MALICIOUS

Classifications: Wiper | PUA | Ransomware | Spyware

Threat Names: App/Generic-AB

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe**
ID	#3519526
MD5	7cdf50ee4f3d0febc70dd36298ed07da
SHA1	0170c2deae4486a43894c202ea92d43556218e1c
SHA256	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef
File Size	32.00 KB
Report Created	2022-02-15 11:36 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 64 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies the content of multiple user files.			
5/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe deletes multiple user files.			
5/5	User Data Modification	Modifies Windows automatic backups	2	-
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe deletes Windows volume shadow copies. • (Process #8) cmd.exe deletes Windows volume shadow copies.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Total Commander, Internet Explorer / Edge, The Bat!, git.			
4/5	System Modification	Disables a crucial system tool	1	-
	• (Process #29) reg.exe disables the Registry Editor via registry.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe deletes executed executable "c:\users\rdhj0cnfevzx\desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe".			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Reputation	Known suspicious file	1	PUA
	• Reputation analysis labels the sample itself as "App/Generic-AB".			
1/5	Hide Tracks	Creates process with hidden window	15	-

Score	Category	Operation	Count	Classification
		• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #2) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #4) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #6) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #8) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #11) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #15) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #17) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #19) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #21) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #23) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #25) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #27) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #30) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #34) cmd.exe with a hidden window. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe starts (process #38) cmd.exe with a hidden window.		
1/5	Privilege Escalation	Enables process privilege	1	-
		• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe enables process privilege "SeDebugPrivilege".		
1/5	Persistence	Installs system startup script or application	2	-
		• (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe adds "C:\Users\RDhJ0CNFevzX\Desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe" to Windows startup via registry. • (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe adds "c:\programdata\microsoft\windows\start menu\programs\startup\desktop.ini-locked" to Windows startup folder.		
1/5	Hide Tracks	Changes folder appearance	27	-

Score	Category	Operation	Count	Classification

- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\desktop".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\documents".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs\accessibility".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs\accessories".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs\accessories\system tools".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs\administrative tools".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs\maintenance".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs\startup".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\programdata\microsoft\windows\start menu\programs\system tools".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\contacts".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\downloads".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\favorites".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\favorites\links".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\links".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\music".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\onedrive".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\camera roll".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\saved games".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\searches".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\videos".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\public\documents".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\public\pictures".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\public\music".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\public\videos".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe changes the appearance of folder "c:\users\public\desktop".

Score	Category	Operation	Count	Classification
1/5	System Modification	Modifies application directory	7	-

- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies "c:\program files (x86)\common files\active-charge.exe-locked".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies "c:\program files (x86)\common files\active-charge.exe-locked-locked".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies "c:\program files (x86)\common files\oh pain.exe-locked".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies "c:\program files (x86)\common files\designer\msaddndr.olb-locked".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies "c:\program files (x86)\common files\microsoft shared\dao\dao360.dll-locked".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies "c:\program files (x86)\common files\services\verisign.bmp-locked".
- (Process #1) 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe modifies "c:\program files (x86)\common files\system\directdb.dll-locked".

Mitre ATT&CK Matrix

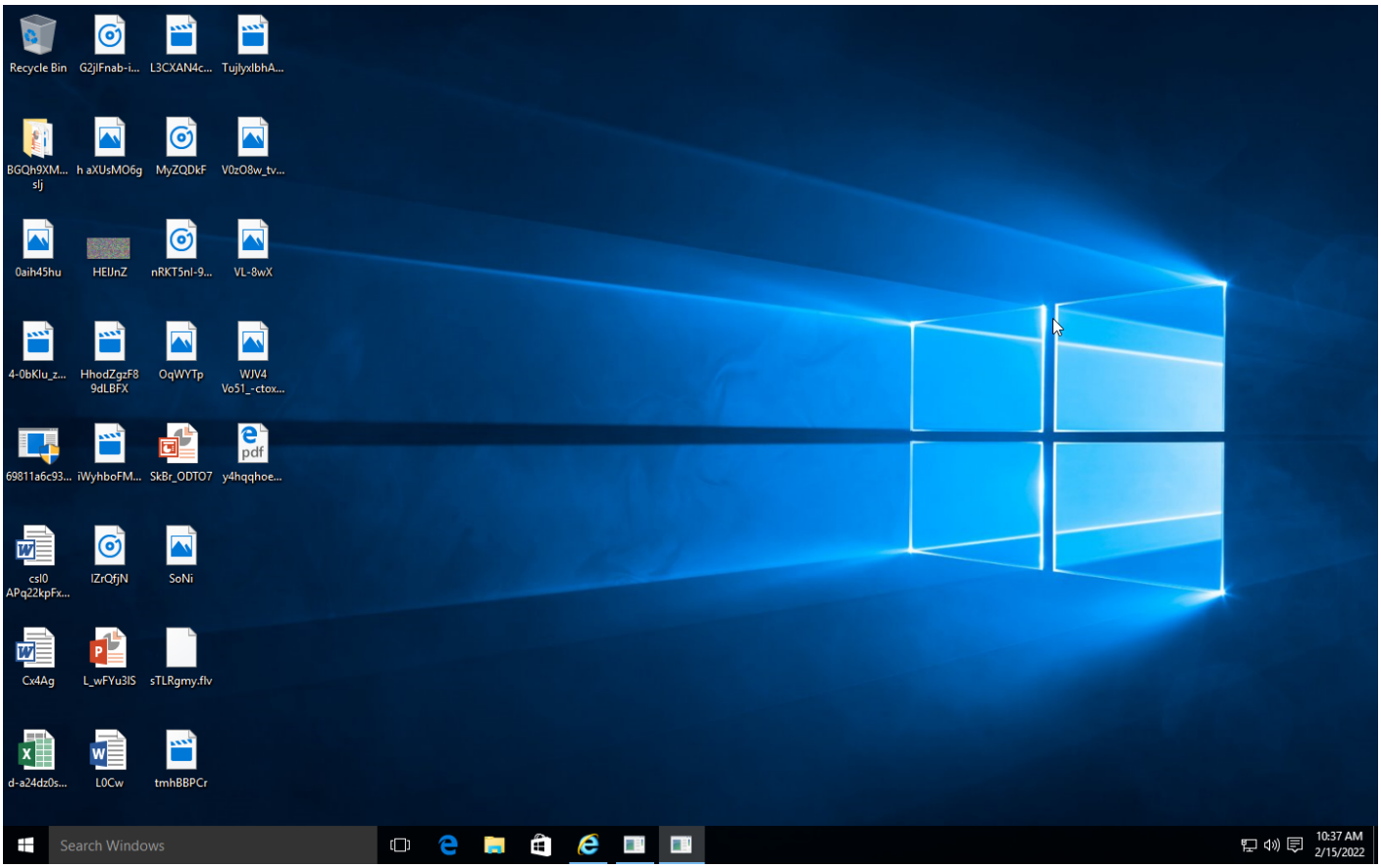
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
				#T1112 Modify Registry				#T1005 Data from Local System			#T1485 Data Destruction
				#T1036 Masquerading							#T1490 Inhibit System Recovery

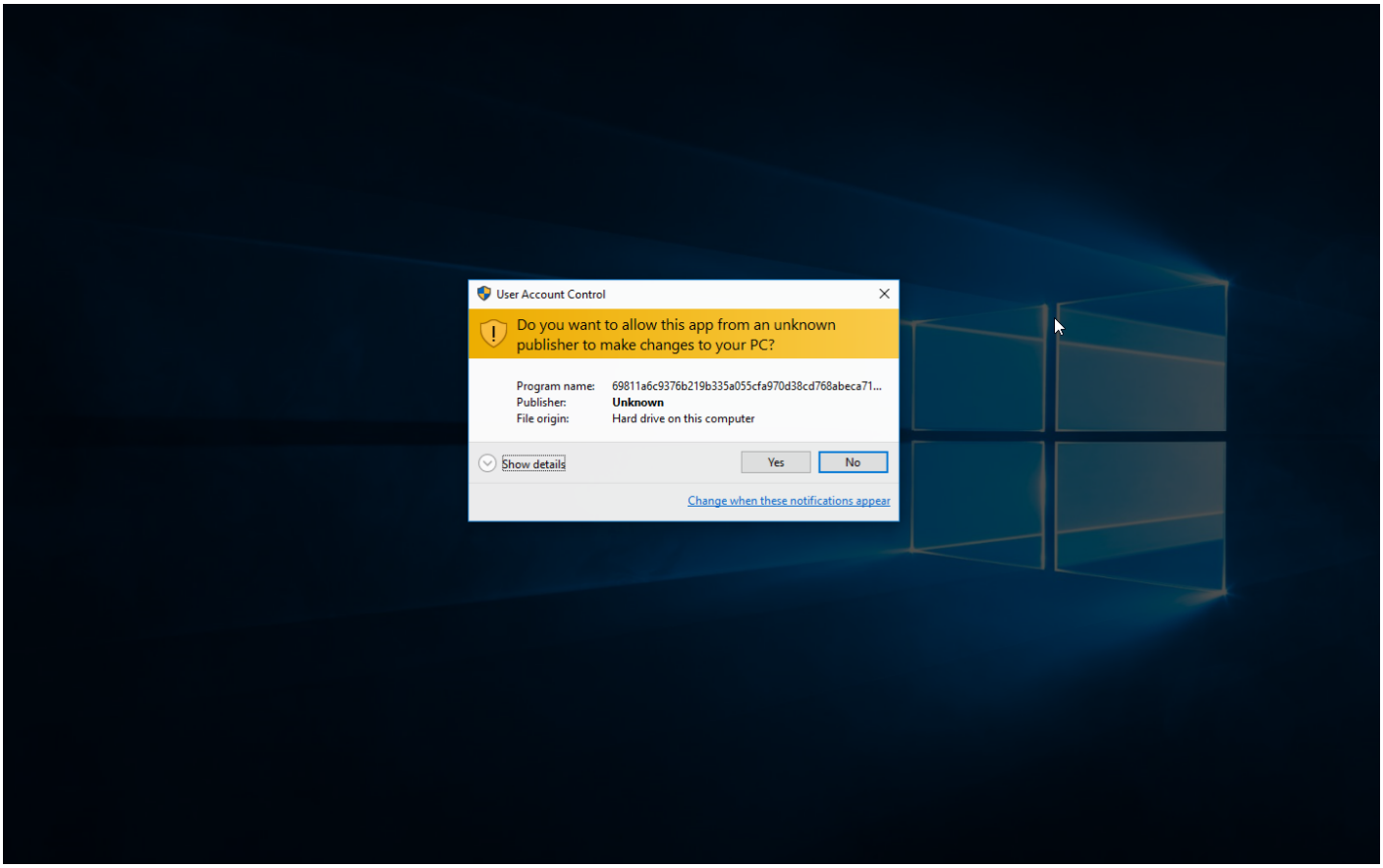
Sample Information

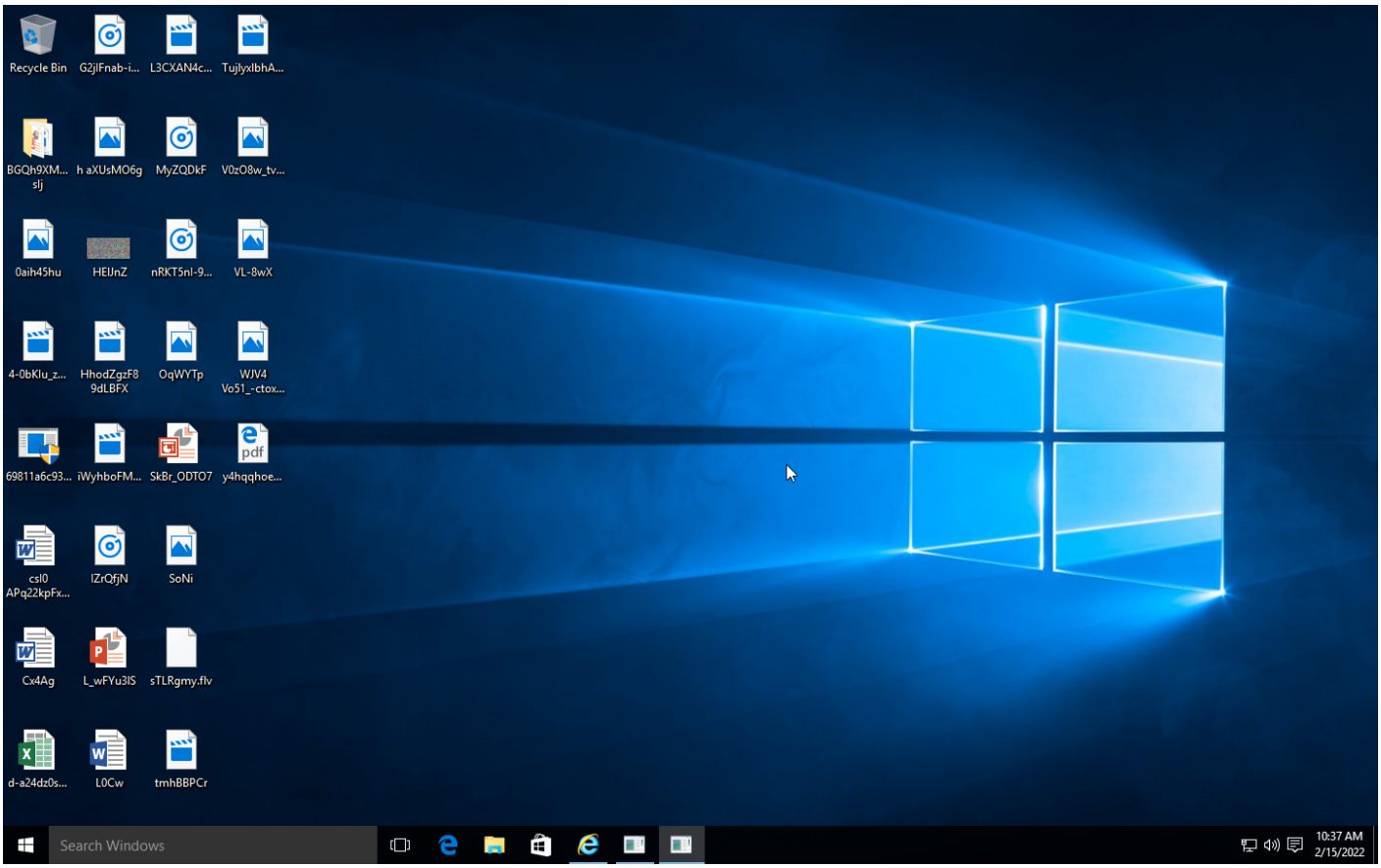
ID	#3519526
MD5	7cdf50ee4f3d0febc70dd36298ed07da
SHA1	0170c2deae4486a43894c202ea92d43556218e1c
SHA256	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef
SSDeep	384:AjdXpgpMf76oJgkB4nokwFwA4Ep/0VUx/Nx9DPxmB++6iCjGnLBs0Rr:adZgpCOagkBRp/0ut9Y++6iCjs2wr
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe
File Size	32.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

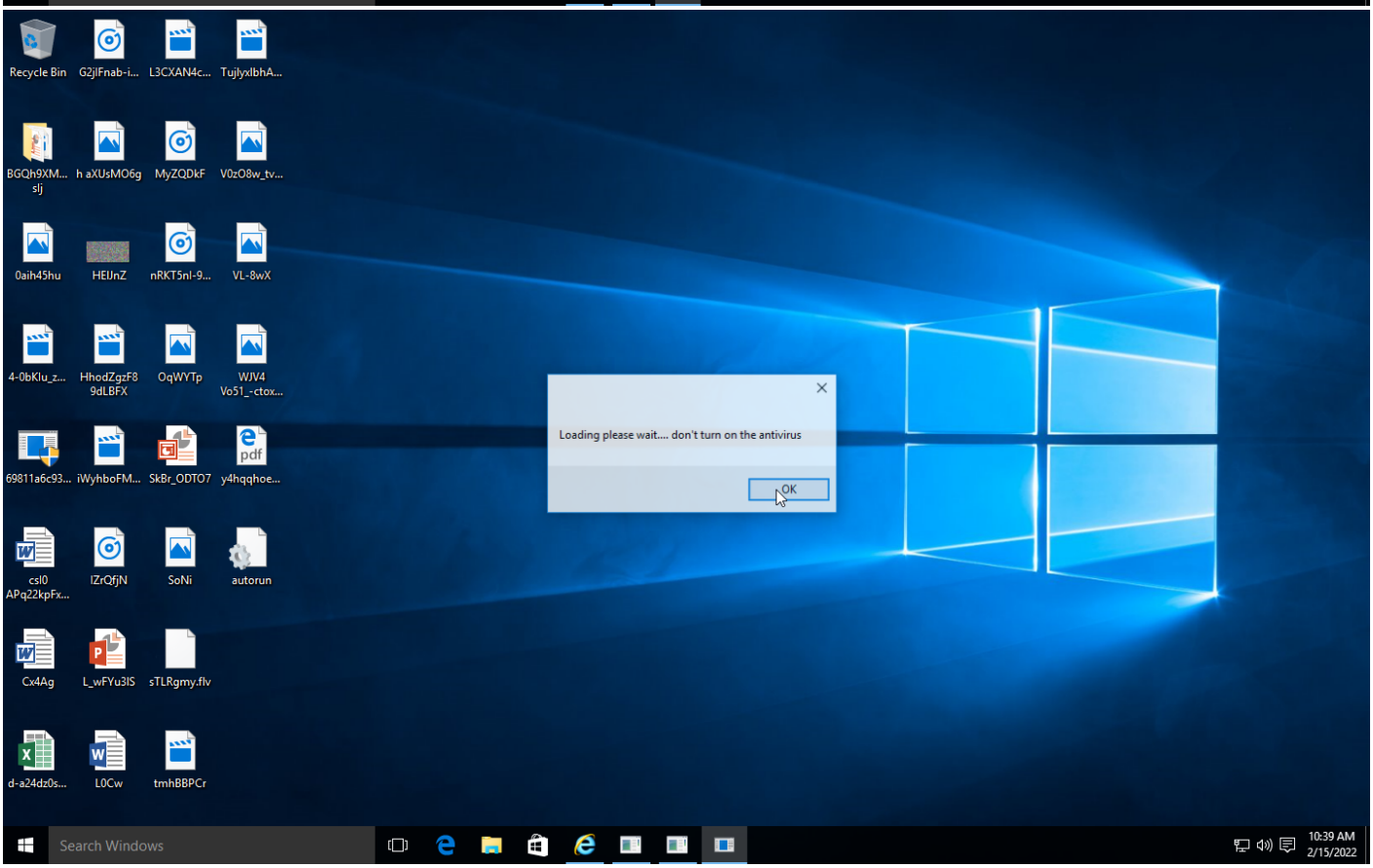
Analysis Information

Creation Time	2022-02-15 11:36 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	24
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
G2jlFnab-i...
L3CXAN4c...
TujlyxlbhA...
BGQh9XM...
slj
h aXUsMO6g
MyZQDkF
V0zO8w_tv...
0aih45hu
HEUnZ
nRKT5nl-9...
VL-8wX
4-0bKlu_z...
HhodZgzF8
9dLBFX
OqWYTp
WJV4
Vo51_-ctox...
69811a6c93...
iWyhboFM...
SkBr_ODTO7
y4hqqhoe...
csl0
APq22kpFx...
IZrQfjN
SoNi
Cx4Ag
L_wFYu3lS
sTLRgmy.flv
d-a24dz0s...
L0Cw
tmhBBPCr
Search Windows
10:37 AM
2/15/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 69811a6c9376b219b335a055cfa970d38cd768abeca71...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

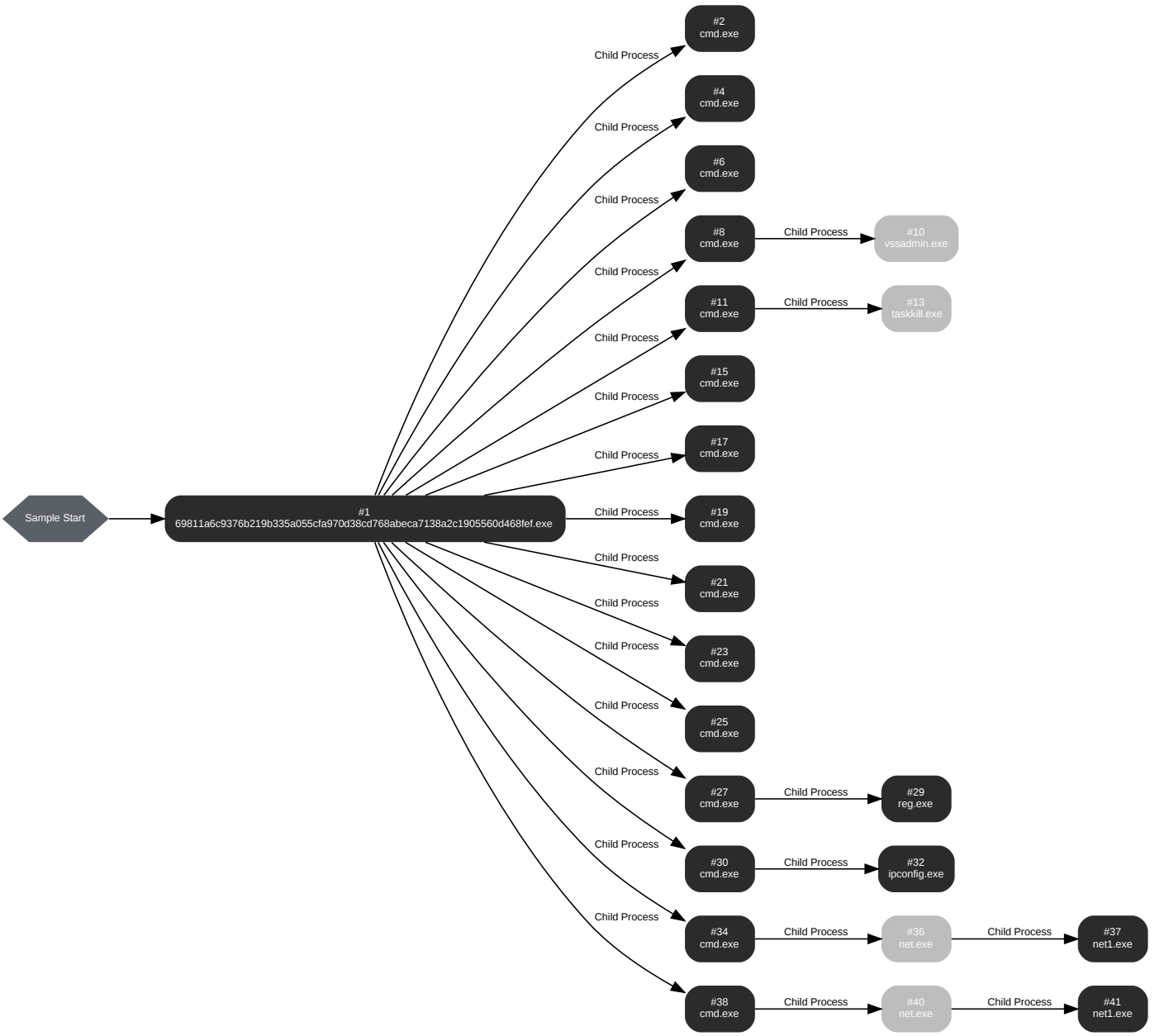
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72658, Reason: Analysis Target
Unmonitor End Time	End Time: 313712, Reason: Terminated by Timeout
Monitor duration	241.05s
Return Code	Unknown
PID	3864
Parent PID	1560
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_Eslj\YZL8R176sHB.swf-Locked-Locked-Locked	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	72
System	2
Window	35
Registry	6
File	2771
Process	15
User	4
Environment	1

Process #2: cmd.exe

ID	2
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C echo ^[autorun^] >autorun.inf
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 128202, Reason: Child Process
Unmonitor End Time	End Time: 146718, Reason: Terminated
Monitor duration	18.52s
Return Code	0
PID	596
Parent PID	3864
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
autorun.inf	65 bytes	3861acedffd29452d2fdb96728f7347652bde9353915d3873a7414843f49b8b1	✖

Host Behavior

Type	Count
Module	8
Registry	17
File	23
Environment	11
System	1

Process #4: cmd.exe

ID	4
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C echo ^open^=KasperskyScan^.exe >>autorun.inf
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 145747, Reason: Child Process
Unmonitor End Time	End Time: 147594, Reason: Terminated
Monitor duration	1.85s
Return Code	0
PID	2948
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	27
Environment	11
System	1

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C echo ^execute=^KasperskyScan^.exe >>autorun.inf
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 146699, Reason: Child Process
Unmonitor End Time	End Time: 149118, Reason: Terminated
Monitor duration	2.42s
Return Code	0
PID	4308
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	27
Environment	11
System	1

Process #8: cmd.exe

ID	8
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet && wmic shadowcopy delete
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 149322, Reason: Child Process
Unmonitor End Time	End Time: 155313, Reason: Terminated
Monitor duration	5.99s
Return Code	2
PID	5020
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #10: vssadmin.exe

ID	10
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin delete shadows /all /quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 150073, Reason: Child Process
Unmonitor End Time	End Time: 154321, Reason: Terminated
Monitor duration	4.25s
Return Code	2
PID	4316
Parent PID	5020
Bitness	32 Bit

Process #11: cmd.exe

ID	11
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C taskkill /im taskmgr.exe /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 246491, Reason: Child Process
Unmonitor End Time	End Time: 257426, Reason: Terminated
Monitor duration	10.94s
Return Code	128
PID	3988
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #13: taskkill.exe

ID	13
File Name	c:\windows\syswow64\taskkill.exe
Command Line	taskkill /im taskmgr.exe /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 248214, Reason: Child Process
Unmonitor End Time	End Time: 257342, Reason: Terminated
Monitor duration	9.13s
Return Code	128
PID	4088
Parent PID	3988
Bitness	32 Bit

Process #15: cmd.exe

ID	15
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C assoc .png=NotSoCleverBotFile
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 256432, Reason: Child Process
Unmonitor End Time	End Time: 258443, Reason: Terminated
Monitor duration	2.01s
Return Code	0
PID	3376
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	20
File	18
Environment	11
System	1

Process #17: cmd.exe

ID	17
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C assoc .vbs=NotSoCleverBotFile
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 257494, Reason: Child Process
Unmonitor End Time	End Time: 261788, Reason: Terminated
Monitor duration	4.29s
Return Code	0
PID	3736
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	20
File	18
Environment	11
System	1

Process #19: cmd.exe

ID	19
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C assoc .html=NotSoCleverBotFile
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 261225, Reason: Child Process
Unmonitor End Time	End Time: 266249, Reason: Terminated
Monitor duration	5.02s
Return Code	0
PID	4132
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	20
File	18
Environment	11
System	1

Process #21: cmd.exe

ID	21
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C assoc .bat=NotSoCleverBotFile
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 265279, Reason: Child Process
Unmonitor End Time	End Time: 270190, Reason: Terminated
Monitor duration	4.91s
Return Code	0
PID	1116
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	20
File	18
Environment	11
System	1

Process #23: cmd.exe

ID	23
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C assoc .jpn=EncryptedFile
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 269382, Reason: Child Process
Unmonitor End Time	End Time: 273114, Reason: Terminated
Monitor duration	3.73s
Return Code	0
PID	2300
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	20
File	18
Environment	11
System	1

Process #25: cmd.exe

ID	25
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C assoc .js=exe1file
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 272144, Reason: Child Process
Unmonitor End Time	End Time: 276148, Reason: Terminated
Monitor duration	4.00s
Return Code	0
PID	1940
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	20
File	18
Environment	11
System	1

Process #27: cmd.exe

ID	27
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_DWORD /d 1 /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 275184, Reason: Child Process
Unmonitor End Time	End Time: 280387, Reason: Terminated
Monitor duration	5.20s
Return Code	0
PID	1400
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #29: reg.exe

ID	29
File Name	c:\windows\syswow64\reg.exe
Command Line	reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_DWORD /d 1 /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 276409, Reason: Child Process
Unmonitor End Time	End Time: 278596, Reason: Terminated
Monitor duration	2.19s
Return Code	0
PID	1556
Parent PID	1400
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Registry	4
File	6

Process #30: cmd.exe

ID	30
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C ipconfig /release
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 278425, Reason: Child Process
Unmonitor End Time	End Time: 292984, Reason: Terminated
Monitor duration	14.56s
Return Code	0
PID	4240
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #32: ipconfig.exe

ID	32
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	ipconfig /release
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 281075, Reason: Child Process
Unmonitor End Time	End Time: 292099, Reason: Terminated
Monitor duration	11.02s
Return Code	0
PID	3108
Parent PID	4240
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
File	22
Environment	10
System	4

Process #34: cmd.exe

ID	34
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C net stop Windows Firewall
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 291983, Reason: Child Process
Unmonitor End Time	End Time: 297188, Reason: Terminated
Monitor duration	5.21s
Return Code	1
PID	3120
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #36: net.exe

ID	36
File Name	c:\windows\syswow64\net.exe
Command Line	net stop Windows Firewall
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292623, Reason: Child Process
Unmonitor End Time	End Time: 297181, Reason: Terminated
Monitor duration	4.56s
Return Code	1
PID	3680
Parent PID	3120
Bitness	32 Bit

Process #37: net1.exe

ID	37
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 stop Windows Firewall
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 294134, Reason: Child Process
Unmonitor End Time	End Time: 296402, Reason: Terminated
Monitor duration	2.27s
Return Code	1
PID	1608
Parent PID	3680
Bitness	32 Bit

Host Behavior

Type	Count
Module	4
File	8

Process #38: cmd.exe

ID	38
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C net stop Network Connections
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 296234, Reason: Child Process
Unmonitor End Time	End Time: 298786, Reason: Terminated
Monitor duration	2.55s
Return Code	1
PID	1848
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #40: net.exe

ID	40
File Name	c:\windows\syswow64\net.exe
Command Line	net stop Network Connections
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 297238, Reason: Child Process
Unmonitor End Time	End Time: 298844, Reason: Terminated
Monitor duration	1.61s
Return Code	1
PID	4896
Parent PID	1848
Bitness	32 Bit

Process #41: net1.exe

ID	41
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 stop Network Connections
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 297425, Reason: Child Process
Unmonitor End Time	End Time: 298843, Reason: Terminated
Monitor duration	1.42s
Return Code	1
PID	4908
Parent PID	4896
Bitness	32 Bit

Host Behavior

Type	Count
Module	4
File	8

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef	C:\Users\RDhJ0CNFevzX\Desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	Sample File	32.00 KB	application/vnd.microsoft.portable-executable	Delete, Access	MALICIOUS
3861acedffd29452d2fdb96728f7347652bde9353915d3873a7414843f49b8b1	C:\Users\RDhJ0CNFevzX\Desktop\autorun.inf, autorun.inf	Dropped File	65 bytes	application/x-setupscript	Create, Delete, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\SYSTEM32\RichEd20.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe.config	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
autorun.inf	Dropped File	Create, Access	CLEAN
C:\	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\autorun.inf	Dropped File	Delete, Access	CLEAN
C:\Windows\SysWOW64\net1.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E slj-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\0aih45hu.jpg-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\0aih45hu.jpg	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\4-0bKlu_zvUdt.mkv-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\4-0bKlu_zvUdt.mkv	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	Sample File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\autorun.inf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\csI0 APq22kpFx84um.doc-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\csI0 APq22kpFx84um.doc	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Cx4Ag.doc-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Cx4Ag.doc	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\d-a24dz0snVX.xlsx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\d-a24dz0snVX.xlsx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\G2jIFnab-iHgfnotUdc.wav-Locked	Accessed File	Create, Delete, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\G2jIFnab-iHgfnotUdc.wav	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\h aXUsMO6g.png-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\h aXUsMO6g.png	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\HElJnZ.bmp-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\HElJnZ.bmp	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\HhodZgzF8 9dLBFX.avi-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\HhodZgzF8 9dLBFX.avi	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\iWyhboFMJLgPq_b7Ud9.avi-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\iWyhboFMJLgPq_b7Ud9.avi	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\lZrQfjN.m4a-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\lZrQfjN.m4a	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\L0Cw.docx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\L0Cw.docx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\L3CXAN4c0b0rw2-.mkv-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\L3CXAN4c0b0rw2-.mkv	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\L_wFYu3lS.pptx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\L_wFYu3lS.pptx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\MyZQDkF.mp3-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\MyZQDkF.mp3	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\nRKT5nI-9Sno8sTzM1P5.wav-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\nRKT5nI-9Sno8sTzM1P5.wav	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\OqWYTp.bmp-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\OqWYTp.bmp	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\SkBr_ODTO7.ppt-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\SkBr_ODTO7.ppt	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\SoNi.jpg-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\SoNi.jpg	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\sTLRgmy.flv-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\sTLRgmy.flv	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\tmhBBPCr.mp4-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\tmhBBPCr.mp4	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\TujIyxIbhAxVP9v1.mp4-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\TujIyxIbhAxVP9v1.mp4	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\V0zO8w_tvkIQjvRX6KqC.jpg-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\V0zO8w_tvkIQjvRX6KqC.jpg	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\VL-8wX.png-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\VL-8wX.png	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WJV4 Vo51_-ctoxSde.gif-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WJV4 Vo51_-ctoxSde.gif	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\y4hqqhoePb18-mRGw.pdf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\y4hqqhoePb18-mRGw.pdf	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\EZB4hlMv59fpDjUh6qT.m4a-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\EZB4hlMv59fpDjUh6qT.m4a	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\eKq_zA-WA.mkv-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\eKq_zA-WA.mkv	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\iTP31jJvGR0dsUQ.wav-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\iTP31jJvGR0dsUQ.wav	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\ixYbal.avi-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\ixYbal.avi	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\SsEwkyDOda_C3BxCH.ppt-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\SsEwkyDOda_C3BxCH.ppt	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\Ujk4snw9z16p4ofDz.mp4-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\Ujk4snw9z16p4ofDz.mp4	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\YZL8R176sHB.swf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\BGQh9XM98-F_E sIj\YZL8R176sHB.swf	Accessed File	Delete, Access	CLEAN
C:\Program Files (x86)\Common Files\active-charge.exe-Locked	Accessed File	Create, Access	CLEAN
C:\Program Files (x86)\Common Files\active-charge.exe	Accessed File	Delete, Access	CLEAN
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Access 2016.lnk-Locked	Accessed File	Create, Access	CLEAN
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Access 2016.lnk	Accessed File	Delete, Access	CLEAN
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini-Locked	Accessed File	Create, Access	CLEAN
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini	Accessed File	Delete, Access	CLEAN
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Desktop.lnk-Locked	Accessed File	Create, Access	CLEAN
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Desktop.lnk	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\1FEg.xlsx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\1FEg.xlsx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\2XKT2 -erD.pptx-Locked	Accessed File	Create, Delete, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\2XKT2 -erD.pptx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4 yebkiYbIGx.xlsx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4 yebkiYbIGx.xlsx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4GH0Y9.pdf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4GH0Y9.pdf	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\88Z1o5.docx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\88Z1o5.docx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9wui5eVHXPKhOlhGPv40.docx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9wui5eVHXPKhOlhGPv40.docx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\awNrFZy3e3qK1nkjdW.pptx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\awNrFZy3e3qK1nkjdW.pptx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\azYkAGkUGGsOX2bnL.rtf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\azYkAGkUGGsOX2bnL.rtf	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\bf c.docx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\bf c.docx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cERxr1OfWdsXa.xlsx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cERxr1OfWdsXa.xlsx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\eUnC2MDENVIC3bG6_9q.xlsx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\eUnC2MDENVIC3bG6_9q.xlsx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FQNOqAqIU_64xnNqSNa.xlsx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FQNOqAqIU_64xnNqSNa.xlsx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fUkbCywvnkWTcZgPOjsY.ppt-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fUkbCywvnkWTcZgPOjsY.ppt	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\HBfGjDyK.doc-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\HBfGjDyK.doc	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\HUM 71h6W.pdf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\HUM 71h6W.pdf	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\joed-0tT3pwKPHxST7.pptx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\joed-0tT3pwKPHxST7.pptx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\jYYuHN3_bnMiF1-mgPtc.ots-Locked	Accessed File	Create, Delete, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\jYYuHN3_bnMiF1-mgPtc.ots	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\NyM PGDB-5 iHZerCT.doc-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\NyM PGDB-5 iHZerCT.doc	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\o4aClzZ-jet.doc-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\o4aClzZ-jet.doc	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\pA5CsH5h5CcswZCjqi.docx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\pA5CsH5h5CcswZCjqi.docx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\W7ZbDBvsnGLTRWeGfJh.pptx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\W7ZbDBvsnGLTRWeGfJh.pptx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\yPcZCDI_IdX.pptx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\yPcZCDI_IdX.pptx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\zBhJ.pdf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\zBhJ.pdf	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\ZFnXJ8 _1nRIfFhG.docx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\ZFnXJ8 _1nRIfFhG.docx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\BVt ejKmCvm0R4EXK.ods-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\BVt ejKmCvm0R4EXK.ods	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\mIKc8RXt4Q.pptx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\mIKc8RXt4Q.pptx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\ppl3T.xlsx-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\ppl3T.xlsx	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\rRshMO_Ed0_wrhaH.pdf-Locked	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y\rRshMO_Ed0_wrhaH.pdf	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\i3bdpGM-nK_y	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\NTUSER.DAT-Locked	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\NTUSER.DAT	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\0aih45hu.jpg-Locked-Locked	Accessed File	Create, Delete, Access	CLEAN

Reduced dataset

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools	write, access, read	reg.exe	MALICIOUS
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	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_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	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\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\.png	create, write, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\.vbs	create, write, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\.html	create, write, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\.bat	create, write, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\.jpn	create, write, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Classes\.js	create, write, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	create, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	access	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	write, access, read	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	CLEAN

Process

Process Name	Commandline	Verdict
69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe	"C:\Users\RDhJ0CNFevzX\Desktop\69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet && wmic shadowcopy delete	SUSPICIOUS
reg.exe	reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_DWORD /d 1 /f	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C echo ^[autorun^] >autorun.inf	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C echo ^open^=KasperskyScan^.exe >>autorun.inf	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C echo ^execute=^KasperskyScan^.exe >>autorun.inf	CLEAN
vssadmin.exe	vssadmin delete shadows /all /quiet	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C taskkill /im taskmgr.exe /f	CLEAN
taskkill.exe	taskkill /im taskmgr.exe /f	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C assoc .png=NotSoCleverBotFile	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C assoc .vbs=NotSoCleverBotFile	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C assoc .html=NotSoCleverBotFile	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C assoc .bat=NotSoCleverBotFile	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C assoc .jpn=EncryptedFile	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C assoc .js=exe1file	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t REG_DWORD /d 1 /f	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C ipconfig /release	CLEAN
ipconfig.exe	ipconfig /release	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C net stop Windows Firewall	CLEAN
net.exe	net stop Windows Firewall	CLEAN
net1.exe	C:\Windows\system32\net1 stop Windows Firewall	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C net stop Network Connections	CLEAN
net.exe	net stop Network Connections	CLEAN
net1.exe	C:\Windows\system32\net1 stop Network Connections	CLEAN

YARA / AV

No YARA or AV matches available.

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	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.11 / 2022-02-11 14:15:45
YARA Built-in Ruleset Version	4.4.1.11

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

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