MALICIOUS

Classifications: Ransomware

Threat Names: BlackEnergy/Voodoo Bear | APT28 | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe**
ID	#7569993
MD5	09250d8b8323c62fb59941b458fa70d1
SHA1	da5f6347207257139ac82b50bc8276de9c1afd9e
SHA256	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8
File Size	133.50 KB
Report Created	2023-04-30 00:31 (UTC)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 69 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies Windows automatic backups	25	-

- (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe deletes Windows volume shadow copies.
- (Process #2) cmd.exe deletes Windows volume shadow copies.
- (Process #4) cmd.exe deletes Windows volume shadow copies.
- (Process #6) cmd.exe deletes Windows volume shadow copies.
- (Process #8) cmd.exe deletes Windows volume shadow copies.
- (Process #10) cmd.exe deletes Windows volume shadow copies.
- (Process #12) cmd.exe deletes Windows volume shadow copies.
- (Process #13) cmd.exe deletes Windows volume shadow copies.
- (Process #16) cmd.exe deletes Windows volume shadow copies.
- (Process #19) cmd.exe deletes Windows volume shadow copies.
- (Process #25) cmd.exe deletes Windows volume shadow copies.
- (Process #31) cmd.exe deletes Windows volume shadow copies.
- (Process #35) cmd.exe deletes Windows volume shadow copies.
- (Process #40) cmd.exe deletes Windows volume shadow copies.
- (Process #44) cmd.exe deletes Windows volume shadow copies.
- (Process #47) cmd.exe deletes Windows volume shadow copies.
- (Process #50) cmd.exe deletes Windows volume shadow copies.
- (Process #52) cmd.exe deletes Windows volume shadow copies.
- (Process #55) cmd.exe deletes Windows volume shadow copies.
- (Process #58) cmd.exe deletes Windows volume shadow copies.
- (Process #61) cmd.exe deletes Windows volume shadow copies.
- (Process #65) cmd.exe deletes Windows volume shadow copies.
- (Process #68) cmd.exe deletes Windows volume shadow copies.
- (Process #71) cmd.exe deletes Windows volume shadow copies.
- (Process #74) cmd.exe deletes Windows volume shadow copies.

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware

- Renames 190 files by appending the extension ".id_c287f3826d6e218_email_enc2@dr.com_.scl".

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	-

- YARA detected "APT28_IMPLANT_4_v5" from ruleset "APTs" in memory dump data from (process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe.

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Encrypts content of user files	1	Ransomware

- (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe encrypts the content of multiple user files.

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Obscures a file's origin	2	-

- (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\Desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe".
- (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\ChromeFlashPlayer_c287f3826d6e218.exe".

Score	Category	Operation	Count	Classification
4/5	Reputation	Contacts known malicious URL	1	-

- Reputation analysis labels the URL "hxxp://5[.]39[.]86[.]86/default.jpg" which was contacted by (process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe as Mal/HTMLGen-A.

Score	Category	Operation	Count	Classification
2/5	Discovery	Executes WMI query	1	-
	• (Process #21) wmic.exe executes WMI query: SELECT * FROM Win32_ShadowCopy.			
2/5	Anti Analysis	Creates an unusually large number of processes	1	-
	• Above average number of processes were monitored.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe creates mutex with name "ChromeReaderHardWress2_c287f3826d6e218".			
1/5	Persistence	Installs system startup script or application	2	-
	• (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe adds ""C:\Users\RDhJ0CNFevzX\Desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe"" to Windows startup via registry. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe adds ""C:\Users\RDhJ0CNFevzX\AppData\Roaming\ChromeFlashPlayer_c287f3826d6e218.exe"" to Windows startup via registry.			
1/5	System Modification	Modifies application directory	4	-
	• (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe modifies "C:\Program Files\HELP_DECRYPT_YOUR_FILES.TXT". • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe modifies "C:\Program Files\HELP_DECRYPT_YOUR_FILES.HTML". • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe modifies "C:\Program Files (x86)\HELP_DECRYPT_YOUR_FILES.TXT". • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe modifies "C:\Program Files (x86)\HELP_DECRYPT_YOUR_FILES.HTML".			
1/5	System Modification	Modifies operating system directory	2	-
	• (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe creates file "C:\Windows\HELP_DECRYPT_YOUR_FILES.TXT" in the OS directory. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe creates file "C:\Windows\HELP_DECRYPT_YOUR_FILES.HTML" in the OS directory.			
1/5	Hide Tracks	Creates process with hidden window	27	-

Score	Category	Operation	Count	Classification
		• (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #2) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #4) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #6) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #8) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #10) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #12) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #13) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #16) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #19) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #25) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #31) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #35) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #40) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #44) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #47) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #50) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #52) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #55) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #58) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #61) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #65) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #68) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #71) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #74) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #77) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts (process #80) cmd.exe with a hidden window. • (Process #1) 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe starts Anonymous Process with a hidden window.		
-	Trusted	Known clean file	1	-
		• Embedded file "" is a known clean file.		
-	Trusted	File has embedded known clean URL	1	-
		• Extracted URL "https://translate.google.com" is a known clean URL.		

Mitre ATT&CK Matrix

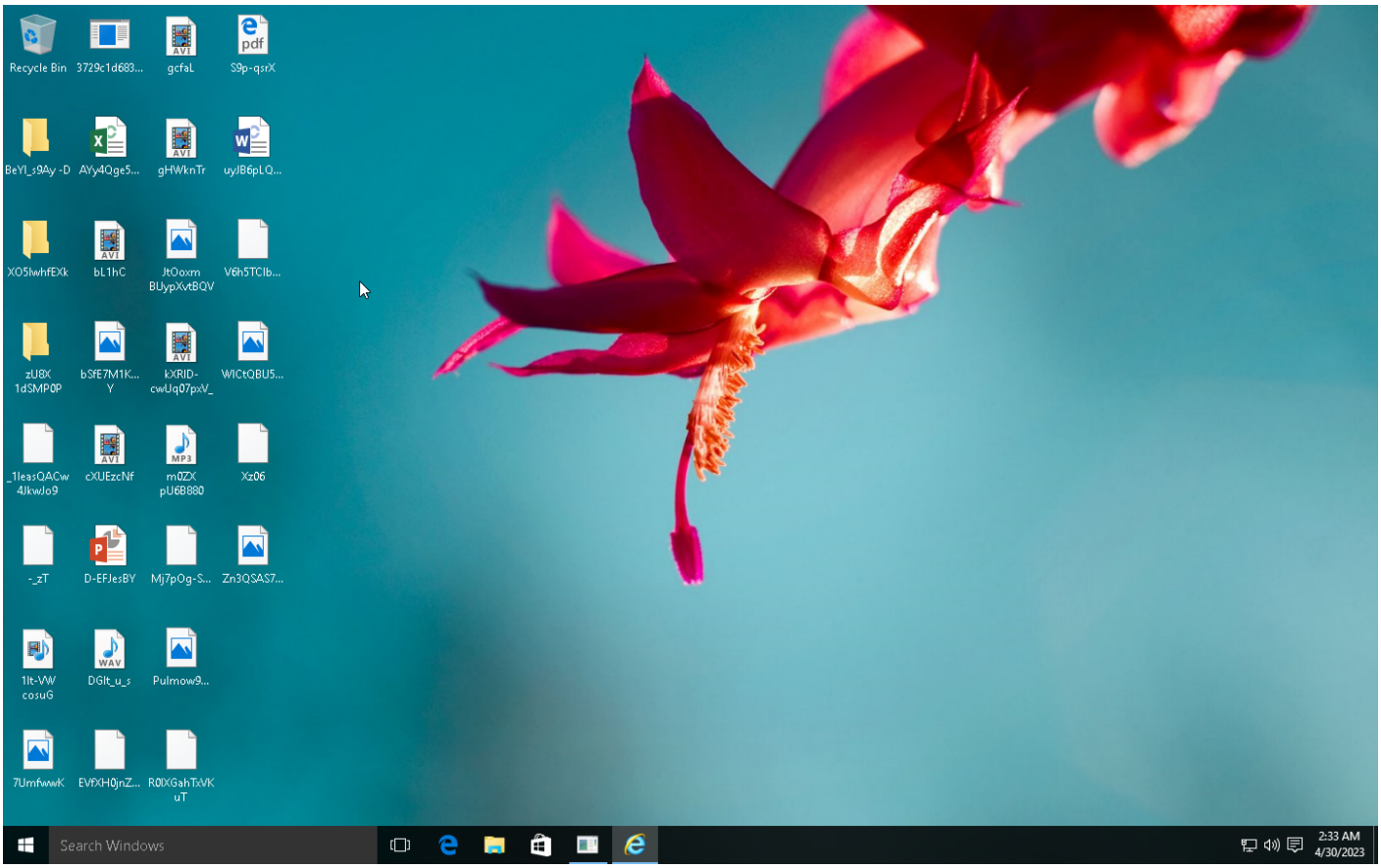
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1096 NTFS File Attributes							#T1490 Inhibit System Recovery
				#T1112 Modify Registry							#T1486 Data Encrypted for Impact
				#T1143 Hidden Window							

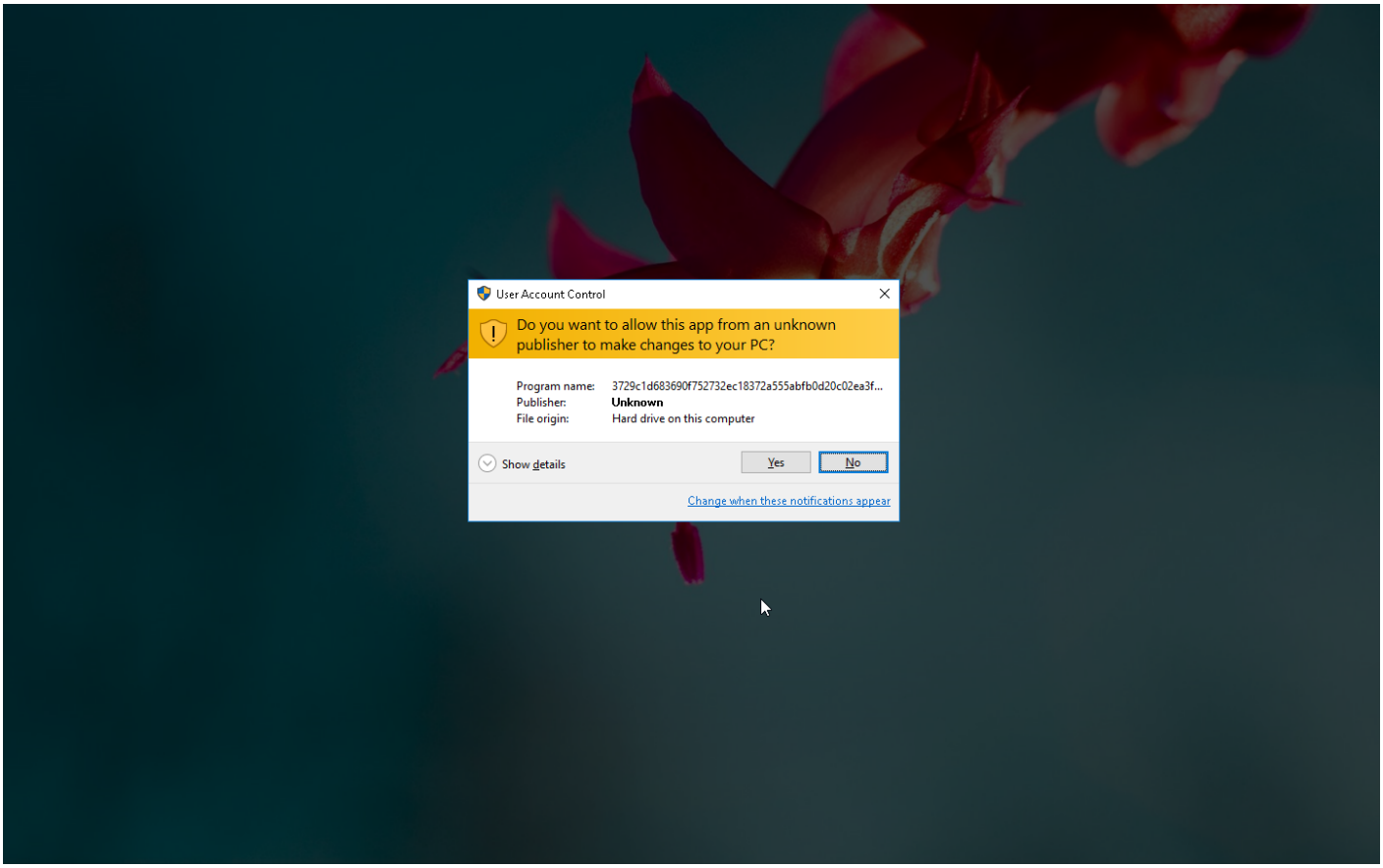
Sample Information

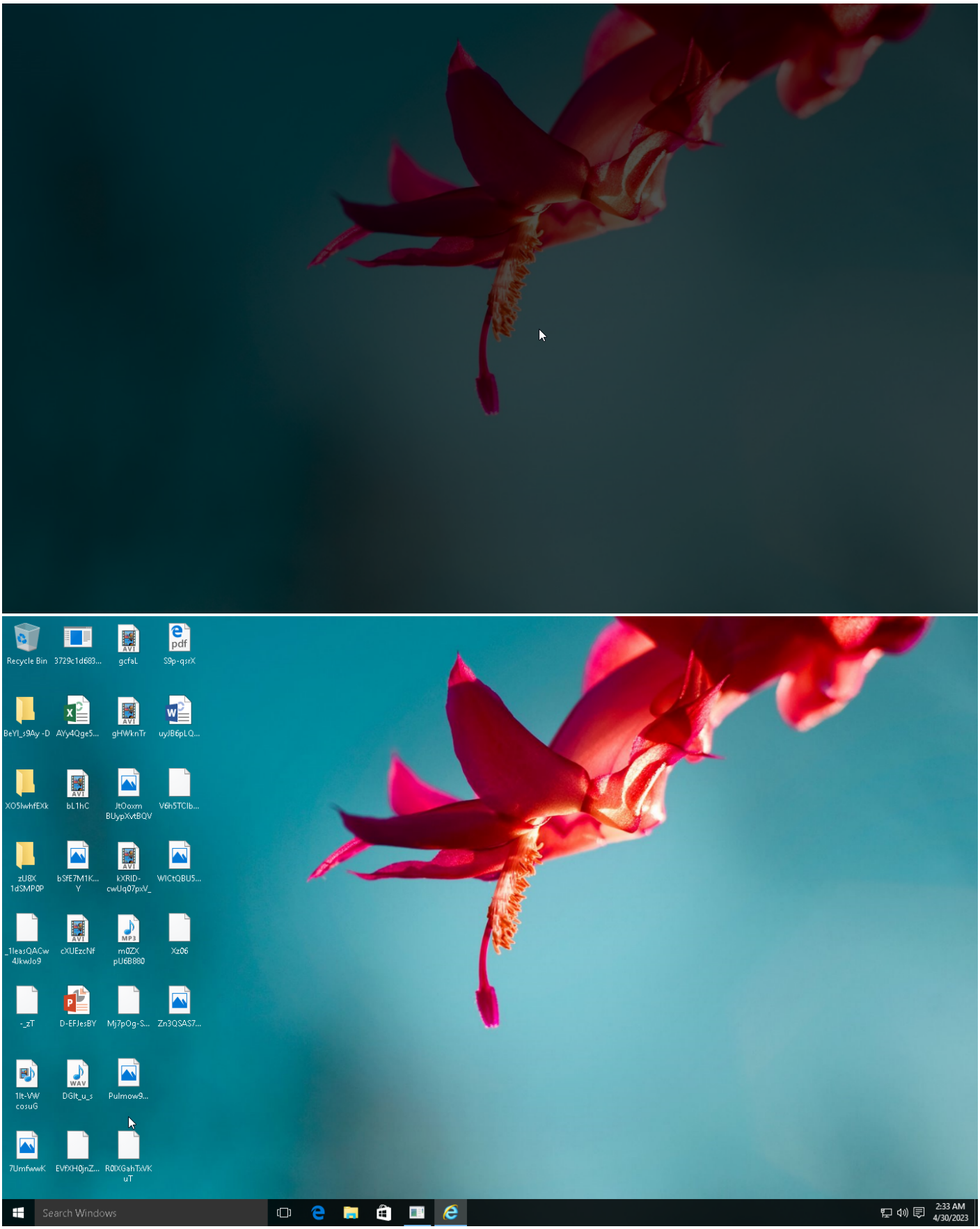
ID	#7569993
MD5	09250d8b8323c62fb59941b458fa70d1
SHA1	da5f6347207257139ac82b50bc8276de9c1afd9e
SHA256	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8
SSDeep	3072:00xSw+RJ356rtdzOXAkn0bioX13JDDNqS:0lSwk6toQCADv
ImpHash	a37e461efaa9819419d9e9c262f3e1fe
File Name	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe
File Size	133.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-04-30 00:31 (UTC)
Analysis Duration	00:03:00
Termination Reason	Timeout
Number of Monitored Processes	54
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	2


Recycle Bin
3729c1d683...
gcfaL
S9p-qsrX
BeYLs9Ay -D
AYy4Qge5...
gHWknTr
uyJB6pLQ...
XO5IwhfEKk
bL1hC
JtOoxm BUypXvtBQV
V6h5TCIb...
zU8X 1dSMP0P
bSfE7M1K... Y
kXRID-cwUq07pxV_
WICtQBU5...
_1IeasQACw 4JkwJo9
cXUEzcNf
m0ZX pU6B880
Xz06
-_zT
D-EFJesBY
Mj7pOg-S...
Zn3QSAS7...
1It-VW cosuG
DGIt_u_s
Pulmow9...
7UmfwwK
EVfXH0jnZ...
R0IXGahTxVK uT
Search Windows
2:33 AM
4/30/2023


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 3729c1d683690f752732ec18372a555abfb0d20c02ea3f...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

361 bytes total sent

694 bytes total received

1 ports 80

1 contacted IP addresses

2 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

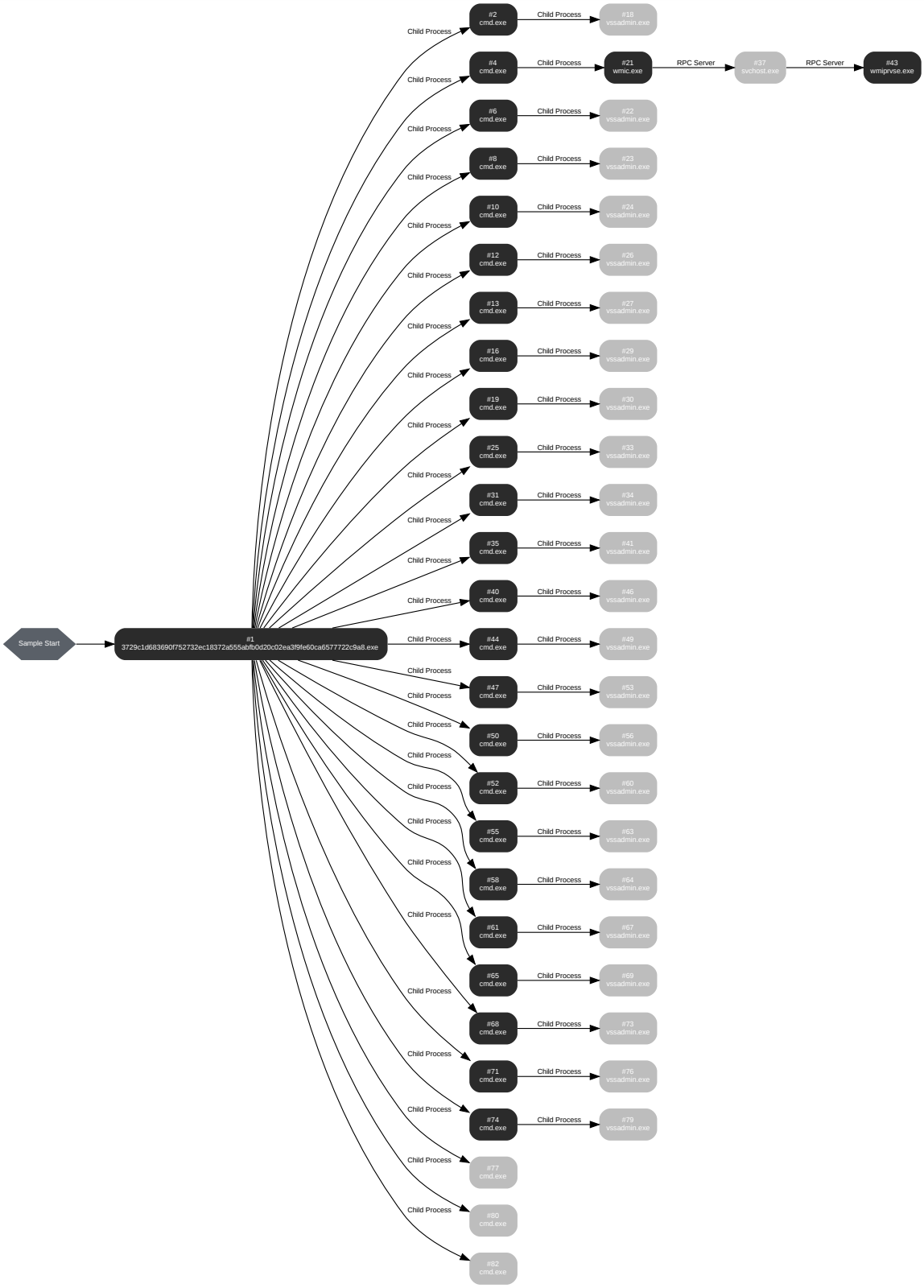
1 sessions, 361 bytes sent, 694 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://en[.]wikipedia[.]org/wiki/RSA_(cryptosystem)	-	-	-	0 bytes	CLEAN
GET	hxxp://5[.]39[.]86[.]86/default.jpg	-	-	-	0 bytes	MALICIOUS
GET	hxxps://translate[.]google[.]com	-	-	-	0 bytes	CLEAN

BEHAVIOR

Process Graph



Process #1: 3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 143084, Reason: Analysis Target
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	178.69s
Return Code	Unknown
PID	4476
Parent PID	1060
Bitness	32 Bit

Dropped Files (34)

File Name	File Size	SHA256	YARA Match
-	6.39 KB	512f4c514e7d3bb5d5e4c2d6ea00bbdc1b3331e11046ecb440de034e4ccb6391	✖
C:\Program Files\HELP_DECRYPT_YOUR_FILES.TXT	3.12 KB	10d00784bbd076a64280147e2b127838e6993338799a56c0f0d48443e0d8c58f	✖
C:\ProgramData\HELP_DECRYPT_YOUR_FILES.HTML	2.07 KB	6d5f7677cb005a319da2a44f06c042cfde0a433d98cee3ecc3503c288889ec62	✖
-	560 bytes	e100148f841dfc48c0e332bb4aecf798b7eb0f0c7a814d215a8bd676dc97454f	✖
-	208 bytes	0bb037cc38573903153c7477abb88be3f4ad0bb42de1ad978975d885bd3638e3	✖
-	7.17 KB	bd5cd42d7f5823b6b479601b363af1aba24f5e8568f17cf1c49c6dcc62682075	✖
-	2.19 KB	8a69509b25bb0e171bfe8bf47e08b0b70b28f63bb26d6123285453366a783453	✖
-	272 bytes	4d2f5cb1e86e821a28f0e6d6dbe3dbe3cfbd53e2f91bb166177bdd3af59fef8b	✖
-	1.78 KB	1f862eaba10bc82b80c6de40df5030ae74bf5dc7e6d4c8e1d9a5e7900a4dca6f	✖
-	1.94 KB	fbe372ff46a316840852ffdd35c468e1b8539a29a0783560e77254aff5f6543d	✖
-	832 bytes	2ebeb822006c66f1847d9147742c9ce0dbe4ad53eeca500b2094b43eb02ee981	✖
-	592 bytes	9f2a732a0668740f533c041a1a157226ad0d8e9213fc535bfc08e8d3ec023f2b	✖
-	3629.45 KB	d721d02e5bc5ac0f8a7267c079395b834b18ad55f92455d88e6fd2865644e56b	✖
-	3.66 KB	efd2518e06a11f557aaf9b1a4b0db00f364bca6ebada0489f7c435b790b7a9b6	✖
-	1.23 KB	fc564dcd00e0c8d164597caf6e91165ea77b4da4500d14f582a40db5fb0e2ea0	✖
C:\Users\RDhJ0CNFevzX\Desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	133.50 KB	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8	✖
-	880 bytes	b359806c78be307c5c3010d81dfa01d795c5f425e966e66b7aab02b9d5cc4304	✖
-	7.81 KB	ba58a5d95ec5cd5fad0b46ab103aa581f1c4472929e42b17eada0f58d9aa782e	✖

File Name	File Size	SHA256	YARA Match
-	21.86 KB	b3a53a64d6fad6fd8f74da67e04e4a5dc7fd4cf8d326aafa2e68bf6e63dd7ddd	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	352 bytes	cec550e9898ff0a757197babaca9afaa8cfd03ed46f4759562675aaf899fdbbb	✖
-	1.94 KB	24a324a50539b8f95b2ba05cbb3f17681eb30fc6e53c2971e0e5621bfae2e87a	✖
-	320 bytes	ea1445aebbe3d005a7991c37c8f443db959037ba3c080cae29516c793b90ceb0	✖
-	5.41 KB	e47c99f71f3f21b00fcb026bc6d3e7503f0e4b4007061e8d5a5270fd163bf2e6	✖
-	352 bytes	78453f1de270f93081b1589ae76506e792d190e06c9280564d733031f72d8706	✖
-	1.36 KB	6486faeb5877ef10cc77f3b27fc6f7c4a0a5390b9f1eaa31a8a151a788532569	✖
-	560 bytes	ca16950451e098bd805e95cff63997cd5398a253df806b405adde6d7e747c82f	✖
-	864.47 KB	ee2b6c0cee193353479a627a7ee7ee2c7fa871f852817aaa5ba922614fe459e0	✖
-	2.17 KB	b0ffae8185617b120c7a1f16a63458ef34234991fe19388f8e239b470397bc7e	✖
-	20.55 KB	aeb5b9a120887d59eb4492cd2051d5743aca43ef3132e906c15215b442422783	✖
-	1.41 KB	7c5ab5a5e01b02eadec267a0a06292569980027e060d9f0e1073950434213712	✖
-	3.28 KB	15561652a46531fda22a4318934dae007459aed43d4664b6c9c5a5f890099a24	✖
-	448 bytes	64667670cdb26c6687fd59934fa78d33968a4d571b2912af0432deb3c5e7312d	✖
-	1.61 KB	57f75d5ffbf00b8b998d91791431e51e889c8ebcd85a2caaa92976818d1b9fc6	✖

Host Behavior

Type	Count
Module	16262
File	4121
Environment	1
System	31
Keyboard	1
User	768
Mutex	1
Registry	26
Process	27

Network Behavior

Type	Count
HTTP	1

Process #2: cmd.exe

ID	2
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin.exe Delete Shadows /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 221323, Reason: Child Process
Unmonitor End Time	End Time: 257141, Reason: Terminated
Monitor duration	35.82s
Return Code	2
PID	3448
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	9
Environment	8
Process	1

Process #4: cmd.exe

ID	4
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C wmic shadowcopy delete
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 221978, Reason: Child Process
Unmonitor End Time	End Time: 294897, Reason: Terminated
Monitor duration	72.92s
Return Code	2147749908
PID	4844
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	10
Process	1

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=Z: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 223657, Reason: Child Process
Unmonitor End Time	End Time: 258319, Reason: Terminated
Monitor duration	34.66s
Return Code	2
PID	4812
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	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 /For=Y: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 224520, Reason: Child Process
Unmonitor End Time	End Time: 258757, Reason: Terminated
Monitor duration	34.24s
Return Code	2
PID	3532
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #10: cmd.exe

ID	10
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=X: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 225645, Reason: Child Process
Unmonitor End Time	End Time: 261376, Reason: Terminated
Monitor duration	35.73s
Return Code	2
PID	3608
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #12: cmd.exe

ID	12
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=W: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 226633, Reason: Child Process
Unmonitor End Time	End Time: 262119, Reason: Terminated
Monitor duration	35.49s
Return Code	2
PID	4700
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #13: cmd.exe

ID	13
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=V: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 228033, Reason: Child Process
Unmonitor End Time	End Time: 262011, Reason: Terminated
Monitor duration	33.98s
Return Code	2
PID	4900
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #16: cmd.exe

ID	16
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=U: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 229984, Reason: Child Process
Unmonitor End Time	End Time: 262074, Reason: Terminated
Monitor duration	32.09s
Return Code	2
PID	3824
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #18: vssadmin.exe

ID	18
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin.exe Delete Shadows /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 234140, Reason: Child Process
Unmonitor End Time	End Time: 256179, Reason: Terminated
Monitor duration	22.04s
Return Code	2
PID	3920
Parent PID	3448
Bitness	32 Bit

Process #19: cmd.exe

ID	19
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=T: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 234194, Reason: Child Process
Unmonitor End Time	End Time: 263433, Reason: Terminated
Monitor duration	29.24s
Return Code	2
PID	3944
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #21: wmic.exe

ID	21
File Name	c:\windows\syswow64\wbem\wmic.exe
Command Line	wmic shadowcopy delete
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 234974, Reason: Child Process
Unmonitor End Time	End Time: 292310, Reason: Terminated
Monitor duration	57.34s
Return Code	2147749908
PID	4048
Parent PID	4844
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

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

Process #22: vssadmin.exe

ID	22
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=Z: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237213, Reason: Child Process
Unmonitor End Time	End Time: 257017, Reason: Terminated
Monitor duration	19.80s
Return Code	2
PID	4772
Parent PID	4812
Bitness	32 Bit

Process #23: vssadmin.exe

ID	23
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=Y: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237635, Reason: Child Process
Unmonitor End Time	End Time: 257373, Reason: Terminated
Monitor duration	19.74s
Return Code	2
PID	4136
Parent PID	3532
Bitness	32 Bit

Process #24: vssadmin.exe

ID	24
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=X: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 238286, Reason: Child Process
Unmonitor End Time	End Time: 259982, Reason: Terminated
Monitor duration	21.70s
Return Code	2
PID	5016
Parent PID	3608
Bitness	32 Bit

Process #25: cmd.exe

ID	25
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=S: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 238756, Reason: Child Process
Unmonitor End Time	End Time: 265748, Reason: Terminated
Monitor duration	26.99s
Return Code	2
PID	4356
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #26: vssadmin.exe

ID	26
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=W: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 239362, Reason: Child Process
Unmonitor End Time	End Time: 259877, Reason: Terminated
Monitor duration	20.52s
Return Code	2
PID	1616
Parent PID	4700
Bitness	32 Bit

Process #27: vssadmin.exe

ID	27
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=V: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 240308, Reason: Child Process
Unmonitor End Time	End Time: 260071, Reason: Terminated
Monitor duration	19.76s
Return Code	2
PID	1388
Parent PID	4900
Bitness	32 Bit

Process #29: vssadmin.exe

ID	29
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=U: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 243353, Reason: Child Process
Unmonitor End Time	End Time: 260298, Reason: Terminated
Monitor duration	16.95s
Return Code	2
PID	4996
Parent PID	3824
Bitness	32 Bit

Process #30: vssadmin.exe

ID	30
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=T: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 244760, Reason: Child Process
Unmonitor End Time	End Time: 262011, Reason: Terminated
Monitor duration	17.25s
Return Code	2
PID	4160
Parent PID	3944
Bitness	32 Bit

Process #31: cmd.exe

ID	31
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=R: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 245777, Reason: Child Process
Unmonitor End Time	End Time: 269937, Reason: Terminated
Monitor duration	24.16s
Return Code	2
PID	5116
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #33: vssadmin.exe

ID	33
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=S: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 246421, Reason: Child Process
Unmonitor End Time	End Time: 263944, Reason: Terminated
Monitor duration	17.52s
Return Code	2
PID	140
Parent PID	4356
Bitness	32 Bit

Process #34: vssadmin.exe

ID	34
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=R: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 250983, Reason: Child Process
Unmonitor End Time	End Time: 268579, Reason: Terminated
Monitor duration	17.60s
Return Code	2
PID	2976
Parent PID	5116
Bitness	32 Bit

Process #35: cmd.exe

ID	35
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=Q: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 251064, Reason: Child Process
Unmonitor End Time	End Time: 273732, Reason: Terminated
Monitor duration	22.67s
Return Code	2
PID	2740
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

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: 252863, Reason: RPC Server
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	68.92s
Return Code	Unknown
PID	868
Parent PID	4048
Bitness	64 Bit

Process #40: cmd.exe

ID	40
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=P: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 256470, Reason: Child Process
Unmonitor End Time	End Time: 282748, Reason: Terminated
Monitor duration	26.28s
Return Code	2
PID	3128
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #41: vssadmin.exe

ID	41
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=Q: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 256559, Reason: Child Process
Unmonitor End Time	End Time: 272592, Reason: Terminated
Monitor duration	16.03s
Return Code	2
PID	3144
Parent PID	2740
Bitness	32 Bit

Process #43: wmiprvse.exe

ID	43
File Name	c:\windows\syswow64\wbem\wmiprvse.exe
Command Line	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 261381, Reason: RPC Server
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	60.40s
Return Code	Unknown
PID	3200
Parent PID	868
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Mutex	1
Module	22
Registry	4
File	1

Process #44: cmd.exe

ID	44
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=O: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 262299, Reason: Child Process
Unmonitor End Time	End Time: 293871, Reason: Terminated
Monitor duration	31.57s
Return Code	2
PID	3228
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #46: vssadmin.exe

ID	46
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=P: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 263736, Reason: Child Process
Unmonitor End Time	End Time: 280052, Reason: Terminated
Monitor duration	16.32s
Return Code	2
PID	4756
Parent PID	3128
Bitness	32 Bit

Process #47: cmd.exe

ID	47
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=N: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 266155, Reason: Child Process
Unmonitor End Time	End Time: 297965, Reason: Terminated
Monitor duration	31.81s
Return Code	2
PID	4260
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #49: vssadmin.exe

ID	49
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=O: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 269635, Reason: Child Process
Unmonitor End Time	End Time: 291750, Reason: Terminated
Monitor duration	22.11s
Return Code	2
PID	4932
Parent PID	3228
Bitness	32 Bit

Process #50: cmd.exe

ID	50
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=M: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 270137, Reason: Child Process
Unmonitor End Time	End Time: 306224, Reason: Terminated
Monitor duration	36.09s
Return Code	2
PID	2604
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #52: cmd.exe

ID	52
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=L: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 273212, Reason: Child Process
Unmonitor End Time	End Time: 308008, Reason: Terminated
Monitor duration	34.80s
Return Code	2
PID	3244
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #53: vssadmin.exe

ID	53
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=N: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 274286, Reason: Child Process
Unmonitor End Time	End Time: 295517, Reason: Terminated
Monitor duration	21.23s
Return Code	2
PID	3024
Parent PID	4260
Bitness	32 Bit

Process #55: cmd.exe

ID	55
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=K: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 280516, Reason: Child Process
Unmonitor End Time	End Time: 311959, Reason: Terminated
Monitor duration	31.44s
Return Code	2
PID	3276
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #56: vssadmin.exe

ID	56
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=M: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 281074, Reason: Child Process
Unmonitor End Time	End Time: 304905, Reason: Terminated
Monitor duration	23.83s
Return Code	2
PID	2544
Parent PID	2604
Bitness	32 Bit

Process #58: cmd.exe

ID	58
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=J: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 283554, Reason: Child Process
Unmonitor End Time	End Time: 313232, Reason: Terminated
Monitor duration	29.68s
Return Code	2
PID	4508
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #60: vssadmin.exe

ID	60
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=L: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 286541, Reason: Child Process
Unmonitor End Time	End Time: 307472, Reason: Terminated
Monitor duration	20.93s
Return Code	2
PID	568
Parent PID	3244
Bitness	32 Bit

Process #61: cmd.exe

ID	61
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=I: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292200, Reason: Child Process
Unmonitor End Time	End Time: 316554, Reason: Terminated
Monitor duration	24.35s
Return Code	2
PID	1268
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #63: vssadmin.exe

ID	63
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=K: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 294099, Reason: Child Process
Unmonitor End Time	End Time: 309960, Reason: Terminated
Monitor duration	15.86s
Return Code	2
PID	636
Parent PID	3276
Bitness	32 Bit

Process #64: vssadmin.exe

ID	64
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=J: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 295834, Reason: Child Process
Unmonitor End Time	End Time: 311755, Reason: Terminated
Monitor duration	15.92s
Return Code	2
PID	4680
Parent PID	4508
Bitness	32 Bit

Process #65: cmd.exe

ID	65
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=H: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 299010, Reason: Child Process
Unmonitor End Time	End Time: 319421, Reason: Terminated
Monitor duration	20.41s
Return Code	2
PID	1580
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #67: vssadmin.exe

ID	67
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=I: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 300463, Reason: Child Process
Unmonitor End Time	End Time: 315661, Reason: Terminated
Monitor duration	15.20s
Return Code	2
PID	2952
Parent PID	1268
Bitness	32 Bit

Process #68: cmd.exe

ID	68
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=G: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 304362, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	17.42s
Return Code	Unknown
PID	4552
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	8
Process	1

Process #69: vssadmin.exe

ID	69
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=H: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 304595, Reason: Child Process
Unmonitor End Time	End Time: 317865, Reason: Terminated
Monitor duration	13.27s
Return Code	2
PID	4660
Parent PID	1580
Bitness	32 Bit

Process #71: cmd.exe

ID	71
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=F: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 308326, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	13.45s
Return Code	Unknown
PID	5060
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	4
File	5
Process	1

Process #73: vssadmin.exe

ID	73
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=G: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 309474, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	12.30s
Return Code	Unknown
PID	4788
Parent PID	4552
Bitness	32 Bit

Process #74: cmd.exe

ID	74
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=E: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 313486, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	8.29s
Return Code	Unknown
PID	4712
Parent PID	4476
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	4
File	5
Process	1

Process #76: vssadmin.exe

ID	76
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=F: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 314253, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	7.53s
Return Code	Unknown
PID	4800
Parent PID	5060
Bitness	32 Bit

Process #77: cmd.exe

ID	77
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=D: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 316262, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	5.52s
Return Code	Unknown
PID	3592
Parent PID	4476
Bitness	32 Bit

Process #79: vssadmin.exe

ID	79
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin Delete Shadows /For=E: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 318306, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	3.47s
Return Code	Unknown
PID	3844
Parent PID	4712
Bitness	32 Bit

Process #80: cmd.exe

ID	80
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=C: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 318782, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	3.00s
Return Code	Unknown
PID	4832
Parent PID	4476
Bitness	32 Bit

Process #82: cmd.exe

ID	82
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=B: /All /Quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 321778, Reason: Child Process
Unmonitor End Time	End Time: 321778, Reason: Terminated by timeout
Monitor duration	0.00s
Return Code	Unknown
PID	1528
Parent PID	4476
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
99de44e4486bde4e3023e4292f7ee9d6d8ef4a927ccc65692db9d5dc66971237	-	Memory Dump	36.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8	C:\Users\RDhJ0CNFevzX\Desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\ChromeFlashPlayer_c287f3826d6e218.exe	Dropped File	133.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
512f4c514e7d3bb5d5e4c2d6ea00bbdc1b3331e11046ecb440de034e4ccb6391	c:\programdata\microsoft\provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	6.39 KB	application/octet-stream	-	CLEAN
10d00784bbd076a64280147e2b127838e6993338799a56c0f0d48443e0d8c58f	C:\Program Files\HELP_DECRYPT_YOUR_FILES.TXT, C:\MSOCache\HELP_DECRYPT_YOUR_FILES.TXT, C:\Users\Public\Desktop\HELP_DECRYPT_YOUR_F... ...e-737f-47a1-a541-6e7b0761ed19}\help_decrypt_your_files.txt, c:\programdata\microsoft\diagnosis\siufloc\help_decrypt_your_files.txt	Dropped File	3.12 KB	application/octet-stream	Access, Create, Write	CLEAN
6d5f7677cb005a319da2a44f06c042cfde0a433d98cee3ecc3503c288889ec62	C:\ProgramData\HELP_DECRYPT_YOUR_FILES.HTML, C:\Users\Public\Desktop\HELP_DECRYPT_YOUR_FILES.HTML, C:\$Recycle.Bin\HELP_DECRYPT_YO... ...pt_your_files.html, c:\programdata\microsoft\provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\prov\help_decrypt_your_files.html	Dropped File	2.07 KB	text/html	Access, Create, Write	CLEAN
e100148f841dfc48c0e332bb4aecf798b7eb0f0c7a814d215a8bd676dc97454f	c:\programdata\microsoft\provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	560 bytes	application/octet-stream	-	CLEAN
0bb037cc38573903153c7477abb88be3f4ad0bb42de1ad978975d885bd3638e3	c:\programdata\microsoft\provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	208 bytes	application/octet-stream	-	CLEAN
bd5cd42d7f5823b6b479601b363af1aba24f5e8568f17cf1c49c6dcc62682075	c:\programdata\microsoft\provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	7.17 KB	application/octet-stream	-	CLEAN
8a69509b25bb0e171bfe8bf47e08b0b70b28f63bb26d6123285453366a783453	c:\programdata\microsoft\provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	2.19 KB	application/octet-stream	-	CLEAN
4d2f5cb1e86e821a28f0e6d6dbe3dbe3cfbd53e2f91bb166177bdd3af59fef8b	c:\programdata\microsoft\provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\masterdatastore.xml.id_c287f3826d6e218_email_enc2@dr.... ...amdata\microsoft\provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\masterdatastore.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	272 bytes	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1f862eaba10bc82b80c6de40df5030ae74bf5dc7e6d4c8e1d9a5e7900a4dca6f	c:\programdata\microsoft\provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	1.78 KB	application/octet-stream	-	CLEAN
fbe372ff46a316840852ffdd35c468e1b8539a29a0783560e77254aff5f6543d	c:\programdata\microsoft\clicktorun\deploymentconfig.1.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	1.94 KB	application/octet-stream	-	CLEAN
2ebeb822006c66f1847d9147742c9ce0dbe4ad53eeca500b2094b43eb02ee981	c:\programdata\microsoft\diagnosis\downloadedsettings\telemetry.asm-windowsdefault.json.bk.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	832 bytes	application/octet-stream	-	CLEAN
9f2a732a0668740f533c041a1a157226ad0d8e9213fc535bfc08e8d3ec023f2b	c:\programdata\microsoft\provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	592 bytes	application/octet-stream	-	CLEAN
d721d02e5bc5ac0f8a7267c079395b834b18ad55f92455d88e6fd2865644e56b	c:\programdata\microsoft\clicktorun\9566930b-d1dd-4075-bfe6-74dd69b13189\x-none.16\stream.x86.x-none.man.dat.id_c287f3826d6e218_em... ...soft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\x-none.16\stream.x86.x-none.man.dat.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	3629.45 KB	application/octet-stream	-	CLEAN
efd2518e06a11f557aaf9b1a4b0db00f364bca6ebada0489f7c435b790b7a9b6	c:\programdata\microsoft\provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	3.66 KB	application/octet-stream	-	CLEAN
80c3fe2ae1062abf56456f52518bd670f9ec3917b7f85e152b347ac6b6faf880	-	Downloaded File	196 bytes	text/html	-	CLEAN
fc564dcd00e0c8d164597caf6e91165ea77b4da4500d14f582a40db5fb0e2ea0	c:\programdata\microsoft\provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	1.23 KB	application/octet-stream	-	CLEAN
b359806c78be307c5c3010d81dfa01d795c5f425e966e66b7aab02b9d5cc4304	c:\programdata\microsoft\provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	880 bytes	application/octet-stream	-	CLEAN
ba58a5d95ec5cd5fad0b46ab103aa581f1c4472929e42b17eada0f58d9aa782e	c:\programdata\microsoft\provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	7.81 KB	application/octet-stream	-	CLEAN
b3a53a64d6fad6fd8f74da67e04e4a5dc7fd4cf8d326aafa2e68bf6e63dd7ddd	c:\programdata\microsoft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\en-us.16\masterdescriptor.en-us.xml.id_c287f3826d6e218_em... ...soft\clicktorun\9566930b-d1dd-4075-bfe6-74dd69b13189\en-us.16\masterdescriptor.en-us.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	21.86 KB	application/octet-stream	-	CLEAN
cec550e9898ff0a757197babaca9afaa8cfd03ed46f4759562675aaf899fdbbb	c:\programdata\microsoft\provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	352 bytes	application/octet-stream	-	CLEAN
24a324a50539b8f95b2ba05cbb3f17681eb30fc6e53c2971e0e5621bfae2e87a	c:\programdata\microsoft\clicktorun\deploymentconfig.0.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	1.94 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ea1445aebbe3d005a7991c37c8f443db959037ba3c080cae29516c793b90ceb0	c:\programdata\microsoft\provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com... ...ogramdata\microsoft\provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	320 bytes	application/octet-stream	-	CLEAN
e47c99f71f3f21b00fcb026bc6d3e7503f0e4b4007061e8d5a5270fd163bf2e6	c:\programdata\microsoft\provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	5.41 KB	application/octet-stream	-	CLEAN
78453f1de270f93081b1589ae76506e792d190e06c9280564d733031f72d8706	c:\programdata\microsoft\provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com... ...ogramdata\microsoft\provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	352 bytes	application/octet-stream	-	CLEAN
6486faeb5877ef10cc77f3b27fc6f7c4a0a5390b9f1eaa31a8a151a788532569	c:\programdata\microsoft\clicktorun\deploymentconfig.2.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	1.36 KB	application/octet-stream	-	CLEAN
ca16950451e098bd805e95cff63997cd5398a253df806b405adde6d7e747c82f	c:\programdata\microsoft\provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	560 bytes	application/octet-stream	-	CLEAN
ee2b6c0cee193353479a627a7ee7ee2c7fa871f852817aaa5ba922614fe459e0	c:\programdata\microsoft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\en-us.16\stream.x86.en-us.man.dat.id_c287f3826d6e218_emai... ...rosoft\clicktorun\9566930b-d1dd-4075-bfe6-74dd69b13189\en-us.16\stream.x86.en-us.man.dat.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	864.47 KB	application/octet-stream	-	CLEAN
b0ffae8185617b120c7a1f16a63458ef34234991fe19388f8e239b470397bc7e	c:\programdata\microsoft\provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	2.17 KB	application/octet-stream	-	CLEAN
aeb5b9a120887d59eb4492cd2051d5743aca43ef3132e906c15215b442422783	c:\programdata\microsoft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\x-none.16\masterdescriptor.x-none.xml.id_c287f3826d6e218_... ...ft\clicktorun\9566930b-d1dd-4075-bfe6-74dd69b13189\x-none.16\masterdescriptor.x-none.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	20.55 KB	application/octet-stream	-	CLEAN
7c5ab5a5e01b02eadec267a0a062925699800 27e060d9f0e1073950434213712	c:\programdata\microsoft\diagnosis\downloadedsettings\utc.app.json.bk.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	1.41 KB	application/octet-stream	-	CLEAN
15561652a46531fda22a4318934dae007459aed43d4664b6c9c5a5f890099a24	c:\programdata\microsoft\provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	3.28 KB	application/octet-stream	-	CLEAN
64667670cdb26c6687fd59934fa78d33968a4d571b2912af0432deb3c5e7312d	c:\programdata\microsoft\provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\prov\runtime.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	448 bytes	application/octet-stream	-	CLEAN
57f75d5ffbf00b8b998d91791431e51e889c8ebcd85a2caaa92976818d1b9fc6	c:\programdata\microsoft\provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\customizations.xml.id_c287f3826d6e218_email_enc2@dr.com_.scl	Dropped File	1.61 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\music\381iz9biyf\hxbbqmjvgue\0tl74kvj.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\zzm5x5jxuesk93xmmp.rtf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\y_fz9pz08c.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\kctv nkg6\wu9rmpx3t2rmzf3qvbg\vuzp5x8.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\bha7xl9pvfipksxlxcfg.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\pfrh0 ehmta6.jpg.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\bxtp1ubjz_.jpg.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\zu8x 1dsmp0p\exmpmpcf6ejoq9scdj.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\izigkemouwxcnezndl\c1fpy4-8p1n\uya w3gj.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\wcvbxknnmpvb-skuig.xls.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\pz4qofg\v0ot\b58le_nsymjbdwicv.mp4.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\izigkemouwxcnezndl\sarxnz6avb1lkhe2u.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\f_d-.bmp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\zuujv6og4lf3pg.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\ziwxnlovm1.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\xz06.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\beyl_s9ay -d\uxzz\fbjw5d4nfat2adqdtg.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\izigkemouwxcnezndl\c1fpy4-8p1n\uf ibx-mj-z3dshsxti.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\ChromeFlashPlayer_c287f3826d6e218.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\0jwpqvra-.xlsx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\0fgwkow4jv4zzl-25zz9.odt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\lny0-uli.jpg.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\hp_ehy49u8gtio_zgw.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\ljd6k_jcpnmqhcg6tihm.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\jntt-vv vfzhdmuv\he_m_wdbcnl.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\dzwk6xa.odt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\a4j36w_yzqhx9oiq.odp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\pyf2.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\3h3uvqnynsqrnc.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\tcbfftgd3-w7dzc.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\xo5lwhfexk\xs8rf2qg_ha6ykea1jet.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\hg1hf_lrt.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\kipouqk1rgay1fz.ppt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\7n6b8ii7i7.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\ifm43t.jpg.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\wc7c7gil2.pptx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\ayy4qge5axllktej45b.ods.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\r0lxgahtxvk ut.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\hxbbqmjvgue\v8f8_.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\cgfboykuyf.pdf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\vyvcuxi7nluwawqyke.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\0ahak j1pizvk7bc.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\h8lzk9u.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\hzoe.rtf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\deo9rsf3b2dx88.xls.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\izigkemouwxcnezнll\idc41.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\beyl_s9ay -d\22_uir_zgnsods5-vj.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\3sc2nse6i.ods.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\z0iork9q93ymj.csv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\a-_m2\fvwv8r1sa5k.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\wqwc5lrtjgp.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\kctv nkg6\wu9rmpx3t2rmzf3qvbg\7upxtvszgekuh-t.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\ck0z.m4a.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\htfjvrtf5zhv-gvv.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\3v9wxvgs.ppt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\kctv nkg6\cr_kbnc3kb_vylq.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\gbhwyejwrouo.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\gruycjv3nf.ods.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\ytsehq8ia1pz-.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\kphevwvu--mnrrobfp5d.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\izigkemouwxcnezнll\c1fpy4-8p1n\uwzxj0yl2nk.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\1it-vw cosug.mkv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\dokctgdprst.jpg.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\vy9x-mc7wsgckhxyx.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\d-efjesby.pptx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\xvbk0emv3rdkqgynq3.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\beyl_s9ay -d\uxzz_uplqiqusdinydia4xz-.mp4.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\r5m3rr4fp_k2fkf4.jpg.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\pictures\7aqvlowxb6rold9vria4.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\-_zt.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\x8zc5.xls.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\-9z1.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\la62fm2gbg9o.xlsx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\k6x1lbrqivx-.jpg.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\yxgmv9tma2.ppt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\gnasynz.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\cbjpukd2xjgfv_y57goc.pptx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\f1zd8ug2krjm.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\9wryc98w.rtf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\s9p-qsrx.pdf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\xo5lwhfexk\9lc2m1bibxn3uehcgc.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\zn3qsas7zk7m3a.bmp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\nsj6mwta.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\pqfubbksgc8n6wqpml.pptx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\3hnghp4u.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\ymafvurvguz8pq7s.ots.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\fvlv d.odt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\we1ovw4nq.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\ptvggb4.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\pulmow9bvn4haf5vv1.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\hxbbqmjvgue\kexa.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\izigkemouwxcneznll\c1fpy4-8p1n\hfo3g0iul3kxjhrxd0-o.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\ao66kkoo-.ods.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\v-rzbut.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\kctv nkg6\wu9rmpx3t2rmzf3qvbg\cbrqjym\cl1o0yrsa.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\wictqbu5lb69gnf.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\kctv nkg6\wu9rmpx3t2rmzf3qvbg\60jdjqn9l5w2ukepxx.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\swx3yplraf4uemxfmvji.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\oqppyb09odsqs8rb6b.pptx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\xo5lwhfexk\amgg0wai-5.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\pacjpuc.ods.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\ku2urug.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\hxbbqmjvgue\tkww00x4od.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\hxbbqmjvgue\x0brndlbb4dbqtczopao.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\k0sx.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\nakuksj-6.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\hxbbqmjvgue\2fzsan9cbqsfz_9.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\pwnrgyqqhld5-c.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	Accessed File, Sample File	Access	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\k959wnyk.bmp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\h-7uuny_qd0.bmp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\evfxh0jnzn86.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\jtooxm buypxvtbqv.bmp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\vc5it4mey5fnqy5bf5s.xls.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\beyl_s9ay - duxzz\ngcmroclewn1vtz.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\desktop\xo5lwhfexk\kt2grvxjb8knckn865l.mkv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\5ynswxxlgy9gvmdmwup.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\zu8x1dsmp0p\fwbkn_rdsivw.doc.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\pz4qofgv0ot\ljfqsspz60hkke5.mp4.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\a-_m2\7v2v.mp4.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\qlk2er5ibu4cw97.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\izigkemouwxcneznll\qcnfjxg4t34hehxggp.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\jntt-vvvfzhdmuv\651ijdw0jxrz3jh.flv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\quwg7c_8dv6tfar.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\5kqhpe_jl-ui\hg5hwqecsvicbr7x.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\5vrihtsjyx.mkv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\beyl_s9ay - d\uxzz\zx28zquixc5h.odp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\a-_m2\1nnjaiktbaoed3bu.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\z2radgjxb42cwjf.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\beyl_s9ay - d\z02m6kpvhtj.rtf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\6ho5dpxnqp.ppt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\4 weffayw8qt-mrv\qffscmksuu.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop_1ieasqacw4jkwjo9.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\pua1eq-hg-njginjnl.odp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\ibsr-q.wav.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\381iz9biyf\um41juevttvcc2z.mp3.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\pz4qofg\ffcpakhrpmqfmcr.mkv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\mj7pog-sftgg.ots.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\pictures\gfn5uwhvoca7ihha.gif.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\vnt7g2bfzefn4rcpt3r.odp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\ijljdu.pptx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\zu8x 1dsmp0p\ij43i7a8s3av.png.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\xo5lwhfexk\-srnrgsbo-cmjxi.mp4.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\6umj9sfomg6z58wfzt\3zsyulzns be\kctv nkg6\wu9rmpx3t2rmzf3qvbg\9upc.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\yf-jfd9lccg7helac.xlsx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\preumk814_qyh888fxol.bmp.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\hnibzne3e.docx.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\9irupr75kfhemeucfkfj\pz4qofg\v0ot\fjpb77qh_86nw7s-hy.swf.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\d-w1g.csv.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xmrbek9xvyp4rzta6st\zrxhjzssjtmtcblglvy\qcuqe.ppt.id_c287f3826d6e218_email_enc2@dr.com_.scl	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://5[.]39[.]86[.]86/default.jpg	Contacted, Extracted	5.39.86.86	France	GET	MALICIOUS
hxxp://en[.]wikipedia[.]org/wiki/RSA_(cryptosystem)	Extracted	-	-	-	CLEAN
hxxps://translate[.]google[.]com	Extracted	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
en[.]wikipedia[.]org	-	-	-	CLEAN
translate[.]google[.]com	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
5.39.86.86	-	France	HTTP, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
ChromeReaderHardWress2_c287f3826d6e218	access	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN

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_CURRENT_USER\SoftWare\ChromeFirstVersionHardWare32	access, write, read	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\Run\Chrome Reader UpdateHardWare	access, write	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	access, read	wmic.exe	CLEAN
HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\Run	access	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\RunOnce*ChromeFlashPlayers32	access, write	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM	access, create	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\RunOnce	access	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\Run\ChromeFlashPlayersHardWare	access, write	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\EnableObjectValidation	access, read	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	access, read	wmic.exe	CLEAN
HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\RunOnce*Chrome Reader Update32	access, write	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_CURRENT_USER\SoftWare	access	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_CURRENT_USER\SoftWare\ChromeLicensionHWare	access, write, read, delete	3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	CLEAN

Process

Process Name	Commandline	Verdict
3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe	"C:\Users\RDhJ0CNFevzX\Desktop\3729c1d683690f752732ec18372a555abfb0d20c02ea3f9fe60ca6577722c9a8.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin.exe Delete Shadows /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C wmic shadowcopy delete	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=Z: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=Y: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=X: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=W: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=V: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=U: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=T: /All /Quiet	SUSPICIOUS
wmic.exe	wmic shadowcopy delete	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=S: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=R: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=Q: /All /Quiet	SUSPICIOUS

Process Name	Commandline	Verdict
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=P: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=O: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=N: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=M: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=L: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=K: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=J: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=I: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=H: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=G: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=F: /All /Quiet	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=E: /All /Quiet	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
vssadmin.exe	vssadmin.exe Delete Shadows /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=Z: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=Y: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=X: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=W: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=V: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=U: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=T: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=S: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=R: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=Q: /All /Quiet	CLEAN
wmiprvse.exe	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=P: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=O: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=N: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=M: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=L: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=K: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=J: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=I: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=H: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=G: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=F: /All /Quiet	CLEAN

Process Name	Commandline	Verdict
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=D: /All /Quiet	CLEAN
vssadmin.exe	vssadmin Delete Shadows /For=E: /All /Quiet	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=C: /All /Quiet	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin Delete Shadows /For=B: /All /Quiet	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
APTs	APT28_IMPLANT_4_v5	BlackEnergy / Voodoo Bear Implant by APT28	Memory Dump	-	-	5/5
APTs	APT28_IMPLANT_4_v5	BlackEnergy / Voodoo Bear Implant by APT28	Memory Dump	-	-	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	2023.2.0
Dynamic Engine Version	2023.2.0 / 04/13/2023 04:20
Static Engine Version	2023.2.0.0 / 2023-04-13 03:00:20
AV Exceptions Version	2023.2.1.4 / 2023-04-17 18:38:13
Link Detonation Heuristics Version	2023.2.1.4 / 2023-04-17 18:38:13
Smart Memory Dumping Rules Version	2023.2.1.4 / 2023-04-17 18:38:13
Config Extractors Version	2023.2.1.6 / 2023-04-19 09:57:08
Signature Trust Store Version	2023.2.1.4 / 2023-04-17 18:38:13
VMRay Threat Identifiers Version	2023.2.1.6 / 2023-04-19 09:57:08
YARA Built-in Ruleset Version	2023.2.1.6

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