MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe**
ID	#4693683
MD5	421ed51ff27bb5c8dc7696d0c1479298
SHA1	e865419cdd49791ab1c9e612e5840875dae37b5c
SHA256	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40
File Size	539.50 KB
Report Created	2022-06-21 14:14 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (4 rules, 4 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe renames multiple user files.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Network Connection	Sets up server that accepts incoming connections	1	-
	• (Process #1) cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe starts a TCP server listening on localhost port 49736.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe creates mutex with name "Global\.net clr networking".			

Mitre ATT&CK Matrix

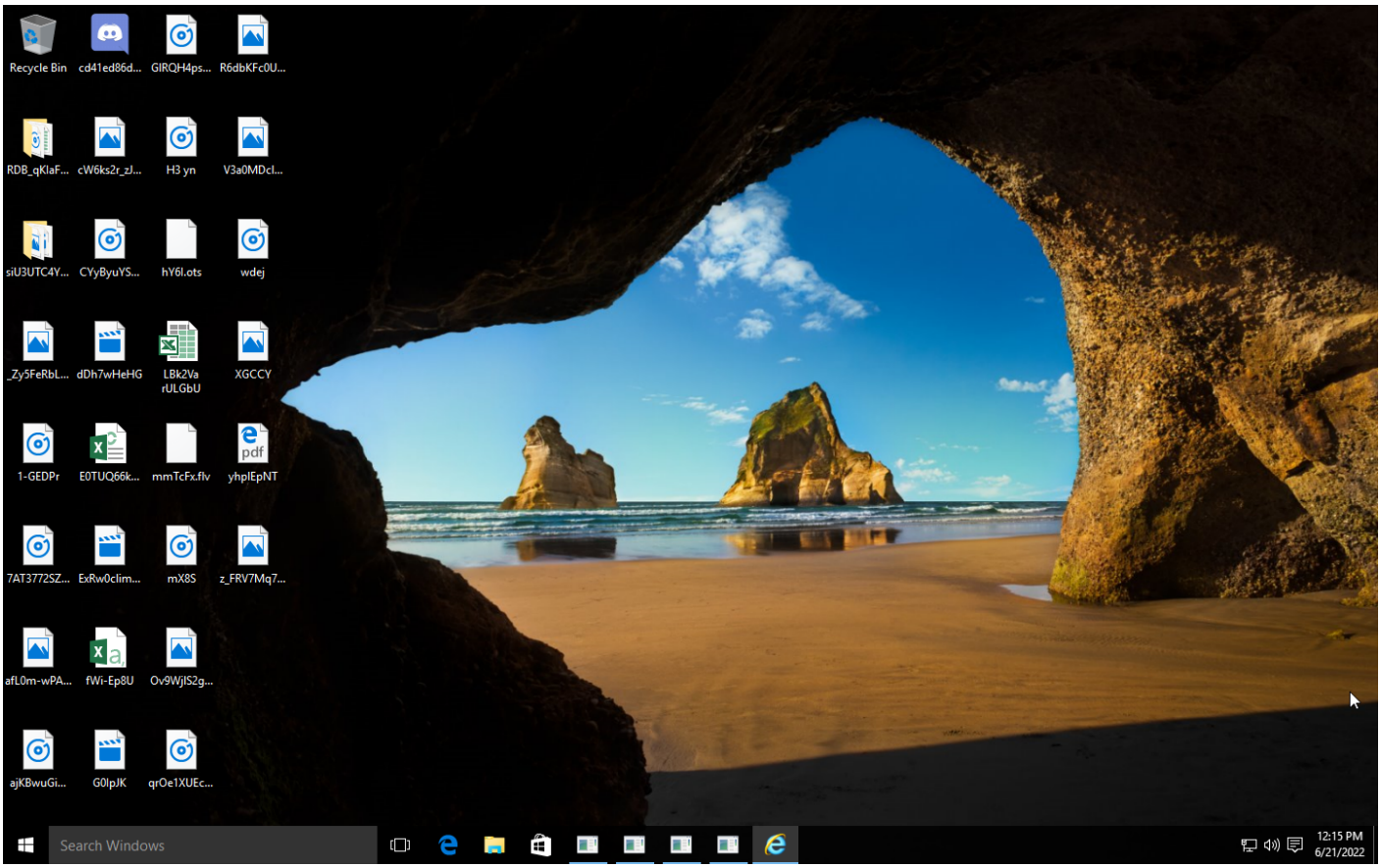
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
					#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
								#T1005 Data from Local System			

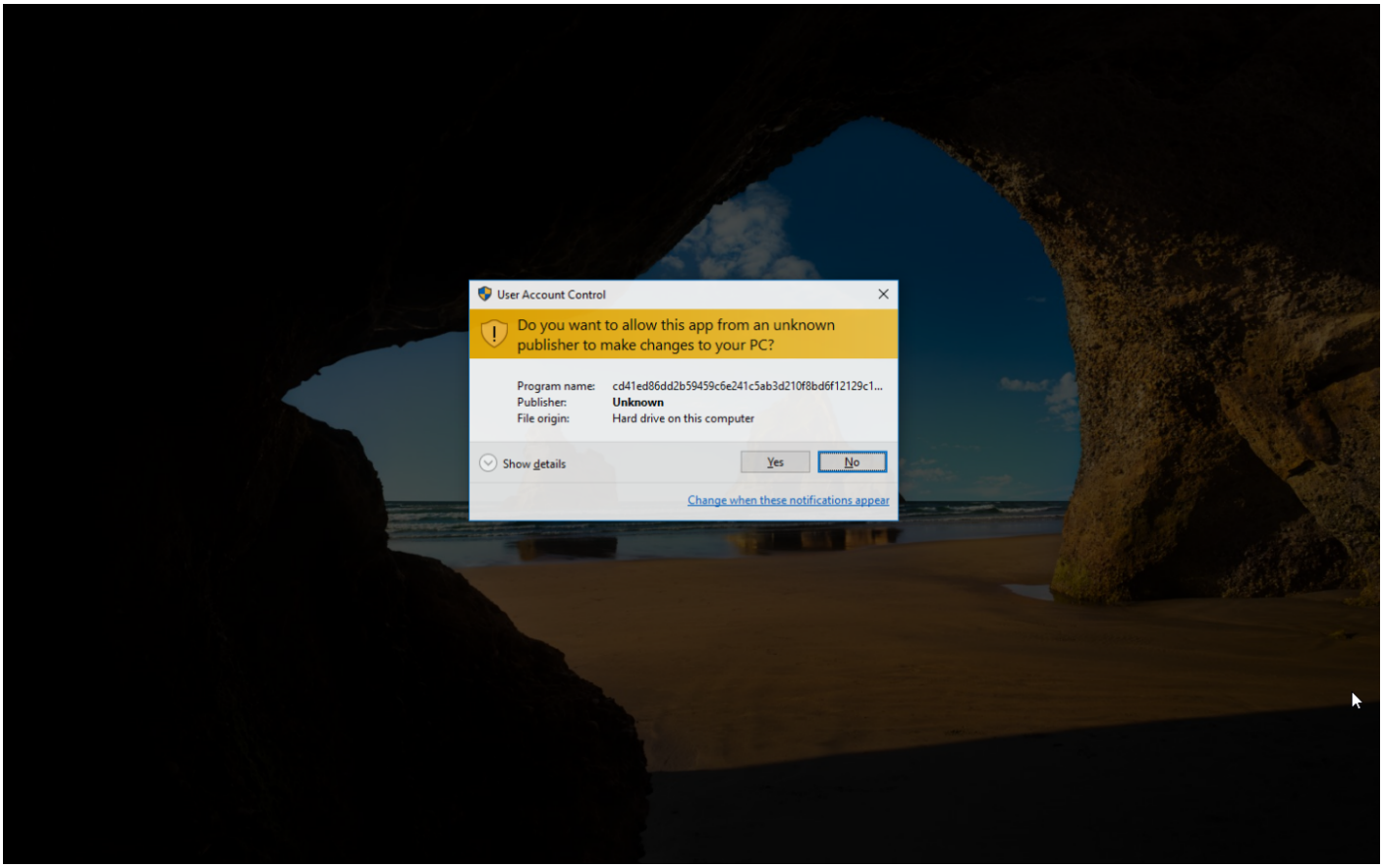
Sample Information

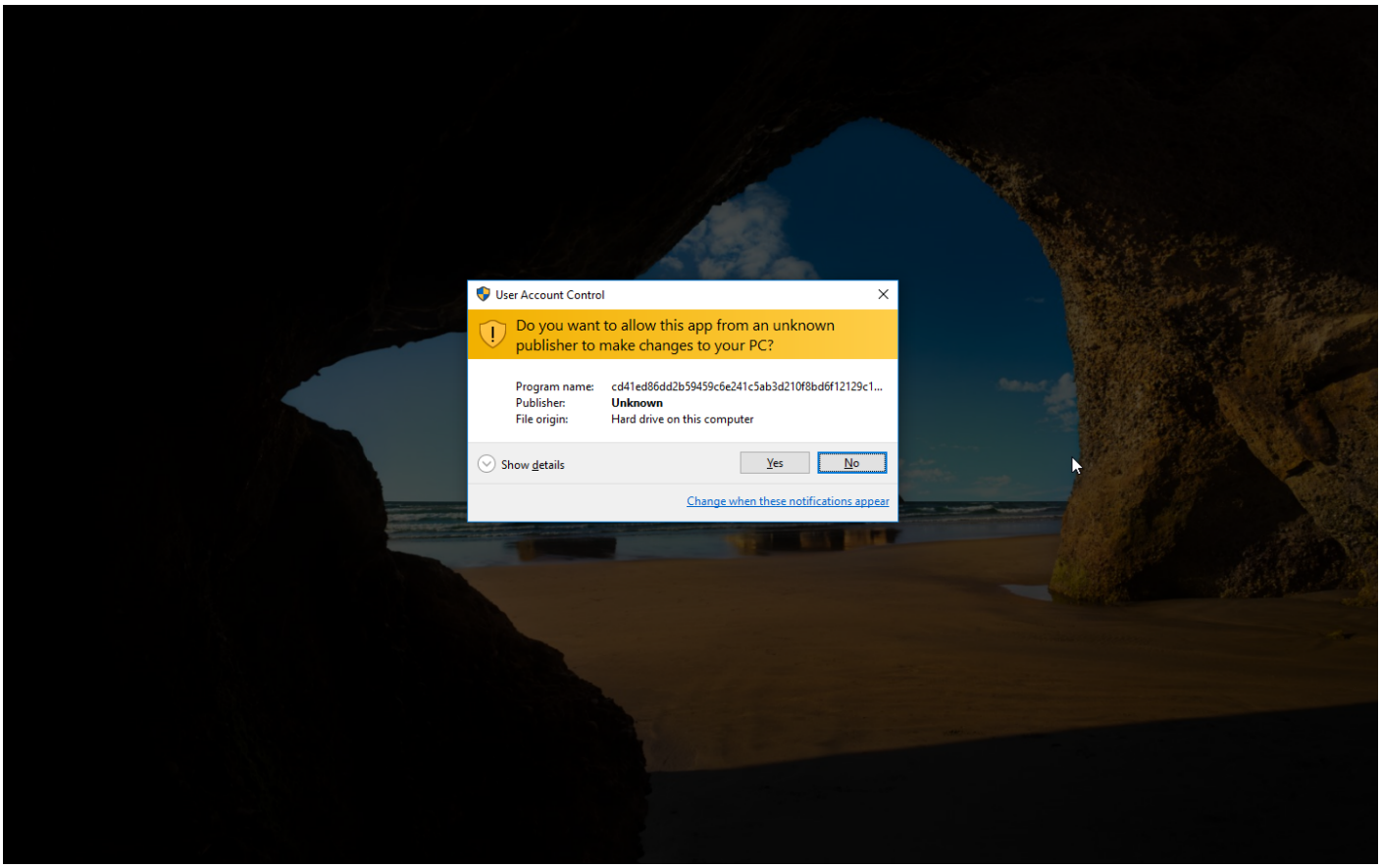
ID	#4693683
MD5	421ed51ff27bb5c8dc7696d0c1479298
SHA1	e865419cdd49791ab1c9e612e5840875dae37b5c
SHA256	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40
SSDeep	3072:D0nRIr9sCkIlr9sCkpEj6lwnXzMMCDtDJniCG:Da99sCkl99sCkGj6lUmtDJni
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe
File Size	539.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-06-21 14:14 (UTC+2)
Analysis Duration	00:03:56
Termination Reason	Timeout
Number of Monitored Processes	1
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
cd41ed86d...
GlRQH4ps...
R6dbKFc0U...
RDB_qKlaF...
cW6ks2r_zJ...
H3 yn
V3a0MDcI...
siU3UTC4Y...
CYyByuYS...
hY6l.ots
wdej
_Zy5FeRbL...
dDh7wHeHG
LBk2Va rULGbU
XGCCY
1-GEDPr
E0TUQ66k...
mmTcFx.flv
yhplEpNT
7AT3772SZ...
ExRw0clim...
mX8S
z_FRV7Mq7...
afL0m-wPA...
fWi-Ep8U
Ov9WjlS2g...
ajKBwuGi...
G0lpJK
qrOe1XUEc...
Search Windows
12:15 PM
6/21/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1...
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

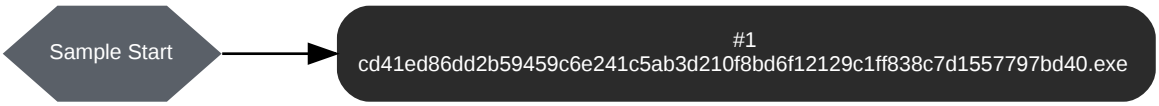
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 85942, Reason: Analysis Target
Unmonitor End Time	End Time: 243499, Reason: Terminated by timeout
Monitor duration	157.56s
Return Code	Unknown
PID	1904
Parent PID	2076
Bitness	64 Bit

Dropped Files (7)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop_Zy5FeRbLQDxmapn0.png_encrypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDhJ0CNFevzX\Desktop\siU3UTC4Y37SCtPmMaq\oju4fqXzHXxAhQ.png_encrypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDhJ0CNFevzX\Desktop\V3a0MDclW2jjyqOGjLJ.jpg_encrypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDhJ0CNFevzX\Desktop\siU3UTC4Y37SCtPmMaq\1CuHEPj43yz.jpg_encrypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDhJ0CNFevzX\Desktop\yhplEpNT.pdf_encrypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDhJ0CNFevzX\Desktop\XGCCY.jpg_encrypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDhJ0CNFevzX\Desktop\cW6ks2r_zJ4J9Z8xyYc.jpg_encrypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	6442
-	115
Module	31
Mutex	23
File	64
Registry	20
Window	18
-	3
Keyboard	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40	C:\Users\RDhJ0CNFevzX\Desktop\cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	Sample File	539.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
f67fc5c8e04c1ad5be0041f16e320e704988d685ebaeff7de2e89af129174c09	-	Extracted File	18.89 KB	image/png	-	CLEAN
760341bf512dc05a438eba3e2ff68e3c06cbc4a85c87b08027ce517f3efea96f	-	Extracted File	8.90 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	Sample File, VM File	-	MALICIOUS
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop_Zy5FeRbLQDxmapn0.png_encrypted	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\siU3UTC4Y37SCtPmMaq\oju4fqXzHXxAhQ.png_encrypted	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\V3a0MDclW2jjyqOGjLJ.jpg_encrypted	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\siU3UTC4Y37SCtPmMaq\1CuHEPj43yz.jpg_encrypted	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\yhplEpNT.pdf_encrypted	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\XGCCY.jpg_encrypted	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\cW6ks2r_zJ4J9Z8xyYc.jpg_encrypted	Dropped File, Accessed File, Not Extracted	Access, Create, Write	CLEAN
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Config\machine.config	Accessed File	Access, Read	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\.net clr networking	access, delete	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\First Counter	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\Library	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance	access	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\CategoryOptions	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\FileMappingSize	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\IsMultiInstance	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance	access	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\Counter Names	access, read	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	CLEAN

Process

Process Name	Commandline	Verdict
cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe	"C:\Users\RDhJ0CNFevzX\Desktop\cd41ed86dd2b59459c6e241c5ab3d210f8bd6f12129c1ff838c7d1557797bd40.exe"	SUSPICIOUS

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	4.5.1
Dynamic Engine Version	4.5.1 / 05/09/2022 04:24
Static Engine Version	4.5.1.0 / 2022-05-09 03:00:28
AV Exceptions Version	4.5.1.25 / 2022-04-28 14:12:58
Link Detonation Heuristics Version	4.5.1.36 / 2022-06-03 13:04:14
Smart Memory Dumping Rules Version	4.5.1.38 / 2022-06-13 09:02:33
Config Extractors Version	4.5.1.38 / 2022-06-13 09:02:33
Signature Trust Store Version	4.5.1.30 / 2022-05-16 06:57:54
VMRay Threat Identifiers Version	4.5.1.41 / 2022-06-16 13:30:53
YARA Built-in Ruleset Version	4.5.1.38

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