MALICIOUS

Classifications: Spyware

Threat Names: Trojan.GenericKDZ.75562

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll**
ID	#969334
MD5	c50f692a715db805e68e9655ff6a9ab2
SHA1	229b257301ed99d518364afd22c4276daa5b3d20
SHA256	ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033
File Size	1084.00 KB
Report Created	2021-09-28 14:36 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 116 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) owfwyl.exe alters context of (process #7) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.75562". • Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\VERSION.dll as "Trojan.GenericKDZ.75562". • Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\FVEWIZ.dll as "Trojan.GenericKDZ.75562". • Built-in AV detected a memory dump of (process #7) explorer.exe as "Trojan.GenericKDZ.75562".			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #7) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #7) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #7) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\yfh\dvdupgrd.exe".			
1/5	Discovery	Reads system data	12	-
	• (Process #2) owfwyl.exe reads the Windows installation date from registry. • (Process #3) owfwyl.exe reads the Windows installation date from registry. • (Process #4) owfwyl.exe reads the Windows installation date from registry. • (Process #5) owfwyl.exe reads the Windows installation date from registry. • (Process #6) owfwyl.exe reads the Windows installation date from registry. • (Process #7) explorer.exe reads the Windows installation date from registry. • (Process #8) owfwyl.exe reads the Windows installation date from registry. • (Process #14) owfwyl.exe reads the Windows installation date from registry. • (Process #15) owfwyl.exe reads the Windows installation date from registry. • (Process #21) owfwyl.exe reads the Windows installation date from registry. • (Process #22) owfwyl.exe reads the Windows installation date from registry. • (Process #24) owfwyl.exe reads the Windows installation date from registry.			
1/5	Mutex	Creates mutex	83	-

- (Process #2) owfwyl.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{20974a93-a551-df17-8967-748358091d34}".
- (Process #7) explorer.exe creates mutex with name "0".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{389fe546-d029-33a7-6305-2ca1cede0678}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{e8b6fe55-d858-d6e4-ef99-a80106642ab4}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{03b2a674-5295-21d6-da36-fc13faee0e98}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{d439f686-d570-7182-3906-1e2d175d1088}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{27dcbb6c-b6b1-b5c0-be37-17f0c21939fa}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{e33e87ed-6b47-d015-096b-848dadf4080b}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{9a19a950-2459-434e-9c59-a982629f26dd}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{9666bd67-64c1-5269-b5bb-b889b9fea609}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{af33e402-09cc-a6cc-e5da-4bf4b32d667d}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{4f8955dd-c023-639c-9d54-a0e485c7012a}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{201ba18c-1db5-3773-b8bd-628af5f5deba}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{263ffa84-4558-3562-0b37-9f47f49f6a79}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{71dba081-a28d-be08-fa55-bf22ddb35cb9}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{9a933d33-e195-3556-503e-c5c0a921498c}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{05747a50-933e-c4fd-7a3d-44fed7350072}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{153471c9-9d0a-7104-5275-71ac64b2065e}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{4236a99f-3514-853f-daf5-e82e3c1b0317}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{e79e5240-aa8e-0f63-d6a1-8a07649cdc90}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{38e7db7a-75ef-8cef-8130-9e11aa96557f}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{d721bcec-0f69-129d-7108-0656474a0b0a}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{dbe86ec5-1230-23f0-4ccf-a65084617422}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{44869c43-a49e-bce0-8271-dbb71cb12c79}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{0ae6b514-0674-d8a5-a624-343329b398d5}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{0eb707bd-e520-a26e-500a-bbb6baa1f707}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{b386415a-cf2b-b133-badc-6ec70cc36294}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{14fe886f-f5af-a8a1-1712-9042f79a83dc}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{8a4d728e-1a95-daee-efb3-d49c856d805e}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{a3dce688-6117-3ea3-fbbd-1defec717462}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{a2e3a1c4-1044-26ac-2fa3-30ee391a0657}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{7cc6ae5f-2c94-8c18-e20d-28bccdbd00c3}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{b4de3d46-efec-a98a-f706-8745d35ed7f2}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{d1575404-3469-2df0-db6b-3bcf4439344f}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{3c33918e-27da-9f35-2586-b9f012933134}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{6c570128-9202-fd64-daa4-72143d141e8a}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{822894df-44a8-add7-294a-a446b174fbef}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{6fe25233-3c10-d1be-fd07-8467d220e8d6}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{bc97cda8-f351-7a60-8d28-728a4afb7aec}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{bb0cabed-1ffc-1a16-fd9e-e02cab733680}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{fcd273ea-02e9-5a8a-4a8b-7848d0895772}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{e28905fd-15de-b796-44d3-7a7876237780}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ede07ea5-2e12-7d74-5185-75bb288d7c70}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{fef37f2e-4f56-9012-852a-59484b5fed7e}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{ad5d057c-012c-b276-1470-f24990f0a7eb}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{8d859e8a-cd3c-3ac0-0451-ab11d6131acd}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{1439a690-60db-c7ba-74ad-63f3b3396ce4}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{d65528a1-3ef5-a115-0995-914008bd9a62}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{71bb662b-e609-45a6-82d2-d177df9706bc}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{5448aec8-10c2-e89b-6654-58a5f2a67f29}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{946d3aec-f0be-460d-b2db-c49c07ac46ae}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{b894408f-30d6-e44c-93a0-15251ca9bab4}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{497f1ddf-1131-8869-1c4d-19bc3c1533f0}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{867eeaaa-9095-7d70-5174-9d6e7d728884}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{1da4e1aa-6eb1-9190-a173-cc15c94ce697}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{f9e73e00-f006-b49c-1dcf-ff85215b0c68}".
- (Process #7) explorer.exe creates mutex with name "\Sessions\1\BaseNamedObjects\{6a4fe6c6-ce4d-124b-9924-4da205e310d4}".

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	6	-

- (Process #7) explorer.exe starts C:\Windows\system32\Magnify.exe with a hidden window.
- (Process #7) explorer.exe starts C:\Windows\system32\ComputerDefaults.exe with a hidden window.
- (Process #7) explorer.exe starts (process #19) dvdupgrd.exe with a hidden window.
- (Process #7) explorer.exe starts (process #20) dvdupgrd.exe with a hidden window.
- (Process #7) explorer.exe starts (process #28) bitlockerwizard.exe with a hidden window.
- (Process #7) explorer.exe starts C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe with a hidden window.

Score	Category	Operation	Count	Classification
1/5	Execution	Drops PE file	4	-

- (Process #7) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\VERSION.dll".
- (Process #7) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\FVEWIZ.dll".
- (Process #7) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe".
- (Process #7) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe".

Score	Category	Operation	Count	Classification
1/5	Execution	Executes dropped PE file	2	-

- Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe".
- Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe".

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	2	-

- File "C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe" is a known clean file.
- File "C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe" is a known clean file.

Mitre ATT&CK Matrix

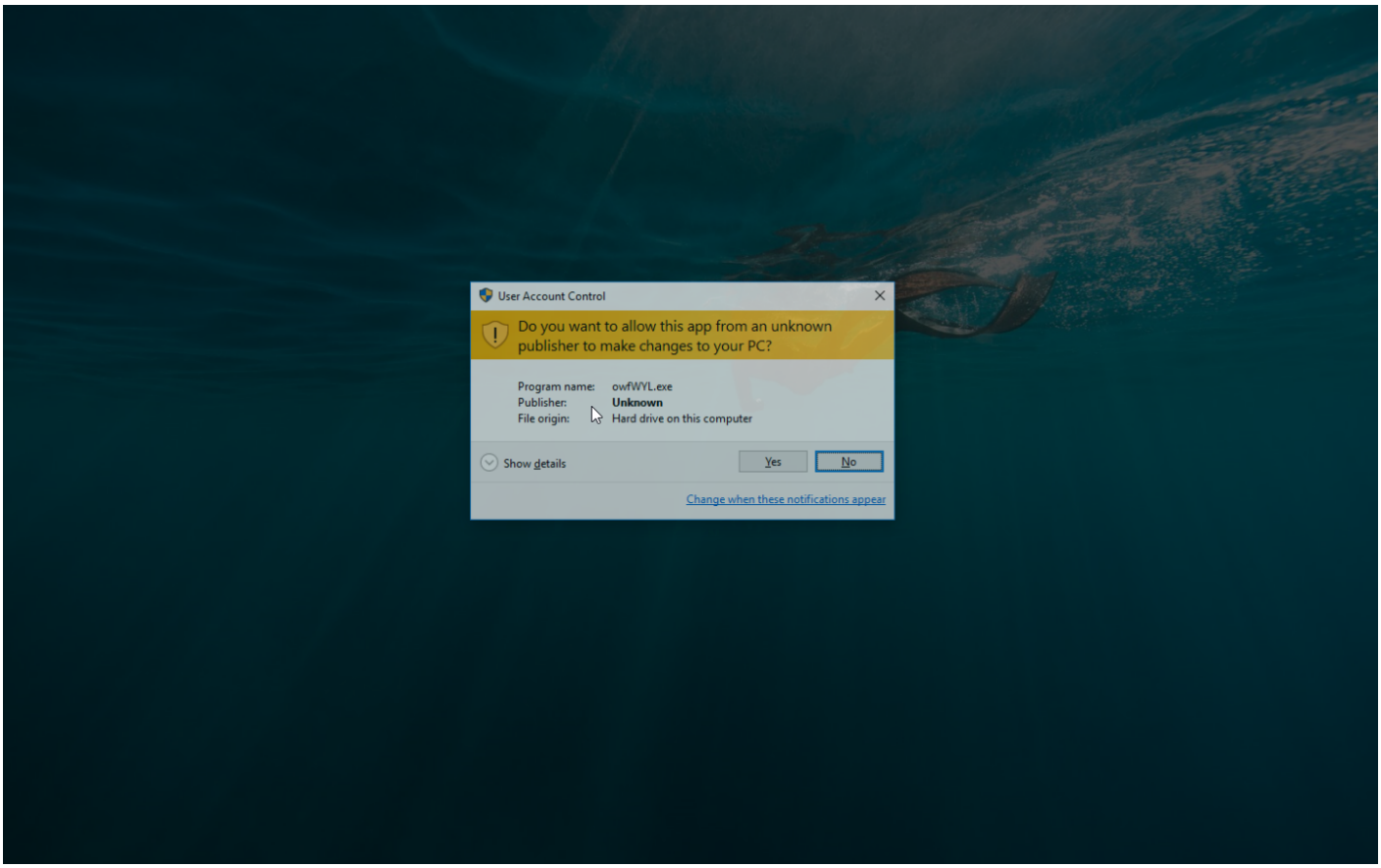
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
						#T1012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

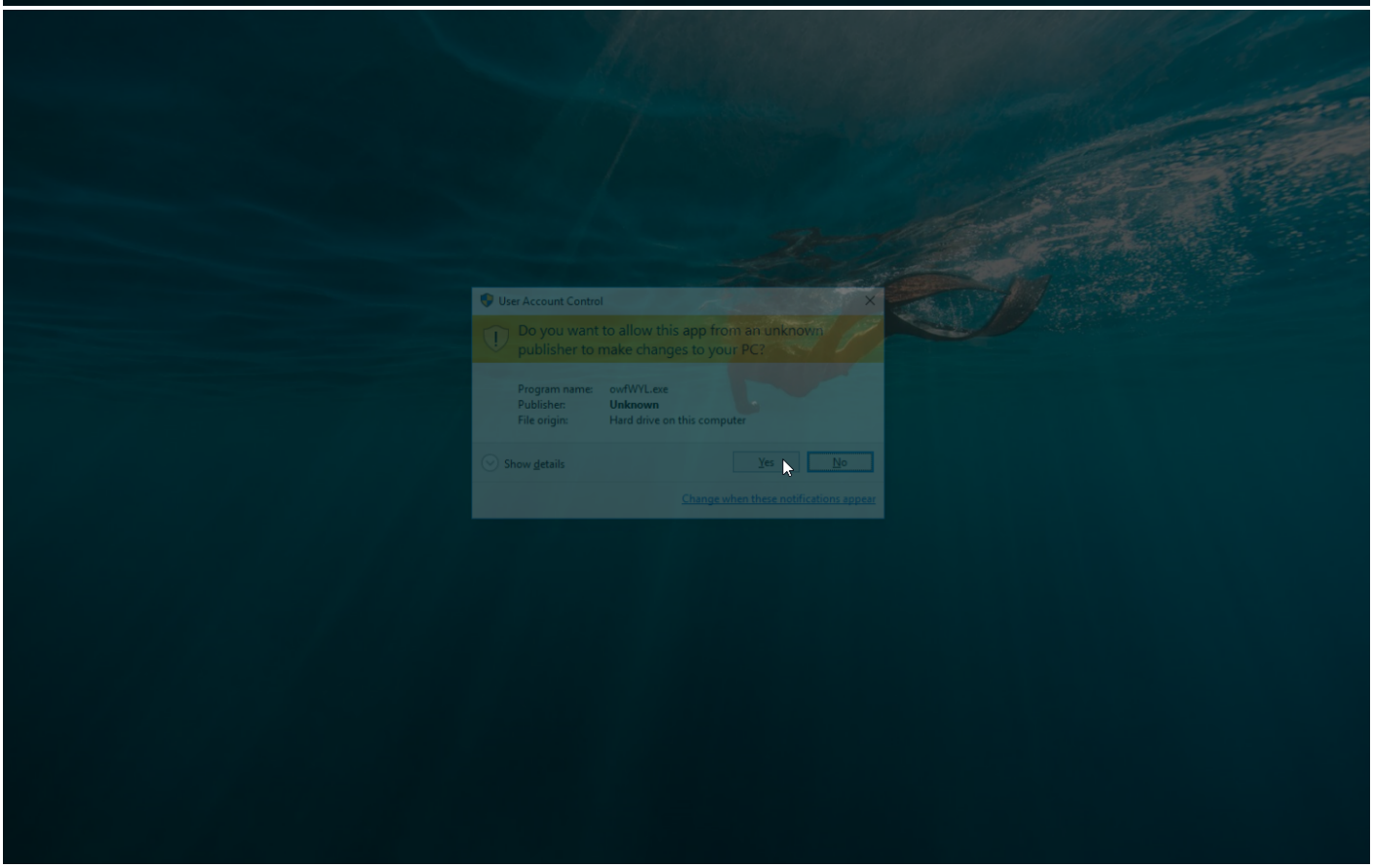
Sample Information

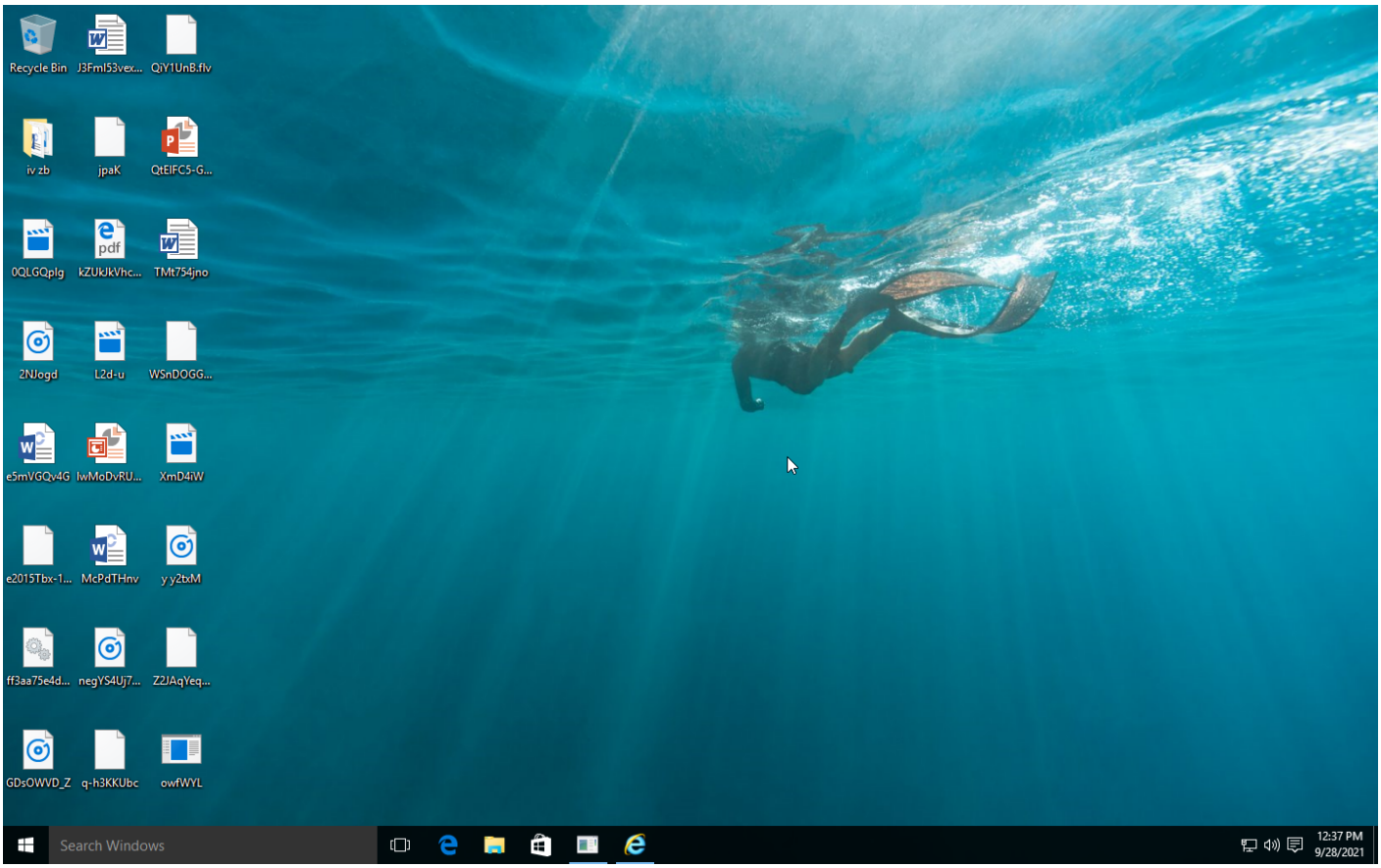
ID	#969334
MD5	c50f692a715db805e68e9655ff6a9ab2
SHA1	229b257301ed99d518364afd22c4276daa5b3d20
SHA256	ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033
SSDeep	12288:4dMIwS97wJs6tSKDXEabXaC+jhc1S8XXk7CZzHsZH9dq0T:SMIJxSDX3bqjhcfHk7MzH6z
ImpHash	c6b4c2eec8a93016c63563421e15f011
File Name	ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll
File Size	1084.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:36 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	28
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


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


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


Recycle Bin
J3FmI53vex...
QiY1UnB.flv
iv zb
jpaK
QtEIFC5-G...
0QLGQplg
kZUkJkVhc...
TMt754jno
2NJogd
L2d-u
WSnDOGG...
e5mVGQv4G
lwMoDvRU...
XmD4iW
e2015Tbx-1...
McPdTHnv
y y2txM
ff3aa75e4d...
negYS4Uj7...
Z2JAqYeq...
GDsOWVD_Z
q-h3KKUbc
owfWYL
Search Windows
12:37 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

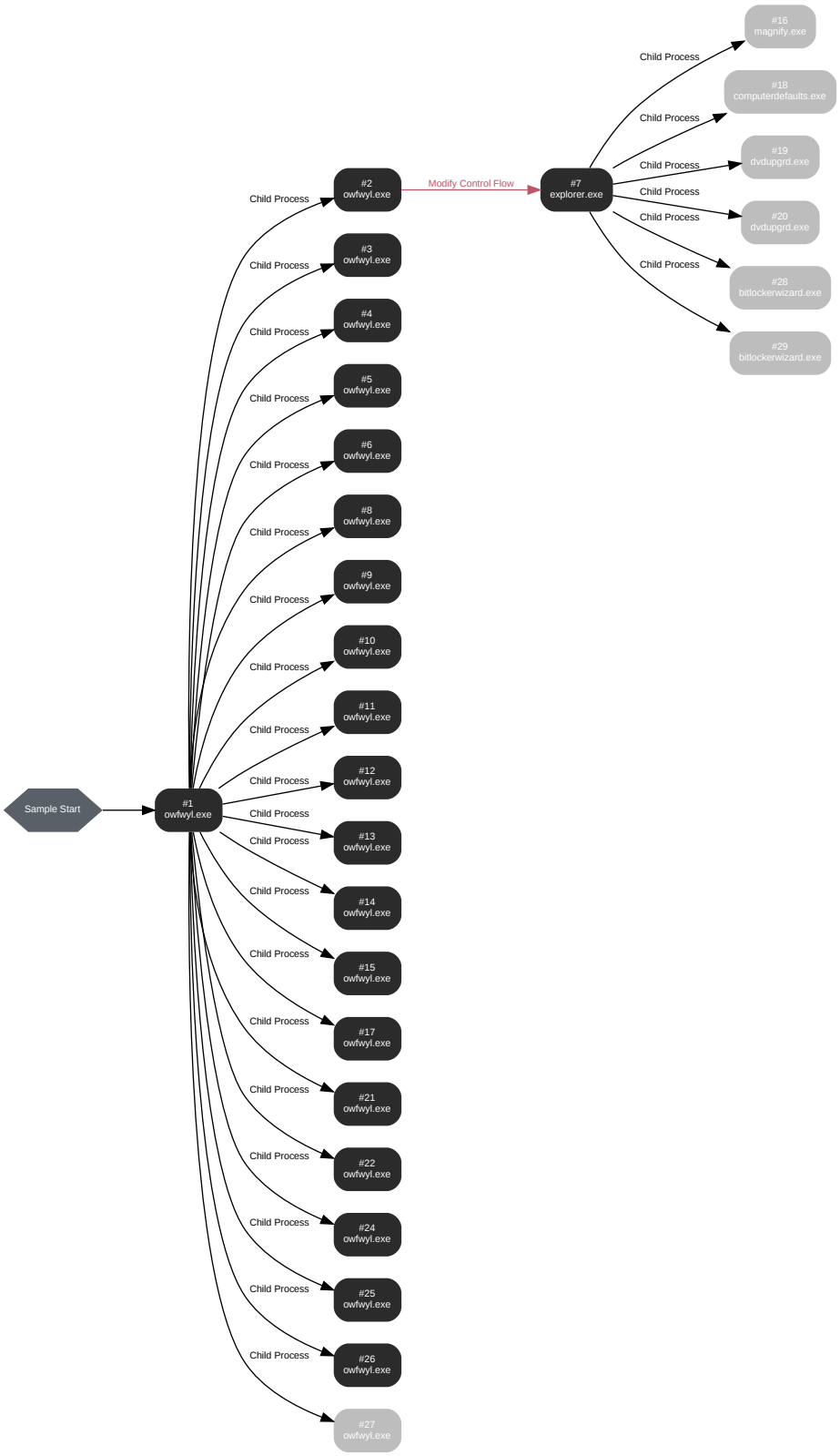
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: owfwyl.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpe84r7mfn" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 62071, Reason: Analysis Target
Unmonitor End Time	End Time: 303172, Reason: Terminated by Timeout
Monitor duration	241.10s
Return Code	Unknown
PID	4732
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	21

Process #2: owfwyl.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=CheckDriverSoftwareDependenciesSatisfied
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 79914, Reason: Child Process
Unmonitor End Time	End Time: 149007, Reason: Terminated
Monitor duration	69.09s
Return Code	0
PID	5052
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	35
File	13
System	36
Environment	1
Registry	539
User	1
Mutex	4
-	126

Process #3: owfwyl.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DeviceInternetSettingUiW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81318, Reason: Child Process
Unmonitor End Time	End Time: 140064, Reason: Terminated
Monitor duration	58.75s
Return Code	0
PID	1376
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	25
File	13
System	40
Environment	1
Registry	539
User	1
Mutex	36

Process #4: owfwyl.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiInstallDevice
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 83734, Reason: Child Process
Unmonitor End Time	End Time: 149033, Reason: Terminated
Monitor duration	65.30s
Return Code	0
PID	3492
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	25
File	13
System	30
Environment	1
Registry	539
User	1
Mutex	26

Process #5: owfwyl.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DllInstallDriverA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 86855, Reason: Child Process
Unmonitor End Time	End Time: 156189, Reason: Terminated
Monitor duration	69.33s
Return Code	0
PID	1824
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	25
File	13
System	19
Environment	1
Registry	539
User	1
Mutex	15

Process #6: owfwyl.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DllInstallDriverW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 90376, Reason: Child Process
Unmonitor End Time	End Time: 156500, Reason: Terminated
Monitor duration	66.12s
Return Code	0
PID	1788
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	25
File	13
System	18
Environment	1
Registry	545
User	1
Mutex	14

Process #7: explorer.exe

ID	7
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 90744, Reason: Injection
Unmonitor End Time	End Time: 303172, Reason: Terminated by Timeout
Monitor duration	212.43s
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\owfwyl.exe	0x13c8 / 0x668	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x690	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x694	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x6ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x6b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x6b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x6b8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x6bc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x6dc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x6e8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x71c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x734	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x73c	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x74c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x798	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x7a8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x7b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x7d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x7ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x7f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x460	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x83c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x954	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x95c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x9c0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0xbec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x4c4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x4ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x8b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x984	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x97c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0xa20	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0xb9c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x628	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x974	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0xb5c	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0xb54	0x7ffc5f8b4f00(140721911451392)	-	✘	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x41c	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x3d4	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0xd24	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0xcd0	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x11e8	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x11f0	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x1234	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x1238	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x124c	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5f8bb580(140721911477632)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5f8bb580(140721911477632)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\owfwyl.exe	0x13c8 / 0x66c	0x7ffc5ecdce60(140721899032160)	-	✔	1

Dropped Files (8)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\VERSION.dll	1088.00 KB	20c6936caa6a742435ff7f5dcc3b1cf62036fbcec0cea9024ea10aa86fdcd62a	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe	27.50 KB	dd5da1c14bc303e137338330c6871c6a5ae013a472c0d29f9158e244aea50f2b	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\FVEWIZ.dll	1088.00 KB	6d629a44acf0a5dc1bca33fb840b888f441b697a7e44e648913ff6d62ca2f285	✘
C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe	100.00 KB	124cf0f3fa82ad26939a649d4351186e56fcbf47e5b4ae93f356d359dbb4832a	✘
-	1.42 KB	a275ad52fb843562197b67a56bfb5e284a064a0bea54794eae835795739b51ab	✘

File Name	File Size	SHA256	YARA Match
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✗
-	1.42 KB	3ab99e33693bf1aab02c810e0d51bccda300b27c9837c66edc410fc653b8ecdd	✗

Host Behavior

Type	Count
Module	26
System	19
File	774
Process	9
Registry	2744
User	1
Mutex	155
COM	2
Environment	1

Process #8: owfwyl.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiRollbackDriver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94003, Reason: Child Process
Unmonitor End Time	End Time: 288233, Reason: Terminated
Monitor duration	194.23s
Return Code	0
PID	1888
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	6
Environment	1
Registry	558
User	1
Mutex	2

Process #9: owfwyl.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiShowUpdateDevice
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96637, Reason: Child Process
Unmonitor End Time	End Time: 292245, Reason: Terminated
Monitor duration	195.61s
Return Code	0
PID	1516
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	7
Environment	1
Registry	277
User	1
Mutex	2

Process #10: owfwyl.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiShowUpdateDriver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 97518, Reason: Child Process
Unmonitor End Time	End Time: 290559, Reason: Terminated
Monitor duration	193.04s
Return Code	0
PID	2192
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	6
Environment	1
Registry	556
User	1
Mutex	1

Process #11: owfwyl.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiUninstallDevice
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100028, Reason: Child Process
Unmonitor End Time	End Time: 291709, Reason: Terminated
Monitor duration	191.68s
Return Code	0
PID	1692
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	6
Environment	1
Registry	521
User	1
Mutex	1

Process #12: owfwyl.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiUninstallDriverA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 152967, Reason: Child Process
Unmonitor End Time	End Time: 294825, Reason: Terminated
Monitor duration	141.86s
Return Code	0
PID	3160
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	7
Environment	1
Registry	536
User	1
Mutex	2

Process #13: owfwyl.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiUninstallDriverW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 192786, Reason: Child Process
Unmonitor End Time	End Time: 292698, Reason: Terminated
Monitor duration	99.91s
Return Code	0
PID	4760
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	4
Environment	1
Registry	536
User	1
Mutex	1

Process #14: owfwyl.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=GetInternetPolicies
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237767, Reason: Child Process
Unmonitor End Time	End Time: 295720, Reason: Terminated
Monitor duration	57.95s
Return Code	0
PID	4892
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	7
Environment	1
Registry	532
User	1
Mutex	3

Process #15: owfwyl.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallNewDevice
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 263856, Reason: Child Process
Unmonitor End Time	End Time: 296308, Reason: Terminated
Monitor duration	32.45s
Return Code	0
PID	3068
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	7
Environment	1
Registry	536
User	1
Mutex	2

Process #16: magnify.exe

ID	16
File Name	c:\windows\system32\magnify.exe
Command Line	C:\Windows\system32\Magnify.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 276900, Reason: Child Process
Unmonitor End Time	End Time: 280627, Reason: Terminated
Monitor duration	3.73s
Return Code	3221226540
PID	4272
Parent PID	1636
Bitness	64 Bit

Process #17: owfwyl.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallSelectedDriver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 278082, Reason: Child Process
Unmonitor End Time	End Time: 296046, Reason: Terminated
Monitor duration	17.96s
Return Code	0
PID	4296
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	7
Environment	1
Registry	536
User	1
Mutex	3

Process #18: computerdefaults.exe

ID	18
File Name	c:\windows\system32\computerdefaults.exe
Command Line	C:\Windows\system32\ComputerDefaults.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 280497, Reason: Child Process
Unmonitor End Time	End Time: 281898, Reason: Terminated
Monitor duration	1.40s
Return Code	3221226540
PID	3864
Parent PID	1636
Bitness	64 Bit

Process #19: dvdupgrd.exe

ID	19
File Name	c:\windows\system32\dvdupgrd.exe
Command Line	C:\Windows\system32\dvdupgrd.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 280966, Reason: Child Process
Unmonitor End Time	End Time: 282735, Reason: Terminated
Monitor duration	1.77s
Return Code	0
PID	2480
Parent PID	1636
Bitness	64 Bit

Process #20: dvdupgrd.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\appdata\local\yfh\dvdupgrd.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 282070, Reason: Child Process
Unmonitor End Time	End Time: 285925, Reason: Terminated
Monitor duration	3.85s
Return Code	0
PID	4048
Parent PID	1636
Bitness	64 Bit

Process #21: owfwyl.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallWindowsUpdateDriver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 283780, Reason: Child Process
Unmonitor End Time	End Time: 297939, Reason: Terminated
Monitor duration	14.16s
Return Code	0
PID	2124
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	19
File	13
System	7
Environment	1
Registry	538
User	1
Mutex	3

Process #22: owfwyl.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallWindowsUpdateDriverEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 291293, Reason: Child Process
Unmonitor End Time	End Time: 299408, Reason: Terminated
Monitor duration	8.12s
Return Code	0
PID	3796
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	7
Environment	1
Registry	538
User	1
Mutex	3

Process #24: owfwyl.exe

ID	24
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallWindowsUpdateDrivers
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 296045, Reason: Child Process
Unmonitor End Time	End Time: 300253, Reason: Terminated
Monitor duration	4.21s
Return Code	0
PID	4740
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	13
System	7
Environment	1
Registry	538
User	1
Mutex	3

Process #25: owfwyl.exe

ID	25
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=QueryWindowsUpdateDriverStatus
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 298028, Reason: Child Process
Unmonitor End Time	End Time: 303172, Reason: Terminated by Timeout
Monitor duration	5.14s
Return Code	Unknown
PID	2080
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	24
File	8
System	3
Environment	1

Process #26: owfwyl.exe

ID	26
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=SetInternetPolicies
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 299115, Reason: Child Process
Unmonitor End Time	End Time: 303172, Reason: Terminated by Timeout
Monitor duration	4.06s
Return Code	Unknown
PID	4756
Parent PID	4732
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #27: owfwyl.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\owfwyl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=UpdateDriverForPlugAndPlayDevicesA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 300252, Reason: Child Process
Unmonitor End Time	End Time: 303172, Reason: Terminated by Timeout
Monitor duration	2.92s
Return Code	Unknown
PID	4924
Parent PID	4732
Bitness	64 Bit

Process #28: bitlockerwizard.exe

ID	28
File Name	c:\windows\system32\bitlockerwizard.exe
Command Line	C:\Windows\system32\BitLockerWizard.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 300654, Reason: Child Process
Unmonitor End Time	End Time: 302451, Reason: Terminated
Monitor duration	1.80s
Return Code	0
PID	2580
Parent PID	1636
Bitness	64 Bit

Process #29: bitlockerwizard.exe

ID	29
File Name	c:\users\rdhj0cnfevzx\appdata\local\cvf9g\bitlockerwizard.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 303172, Reason: Child Process
Unmonitor End Time	End Time: 303172, Reason: Terminated by Timeout
Monitor duration	0.00s
Return Code	Unknown
PID	4912
Parent PID	1636
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033	C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll, C:\Users\RDhJ0CNFevzX\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll	Sample File	1084.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
20c6936caa6a742435ff7f5dcc3b1cf62036fbcec0cea9024ea10aa86fdcd62a	C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\VERSION.dll, C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\VE05r\VERSION.dll	Dropped File	1088.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	MALICIOUS
6d629a44acf0a5dc1bca33fb840b888f441b697a7e44e648913ff6d62ca2f285	C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\FVEWIZ.dll	Dropped File	1088.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Access	MALICIOUS
dd5da1c14bc303e137338330c6871c6a5ae013a472c0d29f9158e244aea50f2b	C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\VE05r\dvdupgrd.exe	Dropped File	27.50 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	SUSPICIOUS
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
124cf0f3fa82ad26939a649d4351186e56fcbf47e5b4ae93f356d359dbb4832a	C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe	Dropped File	100.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Access	CLEAN
a275ad52fb843562197b67a56bfb5e284a064a0bea54794eae835795739b51ab	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
3ab99e33693bf1aab02c810e0d51bccda300b27c9837c66edc410fc653b8ecdd	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\owfWYL.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpe84r7mfn	Accessed File	Read, Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll	Accessed File	Read, Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Adobe\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Adobe\Flash Player\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Adobe\Flash Player\NativeCache\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\AddIns\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Bibliography\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Credentials\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Crypto\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Crypto\RSA\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Document Building Blocks\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Document Building Blocks\1033\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Excel\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Excel\XLSTART\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\ImplicitAppShortcuts\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\MMC\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Network\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Network\Connections\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Network\Connections\Pbk\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Spelling\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\SystemCertificates\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Document Themes\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Office\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Outlook\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Protect\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Vault\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Word\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Bibliography\Style\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-1560258661-3990802383-1811730007-1000\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Document Building Blocks\1033\16\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Network\Connections\Pbk_hiddenPbk\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Office\Recent\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Protect\S-1-5-21-1560258661-3990802383-1811730007-1000\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Spelling\en-US\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\SystemCertificates\My\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Bibliography Styles\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Document Themes\1033\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\1033\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Document Themes\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\SmartArt Graphics\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Word Document Bibliography Styles\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Word Document Building Blocks\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Document Themes\1033\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\SmartArt Graphics\1033\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\User\Word Document Building Blocks\1033\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\AccountPictures\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Libraries\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Network Shortcuts\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\SendTo\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Templates\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Themes\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\VE05r	Accessed File	Create, Access	CLEAN
C:\Windows\system32\help.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\SrTasks.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\eventvwr.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\SmartScreenSettings.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\immersivetpmvscmgrsvr.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\CredentialUIBroker.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\DeviceEject.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\rwinsta.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\compact.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\CastSrv.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\CompatTelRunner.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\nltest.exe	Accessed File	Read, Access	CLEAN
C:\Program Files\Windows Journal\outlook.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\ClipUp.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\lpremove.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\UsoClient.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\PkgMgr.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\qappsrv.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\tasklist.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\pcalua.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\lodctr.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\openfiles.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\dmclient.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\NETSTAT.EXE	Accessed File	Read, Access	CLEAN
C:\Windows\system32\Magnify.exe	Accessed File	Read, Access	CLEAN
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
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
C:\Windows\system32\SpaceMan.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\certreq.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\dispdiag.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\whoami.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\reg.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\ComputerDefaults.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\mtstocom.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\dvdupgrd.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\VERSION.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\VERSION.dll	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe	Dropped File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\VE05r\VERSION.dll	Dropped File	Write, Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\VE05r\dvdupgrd.exe	Dropped File	Write, Create, Access	CLEAN
C:\Windows\system32\dstokenclean.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\mcbuilder.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\cliconfg.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\BitLockerWizard.exe	Accessed File	Read, Access	CLEAN
C:\Windows\system32\FVEWIZ.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\FVEWIZ.dll	Dropped File	Write, Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe	Dropped File	Write, Create, Access	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
\Sessions\1\BaseNamedObjects\{0aa26147-58aa-e888-6782-4bac88c336bd}	access	owfwyl.exe	CLEAN
\Sessions\1\BaseNamedObjects\{20974a93-a551-df17-8967-748358091d34}	access	owfwyl.exe	CLEAN
0	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{389fe546-d029-33a7-6305-2ca1cede0678}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{e8b6fe55-d858-d6e4-ef99-a80106642ab4}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
\Sessions\1\BaseNamedObjects\{03b2a674-5295-21d6-da36-fc13faee0e98}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{d439f686-d570-7182-3906-1e2d175d1088}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{27dcbb6c-b6b1-b5c0-be37-17f0c21939fa}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{e33e87ed-6b47-d015-096b-848dadf4080b}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{9a19a950-2459-434e-9c59-a982629f26dd}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{9666bd67-64c1-5269-b5bb-b889b9fea609}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{af33e402-09cc-a6cc-e5da-4bf4b32d667d}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{4f8955dd-c023-639c-9d54-a0e485c7012a}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{201ba18c-1db5-3773-b8bd-628af5f5deba}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{263ffa84-4558-3562-0b37-9f47f49f6a79}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{71dba081-a28d-be08-fa55-bf22ddb35cb9}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{9a933d33-e195-3556-503e-c5c0a921498c}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{05747a50-933e-c4fd-7a3d-44fed7350072}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{153471c9-9d0a-7104-5275-71ac64b2065e}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{4236a99f-3514-853f-daf5-e82e3c1b0317}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{e79e5240-aa8e-0f63-d6a1-8a07649cdc90}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{38e7db7a-75ef-8cef-8130-9e11aa96557f}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{d721bcec-0f69-129d-7108-0656474a0b0a}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{dbe86ec5-1230-23f0-4ccf-a65084617422}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{44869c43-a49e-bce0-8271-dbb71cb12c79}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{0ae6b514-0674-d8a5-a624-343329b398d5}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{0eb707bd-e520-a26e-500a-bbb6baa1f707}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{b386415a-cf2b-b133-badc-6ec70cc36294}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{14fe886f-f5af-a8a1-1712-9042f79a83dc}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{8a4d728e-1a95-daee-efb3-d49c856d805e}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{a3dce688-6117-3ea3-fbbd-1defec717462}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{a2e3a1c4-1044-26ac-2fa3-30ee391a0657}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{7cc6ae5f-2c94-8c18-e20d-28bccdbd00c3}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
\Sessions\1\BaseNamedObjects\{b4de3d46-efec-a98a-f706-8745d35ed7f2}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{d1575404-3469-2df0-db6b-3bcf4439344f}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{3c33918e-27da-9f35-2586-b9f012933134}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{6c570128-9202-fd64-daa4-72143d141e8a}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{822894df-44a8-add7-294a-a446b174fbef}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{6fe25233-3c10-d1be-fd07-8467d220e8d6}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{bc97cda8-f351-7a60-8d28-728a4afb7aec}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{bb0cabed-1ffc-1a16-fd9e-e02cab733680}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{fcd273ea-02e9-5a8a-4a8b-7848d0895772}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{e28905fd-15de-b796-44d3-7a7876237780}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{ede07ea5-2e12-7d74-5185-75bb288d7c70}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{fef37f2e-4f56-9012-852a-59484b5fed7e}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{ad5d057c-012c-b276-1470-f24990f0a7eb}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{8d859e8a-cd3c-3ac0-0451-ab11d6131acd}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{1439a690-60db-c7ba-74ad-63f3b3396ce4}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{d65528a1-3ef5-a115-0995-914008bd9a62}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{71bb662b-e609-45a6-82d2-d177df9706bc}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{5448aec8-10c2-e89b-6654-58a5f2a67f29}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{946d3aec-f0be-460d-b2db-c49c07ac46ae}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{b894408f-30d6-e44c-93a0-15251ca9bab4}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{497f1ddf-1131-8869-1c4d-19bc3c1533f0}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{867eeaaa-9095-7d70-5174-9d6e7d728884}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{1da4e1aa-6eb1-9190-a173-cc15c94ce697}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{f9e73e00-f006-b49c-1dcf-ff85215b0c68}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{6a4fe6c6-ce4d-1240-9924-4da205e310d4}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{92072f54-0b93-095f-1e25-932462e67c3e}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{8874da96-f7ee-262d-50ac-d480c6318c76}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{204ccede-cf27-6aa3-cbb0-8bee83f524ea}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
\Sessions\1\BaseNamedObjects\{a5a67534-fa42-ee17-0f42-7894e1acd27e}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{6ff03553-8c1f-eaac-a9cf-dffee1d0e05c}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{9b6e053f-0de2-32a4-79d5-d31fb6cfceba}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{0fe620b0-69ae-dee7-2d6b-018cf8c7d19c}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{be160789-1fd9-ee8b-3528-3c09aeed0e96}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{614957d1-9bd1-e6ec-a276-c7f895abc543}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{12043912-5ec8-510a-c738-72cae9f9f205}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{8c972fde-9d5f-1cce-6885-fb3e3e78e2a1}	access	explorer.exe	CLEAN
\Sessions\1\BaseNamedObjects\{e36d9c70-e050-032a-b419-be29916de4a8}	access	explorer.exe	CLEAN

Registry

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

Registry Key	Operations	Parent Process Name	Verdict
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_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\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\{2ABB94BE-777C-6F7B-24D2-F7F89D3B1A1A}	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{B7C77642-8C45-6D49-2FD3-ACD4B7F7D95A}	write, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6D5BA165-497C-24C3-5D8E-5F18E61D6C19}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6D5BA165-497C-24C3-5D8E-5F18E61D6C19}\ShellFolder\{1C538F3F-97C2-48F0-C0D7-6E9B4AF3DE2C}	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

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4D2056E1-92AF-EC5C-2615-AA80579018DA}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{368B1D7B-EAC9-2EB9-9178-5819EFDD132A}\ShellFolder	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9D74D8D1-A2C2-8A4E-2A5F-EBAAE5390403}\ShellFolder	create, access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpe84r7mfn" /s	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=CheckDriverSoftwareDependenciesSatisfied	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DeviceInternetSettingUiW	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiInstallDevice	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiInstallDriverA	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiInstallDriverW	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiRollbackDriver	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiShowUpdateDevice	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiShowUpdateDriver	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiUninstallDevice	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiUninstallDriverA	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=DiUninstallDriverW	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=GetInternetPolicies	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallNewDevice	CLEAN
magnify.exe	C:\Windows\system32\Magnify.exe	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallSelectedDriver	CLEAN
computerdefaults.exe	C:\Windows\system32\ComputerDefaults.exe	CLEAN
dvdupgrd.exe	C:\Windows\system32\dvdupgrd.exe	CLEAN
dvdupgrd.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\dvdupgrd.exe	CLEAN

Process Name	Commandline	Verdict
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallWindowsUpdateDriver	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallWindowsUpdateDriverEx	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=InstallWindowsUpdateDrivers	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=QueryWindowsUpdateDriverStatus	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=SetInternetPolicies	CLEAN
owfwyl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\owfWYL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll" /fn_id=UpdateDriverForPlugAndPlayDevicesA	CLEAN
bitlockerwizard.exe	C:\Windows\system32\BitLockerWizard.exe	CLEAN
bitlockerwizard.exe	C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\BitLockerWizard.exe	CLEAN

YARA / AV

Antivirus (4)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.75562	C:\Users\RDhJ0CNFevzX\Desktop\ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033.exe.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.75562	C:\Users\RDhJ0CNFevzX\AppData\Local\YFh\VERSION.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.75562	C:\Users\RDhJ0CNFevzX\AppData\Local\cVf9G\FVEWIZ.dll	MALICIOUS
Memory Dump	Trojan.GenericKDZ.75562	-	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