MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll**
ID	#969370
MD5	ecdfff8b0ece2175cd699e690de1fcaf
SHA1	9359770d71e743832ca22597db917dfa817038b2
SHA256	dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3
File Size	1220.00 KB
Report Created	2021-09-28 14:53 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 110 matches)

Score	Category	Operation	Count	Classification
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) htdmoym.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #9) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #14) htdmoym.exe as "Gen:Variant.Mikey.113998".			
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #2) htdmoym.exe alters context of (process #9) explorer.exe. • (Process #2) htdmoym.exe alters context of (process #10) shellexperiencehost.exe.			
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 #9) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #9) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #9) explorer.exe has a thread which sleeps more than 5 minutes.			
1/5	Discovery	Reads system data	8	-
	• (Process #2) htdmoym.exe reads the Windows installation date from registry. • (Process #3) htdmoym.exe reads the Windows installation date from registry. • (Process #4) htdmoym.exe reads the Windows installation date from registry. • (Process #5) htdmoym.exe reads the Windows installation date from registry. • (Process #6) htdmoym.exe reads the Windows installation date from registry. • (Process #7) htdmoym.exe reads the Windows installation date from registry. • (Process #9) explorer.exe reads the Windows installation date from registry. • (Process #8) htdmoym.exe reads the Windows installation date from registry.			
1/5	Mutex	Creates mutex	87	-

- (Process #2) htdmoym.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #3) htdmoym.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) htdmoym.exe creates mutex with name "{20974a93-a551-df17-8967-748358091d34}".
- (Process #4) htdmoym.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) htdmoym.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) htdmoym.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) htdmoym.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #9) explorer.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #9) explorer.exe creates mutex with name "{298ddcca-efe5-2f07-cbb5-e91e37797537}".
- (Process #9) explorer.exe creates mutex with name "{389fe546-d029-33a7-6305-2ca1cede0678}".
- (Process #9) explorer.exe creates mutex with name "{e8b6fe55-d858-d6e4-ef99-a80106642ab4}".
- (Process #9) explorer.exe creates mutex with name "{03b2a674-5295-21d6-da36-fc13faee0e98}".
- (Process #9) explorer.exe creates mutex with name "{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}".
- (Process #9) explorer.exe creates mutex with name "{d439f686-d570-7182-3906-1e2d175d1088}".
- (Process #9) explorer.exe creates mutex with name "{dc2eeabe-ea3b-fc8c-9e30-5b454dae0199}".
- (Process #9) explorer.exe creates mutex with name "{0f7daade-cabb-071c-b422-48138f19f093}".
- (Process #9) explorer.exe creates mutex with name "{d403fc5c-718c-8546-54e4-88a5fca09073}".
- (Process #9) explorer.exe creates mutex with name "{02a8695f-288f-8425-5a00-ed7ca3db1713}".
- (Process #9) explorer.exe creates mutex with name "{8aadbf32-a058-ae7b-e2fa-32a552670e17}".
- (Process #9) explorer.exe creates mutex with name "{e488bcbc-fbee-5b9f-db88-09e52deb9054}".
- (Process #9) explorer.exe creates mutex with name "{e2a078c8-ea83-b06c-9312-8ffbd26d8215}".
- (Process #9) explorer.exe creates mutex with name "{3d57add5-0f6b-0200-0662-1b09ecfcf9e5}".
- (Process #9) explorer.exe creates mutex with name "{8cd92000-a2e9-0bbf-6791-44a791672317}".
- (Process #9) explorer.exe creates mutex with name "{c2f29d54-8e22-4aed-dde9-8dbc7ae9afe3}".
- (Process #9) explorer.exe creates mutex with name "{e81f285f-e2d5-843a-2b19-3e6bebf2c463}".
- (Process #9) explorer.exe creates mutex with name "{c0b7ed59-c58a-52c9-bb95-ac3e2fb7a217}".
- (Process #9) explorer.exe creates mutex with name "{3cf5819b-7163-609f-286f-edc923bb4ae9}".
- (Process #9) explorer.exe creates mutex with name "{4a672f28-9e81-ce55-512e-6eadd5d036ec}".
- (Process #9) explorer.exe creates mutex with name "{19a9def8-7e87-44e0-b180-e8de92fad2a5}".
- (Process #9) explorer.exe creates mutex with name "{9d2797ce-b360-8612-a42a-fb0e1ac79170}".
- (Process #9) explorer.exe creates mutex with name "{12b8edc4-0a41-4e70-9aef-644fb06cc02b}".
- (Process #9) explorer.exe creates mutex with name "{65332ccb-f024-e4c5-63d6-0398a3f645c3}".
- (Process #9) explorer.exe creates mutex with name "{0969e291-b21e-da66-8a27-2c05635de7c1}".
- (Process #9) explorer.exe creates mutex with name "{9666bd67-64c1-5269-b5bb-b889b9fea609}".
- (Process #9) explorer.exe creates mutex with name "{1fd4ce32-1652-23b5-f64f-63e609c14ad1}".
- (Process #7) htdmoym.exe creates mutex with name "{20974a93-a551-df17-8967-748358091d34}".
- (Process #9) explorer.exe creates mutex with name "{aadb65f8-5aae-bb01-afa3-e769be98792f}".
- (Process #9) explorer.exe creates mutex with name "{a6b08019-eab0-90f4-ce43-6184de4f14be}".
- (Process #9) explorer.exe creates mutex with name "{38e7db7a-75ef-8cef-8130-9e11aa96557f}".
- (Process #9) explorer.exe creates mutex with name "{a0997771-1481-fafe-76ec-19caa3547787}".
- (Process #9) explorer.exe creates mutex with name "{3874444c-1610-2d0c-d5c6-97a8ca323dc0}".
- (Process #9) explorer.exe creates mutex with name "{63e78bd0-59a8-0372-0a57-0e409e664ec4}".
- (Process #9) explorer.exe creates mutex with name "{8d43a83e-bd41-b3a4-0fdf-78d827ec82a0}".
- (Process #9) explorer.exe creates mutex with name "{7ba3817f-aeba-298a-7847-ab3c2bff153d}".
- (Process #9) explorer.exe creates mutex with name "{e587491f-9a6e-882a-817e-9786768f022b}".
- (Process #9) explorer.exe creates mutex with name "{38766670-afb4-3a11-e501-6087f79d5664}".
- (Process #9) explorer.exe creates mutex with name "{8f4fb38c-7a0f-fbf2-af5d-ee113ce17eb9}".
- (Process #9) explorer.exe creates mutex with name "{71dba081-a28d-be08-fa55-bf22ddb35cb9}".
- (Process #9) explorer.exe creates mutex with name "{28f52da9-03cf-d977-002b-a8858ed6ee74}".
- (Process #9) explorer.exe creates mutex with name "{25fdcad7-f614-d8db-5c91-5ebad4f4d05e}".
- (Process #9) explorer.exe creates mutex with name "{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}".
- (Process #9) explorer.exe creates mutex with name "{a3dce688-6117-3ea3-fbbd-1defec717462}".
- (Process #9) explorer.exe creates mutex with name "{879e93b3-0521-56c3-08cb-cd0d806e6ccf}".
- (Process #9) explorer.exe creates mutex with name "{9c5d6caa-c049-2b54-7a0b-b579bca5b578}".
- (Process #9) explorer.exe creates mutex with name "{daa370fa-1379-7113-c11a-e30a38c99e5d}".
- (Process #9) explorer.exe creates mutex with name "{01f24baa-a48c-b675-d94f-c4d185fa1b74}".
- (Process #9) explorer.exe creates mutex with name "{60d53e50-c02a-fd11-36ca-0f91b9ec3738}".
- (Process #9) explorer.exe creates mutex with name "{1c9185e1-04c2-f876-90d9-8e799aee9797}".
- (Process #9) explorer.exe creates mutex with name "{f7677ce1-197d-c706-bc9e-7239a2ec86e1}".
- (Process #9) explorer.exe creates mutex with name "{ac72e380-225fca96a-c148-d864da64e030}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #2) htdmoym.exe reads from (process #9) explorer.exe. • (Process #7) htdmoym.exe reads from (process #9) explorer.exe.			
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
	• (Process #9) explorer.exe hides 3526 bytes in "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder\{3A5592B3-1C96-7108-AB0E-F79713649A82}".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #9) explorer.exe starts (process #17) mdmappinstaller.exe with a hidden window.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #9) explorer.exe resolves 26 API functions by name.			

Mitre ATT&CK Matrix

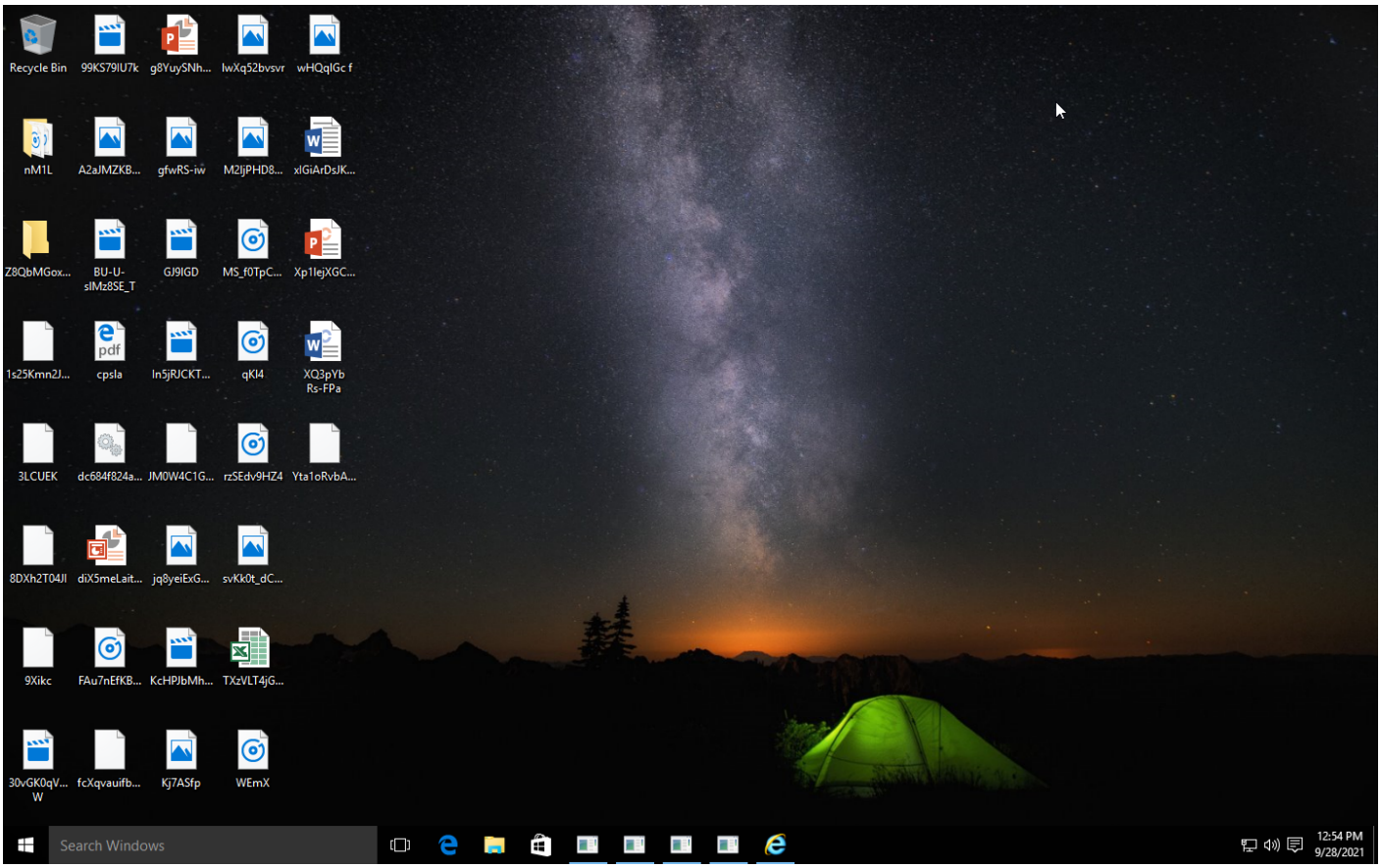
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1112 Modify Registry	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1143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

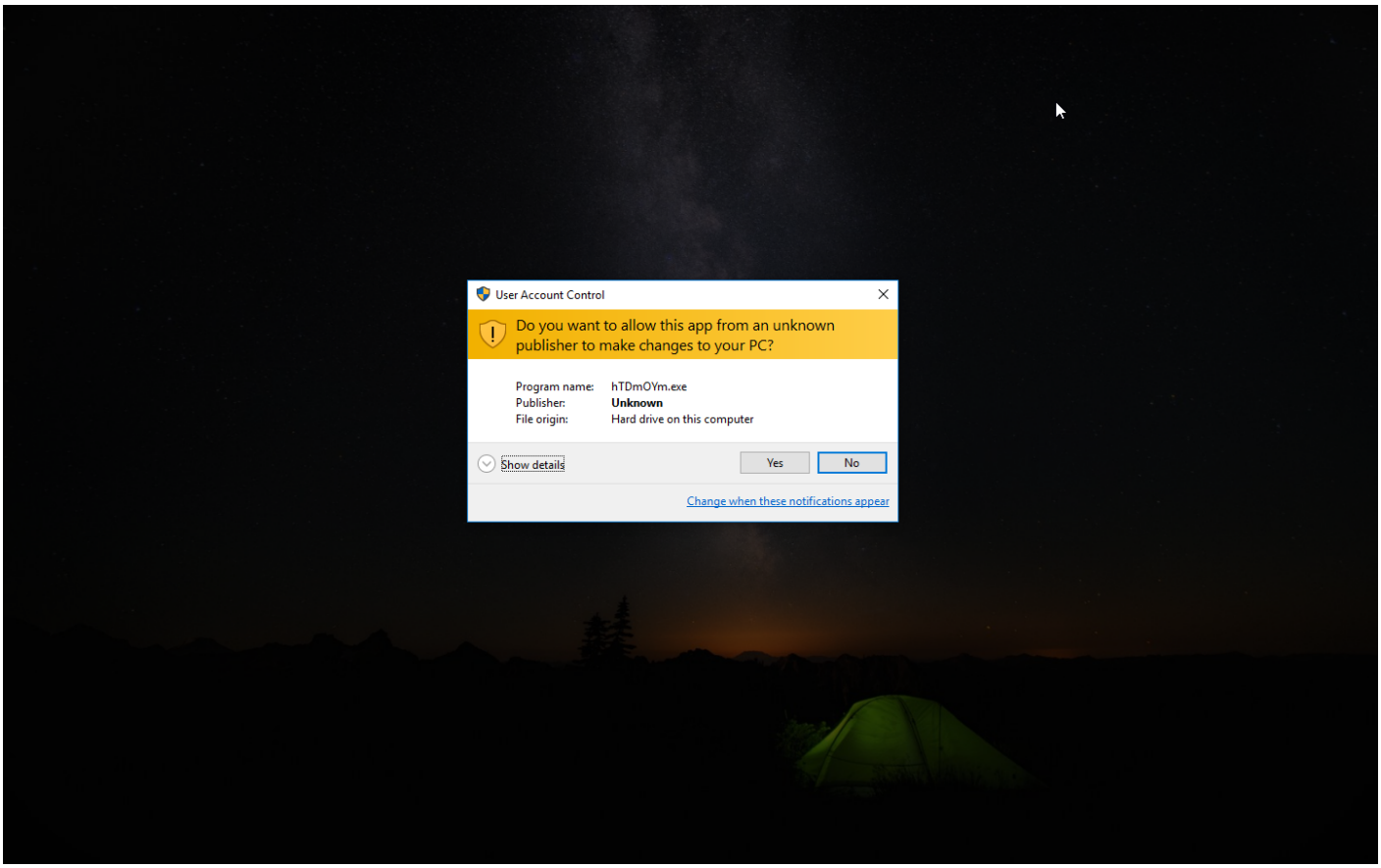
Sample Information

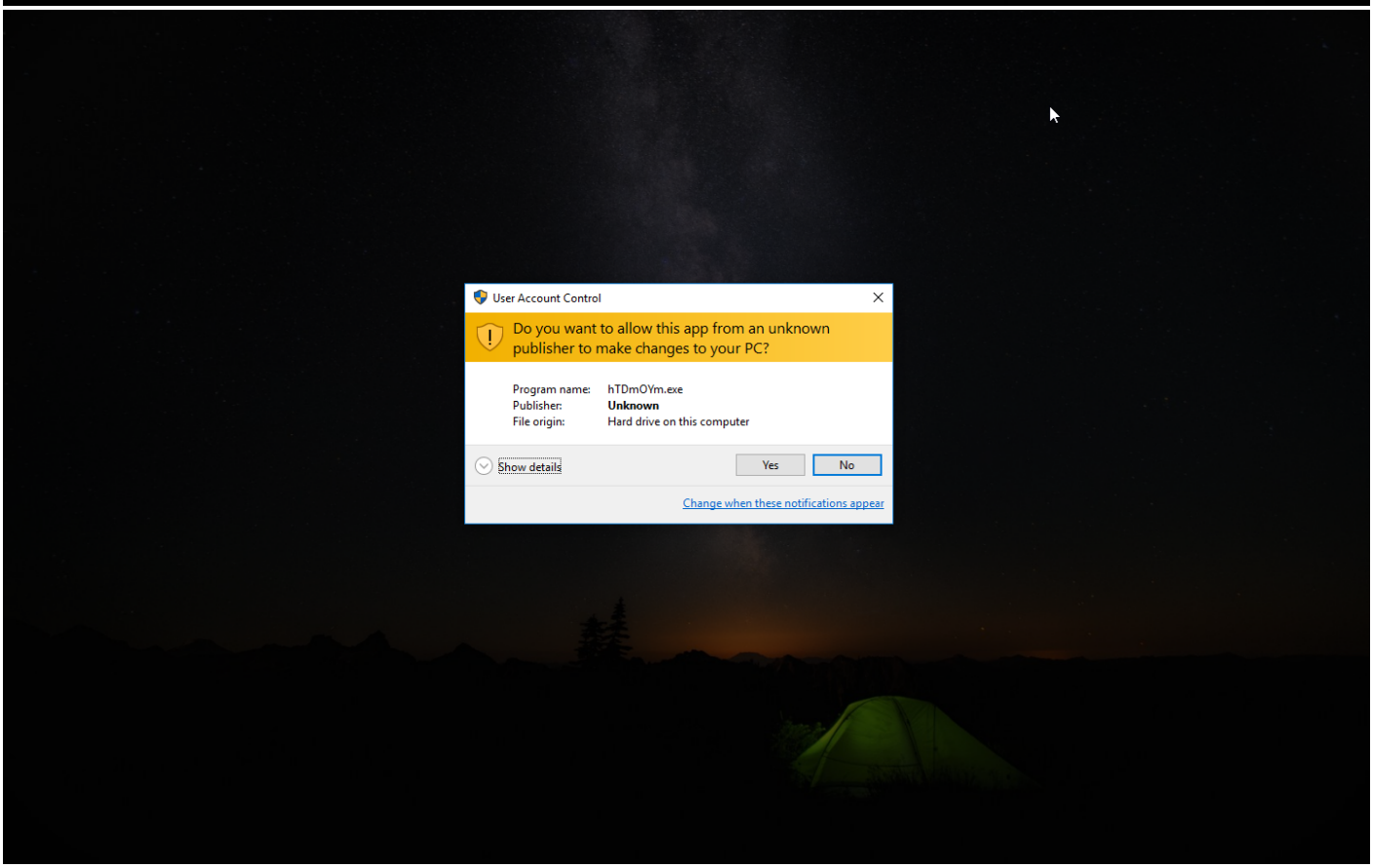
ID	#969370
MD5	ecdfff8b0ece2175cd699e690de1fcaf
SHA1	9359770d71e743832ca22597db917dfa817038b2
SHA256	dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3
SSDeep	12288:YVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:NfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll
File Size	1220.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:53 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	18
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	4
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
99KS79IU7k
g8YuySNh...
lwXq52bvsvr
wHQqIGc f
nM1L
A2aJMZKB...
gfwRS-iw
M2ljPHD8...
xlGiArDsJK...
Z8QbMGox...
BU-U-
sIMz8SE_T
GJ9IGD
MS_f0TpC...
Xp1lejXGC...
1s25Kmn2J...
cpsla
ln5jRJCKT...
qKI4
XQ3pYb
Rs-FPa
3LCUEK
dc684f824a...
JM0W4C1G...
rzSEdv9HZ4
Yta1oRvbA...
8DXh2T04JI
diX5meLait...
jq8yeiExG...
svKk0t_dC...
9Xikc
FAu7nEfKB...
KcHPJbMh...
TXzVLT4jG...
30vGK0qV...
W
fcXqvauifb...
Kj7ASfp
WEmX
Search Windows
12:54 PM
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

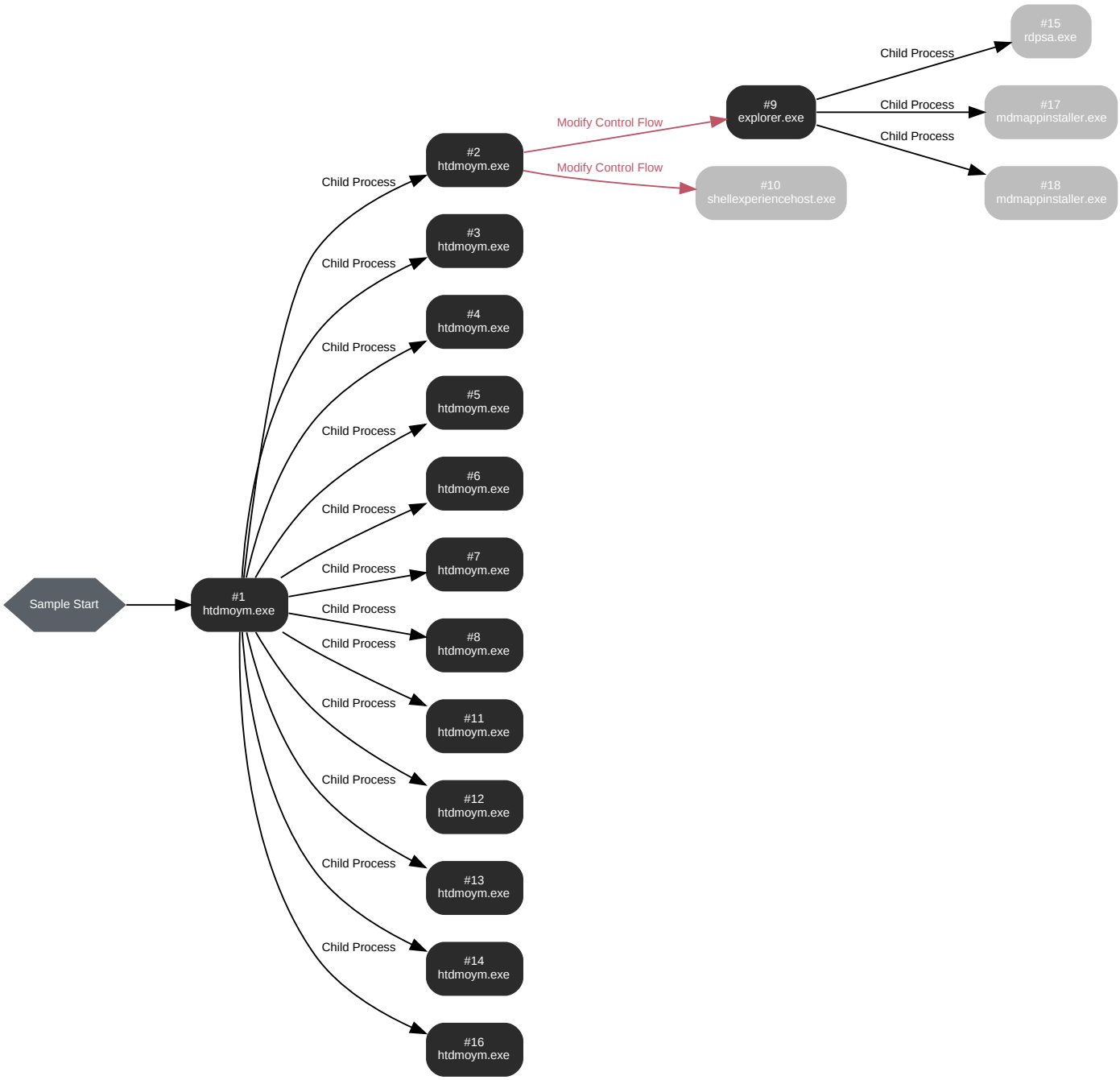
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: htdmoym.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmph5cze6pt" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 70666, Reason: Analysis Target
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	240.40s
Return Code	Unknown
PID	4880
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	13

Process #2: htdmoym.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=#2
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 93380, Reason: Child Process
Unmonitor End Time	End Time: 225659, Reason: Terminated
Monitor duration	132.28s
Return Code	0
PID	3728
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	35
Environment	2
Registry	789
Mutex	6
Process	2
-	49
-	32
-	122

Process #3: htdmoym.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=CloseDriver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 95576, Reason: Child Process
Unmonitor End Time	End Time: 115123, Reason: Terminated
Monitor duration	19.55s
Return Code	0
PID	3628
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #4: htdmoym.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=DefDriverProc
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 97925, Reason: Child Process
Unmonitor End Time	End Time: 119586, Reason: Terminated
Monitor duration	21.66s
Return Code	0
PID	1880
Parent PID	4880
Bitness	64 Bit

Host Behavior

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

Process #5: htdmoym.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=DriverCallback
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100947, Reason: Child Process
Unmonitor End Time	End Time: 124914, Reason: Terminated
Monitor duration	23.97s
Return Code	0
PID	1228
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #6: htdmoym.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=DrvGetModuleHandle
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 106096, Reason: Child Process
Unmonitor End Time	End Time: 130854, Reason: Terminated
Monitor duration	24.76s
Return Code	0
PID	2260
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #7: htdmoym.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=GetDriverModuleHandle
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 112825, Reason: Child Process
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	198.24s
Return Code	Unknown
PID	1016
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	8
Environment	2
Registry	789
Mutex	5
Process	2
-	2
-	1

Process #8: htdmoym.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=OpenDriver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 118824, Reason: Child Process
Unmonitor End Time	End Time: 247082, Reason: Terminated
Monitor duration	128.26s
Return Code	0
PID	1204
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	227
Mutex	4

Process #9: explorer.exe

ID	9
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 123228, Reason: Injection
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	187.84s
Return Code	Unknown
PID	1636
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (73)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x668	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x690	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x694	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6b8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6bc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6dc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6e8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x71c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x734	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x73c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x74c	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x798	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x7a8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x7b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x7d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x7ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x7f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x460	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x83c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x954	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x9c0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xbec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x4c4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x4ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x8b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x984	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x97c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xa20	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xfd8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xfe8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xdbc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xdb4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x62c	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xca4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xbf0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x858	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x4f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x3ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0xd58	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x102c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x11b8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x1238	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x9f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5f8bb580(140721911477632)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5f8bb580(140721911477632)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\htdmoym.exe	0xd50 / 0x6ac	0x7ffc5ecdce60(140721899032160)	-	✓	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✗
-	1.42 KB	0f2f52b7662aa6edf6771479355fb29af98851a2ab6336412e8cd8f78bd75bfc	✗
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✗
-	1.42 KB	c289b6e0236a9d9a8ea921a81c9ef3fc1598c913b4391766d8d914666ebe0264	✗

Host Behavior

Type	Count
Module	48
File	237
System	750

Type	Count
Process	133
Registry	20502
Environment	2
-	21
Mutex	2082

Process #10: shellexperiencehost.exe

ID	10
File Name	c:\windows\systemapps\shellexperiencehost_cw5n1h2txyewy\shellexperiencehost.exe
Command Line	"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
Initial Working Directory	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\
Monitor Start Time	Start Time: 125066, Reason: Injection
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	186.00s
Return Code	Unknown
PID	2660
Parent PID	628
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\htdmoym.exe	0xd50 / 0x2fc	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Process #11: htdmoym.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=PlaySound
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 128820, Reason: Child Process
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	182.25s
Return Code	Unknown
PID	3740
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #12: htdmoym.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=PlaySoundA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 214770, Reason: Child Process
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	96.30s
Return Code	Unknown
PID	2580
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #13: htdmoym.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=PlaySoundW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 240826, Reason: Child Process
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	70.24s
Return Code	Unknown
PID	2064
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #14: htdmoym.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=SendDriverMessage
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 255274, Reason: Child Process
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	55.79s
Return Code	Unknown
PID	5100
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #15: rdpsa.exe

ID	15
File Name	c:\windows\system32\rdpsa.exe
Command Line	C:\Windows\system32\RdpSa.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 273221, Reason: Child Process
Unmonitor End Time	End Time: 294988, Reason: Terminated
Monitor duration	21.77s
Return Code	3221226540
PID	1676
Parent PID	1636
Bitness	64 Bit

Process #16: htdmoym.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\htdmoym.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=WOWAppExit
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 288367, Reason: Child Process
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	22.70s
Return Code	Unknown
PID	1608
Parent PID	4880
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	112
Environment	1

Process #17: mdmappinstaller.exe

ID	17
File Name	c:\windows\system32\mdmappinstaller.exe
Command Line	C:\Windows\system32\MDMAppInstaller.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 298585, Reason: Child Process
Unmonitor End Time	End Time: 307129, Reason: Terminated
Monitor duration	8.54s
Return Code	0
PID	5024
Parent PID	1636
Bitness	64 Bit

Process #18: mdmappinstaller.exe

ID	18
File Name	c:\users\rdhj0cnfevzx\appdata\local\fp0z85vd8\mdmappinstaller.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\Fp0Z85VD8\MDMAppInstaller.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 306970, Reason: Child Process
Unmonitor End Time	End Time: 311067, Reason: Terminated by Timeout
Monitor duration	4.10s
Return Code	Unknown
PID	4540
Parent PID	1636
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3	C:\Users\RDhJ0CNFevzX\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll, C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll	Sample File	1220.00 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
0f2f52b7662aa6edf6771479355fb29af98851a2ab6336412e8cd8f78bd75bfc	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
c289b6e0236a9d9a8ea921a81c9ef3fc1598c913b4391766d8d914666ebe0264	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\hTDmOYm.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmph5cze6pt	Accessed File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll	Accessed File	Read, Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\system\msmapi\1033\msmapi32.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Adobe\551S	Accessed File	Create, Access	CLEAN
C:\Program Files\WindowsPowerShell\outlook.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\RdpSa.exe	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64win.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64cpu.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\MDMAppInstaller.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\WTSAPI32.dll	Accessed File	Read, Access	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	htdmoym.exe	CLEAN
{20974a93-a551-df17-8967-748358091d34}	access	htdmoym.exe	CLEAN
{298ddcca-efe5-2f07-cbb5-e91e37797537}	access	explorer.exe	CLEAN
{389fe546-d029-33a7-6305-2ca1cede0678}	access	explorer.exe	CLEAN
{e8b6fe55-d858-d6e4-ef99-a80106642ab4}	access	explorer.exe	CLEAN
{03b2a674-5295-21d6-da36-fc13faee0e98}	access	explorer.exe	CLEAN
{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}	access	explorer.exe	CLEAN
{d439f686-d570-7182-3906-1e2d175d1088}	access	explorer.exe	CLEAN
{dc2eeabe-ea3b-fc8c-9e30-5b454dae0199}	access	explorer.exe	CLEAN
{0f7daade-cabb-071c-b422-48138f19f093}	access	explorer.exe	CLEAN
{d403fc5c-718c-8546-54e4-88a5fca09073}	access	explorer.exe	CLEAN
{02a8695f-288f-8425-5a00-ed7ca3db1713}	access	explorer.exe	CLEAN
{8aadbf32-a058-ae7b-e2fa-32a552670e17}	access	explorer.exe	CLEAN
{e488bcbc-fbee-5b9f-db88-09e52deb9054}	access	explorer.exe	CLEAN
{e2a078c8-ea83-b06c-9312-8ffbd26d8215}	access	explorer.exe	CLEAN
{3d57add5-0f6b-0200-0662-1b09ecfcf9e5}	access	explorer.exe	CLEAN
{8cd92000-a2e9-0bbf-6791-44a791672317}	access	explorer.exe	CLEAN
{c2f29d54-8e22-4aed-dde9-8dbc7ae9afe3}	access	explorer.exe	CLEAN
{e81f285f-e2d5-843a-2b19-3e6bebf2c463}	access	explorer.exe	CLEAN
{c0b7ed59-c58a-52c9-bb95-ac3e2fb7a217}	access	explorer.exe	CLEAN
{3cf5819b-7163-609f-286f-edc923bb4ae9}	access	explorer.exe	CLEAN
{4a672f28-9e81-ce55-512e-6eadd5d036ec}	access	explorer.exe	CLEAN
{19a9def8-7e87-44e0-b180-e8de92fad2a5}	access	explorer.exe	CLEAN
{9d2797ce-b360-8612-a42a-fb0e1ac79170}	access	explorer.exe	CLEAN
{12b8edc4-0a41-4e70-9aef-644fb06cc02b}	access	explorer.exe	CLEAN
{65332ccb-f024-e4c5-63d6-0398a3f645c3}	access	explorer.exe	CLEAN
{0969e291-b21e-da66-8a27-2c05635de7c1}	access	explorer.exe	CLEAN
{9666bd67-64c1-5269-b5bb-b889b9fea609}	access	explorer.exe	CLEAN
{1fd4ce32-1652-23b5-f64f-63e609c14ad1}	access	explorer.exe	CLEAN
{aadb65f8-5aae-bb01-afa3-e769be98792f}	access	explorer.exe	CLEAN
{a6b08019-eab0-90f4-ce43-6184de4f14be}	access	explorer.exe	CLEAN
{38e7db7a-75ef-8cef-8130-9e11aa96557f}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{a0997771-1481-fafe-76ec-19caa3547787}	access	explorer.exe	CLEAN
{3874444c-1610-2d0c-d5c6-97a8ca323dc0}	access	explorer.exe	CLEAN
{63e78bd0-59a8-0372-0a57-0e409e664ec4}	access	explorer.exe	CLEAN
{8d43a83e-bd41-b3a4-0fdf-78d827ec82a0}	access	explorer.exe	CLEAN
{7ba3817f-aeba-298a-7847-ab3c2bff153d}	access	explorer.exe	CLEAN
{e587491f-9a6e-882a-817e-9786768f022b}	access	explorer.exe	CLEAN
{38766670-afb4-3a11-e501-6087f79d5664}	access	explorer.exe	CLEAN
{8f4fb38c-7a0f-fbf2-af5d-ee113ce17eb9}	access	explorer.exe	CLEAN
{71dba081-a28d-be08-fa55-bf22ddb35cb9}	access	explorer.exe	CLEAN
{28f52da9-03cf-d977-002b-a8858ed6ee74}	access	explorer.exe	CLEAN
{25fdcad7-f614-d8db-5c91-5ebad4f4d05e}	access	explorer.exe	CLEAN
{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}	access	explorer.exe	CLEAN
{a3dce688-6117-3ea3-fbbd-1defec717462}	access	explorer.exe	CLEAN
{879e93b3-0521-56c3-08cb-cd0d806e6ccf}	access	explorer.exe	CLEAN
{9c5d6caa-c049-2b54-7a0b-b579bca5b578}	access	explorer.exe	CLEAN
{daa370fa-1379-7113-c11a-e30a38c99e5d}	access	explorer.exe	CLEAN
{01f24baa-a48c-b675-d94f-c4d185fa1b74}	access	explorer.exe	CLEAN
{60d53e50-c02a-fd11-36ca-0f91b9ec3738}	access	explorer.exe	CLEAN
{1c9185e1-04c2-f876-90d9-8e799aee9797}	access	explorer.exe	CLEAN
{f7677ce1-197d-c706-bc9e-7239a2ec86e1}	access	explorer.exe	CLEAN
{ac72e331-225f-a96a-c143-d364da64ed30}	access	explorer.exe	CLEAN
{d89ce0d8-125f-38cf-59d4-410119d64fdf}	access	explorer.exe	CLEAN
{6fe25233-3c10-d1be-fd07-8467d220e8d6}	access	explorer.exe	CLEAN
{583163e6-97f6-ca24-26b7-ae90d9895822}	access	explorer.exe	CLEAN
{fcd273ea-02e9-5a8a-4a8b-7848d0895772}	access	explorer.exe	CLEAN
{61cf2e75-7825-7e06-d929-f4f508b6f8c8}	access	explorer.exe	CLEAN
{b6db0ce4-a8d6-ce5e-e65e-78fb826a82a2}	access	explorer.exe	CLEAN
{fef37f2e-4f56-9012-852a-59484b5fed7e}	access	explorer.exe	CLEAN
{53be0c1d-6845-1fb9-9acf-69f1a3b7921b}	access	explorer.exe	CLEAN
{8d859e8a-cd3c-3ac0-0451-ab11d6131acd}	access	explorer.exe	CLEAN
{cbb5112e-b2b9-ce4a-1512-130aeacbcb51}	access	explorer.exe	CLEAN
{1439a690-60db-c7ba-74ad-63f3b3396ce4}	access	explorer.exe	CLEAN
{dcc64ab4-43e3-3cb6-4e2a-9ca7d2b55758}	access	explorer.exe	CLEAN
{71bb662b-e609-45a6-82d2-d177df9706bc}	access	explorer.exe	CLEAN
{946d3aec-f0be-460d-b2db-c49c07ac46ae}	access	explorer.exe	CLEAN
{b894408f-30d6-e44c-93a0-15251ca9bab4}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{867eeaaa-9095-7d70-5174-9d6e7d728884}	access	explorer.exe	CLEAN
{1da4e1aa-6eb1-9190-a173-cc15c94ce697}	access	explorer.exe	CLEAN
{f9e73e00-f006-b49c-1dcf-ff85215b0c68}	access	explorer.exe	CLEAN
{6a4fe6c6-ce4d-1240-9924-4da205e310d4}	access	explorer.exe	CLEAN
{92072f54-0b93-095f-1e25-932462e67c3e}	access	explorer.exe	CLEAN
{6444f54d-a127-9551-45b8-6703303ab458}	access	explorer.exe	CLEAN
{205d5366-f15a-2f49-d587-0637683a4897}	access	explorer.exe	CLEAN
{a5a67534-fa42-ee17-0f42-7894e1acd27e}	access	explorer.exe	CLEAN
{b6ffd8a4-cbf6-6d07-2839-8d519470089a}	access	explorer.exe	CLEAN
{b4ff8e4a-f2fa-18eb-cb94-db0cc7788bc8}	access	explorer.exe	CLEAN
{b4c5217e-775a-862d-a0bd-c504e5eaa60a}	access	explorer.exe	CLEAN
{a17a4699-466f-23a9-3e4a-9fc54e2eb04a}	access	explorer.exe	CLEAN

Registry

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

Registry Key	Operations	Parent Process Name	Verdict
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
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	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InstallDate	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{026F08C5-341A-9406-8117-0A9B26B9732B}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98DFD738-1E78-D107-2616-FA30049BD427}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1384CAC3-17AC-E069-EB5C-4E613FCC6FE4}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5E441BBB-4FA0-7A47-C898-77D45B377F36}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{28ABA520-2C1D-6C61-C0C7-A14CF6B906F1}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{62E4E317-0062-79DE-48F0-1E0765BB0FBB}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3588360E-206F-AD4B-5FE2-CA87B137A0AE}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD715941-4DC5-0356-AE8C-CD7DA56A3E36}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2576763A-EFDC-256B-2964-9C5E743B0B1B}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{92405BE0-7F95-9DE5-BB58-67AC75F6DB46}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder\{2A382849-FC02-3688-50CF-7D5C5136B77C}	write, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{BF3D66A9-F7E1-9A46-B537-9E833BB1E3D9}	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A13D7EA4-5D34-8684-2E14-FDAFDFB3E2D8}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\InstallDate	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\InstallDate	read, access	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
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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayVersion	read, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayVersion	read, access	explorer.exe	CLEAN
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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayVersion	read, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
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
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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	explorer.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmph5cze6pt" /s	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=#2	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=CloseDriver	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=DefDriverProc	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=DriverCallback	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=DrvGetModuleHandle	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=GetDriverModuleHandle	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=OpenDriver	CLEAN
shellexperiencehost.exe	"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=PlaySound	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=PlaySoundA	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=PlaySoundW	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=SendDriverMessage	CLEAN

Process Name	Commandline	Verdict
rdpsa.exe	C:\Windows\system32\RdpSa.exe	CLEAN
htdmoym.exe	"C:\Users\RDhJ0CNFevzX\Desktop\hTDmOYm.exe" /dll="C:\Users\RDHJ0C~1\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll" /fn_id=WOWAppExit	CLEAN
mdmappinstaller.exe	C:\Windows\system32\MDMAppInstaller.exe	CLEAN
mdmappinstaller.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\Fp0Z85VD8\MDMAppInstaller.exe	CLEAN

YARA / AV

Antivirus (4)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	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