83f80a4158e5f10d47c8d9efd59cb1d9330a7ba7e45fff4	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\vault\ac658cb4-9126-49bd-b877-31eedab3f204\policy.vpol.ryk	722 bytes	1afe198a66c44bece2f75dfabe1021a877490651f373843f74ac608f985f0279	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.EXCEL.16.1033.hxn.RYK	626 bytes	ca14a8d68443581f5a4efc76c430e66b9cbdc17a18315eed22efc5939de96d10	✔
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp926F.tmp	4.00 KB	f61c9b2639976995271ea715da57a88ac7cb923966785dbe1a2472949868dedc	✖
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows Live\WLive48x48.png.RYK	4.83 KB	f05f347aa06d9497ac10883925c51b7c4bb0f605847209e32a271cd3705e866e	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.skypefb.16.1033.hxn.ryk	642 bytes	463f8a1761c62e9a3b34e0d6201b18908fca9671646776a66782a473251b851a	✔
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Oracle\Java\installcache_x64\baseimagefam8.RYK	10240.00 KB	03d9c9ddfdeeda042a7355850cc1030d3100861ef8248759b21daa88c42d5c7a	✖
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateUx.002.etl.RYK	4.28 KB	c575cbb547e07fd91e3848ac37fd0db9847079147bdfc57544624f851c952937	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.powerpnt.16.1033.hxn.ryk	658 bytes	2d1d210b81795bdb970f7344e82f51cd77a3da0262e01760757de8215985b332	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.002.etl.ryk	12.28 KB	23950c844160a0c21f26725067a44257d062b6a750963cf4741f9dbc011069c5	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.005.etl.ryk	12.28 KB	0a7c9733f743f0c64d4f2a913f363871a67deabd229a9f444d02ead856324ae2	✔

File Name	File Size	SHA256	YARA Match
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.009.etl.ryk	12.28 KB	3b3596e5fea728c9d77a6ae77443bc0d550928a591745ca3c9be23a0a9083cff	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user-192.png.ryk	2.63 KB	04ff04367782e7afd1ef4c8c6d79536b8cfe751a3e5e26f3188b326fe6d8c810	✔
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.003.etl.ryk	12.28 KB	d819e0bfa8d46967bd9e5be943862778085c542c794fb3a0b862700757271788	✔
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp926F.tmp	4.00 KB	d78bcd9f618eacd48754cc739f29592d836c7e6c61042235f35a64fea7150e2c	✖

Host Behavior

Type	Count
Module	290
File	6562
Environment	2
Window	5
-	2
System	23
Process	433
User	1
-	1
-	9

Process #2: oghbmcipslan.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\oghbmcipslan.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\OgHBMCIPSlan.exe" 8 LAN
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 236705, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	85.28s
Return Code	Unknown
PID	2956
Parent PID	3348
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpEABB.tmp	4.00 KB	efe9c73d0d7d1a5596f037f29b62c0190bff7834da082ec425fb8958a79f4967	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpEABB.tmp	4.00 KB	c7d0f9a20fae1e19911e4871148b3633c46d1c0add986a803a2ff9055ccbed5b	✖

Host Behavior

Type	Count
Module	145
File	526
Environment	2
Window	5
-	2
System	9

Process #3: mcbyiqsuvlan.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\mcbyiqsuvlan.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\MCbYiQSuvlan.exe" 8 LAN
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 242720, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	79.26s
Return Code	Unknown
PID	2164
Parent PID	3348
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp22B.tmp	4.00 KB	af0eb162cd3f3c9154d639bec905cc9b5567d4dd2a54c69f342ea1e9cfdd8390	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp22B.tmp	4.00 KB	2997b6af7f8405dc4ba2d35e974f3294b824abf3df5aba221fc38b8917133c29	✖

Host Behavior

Type	Count
Module	145
File	394
Environment	2
Window	5
-	2
System	8

Process #4: taskkill.exe

ID	4
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 249067, Reason: Child Process
Unmonitor End Time	End Time: 308561, Reason: Terminated
Monitor duration	59.49s
Return Code	0
PID	2672
Parent PID	3348
Bitness	32 Bit

Process #5: cmd.exe

ID	5
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c "WMIC.exe shadowcopy delete"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 249524, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	72.46s
Return Code	Unknown
PID	4180
Parent PID	3348
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	34
Environment	17
System	1
Process	2

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c "vssadmin.exe Delete Shadows /all /quiet"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 249568, Reason: Child Process
Unmonitor End Time	End Time: 320894, Reason: Terminated
Monitor duration	71.33s
Return Code	2
PID	4172
Parent PID	3348
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	22
Environment	20
System	1
Process	2

Process #7: cmd.exe

ID	7
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c "bcdedit /set {default} recoveryenabled No & bcdedit /set {default}"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 249590, Reason: Child Process
Unmonitor End Time	End Time: 283704, Reason: Terminated
Monitor duration	34.11s
Return Code	1
PID	4228
Parent PID	3348
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	37
Environment	15
System	1

Process #8: cmd.exe

ID	8
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c "bootstatuspolicy ignoreallfailures"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 249619, Reason: Child Process
Unmonitor End Time	End Time: 281604, Reason: Terminated
Monitor duration	31.98s
Return Code	1
PID	2420
Parent PID	3348
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	32
Environment	15
System	1

Process #9: icacls.exe

ID	9
File Name	c:\windows\syswow64\icacls.exe
Command Line	icacls "C:*" /grant Everyone:F /T /C /Qÿÿÿÿ
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 249703, Reason: Child Process
Unmonitor End Time	End Time: 272254, Reason: Terminated
Monitor duration	22.55s
Return Code	87
PID	4140
Parent PID	3348
Bitness	32 Bit

Process #16: taskkill.exe

ID	16
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 257359, Reason: Child Process
Unmonitor End Time	End Time: 315150, Reason: Terminated
Monitor duration	57.79s
Return Code	0
PID	2572
Parent PID	3348
Bitness	32 Bit

Process #18: taskkill.exe

ID	18
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 263053, Reason: Child Process
Unmonitor End Time	End Time: 321153, Reason: Terminated
Monitor duration	58.10s
Return Code	128
PID	4356
Parent PID	3348
Bitness	32 Bit

Process #19: net.exe

ID	19
File Name	c:\windows\syswow64\net.exe
Command Line	"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 263736, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	58.24s
Return Code	Unknown
PID	4844
Parent PID	3348
Bitness	32 Bit

Process #22: taskkill.exe

ID	22
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 265997, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	55.98s
Return Code	Unknown
PID	4772
Parent PID	3348
Bitness	32 Bit

Process #23: net.exe

ID	23
File Name	c:\windows\syswow64\net.exe
Command Line	"C:\Windows\System32\net.exe" stop "samss" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 266017, Reason: Child Process
Unmonitor End Time	End Time: 295171, Reason: Terminated
Monitor duration	29.15s
Return Code	2
PID	4792
Parent PID	3348
Bitness	32 Bit

Process #26: vssadmin.exe

ID	26
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin.exe Delete Shadows /all /quiet
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 272461, Reason: Child Process
Unmonitor End Time	End Time: 317092, Reason: Terminated
Monitor duration	44.63s
Return Code	2
PID	4032
Parent PID	4172
Bitness	32 Bit

Process #27: wmic.exe

ID	27
File Name	c:\windows\syswow64\wbem\wmic.exe
Command Line	WMIC.exe shadowcopy delete
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 272654, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	49.33s
Return Code	Unknown
PID	4056
Parent PID	4180
Bitness	32 Bit

Host Behavior

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

Process #28: net.exe

ID	28
File Name	c:\windows\syswow64\net.exe
Command Line	"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 273411, Reason: Child Process
Unmonitor End Time	End Time: 304089, Reason: Terminated
Monitor duration	30.68s
Return Code	2
PID	2660
Parent PID	3348
Bitness	32 Bit

Process #29: net1.exe

ID	29
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 stop "audioendpointbuilder" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 273832, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	48.15s
Return Code	Unknown
PID	4872
Parent PID	4844
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
File	32
-	48
System	8

Process #31: net1.exe

ID	31
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 stop "samss" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 277082, Reason: Child Process
Unmonitor End Time	End Time: 292620, Reason: Terminated
Monitor duration	15.54s
Return Code	2
PID	5052
Parent PID	4792
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
File	10
-	7

Process #32: net1.exe

ID	32
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 stop "audioendpointbuilder" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 285205, Reason: Child Process
Unmonitor End Time	End Time: 302549, Reason: Terminated
Monitor duration	17.34s
Return Code	2
PID	3008
Parent PID	2660
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
File	16
-	14

Process #33: net.exe

ID	33
File Name	c:\windows\syswow64\net.exe
Command Line	"C:\Windows\System32\net.exe" stop "samss" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 285949, Reason: Child Process
Unmonitor End Time	End Time: 314573, Reason: Terminated
Monitor duration	28.62s
Return Code	2
PID	2728
Parent PID	3348
Bitness	32 Bit

Process #34: taskkill.exe

ID	34
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 286148, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	35.83s
Return Code	Unknown
PID	3084
Parent PID	3348
Bitness	32 Bit

Process #37: svchost.exe

ID	37
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 289431, Reason: RPC Server
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	32.55s
Return Code	Unknown
PID	864
Parent PID	2672
Bitness	64 Bit

Process #38: net1.exe

ID	38
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 stop "samss" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 299720, Reason: Child Process
Unmonitor End Time	End Time: 314353, Reason: Terminated
Monitor duration	14.63s
Return Code	2
PID	4760
Parent PID	2728
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
File	10
-	7

Process #39: taskkill.exe

ID	39
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 304042, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	17.94s
Return Code	Unknown
PID	4352
Parent PID	3348
Bitness	32 Bit

Process #40: taskkill.exe

ID	40
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 304144, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	17.84s
Return Code	Unknown
PID	1656
Parent PID	3348
Bitness	32 Bit

Process #43: wmiprvse.exe

ID	43
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 312965, Reason: RPC Server
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	9.02s
Return Code	Unknown
PID	4316
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
Process	71
System	18
-	114

Process #45: taskkill.exe

ID	45
File Name	c:\windows\syswow64\taskkill.exe
Command Line	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 321579, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	0.40s
Return Code	Unknown
PID	5364
Parent PID	3348
Bitness	32 Bit

Process #46: net.exe

ID	46
File Name	c:\windows\syswow64\net.exe
Command Line	"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 321745, Reason: Child Process
Unmonitor End Time	End Time: 321981, Reason: Terminated by timeout
Monitor duration	0.24s
Return Code	Unknown
PID	5372
Parent PID	3348
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
91a293ebea2a111dd8951f4c1d6780c3d27535c343cc75014090e95e3012846c	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.013.etl.RYK	Dropped File	4.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
738524dde96cb4b0e10793c9e4019dde2408b47cd92c0f5ad087ebb9a5bf51d9	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...a\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\SharePointTeamSite.ico.RYK	Dropped File	24.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e47e6623f7dcc689e7b3ff27d7443a38bcd989e23c9ae7defa42b3883f3aff22	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion data\application data\application data\application data\usosharedlogs\updatesessionorchestration.012.etl.ryk	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a68e96d5b1f6c36954eff6edee47090003ac12eca2736abf2e1c1498b6f769ad	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...on data\application data\application data\application data\application data\microsoft\office\assetlibrary.ico.ryk	Dropped File	5.58 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9f62df03c3ea01470db38bb3e63ed4e614eaefa5fa962f2f6f41769a88a4df65	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...plication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Scans\MpDiag.bin.RYK	Dropped File	402 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
45f1ea3c7a1de2be7788332d0d0b215ba70311e9dbfa689bc138e8a3294dc8c3	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...n Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC.16.1033.hxn.RYK	Dropped File	626 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
b04f0c7cf88c4f9709776698cad0eaed6726fd4dc69d2f5bfedfb1c3448c9261	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication data\application data\application data\application data\microsoft\user account pictures\user-40.png.ryk	Dropped File	722 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
e702e7759000c0d335a54404e5b2fe82be3c85e0f92fa51548096c0d9bbd30aa	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion data\application data\application data\application data\usosharedlogs\updatesessionorchestration.004.etl.ryk	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a5b9c2e079045bdc8a3f2f5a9b61713043fc2121ceecef8c4fca4a0ce7c8fb71	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\application data\application data\application data\microsoft\diagnosis\downloadedsettings\utc.app.json.bk.ryk	Dropped File	1.67 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2de7e218c5647016541bc63d43f3959a012b976f170b6906ec94f59f20f80715	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...application data\application data\application data\microsoft\diagnosis\downloadedscenarios\windows.uif.static.ryk	Dropped File	2.83 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3a672469aae2c351681f69319e8f4f857969142162396 42ebfd0b0e592484f1f	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ... \application data\application data\application data\application data\application data\microsoft help\ms.lync_basic.16.1033.hxn.ryk	Dropped File	658 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
6ecb4dbcf592412cc91c55a149cfa685727f318840ca7fcfb0d380333d295f6d	c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ... Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.MSPUB.16.1033.hxn.RYK	Dropped File	626 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
a5705881063c4db4be0d4316405fb380894fd380c136ccb241a344e684bcc96d	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ... \application data\application data\application data\application data\application data\application data\microsoft\mf\active.grl.ryk	Dropped File	14.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9d6607247f10dbbf6e1fd4abb3cebb99f54d57e80b5c8a0cb8d75d56eee8286a	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...n data\application data\application data\application data\application data\application data\microsoft\office\mysharepoints.ico.ryk	Dropped File	97.22 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ee0583838757f338e22b622347f36fa2a914b02c3d114d4f4873eafdb1aaf62d	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...application data\application data\application data\application data\application data\microsoft\user account pictures\guest.png.ryk	Dropped File	5.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4d240bf4e25f4a1292f6be7e81d2878e43e3d15ea64d63c66ae4a72edf3c5797	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...pplication Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\nslist.hxl.RYK	Dropped File	6.39 KB	application/octet-stream	Access, Create, Write	MALICIOUS
80076b661fdca66fc588570c7b89318d85ffa6460342b47388facc6800e8853c	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ... Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.MSOUC.16.1033.hxn.RYK	Dropped File	626 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
274a2ee70dab3fdb121cd2e772455145151bb6ef69f1e894cc3c5446c4d8d312	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ication Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.DATABASECOMPARE.16.1033.hxn.RYK	Dropped File	706 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
8377205bffb5783d5ef13a382c3f908d2dc58231194c08393d72358b4ff0c02d	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...application data\application data\application data\application data\application data\microsoft help\ms.lync_online.16.1033.hxn.ryk	Dropped File	674 bytes	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
29d5d06810cb5058d1b92edc34958a0fbfffaa0a8dc58fac7624b04f0d12a0cd	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion data\application data\application data\application data\usoshared\logs\updatesessionorchestration.008.etl.ryk	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
8e093383eafb7ae2232b22d72dbf2f4da6d3192c4a2f33939b4ed951d42e8d48	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.011.etl.RYK	Dropped File	8.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c000e5c49d31c18502772e174156f5ffef3bf43bedce64258dcfbcc8fdf938d8	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication data\application data\application data\application data\start menu\programs\java\visit java.com.url.ryk	Dropped File	466 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
ec1f536f7da56cdb2def008a5fa656a41c56da0e965333b3280a536539205787	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication data\application data\application data\application data\microsoft\user account pictures\user-32.png.ryk	Dropped File	690 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
9e400d222f2dedd866c64e2689d56a907fd1851ec40f52bfd030fbaa3b719dbc	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ... Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.GRAPH.16.1033.hxn.RYK	Dropped File	626 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
36b44a2a7d2dd2ce9d376b9a7884f5fabc2276c44e48a09d97dbcabb3d99edcf	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion data\application data\application data\application data\usoshared\logs\updatesessionorchestration.007.etl.ryk	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c2321e20148c0ba4f654faab4fe2d86289b90a868a2d27015ec12bca1ad2851e	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.006.etl.RYK	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ba15d3586f36bb62eb56d86149da5b87b7b338f9228a6ef3409816d3f73faacb	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ... \application data\application data\application data\application data\microsoft\user account pictures\user.png.ryk	Dropped File	5.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
5d0ab6959c734aeac448b074347f527ffc20e7e8c7deac6d3bb2d498673b3b26	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...application data\application data\application data\application data\microsoft\user account pictures\guest.bmp.ryk	Dropped File	588.33 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e	C:\Users\RDhJ0CNFevzX\Desktop\OgHBMCIPSlan.exe, C:\Users\RDhJ0CNFevzX\Desktop\MCbYiQSuvlan.exe, C:\Users\RDhJ0CNFevzX\Desktop\a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe	Dropped File	548.30 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4d9fdfcbcd896f6792f729be94c6173d21d30ca9585d7c71f047a178a555087a	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...lication data\application data\application data\application data\application data\application data\microsoft\office\mysite.ico.ryk	Dropped File	24.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
49eb6105406472317ebdc2d60171fc87fe1181383d84d08cd4f2e6b69a930a35	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.014.etl.RYK	Dropped File	4.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
466408313d9776af4733ba030809464642071c85183f86531096fb620dd46d01	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...a\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\DocumentRepository.ico.RYK	Dropped File	24.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e34b5285b6cc568f77db6f73292f70360787ee9a127455a867b6f4d7faf2965a	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\application data\application data\application data\application data\microsoft help\ms.setlang.16.1033.hxn.ryk	Dropped File	642 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
3b46002d7576c4df9ba09083baea4db777cbf2e60255e95b8437d61b60c6a0da	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...data\application data\application data\application data\application data\microsoft help\ms.groove.16.1033.hxn.ryk	Dropped File	642 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
a398774de5e5291af21166ff679343a8de761a2d954ba2f70fbb611334d2505e	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.ONENOTE.16.1033.hxn.RYK	Dropped File	642 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
b83ddaa082defa65e5de6fc74a7b83e6116ed18a1c1f4baaef1172920e0d4c42	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication data\application data\application data\application data\microsoft help\ms.skypefb_basic.16.1033.hxn.ryk	Dropped File	674 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
66766a20d1cb01868051b477dae5dcd7a4af8dbb2106b44d1982d5a75654bdd1	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.OUTLOOK.16.1033.hxn.RYK	Dropped File	642 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
3d88859c0c7024645303820519b5689f0b571a146c319c347b0fc884d82fe2aa	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ication data\application data\application data\application data\microsoft help\ms.skypefb_onlineg.16.1033.hxn.ryk	Dropped File	690 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
db88d1b85eed9a7255a807f2c28492875702027 73a32520333edf1b9175f670f	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.WINWORD.16.1033.hxn.RYK	Dropped File	642 bytes	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
83dee63000b5ced17e617ee51e66e0ee081e680bd78720e42ac73442cb2d6087	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...lication data\application data\application data\application data\application data\microsoft help\ms.skypefb_online.16.1033.hxn.ryk	Dropped File	690 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
d1fcce0e0b5a97910bfc9ead474347f804659e0d499c8a62c926fb540d3e676b	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...plication Data\Application Data\Application Data\Application Data\Microsoft\ClickToRun\DeploymentConfig.0.xml.RYK	Dropped File	2.21 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a6fa9a878a46687334feea32c96feee860b8879b9fb46e97b287725e3f63073a	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.001.etl.ryk	Dropped File	16.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
12a9c9f234fec7ef277a09a5b7cc2233ff5268c7f86e32d7d4c8131828a96c17	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion data\application data\application data\application data\application data\microsoft help\ms.spreadsheetcompare.16.1033.hxn.ryk	Dropped File	722 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
1bbeef8805086288d42ed1bfba2959835046d20c5858997c2038b2ce9227b436	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...plication Data\Application Data\Application Data\Application Data\Application Data\Microsoft\ClickToRun\DeploymentConfig.1.xml.RYK	Dropped File	2.21 KB	application/octet-stream	Access, Create, Write	MALICIOUS
aba383de58595987ad2fb01ca71d1f1f767f4ce3470226afa907ad892710e7a1	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...plication Data\Application Data\Application Data\Application Data\Microsoft\ClickToRun\DeploymentConfig.2.xml.RYK	Dropped File	1.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c24e976b80ab4f1f4bf1ed8898b41d795b6c61265cee87b72c5d9b23c88d6c0a	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.010.etl.ryk	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c99f43dfb9b4cd902046e9760d8d243e6144aa641682a59ac400670e3f793510	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...application data\application data\application data\application data\application data\microsoft\mf\pending.grl.ryk	Dropped File	14.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e4c87bf294abcf8efca9f33eebde2f3f9d6f1ebb8ed475607ca2635d69b6eff9	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion data\application data\application data\application data\application data\usoshared\logs\updateux.001.etl.ryk	Dropped File	4.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
bc980be8f527b75aa0e1d189f5225b932d2e0f984ada469bec53328db8364746	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...application data\application data\application data\application data\application data\microsoft\office\sharepointportalsite.ico.ryk	Dropped File	24.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b80021103fc58db012883590e488f4abbcdb5eb1c572e367f042540c13f0517d	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.015.etl.ryk	Dropped File	8.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dfa875efb5856c5ac1c53c92edbeb56bce352b73b05ef19c0d54faf53e6eaa1b	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\Application Data\Application Data\Application Data\Application Data\Start Menu\Programs\Java\Get Help.url.RYK	Dropped File	466 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
a99f27aa6a7cb4133bbab1cd8be9936f45112596425a61682f95794eb1201c7d	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...plication Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-48.png.RYK	Dropped File	786 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
028cfcb4fbfd9cd1024174c10223f593d92a8a069e6728f5b270dc6f39618919	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ... \Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user.bmp.RYK	Dropped File	588.33 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7dd7d944c73fbbe4a83f80a4158e5f10d47c8d9efd59cb1d9330a7ba7e45fff4	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ta\application data\application data\application data\application data\microsoft help\ms.msaccess.16.1033.hxn.ryk	Dropped File	658 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
1afe198a66c44bece2f75dfabe1021a877490651f373843f74ac608f985f0279	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ation Data\Application Data\Application Data\Application Data\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol.RYK	Dropped File	722 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
ca14a8d68443581f5a4efc76c430e66b9cbdc17a18315eed22efc5939de96d10	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ... data\application data\application data\application data\application data\microsoft help\ms.excel.16.1033.hxn.ryk	Dropped File	626 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
f05f347aa06d9497ac10883925c51b7c4bb0f605847209e32a271cd3705e866e	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\application data\application data\application data\application data\microsoft\windows live\wlive48x48.png.ryk	Dropped File	4.83 KB	application/octet-stream	Access, Create, Write	MALICIOUS
463f8a1761c62e9a3b34e0d6201b18908fca9671646776a66782a473251b851a	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB.16.1033.hxn.RYK	Dropped File	642 bytes	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c575cbb547e07fd91e3848ac37fd0db9847079147bdfc57544624f851c952937	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion data\application data\application data\application data\application data\application data\usoshared\logs\updateux.002.etl.ryk	Dropped File	4.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2d1d210b81795bdb970f7344e82f51cd77a3da0262e01760757de8215985b332	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ta\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.POWERPNT.16.1033.hxn.RYK	Dropped File	658 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
23950c844160a0c21f26725067a44257d062b6a750963cf4741f9dbc011069c5	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.002.etl.RYK	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
0a7c9733f743f0c64d4f2a913f363871a67deabd229a9f444d02ead856324ae2	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.005.etl.RYK	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3b3596e5fea728c9d77a6ae77443bc0d550928a591745ca3c9be23a0a9083cff	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.009.etl.RYK	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
04ff04367782e7afd1ef4c8c6d79536b8cfe751a3e5e26f3188b326fe6d8c810	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...lication Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-192.png.RYK	Dropped File	2.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d819e0bfa8d46967bd9e5be943862778085c542c794fb3a0b862700757271788	c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.003.etl.RYK	Dropped File	12.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
af0eb162cd3f3c9154d639bec905cc9b5567d4dd2a54c69f342ea1e9cfdd8390	C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp22B.tmp	Dropped File	4.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e0661a5f4ae6ac42645a31db263d62b965686ed8df788482c65cbfa5c3e9922d	-	Extracted File	298 bytes	image/png	-	CLEAN
b950c2c3cf4447549a7d11db78fe8abbad74cfd8dbba3a454785ea62aad99307	-	Extracted File	385 bytes	image/png	-	CLEAN
5ccbe44e7595305929197e320877394afb26d47016b00bc27e521be02d87e672	-	Extracted File	1.30 KB	image/png	-	CLEAN
8d97ea59a05f47e6c647529d6b09bb8d05cce92f90804de1bceb4c900e1b773c	-	Extracted File	3.51 KB	image/png	-	CLEAN
2997b6af7f8405dc4ba2d35e974f3294b824abf3df5aba221fc38b8917133c29	C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp22B.tmp	Dropped File	4.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
efe9c73d0d7d1a5596f037f29b62c0190bff7834da082ec425fb8958a79f4967	C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpEABB.tmp	Dropped File	4.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c7d0f9a20fae1e19911e4871148b3633c46d1c0add986a803a2ff9055ccbed5b	C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpEABB.tmp	Dropped File	4.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
a1a21799e98f97f271657ce656076f33dcb020d9370f1f2671d783cafd230294	c:\programdata\microsoft\crypto\rsa\machinekeys\08e575673cce10c72090304839888e02_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	52 bytes	application/octet-stream	-	CLEAN
9d02b65535798947514ce2d4191de4e3789036a05e8b4bdfe87bf5957de8afa3	C:\Boot\el-GR\RyukReadMe.html, C:\Boot\pl-PL\RyukReadMe.html, C:\Boot\lv-LV\RyukReadMe.html, C:\Boot\fi-FI\RyukReadMe.html, C:\Boo... ...: \programdata\microsoft\windows\sqm\manifest\ryukreadme.html, c:\programdata\microsoft\identitycrl\production\temp\ryukreadme.html	Dropped File	627 bytes	text/html	Access, Create, Write	CLEAN
f61c9b2639976995271ea715da57a88ac7cb923966785dbe1a2472949868dedc	C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp926F.tmp	Dropped File	4.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
03d9c9ddfdeeda042a7355850cc1030d3100861ef8248759b21daa88c42d5c7a	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...pplication data\application data\application data\application data\application data\oracle\java\installcache_x64\baseimagefam8.ryk	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN
d78bcd9f618eacd48754cc739f29592d836c7e6c61042235f35a64fea7150e2c	C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp926F.tmp	Dropped File	4.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ation data\application data\application data\microsoft\provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\masterdatastore.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication Data\Application Data\Application Data\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\folder.ico.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.mspub.16.1033.hxn.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...lication data\application data\application data\microsoft\provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\prov\runtime.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...cation data\application data\application data\microsoft\crypto\systemkeys\1fd8a841971dc8f18facf1d9475e3f87_03845cb8-7441-4a2f-8c0f-c90408af5778.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...cation Data\Application Data\Application Data\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\customizations.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...pplication Data\Application Data\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\MasterDescriptor.en-us.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.databasecompare.16.1033.hxn.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.015.etl.ryk	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...Application Data\Application Data\Application Data\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\sync.ico.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.bk.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...lication Data\Application Data\Application Data\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\guest.png.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...n Data\Application Data\Application Data\Microsoft\Windows Defender\Support\MpWppTracing-02112021-122238-00000003-ffffffff.bin.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...tion data\application data\application data\application data\application data\microsoft\smsrouter\messagestore\edbres00001.jrs.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.ONENOTE.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...data\application data\application data\application data\application data\microsoft\smsrouter\messagestore\smsinterceptstore.db.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.013.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ta\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.MSACCESS.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ata\application data\application data\microsoft\windows defender\scans\mpcache-9899dbe4d8bb3d253eb4f285757bebaf1581b50f.bin.83.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\parse.dat.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...n Data\Application Data\Application Data\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\print_property.ico.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion Data\Application Data\Application Data\Application Data\Application Data\Microsoft\SmsRouter\MessageStore\edbres00002.jrs.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...lication data\application data\application data\microsoft\provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\prov\runtime.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\Application Data\Application Data\Microsoft\Windows Defender\Scans\mpcache-9899DBE4D8BB3D253EB4F285757BEBAF1581B50F.bin.5B.RYK	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ation data\application data\application data\microsoft\provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\masterdatastore.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...pplication Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\nslist.hxl.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...application data\application data\application data\application data\application data\microsoft\user account pictures\guest.png.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\AssetLibrary.ico.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Definition Updates\Default\NisBase.vdm.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ... \Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\SmsRouter\MessageStore\edb.log.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.powerpnt.16.1033.hxn.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ation data\application data\application data\microsoft\provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\masterdatastore.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...cation Data\Application Data\Application Data\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\customizations.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ication Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.DATABASECOMPARE.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ation Data\Application Data\Application Data\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\MasterDatastore.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.010.etl.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-40.png.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...lication Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\diagnosis\downloadedscenarios\windows.siuf.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...application data\application data\application data\application data\application data\microsoft help\ms.lync_online.16.1033.hxn.ryk	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...cation data\application data\application data\microsoft\provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\customizations.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.012.etl.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\bcd.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user-48.png.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ata\application data\application data\application data\microsoft\windows defender\network inspection system\support\nislog.txt.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.003.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\application data\application data\microsoft\windows defender\scans\mpcache-9899dbe4d8bb3d253eb4f285757bebaf1581b50f.bin.a0.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ion data\application data\application data\application data\usoshared\logs\updatesessionorchestration.008.etl.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\SmsRouter\MessageStore\edbres00001.jrs.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Definition Updates\Default\MpAsBase.vdm.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...plication data\application data\microsoft\vault\ac658cb4-9126-49bd-b877-31eedab3f204\154e23d0-c644-4e6f-8ce6-5069272f999f.vsch.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\events10.rbs.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\application data\application data\application data\application data\application data\microsoft help\ms.winword.16.1033.hxn.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\smsrouter\messagestore\edb.log.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows Live\WLive48x48.png.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ication data\application data\application data\application data\application data\microsoft help\ms.databasecompare.16.1033.hxn.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Scans\MetaStore\2\00000000000000000.idx.RYK	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...data\application data\application data\application data\application data\microsoft help\ms.groove.16.1033.hxn.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...tion data\application data\application data\application data\application data\microsoft help\ms.spreadsheetcompare.16.1033.hxn.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.014.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...a\application data\application data\application data\application data\application data\microsoft\office\sharepointteamsite.ico.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.009.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.011.etl.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Oracle\Java\installcache_x64\baseimagefam8.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ation data\application data\application data\microsoft\provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\masterdatastore.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...n data\application data\microsoft\crypto\rsa\machinekeys\08e575673cce10c72090304839888e02_03845cb8-7441-4a2f-8c0f-c90408af5778.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ... Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.MSOUC.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.005.etl.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\diagnosis\parse.dat.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.013.etl.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\Application Data\Application Data\Microsoft\Windows Defender\Scans\mpcache-9899DBE4D8BB3D253EB4F285757BEBAF1581B50F.bin.CC.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...application data\application data\application data\application data\microsoft\user account pictures\guest.bmp.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user.bmp.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.002.etl.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.004.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.001.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ... \Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user.bmp.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ta\application data\application data\application data\application data\microsoft\diagnosis\downloadedsettings\cfc.flights.json.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...cation data\application data\application data\microsoft\provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\customizations.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ... \application data\application data\microsoft\clicktorun\9566930b-d1dd-4075-bfe6-74dd69b13189\en-us.16\stream.x86.en-us.man.dat.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Scans\MetaStore\3\0000000000000000.idx.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ... Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.MSPUB.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...cation data\application data\application data\microsoft\provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\customizations.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...tion data\application data\application data\microsoft\device stage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\print_queue.ico.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.007.etl.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.012.etl.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Boot\BCD.LOG1.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.015.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user.png.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\Application Data\Application Data\Microsoft\Windows Defender\Scans\mpcache-9899DBE4D8BB3D253EB4F285757BEBAF1581B50F.bin.7E.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ion Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.007.etl.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\windows defender\scans\mpdiag.bin.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ation data\application data\application data\microsoft\provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\masterdatastore.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ion data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.002.etl.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\windows nt\msscan\welcomescan.jpg.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...lication data\application data\application data\microsoft\provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\prov\runtime.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...n Data\Application Data\Application Data\Microsoft\Windows Defender\Support\MpWppTracing-02112021-124618-00000003-ffffffff.bin.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\application data\application data\microsoft\windows defender\scans\mpcache-9899dbe4d8bb3d253eb4f285757bebaf1581b50f.bin.67.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ation data\application data\application data\microsoft\provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\masterdatastore.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...plication data\application data\application data\application data\microsoft\windows nt\msfax\virtualinbox\en-us\welcomefax.tif.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\ClickToRunPackageLocker.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.outlook.16.1033.hxn.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...cation Data\Application Data\Application Data\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\customizations.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...cation Data\Application Data\Application Data\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\customizations.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\Application Data\Application Data\Microsoft\Windows Defender\Scans\mpcache-9899DBE4D8BB3D253EB4F285757BEBAF1581B50F.bin.80.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\SmsRouter\MessageStore\edb.chk.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Definition Updates\Default\MpAvDlta.vdm.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\diagnosis\events10.rbs.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\events11.rbs.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.lync.16.1033.hxn.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Provisioning\countrytable.xml.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\Application Data\Application Data\Microsoft\Windows Defender\Scans\mpcache-9899DBE4D8BB3D253EB4F285757BEBAF1581B50F.bin.67.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...data\application data\application data\application data\application data\microsoft\smsrouter\messagestore\smsinterceptstore.db.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\windows defender\definition updates\default\mpavbase.vdm.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Applicati... ... \Application Data\Application Data\Application Data\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.009.etl.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.onenote.16.1033.hxn.ryk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\events01.rbs.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...n data\application data\application data\microsoft\windows defender\support\mpwpptracing-02112021-121950-00000003-ffffffff.bin.ryk	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...plication data\application data\microsoft\vault\ac658cb4-9126-49bd-b877-31eedab3f204\3ccd5499-87a8-4b10-a215-608888dd3b55.vsch.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ata\application data\application data\microsoft\windows defender\scans\mpcache-9899dbe4d8bb3d253eb4f285757bebaf1581b50f.bin.cb.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ation Data\Application Data\Application Data\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\MasterDatastore.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn.RYK	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...tion Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\RDhJ0CNFevzX.dat.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Network\Downloader\qmgr0.dat.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\applicati... ...ata\application data\application data\application data\application data\microsoft\diagnosis\downloadedsettings\utc.app.json.bk.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\SmsRouter\MessageStore\edb.log.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ata\Application Data\Application Data\Microsoft\Windows Defender\Scans\mpcache-9899DBE4D8BB3D253EB4F285757BEBAF1581B50F.bin.A0.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\network\downloader\qmgr1.dat.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...on Data\Application Data\Application Data\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\scan_property.ico.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...ication Data\Application Data\Application Data\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\s321033.hash.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Scans\MpDiag.bin.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\SmsRouter\MessageStore\edbtmp.log.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication Data\Application Data\Application Data\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\netfol.ico.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...cation data\application data\microsoft\crypto\systemkeys\1fd8a841971dc8f18facf1d9475e3f87_03845cb8-7441-4a2f-8c0f-c90408af5778.ryk	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\SharePointPortalSite.ico.RYK	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...lication Data\Application Data\Application Data\Microsoft\Provisioning\ {fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime.xml.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...application data\application data\application data\microsoft\diagnosis\downloadedsettings\telemetry.asm-windowsdefault.json.bk.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ... data\application data\application data\application data\application data\application data\microsoft help\ms.graph.16.1033.hxn.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...ation data\application data\application data\microsoft\provisioning\ {ee4aac98-c174-4941-82b1-d121e493e4fb}\masterdatastore.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\MCbYiQSuvlan.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...plication Data\Application Data\Application Data\Application Data\Microsoft\Windows Defender\Scans\History\Service\Unknown.Log.RYK	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...cation data\application data\application data\microsoft\provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\customizations.xml.ryk	Accessed File	Access, Create, Write	MALICIOUS
c:\documents and settings\all users\application data\application data\application data\application data\application data\applicati... ...n data\application data\application data\application data\application data\microsoft\diagnosis\downloadedsettings\utc.app.json.ryk	Accessed File	Access, Create, Write	MALICIOUS
C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Applicati... ...lication Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-192.png.RYK	Accessed File	Access, Create, Write	MALICIOUS

Reduced dataset

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	access, read	wmic.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe	"C:\Users\RDhJ0CNFevzX\Desktop\a9643eb83d509ad4eac20a2a89d8571f8d781979ad078e89f5b75b4bcb16f65e.exe"	MALICIOUS
oghbmcipslan.exe	"C:\Users\RDhJ0CNFevzX\Desktop\OgHBMCIPSlan.exe" 8 LAN	MALICIOUS
mcbyiqsuvlan.exe	"C:\Users\RDhJ0CNFevzX\Desktop\MCbYiQSuvlan.exe" 8 LAN	MALICIOUS
cmd.exe	cmd /c "WMIC.exe shadowcopy delete"	SUSPICIOUS
cmd.exe	cmd /c "vssadmin.exe Delete Shadows /all /quiet"	SUSPICIOUS
wmic.exe	WMIC.exe shadowcopy delete	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F	CLEAN
cmd.exe	cmd /c "bcdedit /set {default} recoveryenabled No & bcdedit /set {default}"	CLEAN
cmd.exe	cmd /c "bootstatuspolicy ignoreallfailures"	CLEAN
icacls.exe	icacls "C:*" /grant Everyone:F /T /C /Qÿÿÿÿ	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F	CLEAN
net.exe	"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F	CLEAN
net.exe	"C:\Windows\System32\net.exe" stop "samss" /y	CLEAN
vssadmin.exe	vssadmin.exe Delete Shadows /all /quiet	CLEAN
net.exe	"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y	CLEAN
net1.exe	C:\Windows\system32\net1 stop "audioendpointbuilder" /y	CLEAN

Process Name	Commandline	Verdict
net1.exe	C:\Windows\system32\net1 stop "samss" /y	CLEAN
net1.exe	C:\Windows\system32\net1 stop "audioendpointbuilder" /y	CLEAN
net.exe	"C:\Windows\System32\net.exe" stop "samss" /y	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F	CLEAN
net1.exe	C:\Windows\system32\net1 stop "samss" /y	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F	CLEAN
taskkill.exe	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F	CLEAN
net.exe	"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y	CLEAN

YARA / AV

YARA (64)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.013.etl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\office\sharepointteamsite.ico.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.012.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\AssetLibrary.ico.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\windows defender\scans\mpdiag.bin.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.lync.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-40.png.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.004.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.bk.RYK	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Diagnosis\DownloadedScenarios\Windows.Uif.static.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC_BASIC.16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.mspub.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\MF\Active.GRL.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\MySharePoints.ico.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\guest.png.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\nslist.hxl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.msouc.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.databasecompare.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn.RYK	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.008.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.011.etl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Start Menu\Programs\Java\Visit Java.com.url.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user-32.png.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.graph.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.007.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.006.etl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\user.png.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\User Account Pictures\guest.bmp.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\MySite.ico.RYK	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.014.etl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\office\documentrepository.ico.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SETLANG.16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.GROOVE.16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.onenote.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.outlook.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.winword.16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn.RYK	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\clicktorun\deploymentconfig.0.xml.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.001.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\microsoft\clicktorun\deploymentconfig.1.xml.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\microsoft\clicktorun\deploymentconfig.2.xml.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.010.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\MF\Pending.GRL.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateUx.001.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Office\SharePointPortalSite.ico.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateSessionOrchestration.015.etl.RYK	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\start menu\programs\java\get help.url.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user-48.png.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user.bmp.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.MSACCESS. 16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\vault\ac658cb4-9126-49 bd-b877-31eedab3f204\policy.vpol.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft Help\MS.EXCEL. 16.1033.hxn.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Microsoft\Windows Live\WLive48x48.png.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.skypefb. 16.1033.hxn.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	C:\Documents and Settings\All Users\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\USOShared\Logs\UpdateUx. 002.etl.RYK	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft help\ms.powerpnt. 16.1033.hxn.ryk	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.002.etl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.005.etl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.009.etl.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\microsoft\user account pictures\user-192.png.ryk	Ransomware	5/5
Ransomware	HermesRyukEncryptedFile	File encrypted by Hermes or Ryuk Ransomware	Dropped File	c:\documents and settings\all users\application data\application data\application data\application data\application data\application data\application data\application data\usoshared\logs\updatesessionorchestration.003.etl.ryk	Ransomware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.1.0
Dynamic Engine Version	2023.1.0 / 01/31/2023 04:27
Static Engine Version	2023.1.0.0 / 2023-01-31 03:00:19
AV Exceptions Version	2023.1.1.6 / 2023-02-03 15:34:21
Link Detonation Heuristics Version	2023.1.1.12 / 2023-02-20 08:47:29
Smart Memory Dumping Rules Version	2023.1.1.6 / 2023-02-03 15:34:21
Config Extractors Version	2023.1.1.13 / 2023-02-24 09:02:43
Signature Trust Store Version	2023.1.1.7 / 2023-02-06 18:37:42
VMRay Threat Identifiers Version	2023.1.1.15 / 2023-03-06 16:55:24
YARA Built-in Ruleset Version	2023.1.1.14

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	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows