MALICIOUS

Classifications: Spyware

Threat Names: Trojan.GenericKDZ.76753 | Gen:Variant.Mikey.113998

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll**
ID	#2782706
MD5	8a6f4fe59b41d74501e04f1b451dc57d
SHA1	064f5eca3efd02c5f40a8c9e7fedb86aa40eeed0
SHA256	d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca
File Size	2072.00 KB
Report Created	2021-09-28 13:01 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 74 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) udmcozw.exe alters context of (process #7) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) udmcozw.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #3) udmcozw.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #7) explorer.exe as "Trojan.GenericKDZ.76753".			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #7) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #7) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #7) explorer.exe has a thread which sleeps more than 5 minutes.			
1/5	Discovery	Reads system data	8	-
	• (Process #2) udmcozw.exe reads the Windows installation date from registry. • (Process #3) udmcozw.exe reads the Windows installation date from registry. • (Process #4) udmcozw.exe reads the Windows installation date from registry. • (Process #5) udmcozw.exe reads the Windows installation date from registry. • (Process #8) udmcozw.exe reads the Windows installation date from registry. • (Process #6) udmcozw.exe reads the Windows installation date from registry. • (Process #7) explorer.exe reads the Windows installation date from registry. • (Process #9) udmcozw.exe reads the Windows installation date from registry.			
1/5	Mutex	Creates mutex	52	-

- (Process #2) udmcozw.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) udmcozw.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #3) udmcozw.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #4) udmcozw.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) udmcozw.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #8) udmcozw.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) udmcozw.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) explorer.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) explorer.exe creates mutex with name "{298ddcca-efe5-2f07-cbb5-e91e37797537}".
- (Process #7) explorer.exe creates mutex with name "{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}".
- (Process #7) explorer.exe creates mutex with name "{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}".
- (Process #7) explorer.exe creates mutex with name "{e8353f60-b296-77d3-712c-682bf3e23f29}".
- (Process #7) explorer.exe creates mutex with name "{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}".
- (Process #7) explorer.exe creates mutex with name "{3efe96e0-aada-6cdc-4854-db5a860aa498}".
- (Process #7) explorer.exe creates mutex with name "{c8f5437c-d6d6-873d-d7d0-da7099dbb1bb}".
- (Process #7) explorer.exe creates mutex with name "{42d854e1-ae99-711c-8f30-1d7624da1673}".
- (Process #7) explorer.exe creates mutex with name "{394a7c3c-ac56-58ce-d288-876ad1f16f45}".
- (Process #7) explorer.exe creates mutex with name "{d4c35d44-6df3-0b96-1ad6-bbc6db4242ff}".
- (Process #7) explorer.exe creates mutex with name "{0543b54c-df93-6503-0f5f-03111d930d96}".
- (Process #7) explorer.exe creates mutex with name "{e81f285f-e2d5-843a-2b19-3e6bebf2c463}".
- (Process #7) explorer.exe creates mutex with name "{c1d71539-741e-8f57-5d51-d78e6b8472d8}".
- (Process #7) explorer.exe creates mutex with name "{742c4235-61f7-6f13-cec8-924c395053dd}".
- (Process #7) explorer.exe creates mutex with name "{f2947db2-76ce-20cf-3821-b4e020fbf40d}".
- (Process #7) explorer.exe creates mutex with name "{0b7ba948-3cca-a9ee-ef68-bca12f0e84a2}".
- (Process #7) explorer.exe creates mutex with name "{c76c4830-ba11-65d9-c31d-e7234b159b82}".
- (Process #7) explorer.exe creates mutex with name "{2ef5cc94-f8a9-2574-5587-7f2a664a4914}".
- (Process #7) explorer.exe creates mutex with name "{09a6eaab-3fa0-0d71-1e5e-c654ef187a0c}".
- (Process #7) explorer.exe creates mutex with name "{d16d5bd5-a9e5-3451-c896-a81deb35e494}".
- (Process #7) explorer.exe creates mutex with name "{3f962b47-4d0a-da84-a641-0744d03cca5e}".
- (Process #7) explorer.exe creates mutex with name "{ac63b745-c10a-8d33-f2f4-c781a6076c4f}".
- (Process #7) explorer.exe creates mutex with name "{06552932-7500-4aaa-456b-93247ed0790e}".
- (Process #7) explorer.exe creates mutex with name "{734ab243-3ba9-e014-2983-224ca430987b}".
- (Process #7) explorer.exe creates mutex with name "{028360ad-a0ce-7a1e-5afd-31cd9bd4d5ea}".
- (Process #7) explorer.exe creates mutex with name "{9b8e3f9b-6a14-ba61-86de-29155d8b4094}".
- (Process #8) udmcozw.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #7) explorer.exe creates mutex with name "{b4c5217e-775a-862d-a0bd-c504e5eaa60a}".
- (Process #7) explorer.exe creates mutex with name "{b33e3c4f-1610-a0b6-186d-a25ba5862812}".
- (Process #7) explorer.exe creates mutex with name "{a3dce688-6117-3ea3-fbbd-1defec717462}".
- (Process #7) explorer.exe creates mutex with name "{ec2954cb-8ed4-cf4d-bef4-2d7135075084}".
- (Process #7) explorer.exe creates mutex with name "{168ee11b-299f-6d76-b48f-88a65a4a58ba}".
- (Process #7) explorer.exe creates mutex with name "{b4de3d46-efec-a98a-f706-8745d35ed7f2}".
- (Process #7) explorer.exe creates mutex with name "{d1575404-3469-2df0-db6b-3bcf4439344f}".
- (Process #7) explorer.exe creates mutex with name "{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}".
- (Process #7) explorer.exe creates mutex with name "{3c33918e-27da-9f35-2586-b9f012933134}".
- (Process #7) explorer.exe creates mutex with name "{6c570128-9202-fd64-daa4-72143d141e8a}".
- (Process #7) explorer.exe creates mutex with name "{d89ce0d8-125f-38cf-59d4-410119d64fdf}".
- (Process #7) explorer.exe creates mutex with name "{c42c174a-1be2-3a72-8667-a20ecc356e75}".
- (Process #7) explorer.exe creates mutex with name "{a05f0669-d546-7c4b-c5ff-6ad44aa5f2b6}".
- (Process #7) explorer.exe creates mutex with name "{95c38542-2405-0d06-534c-428190efb4c6}".
- (Process #7) explorer.exe creates mutex with name "{e28905fd-15de-b796-44d3-7a7876237780}".
- (Process #7) explorer.exe creates mutex with name "{0e00dc0d-6bc0-49b5-4c04-4c9791ff2470}".
- (Process #7) explorer.exe creates mutex with name "{f5908ce7-c5cc-734d-f2cc-bd80fc3637ac}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #2) udmcozw.exe reads from (process #7) explorer.exe. • (Process #8) udmcozw.exe reads from (process #7) explorer.exe.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #7) explorer.exe starts (process #12) wbengine.exe with a hidden window.			
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
	• (Process #7) explorer.exe hides 3526 bytes in "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder\{37533FA7-C036-3C83-FF44-88C4B0C49DDD}".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #7) explorer.exe resolves 26 API functions by name.			

Mitre ATT&CK Matrix

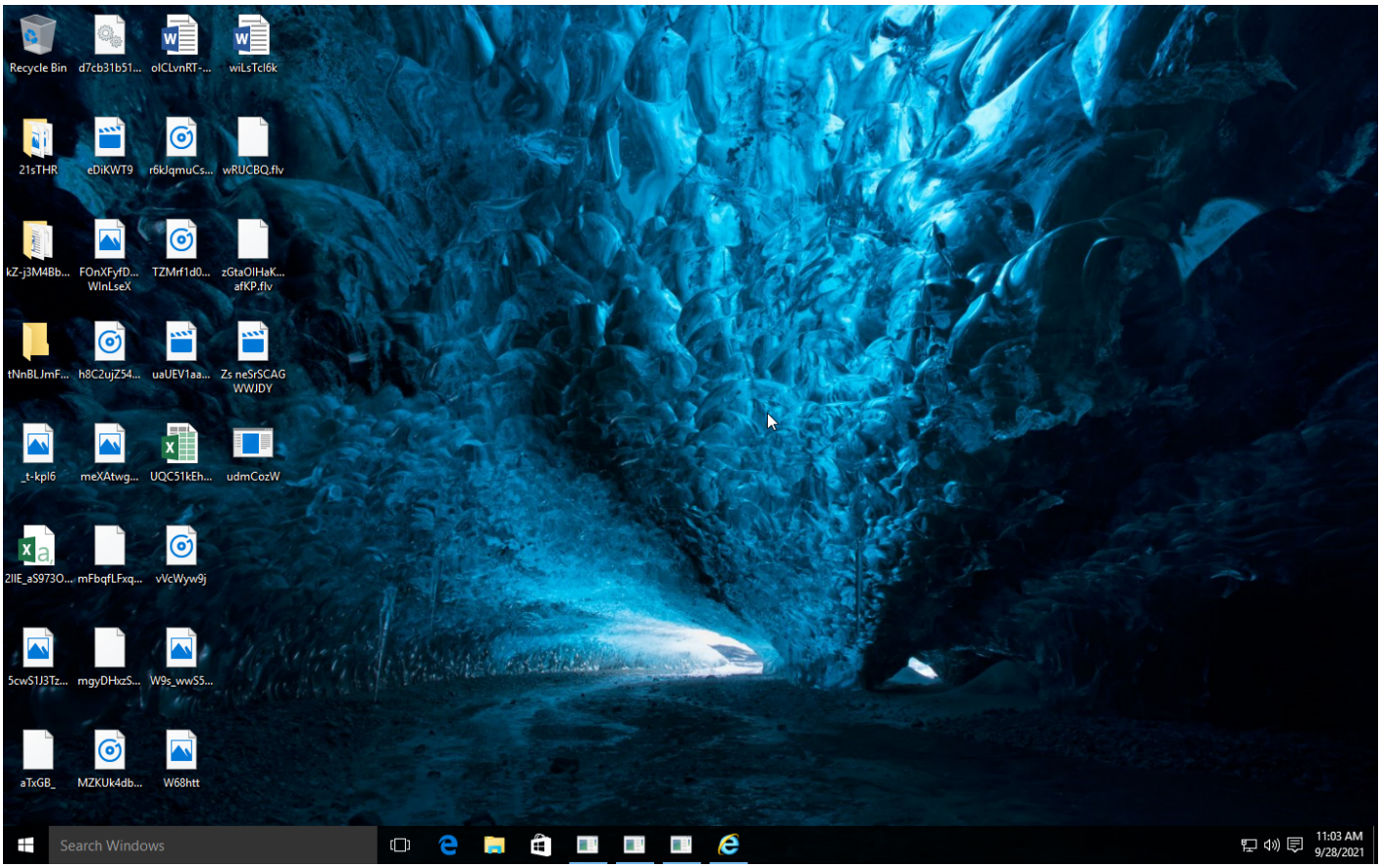
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1112 Modify Registry		#T1012 Query Registry		#T1005 Data from Local System			
				#T1045 Software Packing		#T1083 File and Directory Discovery					

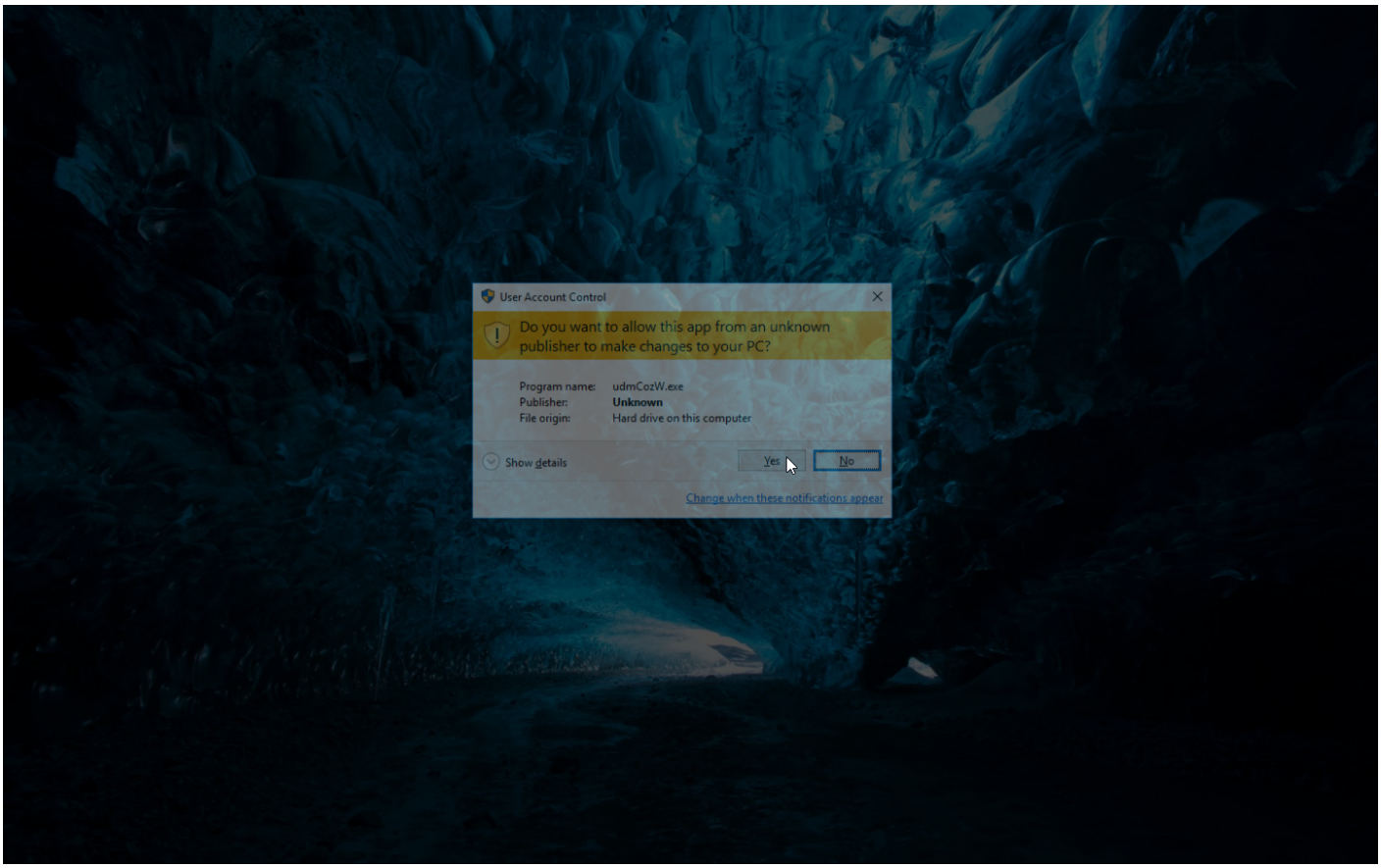
Sample Information

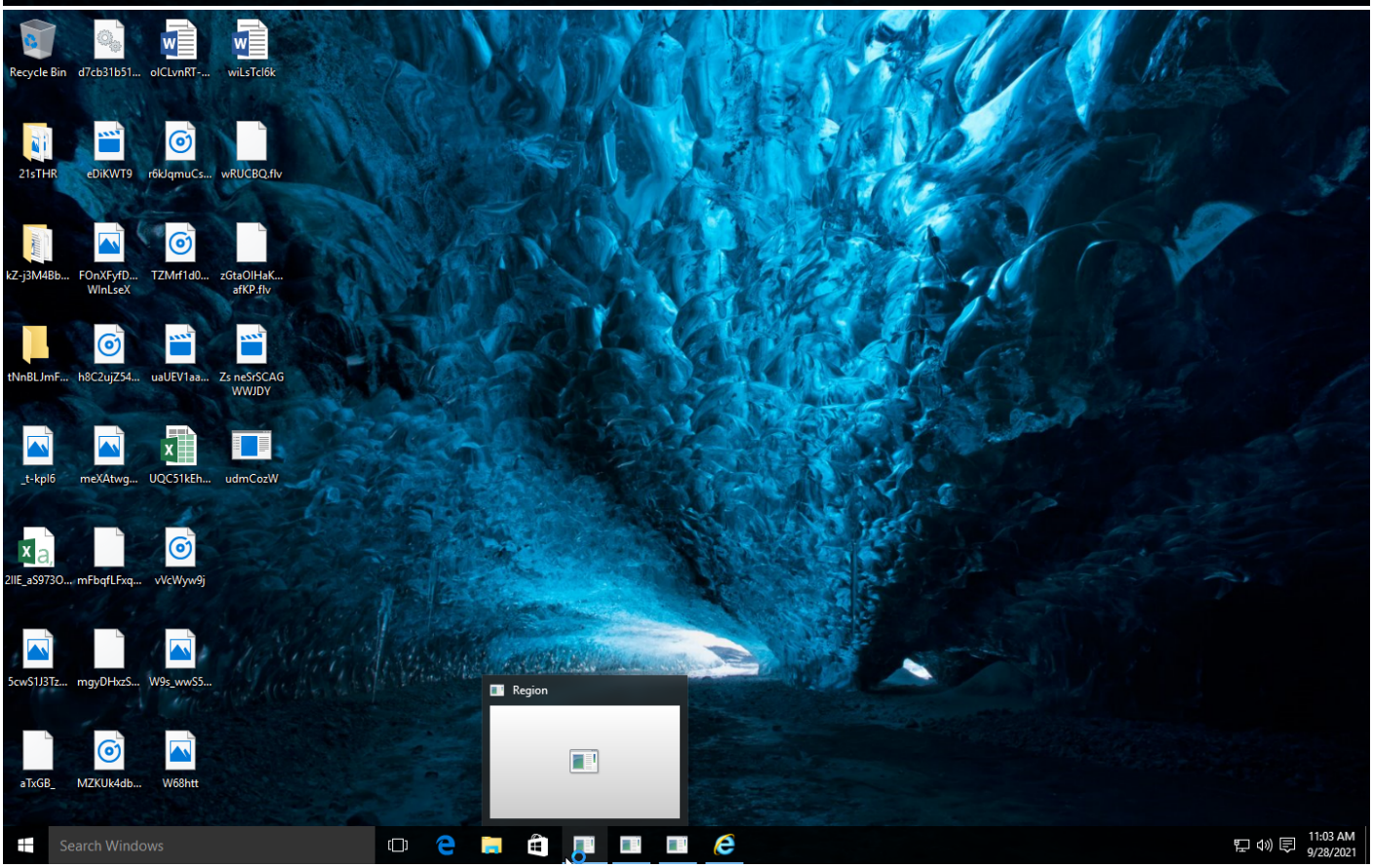
ID	#2782706
MD5	8a6f4fe59b41d74501e04f1b451dc57d
SHA1	064f5eca3efd02c5f40a8c9e7fedb86aa40eeed0
SHA256	d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca
SSDeep	12288:1Vl0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:sfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll
File Size	2072.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 13:01 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	14
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	5
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
d7cb31b51...
olCLvnRT-...
wiLsTcl6k
21sTHR
eDiKWT9
r6kJqmuCs...
wRUCBQ.flv
kZ-j3M4Bb...
FOnXFyfD...
WlnLseX
TZMrf1d0...
zGtaOlHaK...
afKP.flv
tNnBLJmF...
h8C2ujZ54...
uaUEV1aa...
Zs neSrSCAG
WWJDY
_t-kpl6
meXAtwg...
UQC51kEh...
udmCozW
2lIE_aS973O...
mFbqfLFxq...
vVcWyw9j
5cwS1J3Tz...
mgyDHxzS...
W9s_wwS5...
aTxGB_
MZKUk4db...
W68htt
Search Windows
11:03 AM
9/28/2021





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

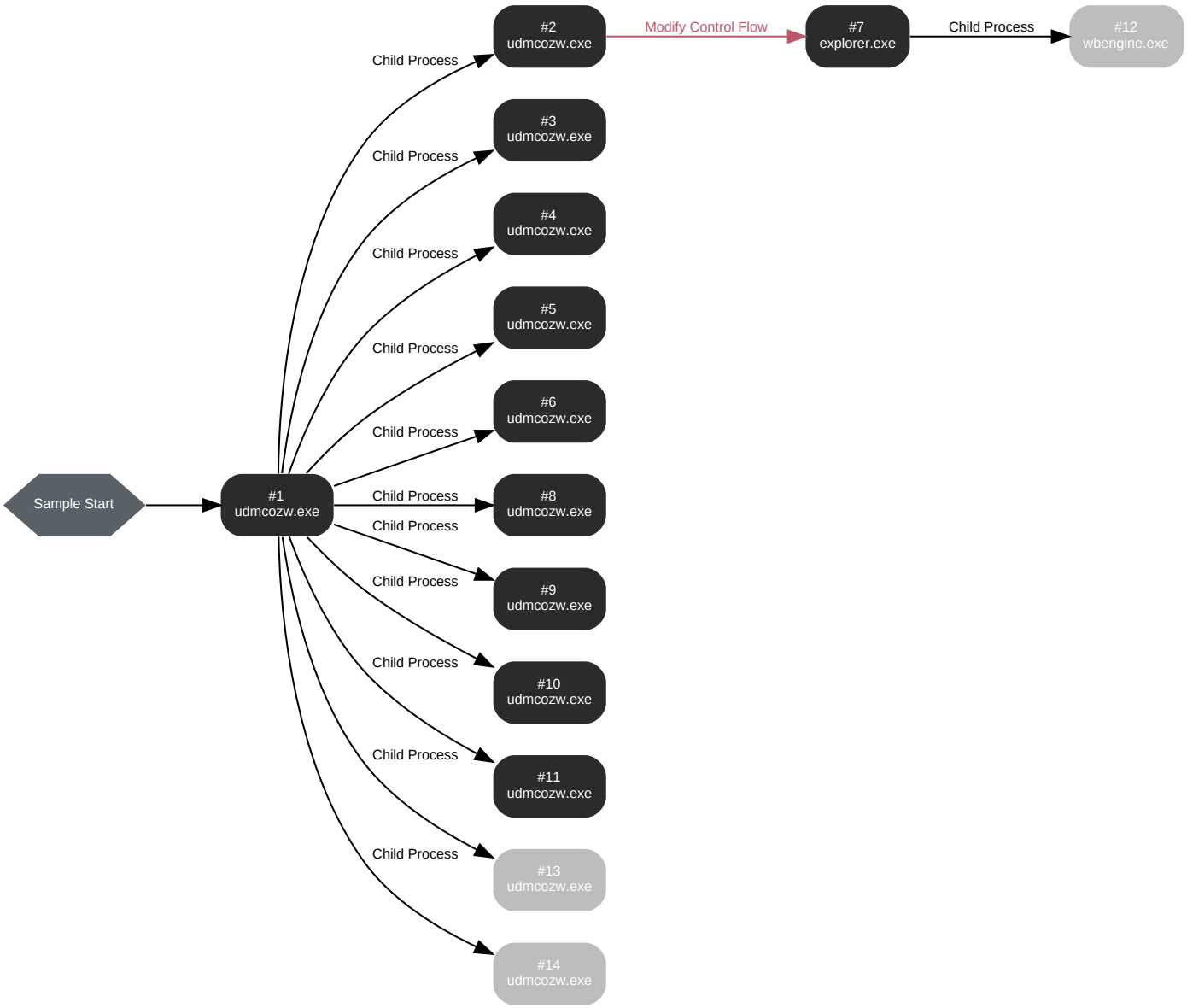
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: udmcozw.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpv3vusit9" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 76509, Reason: Analysis Target
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	245.24s
Return Code	Unknown
PID	5080
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	12

Process #2: udmcozw.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=CopyPropVariant
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100613, Reason: Child Process
Unmonitor End Time	End Time: 238744, Reason: Terminated
Monitor duration	138.13s
Return Code	0
PID	1840
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	30
Environment	2
Registry	571
Mutex	6
Process	2
-	61
-	30

Process #3: udmcozw.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=CreatePropVariant
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 104228, Reason: Child Process
Unmonitor End Time	End Time: 112915, Reason: Terminated
Monitor duration	8.69s
Return Code	0
PID	3008
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	768
Mutex	7

Process #4: udmcozw.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=CreatePropertyStore
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 106385, Reason: Child Process
Unmonitor End Time	End Time: 118906, Reason: Terminated
Monitor duration	12.52s
Return Code	0
PID	3348
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	768
Mutex	7

Process #5: udmcozw.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=DestroyPropVariant
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109161, Reason: Child Process
Unmonitor End Time	End Time: 122985, Reason: Terminated
Monitor duration	13.82s
Return Code	0
PID	1916
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	779
Mutex	7

Process #6: udmcozw.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=FormatTagFromWfx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 112552, Reason: Child Process
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	209.19s
Return Code	Unknown
PID	1968
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	5
Environment	2
Registry	562
Mutex	3

Process #7: explorer.exe

ID	7
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 113584, Reason: Injection
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	208.16s
Return Code	Unknown
PID	1600
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\udmcozw.exe	0x1298 / 0x644	0x1d0000(1900544)	-	✓	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✗
-	1.42 KB	b245a66ea7844ff8765e81570d64b96e75ed81c7ee4ce13d21956ed2bc745e85	✗
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✗
-	1.42 KB	26cf29c1260a48a07f473723e7966f7919c8dd8aa138db546406ce5872c434ad	✗

Host Behavior

Type	Count
Module	43
File	173
System	101
Process	52
Registry	11243
Environment	2
-	18
Mutex	357

Process #8: udmcozw.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=GetAMSubtypeFromD3DFormat
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117368, Reason: Child Process
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	204.38s
Return Code	Unknown
PID	968
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	37
File	118
System	7
Environment	2
Registry	782
Mutex	5
Process	2
-	2
-	1

Process #9: udmcozw.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=GetD3DFormatFromMFSubtype
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 121627, Reason: Child Process
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	200.12s
Return Code	Unknown
PID	1940
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	226

Process #10: udmcozw.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAddPeriodicCallback
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 185470, Reason: Child Process
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	136.28s
Return Code	Unknown
PID	1948
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #11: udmcozw.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAllocateSerialWorkQueue
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 226042, Reason: Child Process
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	95.70s
Return Code	Unknown
PID	2832
Parent PID	5080
Bitness	64 Bit

Host Behavior

Type	Count
Module	15
File	3
Environment	1

Process #12: wbengine.exe

ID	12
File Name	c:\windows\system32\wbengine.exe
Command Line	C:\Windows\system32\wbengine.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 258061, Reason: Child Process
Unmonitor End Time	End Time: 271529, Reason: Terminated
Monitor duration	13.47s
Return Code	0
PID	3720
Parent PID	1600
Bitness	64 Bit

Process #13: udmcozw.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAllocateWorkQueue
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 267673, Reason: Child Process
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	54.07s
Return Code	Unknown
PID	3816
Parent PID	5080
Bitness	64 Bit

Process #14: udmcozw.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\udmcozw.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAllocateWorkQueueEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 305709, Reason: Child Process
Unmonitor End Time	End Time: 321745, Reason: Terminated by Timeout
Monitor duration	16.04s
Return Code	Unknown
PID	4936
Parent PID	5080
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca	C:\Users\RDhJ0CNFevzX\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll, C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll	Sample File	2072.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	53 bytes	application/octet-stream	-	CLEAN
b245a66ea7844ff8765e81570d64b96e75ed81c7ee4ce13d21956ed2bc745e85	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN
4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN
26cf29c1260a48a07f473723e7966f7919c8dd8aa138db546406ce5872c434ad	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpv3vusit9	Accessed File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Windows\system32\XmlLite.dll	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\system\msmapi\1033\msmapi32.dll	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Windows Sidebar\outlook.exe	Accessed File	Access, Read	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	udmcozw.exe	CLEAN
{54137ce8-d76d-e7fc-dec3-c85f290e5b98}	access	udmcozw.exe	CLEAN
{298ddcca-efe5-2f07-cbb5-e91e37797537}	access	explorer.exe	CLEAN
{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}	access	explorer.exe	CLEAN
{e8353f60-b296-77d3-712c-682bf3e23f29}	access	explorer.exe	CLEAN
{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}	access	explorer.exe	CLEAN
{3efe96e0-aada-6cdc-4854-db5a860aa498}	access	explorer.exe	CLEAN
{c8f5437c-d6d6-873d-d7d0-da7099dbb1bb}	access	explorer.exe	CLEAN
{42d854e1-ae99-711c-8f30-1d7624da1673}	access	explorer.exe	CLEAN
{394a7c3c-ac56-58ce-d288-876ad1f16f45}	access	explorer.exe	CLEAN
{d4c35d44-6df3-0b96-1ad6-bbc6db4242ff}	access	explorer.exe	CLEAN
{0543b54c-df93-6503-0f5f-03111d930d96}	access	explorer.exe	CLEAN
{e81f285f-e2d5-843a-2b19-3e6bebf2c463}	access	explorer.exe	CLEAN
{c1d71539-741e-8f57-5d51-d78e6b8472d8}	access	explorer.exe	CLEAN
{742c4235-61f7-6f13-cec8-924c395053dd}	access	explorer.exe	CLEAN
{f2947db2-76ce-20cf-3821-b4e020fbf40d}	access	explorer.exe	CLEAN
{0b7ba948-3cca-a9ee-ef68-bca12f0e84a2}	access	explorer.exe	CLEAN
{c76c4830-ba11-65d9-c31d-e7234b159b82}	access	explorer.exe	CLEAN
{2ef5cc94-f8a9-2574-5587-7f2a664a4914}	access	explorer.exe	CLEAN
{09a6eaab-3fa0-0d71-1e5e-c654ef187a0c}	access	explorer.exe	CLEAN
{d16d5bd5-a9e5-3451-c896-a81deb35e494}	access	explorer.exe	CLEAN
{3f962b47-4d0a-da84-a641-0744d03cca5e}	access	explorer.exe	CLEAN
{ac63b745-c10a-8d33-f2f4-c781a6076c4f}	access	explorer.exe	CLEAN
{06552932-7500-4aaa-456b-93247ed0790e}	access	explorer.exe	CLEAN
{734ab243-3ba9-e014-2983-224ca430987b}	access	explorer.exe	CLEAN
{028360ad-a0ce-7a1e-5afd-31cd9bd4d5ea}	access	explorer.exe	CLEAN
{9b8e3f9b-6a14-ba61-86de-29155d8b4094}	access	explorer.exe	CLEAN
{b4c5217e-775a-862d-a0bd-c504e5eaa60a}	access	explorer.exe	CLEAN
{b33e3c4f-1610-a0b6-186d-a25ba5862812}	access	explorer.exe	CLEAN
{a3dce688-6117-3ea3-fbbd-1defec717462}	access	explorer.exe	CLEAN
{ec2954cb-8ed4-cf4d-bef4-2d7135075084}	access	explorer.exe	CLEAN
{168ee11b-299f-6d76-b48f-88a65a4a58ba}	access	explorer.exe	CLEAN
{b4de3d46-efec-a98a-f706-8745d35ed7f2}	access	explorer.exe	CLEAN
{d1575404-3469-2df0-db6b-3bcf4439344f}	access	explorer.exe	CLEAN
{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}	access	explorer.exe	CLEAN
{3c33918e-27da-9f35-2586-b9f012933134}	access	explorer.exe	CLEAN
{6c570128-9202-fd64-daa4-72143d141e8a}	access	explorer.exe	CLEAN
{d89ce0d8-125f-38cf-59d4-410119d64fdf}	access	explorer.exe	CLEAN
{c42c174a-1be2-3a72-8667-a20ecc356e75}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{a05f0669-d546-7c4b-c5ff-6ad44aa5f2b6}	access	explorer.exe	CLEAN
{95c38542-2405-0d06-534c-428190efb4c6}	access	explorer.exe	CLEAN
{e28905fd-15de-b796-44d3-7a7876237780}	access	explorer.exe	CLEAN
{0e00dc0d-6bc0-49b5-4c04-4c9791ff2470}	access	explorer.exe	CLEAN
{f5908ce7-c5cc-734d-f2cc-bd80fc3637ac}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	access, create	explorer.exe, udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	explorer.exe, udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	access, read	explorer.exe, udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EnableLUA	access, read	explorer.exe, udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ConsentPromptBehaviorAdmin	access, read	explorer.exe, udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PromptOnSecureDesktop	access, read	explorer.exe, udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\InstallDate	access, read	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	access, read	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	access, read	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	access, read	udmcozw.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8C45A918-B075-FEF6-0DED-B5C899623EB0}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InstallDate	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{026F08C5-341A-9406-8117-0A9B26B9732B}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98DFD738-1E78-D107-2616-FA30049BD427}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1384CAC3-17AC-E069-EB5C-4E613FCC6FE4}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5E441BBB-4FA0-7A47-C898-77D45B377F36}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\InstallDate	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\InstallDate	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\InstallDate	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\InstallDate	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder\{C55C17BD-1B1D-6455-A2F0-5AF841FDF299}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{2E618B65-6FC4-2342-2DBA-449C03CF1691}	access, write	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayVersion	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	access, read	explorer.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpv3vusit9" /s	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=CopyPropVariant	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=CreatePropVariant	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=CreatePropertyStore	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=DestroyPropVariant	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=FormatTagFromWfx	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=GetAMSubtypeFromD3DFormat	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=GetD3DFormatFromMFSubtype	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAddPeriodicCallback	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAllocateSerialWorkQueue	CLEAN
wbengine.exe	C:\Windows\system32\wbengine.exe	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAllocateWorkQueue	CLEAN
udmcozw.exe	"C:\Users\RDhJ0CNFevzX\Desktop\udmCozW.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll" /fn_id=MFAllocateWorkQueueEx	CLEAN

YARA / AV

Antivirus (5)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS

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	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 08:04:18+00:00
Built-in AV Database Records	10477558

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