MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll**
ID	#969274
MD5	c10ee36fe08388fce375f320660bc91c
SHA1	6477666e70f87ff53040e98f324660a5167eb4f4
SHA256	d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3
File Size	2044.00 KB
Report Created	2021-09-28 14:19 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 104 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) mvjgboit.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #5) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #12) mvjgboit.exe as "Gen:Variant.Mikey.113998".			
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #2) mvjgboit.exe alters context of (process #5) explorer.exe. • (Process #2) mvjgboit.exe alters context of (process #8) 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 #5) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #5) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #5) explorer.exe has a thread which sleeps more than 5 minutes.			
1/5	Discovery	Reads system data	6	-
	• (Process #2) mvjgboit.exe reads the Windows installation date from registry. • (Process #3) mvjgboit.exe reads the Windows installation date from registry. • (Process #4) mvjgboit.exe reads the Windows installation date from registry. • (Process #9) mvjgboit.exe reads the Windows installation date from registry. • (Process #5) explorer.exe reads the Windows installation date from registry. • (Process #10) mvjgboit.exe reads the Windows installation date from registry.			
1/5	Mutex	Creates mutex	84	-

- (Process #2) mvjgboit.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) mvjgboit.exe creates mutex with name "{20974a93-a551-df17-8967-748358091d34}".
- (Process #3) mvjgboit.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #4) mvjgboit.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #9) mvjgboit.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) explorer.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) explorer.exe creates mutex with name "{298ddcca-efe5-2f07-cbb5-e91e37797537}".
- (Process #5) explorer.exe creates mutex with name "{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}".
- (Process #5) explorer.exe creates mutex with name "{389fe546-d029-33a7-6305-2ca1cede0678}".
- (Process #5) explorer.exe creates mutex with name "{e8b6fe55-d858-d6e4-ef99-a80106642ab4}".
- (Process #5) explorer.exe creates mutex with name "{03b2a674-5295-21d6-da36-fc13faee0e98}".
- (Process #5) explorer.exe creates mutex with name "{d439f686-d570-7182-3906-1e2d175d1088}".
- (Process #5) explorer.exe creates mutex with name "{82761896-27cc-43ce-e454-25a5cf66d6e1}".
- (Process #5) explorer.exe creates mutex with name "{05747a50-933e-c4fd-7a3d-44fed7350072}".
- (Process #5) explorer.exe creates mutex with name "{b59ea4fc-7bc4-2dca-f7bf-d3e31efaff7e}".
- (Process #5) explorer.exe creates mutex with name "{aadb65f8-5aae-bb01-afa3-e769be98792f}".
- (Process #5) explorer.exe creates mutex with name "{263a71f1-3660-151b-0400-e3e3dd0ac0df}".
- (Process #5) explorer.exe creates mutex with name "{dba39a74-6851-509b-e2ec-80b7cc41ee6e}".
- (Process #5) explorer.exe creates mutex with name "{a1a3a205-7ecc-cf7b-12fe-4a103bd3e557}".
- (Process #5) explorer.exe creates mutex with name "{a0997771-1481-fafe-76ec-19caa3547787}".
- (Process #5) explorer.exe creates mutex with name "{dd818112-662e-0206-998c-108a85e1084c}".
- (Process #5) explorer.exe creates mutex with name "{cdac0f5b-6ff9-2ff1-eae0-d785678bb550}".
- (Process #5) explorer.exe creates mutex with name "{fecd5106-17e6-321f-476e-6a34b4725aa9}".
- (Process #5) explorer.exe creates mutex with name "{2dd6aed0-8b49-036d-b43d-843d4804093d}".
- (Process #5) explorer.exe creates mutex with name "{dbe86ec5-1230-23f0-4ccf-a65084617422}".
- (Process #5) explorer.exe creates mutex with name "{a635538e-62a3-67ec-a1d5-5d33d77d7c6e}".
- (Process #5) explorer.exe creates mutex with name "{10d2eaf7-27bb-91e1-afe9-c544f8613c54}".
- (Process #5) explorer.exe creates mutex with name "{28d724ec-22da-95bd-9f65-2e17dc8aecd0}".
- (Process #5) explorer.exe creates mutex with name "{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}".
- (Process #5) explorer.exe creates mutex with name "{a3dce688-6117-3ea3-fbbd-1defec717462}".
- (Process #5) explorer.exe creates mutex with name "{2835d429-2a00-0fb6-5c11-3e59c353659a}".
- (Process #5) explorer.exe creates mutex with name "{168ee11b-299f-6d76-b48f-88a65a4a58ba}".
- (Process #5) explorer.exe creates mutex with name "{7e5d2be3-0634-bb96-47ee-3083eb9bef97}".
- (Process #5) explorer.exe creates mutex with name "{60d53e50-c02a-fd11-36ca-0f91b9ec3738}".
- (Process #5) explorer.exe creates mutex with name "{1c9185e1-04c2-f876-90d9-8e799aee9797}".
- (Process #5) explorer.exe creates mutex with name "{f2a9beb0-e471-4dcd-d679-d29b68da63e0}".
- (Process #5) explorer.exe creates mutex with name "{a1090343-24c0-16c8-e547-9b6fb6d0166b}".
- (Process #5) explorer.exe creates mutex with name "{822894df-44a8-add7-294a-a446b174fbef}".
- (Process #5) explorer.exe creates mutex with name "{c42c174a-1be2-3a72-8667-a20ecc356e75}".
- (Process #5) explorer.exe creates mutex with name "{fcd273ea-02e9-5a8a-4a8b-7848d0895772}".
- (Process #5) explorer.exe creates mutex with name "{61cf2e75-7825-7e06-d929-f4f508b6f8c8}".
- (Process #5) explorer.exe creates mutex with name "{64627196-149f-ef44-f53e-7c34ad6e86ef}".
- (Process #5) explorer.exe creates mutex with name "{fef37f2e-4f56-9012-852a-59484b5fed7e}".
- (Process #5) explorer.exe creates mutex with name "{53be0c1d-6845-1fb9-9acf-69f1a3b7921b}".
- (Process #5) explorer.exe creates mutex with name "{8d859e8a-cd3c-3ac0-0451-ab11d6131acd}".
- (Process #5) explorer.exe creates mutex with name "{74cce2f8-af0d-c651-67a5-40d9130ec8dd}".
- (Process #5) explorer.exe creates mutex with name "{985469d5-c515-9b89-778a-6ffac4b9b8b4}".
- (Process #5) explorer.exe creates mutex with name "{dcc64ab4-43e3-3cb6-4e2a-9ca7d2b55758}".
- (Process #5) explorer.exe creates mutex with name "{5448aec8-10c2-e89b-6654-58a5f2a67f29}".
- (Process #5) explorer.exe creates mutex with name "{149f3d26-9400-88ff-5a28-2eff57c7e377}".
- (Process #5) explorer.exe creates mutex with name "{1bd64204-83e2-f6c8-6072-dc275733e911}".
- (Process #5) explorer.exe creates mutex with name "{ca10318d-d43e-d7f4-54ae-2e3b621216b5}".
- (Process #5) explorer.exe creates mutex with name "{dc1a7d14-4f5e-2174-ea64-bc3105102601}".
- (Process #5) explorer.exe creates mutex with name "{c7b2b8d2-8a6f-fe86-7e84-189671066b5d}".
- (Process #5) explorer.exe creates mutex with name "{59815482-6971-add8-40ce-a9f16f7574f4}".
- (Process #5) explorer.exe creates mutex with name "{18f3145b-23c3-2dd9-e680-9519534e72bf}".
- (Process #5) explorer.exe creates mutex with name "{fdb83606-4ef7-5a58-ba85-687f05c6dbcf}".
- (Process #5) explorer.exe creates mutex with name "{e56de5ae-6e94-b096-e03b-36d0cec5d3a6}".
- (Process #5) explorer.exe creates mutex with name "{6444f54d-a127-9551-45b8-6703303ab458}".
- (Process #5) explorer.exe creates mutex with name "{205d5366-f15a-2f49-d587-d63f683a4897}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #2) mvjgboit.exe reads from (process #5) explorer.exe. • (Process #9) mvjgboit.exe reads from (process #5) explorer.exe.			
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-
	• (Process #5) explorer.exe hides 3526 bytes in "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder\{6BE941D2-F512-6EA8-ECC9-35243548878A}".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #5) explorer.exe resolves 26 API functions by name.			

Mitre ATT&CK Matrix

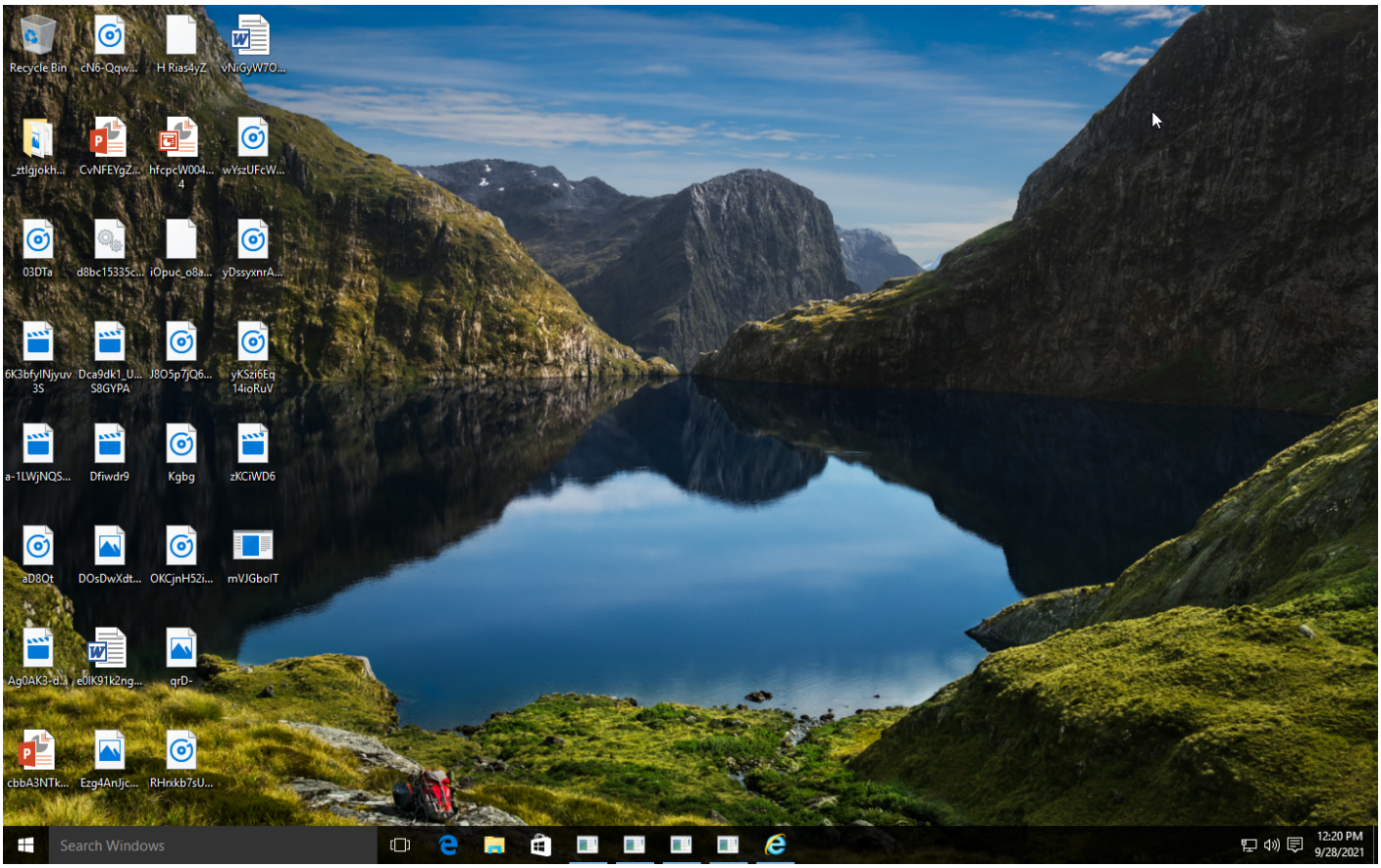
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1112 Modify Registry	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1045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

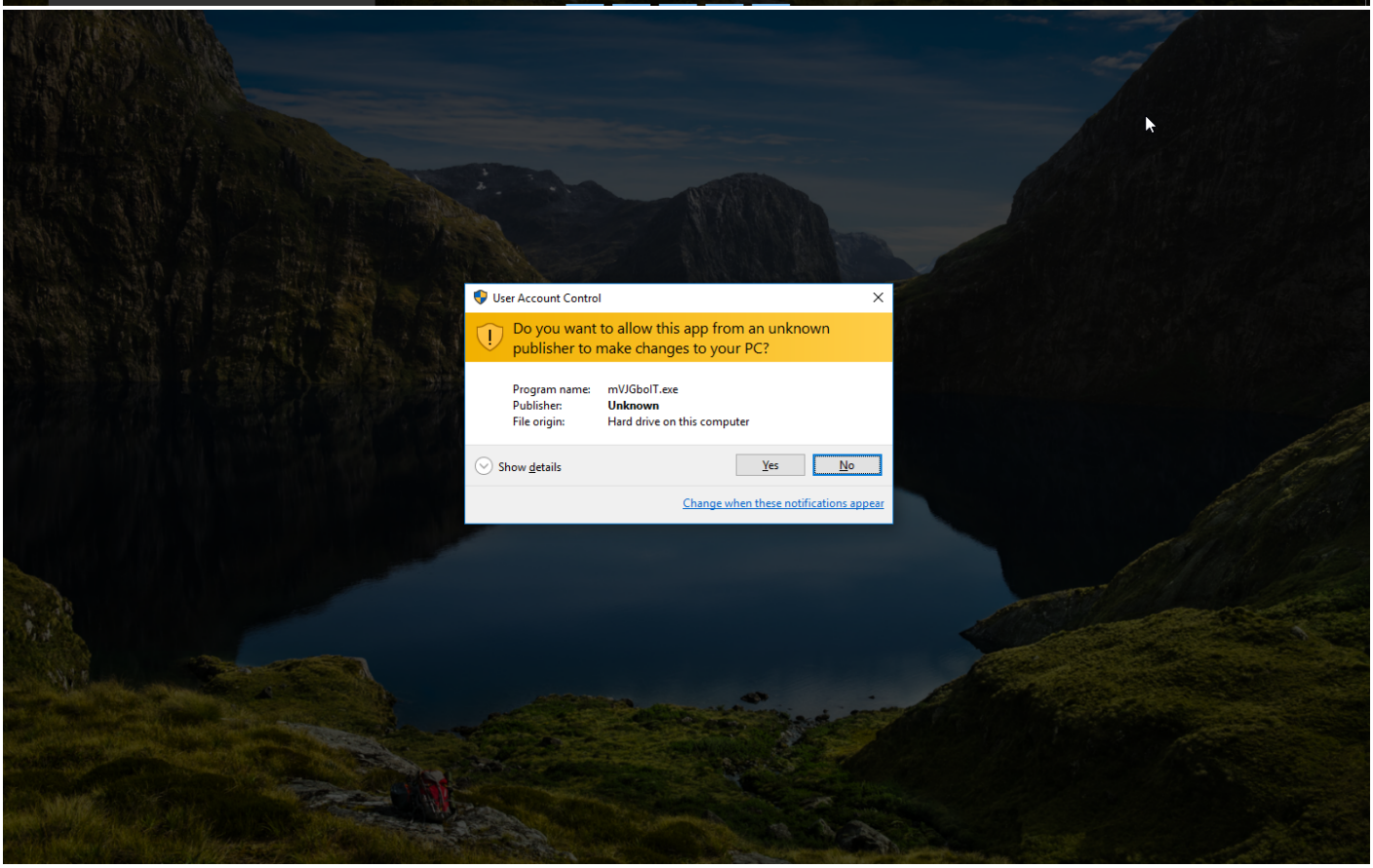
Sample Information

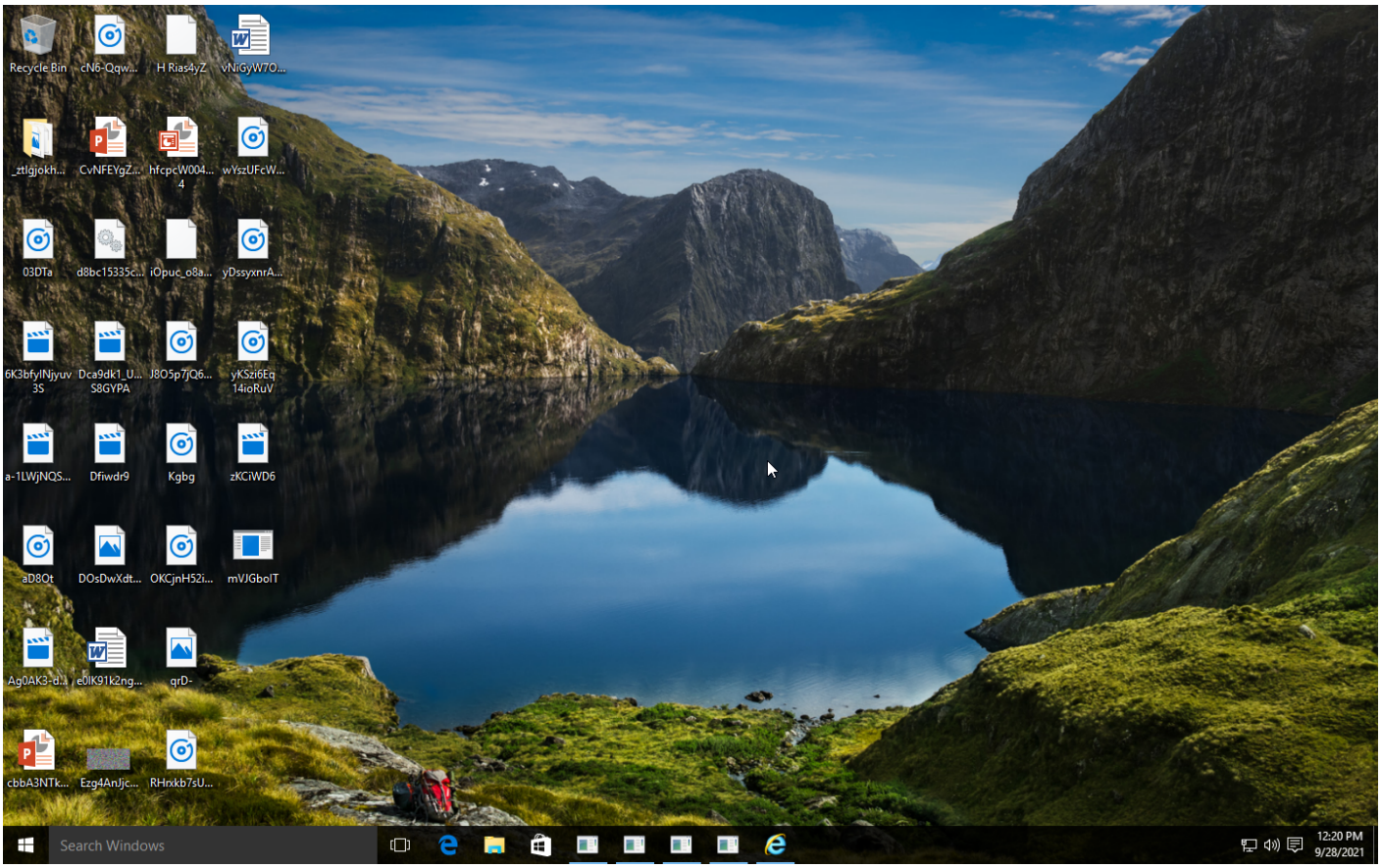
ID	#969274
MD5	c10ee36fe08388fce375f320660bc91c
SHA1	6477666e70f87ff53040e98f324660a5167eb4f4
SHA256	d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3
SSDeep	12288:xVl0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ17:AfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll
File Size	2044.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:19 (UTC+2)
Analysis Duration	00:03:46
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	15
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
cN6-Qqw...
H Rias4yZ
vNiGyW7O...
_ztlgjokh...
CvNFEYgZ...
hfcpcW004...
4
wYszUFcW...
03DTa
d8bc15335c...
iOpuc_o8a...
yDssyxnrA...
6K3bfyINjyuv
3S
Dca9dk1_U...
S8GYPA
J8O5p7jQ6...
yKSzi6Eq
14ioRuV
a-1LWjNQS...
Dfiwdr9
Kgbg
zKCiWD6
aD8Qt
DOsDwXdt...
OKCjnH52i...
mVJGboIT
Ag0AK3-d...
e0lK91k2ng...
qrD-
cbbA3NTk...
Ezg4AnJjc...
RHnxkb7sU...
Search Windows
12:20 PM
9/28/2021


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


Recycle Bin
cN6-Qqw...
H Rias4yZ
vNiGyW7O...
_ztlgjokh...
CvNFEYgZ...
hfcpcW004...
4
wYszUFcW...
03DTa
d8bc15335c...
iOpuc_o8a...
yDssyxnrA...
6K3bfyINjyuv
3S
Dca9dk1_U...
S8GYPA
J8O5p7jQ6...
yKSzi6Eq
14ioRuV
a-1LWjNQS...
Dfiwdr9
Kgbg
zKCiWD6
aD8Qt
DOsDwXdt...
OKCjnH52i...
mVJGboIT
Ag0AK3-d...
e0lK91k2ng...
qrD-
cbbA3NTk...
Ezg4AnJjc...
RHnxkb7sU...
Search Windows
12:20 PM
9/28/2021

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

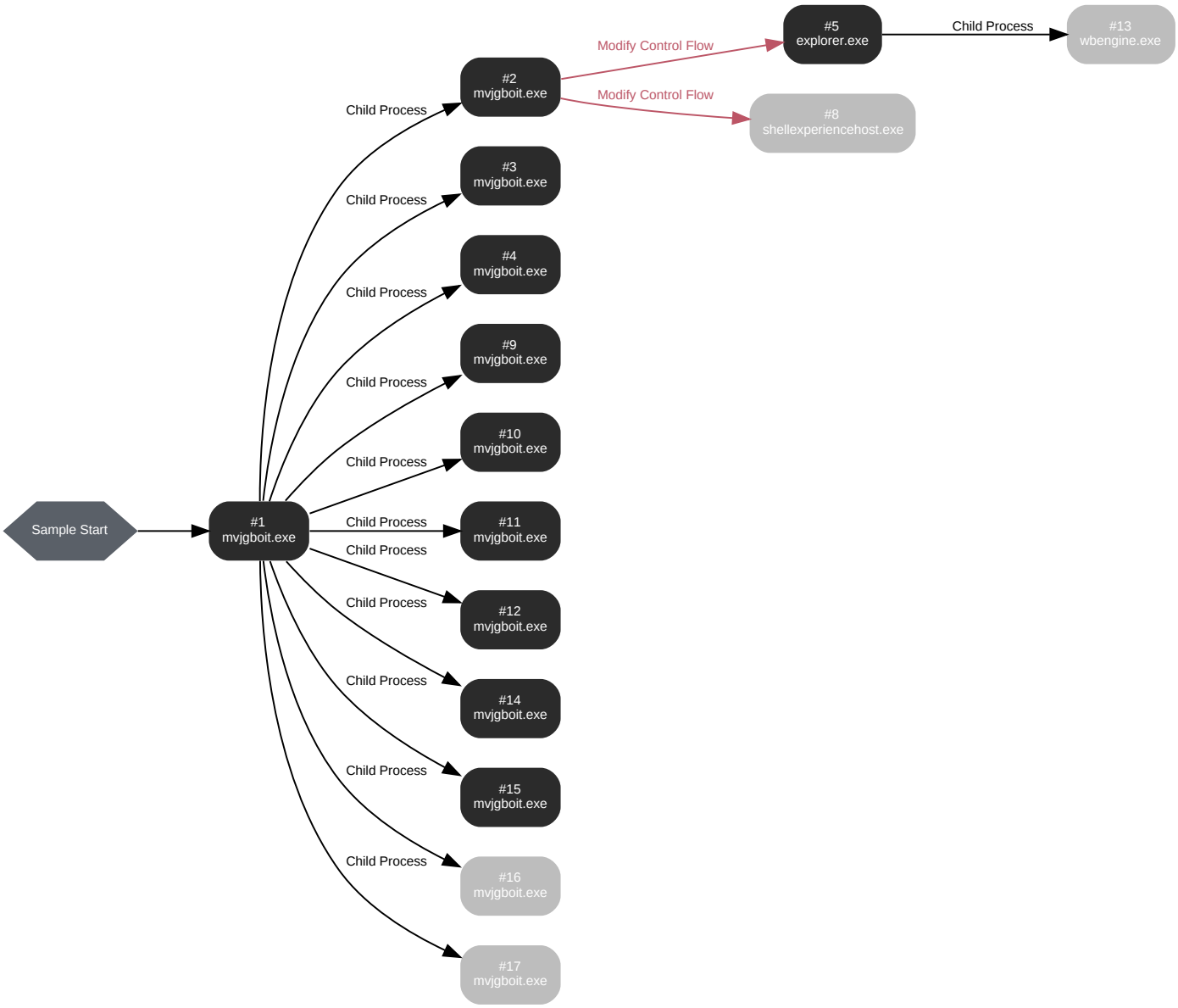
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: mvjgboit.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmphbisknkw" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 65718, Reason: Analysis Target
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	226.56s
Return Code	Unknown
PID	1940
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	11

Process #2: mvjgboit.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#1
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 86868, Reason: Child Process
Unmonitor End Time	End Time: 219564, Reason: Terminated
Monitor duration	132.70s
Return Code	0
PID	2480
Parent PID	1940
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	35
Environment	2
Registry	768
Mutex	6
Process	2
-	52
-	32
-	128

Process #3: mvjgboit.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#10
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 88959, Reason: Child Process
Unmonitor End Time	End Time: 97117, Reason: Terminated
Monitor duration	8.16s
Return Code	0
PID	1608
Parent PID	1940
Bitness	64 Bit

Host Behavior

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

Process #4: mvjgboit.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#100
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 91362, Reason: Child Process
Unmonitor End Time	End Time: 100486, Reason: Terminated
Monitor duration	9.12s
Return Code	0
PID	176
Parent PID	1940
Bitness	64 Bit

Host Behavior

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

Process #5: explorer.exe

ID	5
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 94029, Reason: Injection
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	198.25s
Return Code	Unknown
PID	1636
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (74)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x668	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x690	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x694	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x6ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x6b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x6b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x6b8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x6bc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x6dc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x6e8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x71c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x734	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x73c	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x74c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x798	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x7a8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x7b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x7d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x7ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x7f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x460	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x83c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x954	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x95c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x9c0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xbec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x4c4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x4ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x8b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x984	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x97c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xa20	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xe58	0x7ffc5f8b4f00(140721911451392)	-	✗	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xfd8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x2f8	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xc98	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xcb8	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xa30	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xd6c	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xd60	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x780	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0xf48	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x12a4	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x12b0	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x12d4	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x12dc	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5f8bb580(140721911477632)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5f8bb580(140721947763 2)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe	0x410 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✘
-	1.42 KB	fafed4e96b3d511f9a56a5b6888b6a34fefad41c958d70d2bb71c37e40a01f93	✘
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✘
-	1.42 KB	9b8527cefd77bbcd8decace90f8b8af7016e228b8e9bc95fc30354841da67a57	✘

Host Behavior

Type	Count
Module	48

Type	Count
File	212
System	418
Process	102
Registry	23638
Environment	2
-	20
Mutex	1505

Process #8: shellexperiencehost.exe

ID	8
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: 95341, Reason: Injection
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	196.94s
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\mvjgboit.exe	0x410 / 0x428	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Process #9: mvjgboit.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#101
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 95509, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	196.77s
Return Code	Unknown
PID	2340
Parent PID	1940
Bitness	64 Bit

Host Behavior

Type	Count
Module	37
File	118
System	7
Environment	2
Registry	788
Mutex	5
Process	2
-	2
-	1

Process #10: mvjgboit.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#102
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 97495, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	194.78s
Return Code	Unknown
PID	2596
Parent PID	1940
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	226
Mutex	3

Process #11: mvjgboit.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#103
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100287, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	191.99s
Return Code	Unknown
PID	4824
Parent PID	1940
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #12: mvjgboit.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#104
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 159792, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	132.49s
Return Code	Unknown
PID	2420
Parent PID	1940
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #13: wbengine.exe

ID	13
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: 191359, Reason: Child Process
Unmonitor End Time	End Time: 207611, Reason: Terminated
Monitor duration	16.25s
Return Code	0
PID	3164
Parent PID	1636
Bitness	64 Bit

Process #14: mvjgboit.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#105
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 215203, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	77.08s
Return Code	Unknown
PID	3332
Parent PID	1940
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	112
Environment	1

Process #15: mvjgboit.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#106
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 227050, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	65.23s
Return Code	Unknown
PID	2880
Parent PID	1940
Bitness	64 Bit

Host Behavior

Type	Count
Module	16
File	112
Environment	1

Process #16: mvjgboit.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#107
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 250059, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	42.22s
Return Code	Unknown
PID	2968
Parent PID	1940
Bitness	64 Bit

Process #17: mvjgboit.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\mvjgboit.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll" /fn_id=#108
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 288213, Reason: Child Process
Unmonitor End Time	End Time: 292280, Reason: Terminated by Timeout
Monitor duration	4.07s
Return Code	Unknown
PID	3676
Parent PID	1940
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3	C:\Users\RDhJ0CNFevzX\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll, C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll	Sample File	2044.00 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
fafed4e96b3d511f9a56a5b6888b6a34fefad41c958d70d2bb71c37e40a01f93	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
9b8527cefd77bbcd8decace90f8b8af7016e228b8e9bc95fc30354841da67a57	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\mVJGbolT.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmphbisknkw	Accessed File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.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\Common Files\outlook.exe	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\nst2JnM1	Accessed File	Create, Access	CLEAN
C:\Windows\system32\SPP.dll	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\system\msmapi\1033\msmapi32.dll	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

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	mvjgboit.exe	CLEAN
{20974a93-a551-df17-8967-748358091d34}	access	mvjgboit.exe	CLEAN
{298ddcca-efe5-2f07-cbb5-e91e37797537}	access	explorer.exe	CLEAN
{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}	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
{d439f686-d570-7182-3906-1e2d175d1088}	access	explorer.exe	CLEAN
{82761896-27cc-43ce-e454-25a5cf66d6e1}	access	explorer.exe	CLEAN
{05747a50-933e-c4fd-7a3d-44fed7350072}	access	explorer.exe	CLEAN
{b59ea4fc-7bc4-2dca-f7bf-d3e31efaff7e}	access	explorer.exe	CLEAN
{aadb65f8-5aae-bb01-afa3-e769be98792f}	access	explorer.exe	CLEAN
{263a71f1-3660-151b-0400-e3e3dd0ac0df}	access	explorer.exe	CLEAN
{dba39a74-6851-509b-e2ec-80b7cc41ee6e}	access	explorer.exe	CLEAN
{a1a3a205-7ecc-cf7b-12fe-4a103bd3e557}	access	explorer.exe	CLEAN
{a0997771-1481-fafe-76ec-19caa3547787}	access	explorer.exe	CLEAN
{dd818112-662e-0206-998c-108a85e1084c}	access	explorer.exe	CLEAN
{cdac0f5b-6ff9-2ff1-eae0-d785678bb550}	access	explorer.exe	CLEAN
{fecd5106-17e6-321f-476e-6a34b4725aa9}	access	explorer.exe	CLEAN
{2dd6aed0-8b49-036d-b43d-843d4804093d}	access	explorer.exe	CLEAN
{dbe86ec5-1230-23f0-4ccf-a65084617422}	access	explorer.exe	CLEAN
{a635538e-62a3-67ec-a1d5-5d33d77d7c6e}	access	explorer.exe	CLEAN
{10d2eaf7-27bb-91e1-afe9-c544f8613c54}	access	explorer.exe	CLEAN
{28d724ec-22da-95bd-9f65-2e17dc8aecd0}	access	explorer.exe	CLEAN
{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}	access	explorer.exe	CLEAN
{a3dce688-6117-3ea3-fbbd-1defec717462}	access	explorer.exe	CLEAN
{2835d429-2a00-0fb6-5c11-3e59c353659a}	access	explorer.exe	CLEAN
{168ee11b-299f-6d76-b48f-88a65a4a58ba}	access	explorer.exe	CLEAN
{7e5d2be3-0634-bb96-47ee-3083eb9bef97}	access	explorer.exe	CLEAN
{60d53e50-c02a-fd11-36ca-0f91b9ec3738}	access	explorer.exe	CLEAN
{1c9185e1-04c2-f876-90d9-8e799aee9797}	access	explorer.exe	CLEAN
{f2a9beb0-e471-4dcd-d679-d29b68da63e0}	access	explorer.exe	CLEAN
{a1090343-24c0-16c8-e547-9b6fb6d0166b}	access	explorer.exe	CLEAN
{822894df-44a8-add7-294a-a446b174fbef}	access	explorer.exe	CLEAN
{c42c174a-1be2-3a72-8667-a20ecc356e75}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{fcd273ea-02e9-5a8a-4a8b-7848d0895772}	access	explorer.exe	CLEAN
{61cf2e75-7825-7e06-d929-f4f508b6f8c8}	access	explorer.exe	CLEAN
{64627196-149f-ef44-f53e-7c34ad6e86ef}	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
{74cce2f8-af0d-c651-67a5-40d9130ec8dd}	access	explorer.exe	CLEAN
{985469d5-c515-9b89-778a-6ffac4b9b8b4}	access	explorer.exe	CLEAN
{dcc64ab4-43e3-3cb6-4e2a-9ca7d2b55758}	access	explorer.exe	CLEAN
{5448aec8-10c2-e89b-6654-58a5f2a67f29}	access	explorer.exe	CLEAN
{149f3d26-9400-88ff-5a28-2eff57c7e377}	access	explorer.exe	CLEAN
{1bd64204-83e2-f6c8-6072-dc275733e911}	access	explorer.exe	CLEAN
{ca10318d-d43e-d7f4-54ae-2e3b621216b5}	access	explorer.exe	CLEAN
{dc1a7d14-4f5e-2174-ea64-bc3105102601}	access	explorer.exe	CLEAN
{c7b2b8d2-8a6f-fe86-7e84-189671066b5d}	access	explorer.exe	CLEAN
{59815482-6971-add8-40ce-a9f16f7574f4}	access	explorer.exe	CLEAN
{18f3145b-23c3-2dd9-e680-9519534e72bf}	access	explorer.exe	CLEAN
{fdb83606-4ef7-5a58-ba85-687f05c6dbcf}	access	explorer.exe	CLEAN
{e56de5ae-6e94-b096-e03b-36d0cec5d3a6}	access	explorer.exe	CLEAN
{6444f54d-a127-9551-45b8-6703303ab458}	access	explorer.exe	CLEAN
{205d5366-f15a-2f49-d587-0637683a4897}	access	explorer.exe	CLEAN
{183233cf-2be9-e31f-da70-4a704ab09379}	access	explorer.exe	CLEAN
{e1e9d0d6-b4c6-d504-151c-66183448bd0b}	access	explorer.exe	CLEAN
{8f55ed91-4498-fb0a-46ef-812635b9db60}	access	explorer.exe	CLEAN
{d06416aa-46f7-f2c8-b304-9c261b189ee2}	access	explorer.exe	CLEAN
{4896a380-704f-d883-707a-563b4d24d766}	access	explorer.exe	CLEAN
{4a41b3ad-3965-1b5b-a8df-3adb417679c2}	access	explorer.exe	CLEAN
{7fc82242-34f1-e1df-ba3b-ade8e9d124e8}	access	explorer.exe	CLEAN
{7cf0b6ac-dddc-2486-71ab-c5ee525ce2e5}	access	explorer.exe	CLEAN
{15178be2-63c2-e2cf-38a4-dfb2768aee0d}	access	explorer.exe	CLEAN
{c0a8f40a-1d01-5acb-285e-9fc620d2f0a4}	access	explorer.exe	CLEAN
{238ff016-c2ab-294d-d37f-36516ac88376}	access	explorer.exe	CLEAN
{d42d64f2-dd7c-5da5-5a4d-e151c2207325}	access	explorer.exe	CLEAN
{7dd56f30-d26e-904c-dc7f-63812c4c902b}	access	explorer.exe	CLEAN
{7f77cb8c-5ab9-982b-0712-7770af056c0b}	access	explorer.exe	CLEAN
{88c6c115-ad43-6a69-ede9-b100fed958ff}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{3b2d7b05-41ad-ff52-c90f-8be049d4e8ff}	access	explorer.exe	CLEAN
{f3d66484-fbd0-fc9d-4667-437e9739f284}	access	explorer.exe	CLEAN
{3b7ec73b-c511-a202-2a05-a90bb554c574}	access	explorer.exe	CLEAN
{b6f8d67d-ea71-2491-e114-d996976ba3af}	access	explorer.exe	CLEAN
{b419202c-7566-1987-fa50-e6543f7b60e5}	access	explorer.exe	CLEAN
{8c03a793-72a0-96c8-f9a3-ea05ea731628}	access	explorer.exe	CLEAN
{b7e14e14-6e1c-1cbc-1376-adc5708cb5bf}	access	explorer.exe	CLEAN
{17b2b7f2-2210-b314-72df-d45c353fe112}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	create, access	mvjgboit.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE	access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	mvjgboit.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	read, access	mvjgboit.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	mvjgboit.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EnableLUA	read, access	mvjgboit.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ConsentPromptBehaviorAdmin	read, access	mvjgboit.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PromptOnSecureDesktop	read, access	mvjgboit.exe, explorer.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
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

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{026F08C5-341A-9406-8117-0A9B26B9732B}\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\Explorer\CLSID\{1384CAC3-17AC-E069-EB5C-4E613FCC6FE4}\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\{5E441BBB-4FA0-7A47-C898-77D45B377F36}\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\{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	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder\{C9EC32E3-290C-1132-3432-855BD012355D}	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{D28FAF2B-023A-F47D-AF27-9A3EB5F18B02}	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4D2056E1-92AF-EC5C-2615-AA80579018DA}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\InstallDate	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{37B8F9C7-03FB-3253-8781-2517C99D7C00}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayName	read, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{9016000-008F-0000-1000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{9016000-008F-0000-1000-0000000FF1CE}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{9016000-008F-0000-1000-0000000FF1CE}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{929FBD26-9020-399B-9A7A-751D61F0B942}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	read, access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{EEA66967-97E2-4561-A999-5C22E3CDE428}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayVersion	read, access	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

Registry Key	Operations	Parent Process Name	Verdict
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\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	read, access	mvjgboit.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	read, access	mvjgboit.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
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

Registry Key	Operations	Parent Process Name	Verdict
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
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

Registry Key	Operations	Parent Process Name	Verdict
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
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	read, access	explorer.exe	CLEAN
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	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail	read, access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook\DllPathEx	read, access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder\{6BE941D2-F512-6EA8-ECC9-35243548878A}	write, access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmphbisknkw" /s	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#1	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#10	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#100	CLEAN
shellexperiencehost.exe	"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#101	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#102	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#103	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#104	CLEAN
wbengine.exe	C:\Windows\system32\wbengine.exe	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#105	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#106	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#107	CLEAN
mvjgboit.exe	"C:\Users\RDhJ0CNFevzX\Desktop\mVJGboIT.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a094401767692623 6da3.exe.dll" /fn_id=#108	CLEAN

YARA / AV

Antivirus (5)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	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