MALICIOUS

Classifications: Spyware

Threat Names: Trojan.Generic.30199792, Gen:Variant.Mikey.113998, Trojan.GenericKDZ.76753

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll**
ID	#2782721
MD5	2ab698a4e7608708ae2a693966194322
SHA1	300f4d7d2f462dac7e6ab333d8783bab4f371316
SHA256	3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572
File Size	2200.00 KB
Report Created	2021-09-28 13:15 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (7 rules, 111 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	5	-
	• Built-in AV detected the sample itself as "Trojan.Generic.30199792". • Built-in AV detected a memory dump of (process #2) juujetlws.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #7) juujetlws.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #9) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #13) juujetlws.exe as "Gen:Variant.Mikey.113998".			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) juujetlws.exe alters context of (process #9) explorer.exe.			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
1/5	Discovery	Reads system data	11	-
	• (Process #2) juujetlws.exe reads the Windows installation date from registry. • (Process #3) juujetlws.exe reads the Windows installation date from registry. • (Process #4) juujetlws.exe reads the Windows installation date from registry. • (Process #5) juujetlws.exe reads the Windows installation date from registry. • (Process #6) juujetlws.exe reads the Windows installation date from registry. • (Process #7) juujetlws.exe reads the Windows installation date from registry. • (Process #10) juujetlws.exe reads the Windows installation date from registry. • (Process #8) juujetlws.exe reads the Windows installation date from registry. • (Process #11) juujetlws.exe reads the Windows installation date from registry. • (Process #9) explorer.exe reads the Windows installation date from registry. • (Process #12) juujetlws.exe reads the Windows installation date from registry.			
1/5	Mutex	Creates mutex	90	-

- (Process #2) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #3) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) juujetlws.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #4) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #5) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #8) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #10) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #11) juujetlws.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #10) juujetlws.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #9) explorer.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #9) explorer.exe creates mutex with name "{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}".
- (Process #9) explorer.exe creates mutex with name "{e8353f60-b296-77d3-712c-682bf3e23f29}".
- (Process #9) explorer.exe creates mutex with name "{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}".
- (Process #9) explorer.exe creates mutex with name "{3efe96e0-aada-6cdc-4854-db5a860aa498}".
- (Process #9) explorer.exe creates mutex with name "{0969e291-b21e-da66-8a27-2c05635de7c1}".
- (Process #9) explorer.exe creates mutex with name "{298ddcca-efe5-2f07-cbb5-e91e37797537}".
- (Process #9) explorer.exe creates mutex with name "{ca617e03-c43b-e689-fb55-6daa5ee7afd0}".
- (Process #9) explorer.exe creates mutex with name "{794d917c-1834-7d66-daf9-60090b7d143f}".
- (Process #9) explorer.exe creates mutex with name "{20ac3a9e-af78-6300-0f8d-4f83854bc2ae}".
- (Process #9) explorer.exe creates mutex with name "{e232db4a-6058-9dc3-05c2-f08eab1aff8b}".
- (Process #9) explorer.exe creates mutex with name "{d16d5bd5-a9e5-3451-c896-a81deb35e494}".
- (Process #9) explorer.exe creates mutex with name "{2d42d2db-a175-1095-da60-d7c547321259}".
- (Process #9) explorer.exe creates mutex with name "{ffd3ea5a-0bdc-be0c-871f-c2fe4aa06898}".
- (Process #9) explorer.exe creates mutex with name "{4eb5ef4a-8c84-962c-99cb-f08513493246}".
- (Process #9) explorer.exe creates mutex with name "{4784410d-e3f9-554d-7932-46a2951b1a14}".
- (Process #9) explorer.exe creates mutex with name "{7a6d2748-578c-61de-d634-d36a39ae9499}".
- (Process #9) explorer.exe creates mutex with name "{0b7ba948-3cca-a9ee-ef68-bca12f0e84a2}".
- (Process #9) explorer.exe creates mutex with name "{5bffd7b8-454a-d897-55b3-ba9b73e0f7e8}".
- (Process #9) explorer.exe creates mutex with name "{fe886e8c-a23d-7a39-eb2b-a2f6429f4e23}".
- (Process #9) explorer.exe creates mutex with name "{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}".
- (Process #9) explorer.exe creates mutex with name "{56890943-b990-1d76-48d6-16063e4d02b0}".
- (Process #9) explorer.exe creates mutex with name "{2909efc7-e828-45b2-19c5-01ec2ef0c97b}".
- (Process #9) explorer.exe creates mutex with name "{e697b08b-6228-db49-1b5f-122d452e86b1}".
- (Process #9) explorer.exe creates mutex with name "{9ffb2102-4ed7-3d87-65ab-805271e438f1}".
- (Process #9) explorer.exe creates mutex with name "{16770cb7-b91c-ef6e-e0ce-9944b6f847e9}".
- (Process #9) explorer.exe creates mutex with name "{bc738eef-d34f-5290-c271-80f802b0874e}".
- (Process #9) explorer.exe creates mutex with name "{076cdbc3-53e2-4ed4-7b49-76a741cb0f92}".
- (Process #9) explorer.exe creates mutex with name "{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}".
- (Process #9) explorer.exe creates mutex with name "{1bc6a851-4ae7-d17d-9611-affa9e1d58b2}".
- (Process #9) explorer.exe creates mutex with name "{2835d429-2a00-0fb6-5c11-3e59c353659a}".
- (Process #9) explorer.exe creates mutex with name "{daa370fa-1379-7113-c11a-e30a38c99e5d}".
- (Process #9) explorer.exe creates mutex with name "{01f24baa-a48c-b675-d94f-c4d185fa1b74}".
- (Process #9) explorer.exe creates mutex with name "{7e5d2be3-0634-bb96-47ee-3083eb9bef97}".
- (Process #9) explorer.exe creates mutex with name "{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}".
- (Process #9) explorer.exe creates mutex with name "{3c33918e-27da-9f35-2586-b9f012933134}".
- (Process #9) explorer.exe creates mutex with name "{ac72e331-225f-a96a-c143-d364da64ed30}".
- (Process #9) explorer.exe creates mutex with name "{a1090343-24c0-16c8-e547-9b6fb6d0166b}".
- (Process #9) explorer.exe creates mutex with name "{6fe25233-3c10-d1be-fd07-8467d220e8d6}".
- (Process #9) explorer.exe creates mutex with name "{583163e6-97f6-ca24-26b7-ae90d9895822}".
- (Process #9) explorer.exe creates mutex with name "{2b88fe55-b6c3-eb01-2f71-f3795770c574}".
- (Process #9) explorer.exe creates mutex with name "{fcd273ea-02e9-5a8a-4a8b-7848d0895772}".
- (Process #9) explorer.exe creates mutex with name "{ede07ea5-2e12-7d74-5185-75bb288d7c70}".
- (Process #9) explorer.exe creates mutex with name "{fc948bb7-3cee-2bf7-f8c9-909cf6db89de}".
- (Process #9) explorer.exe creates mutex with name "{b707c8db-10a1-da7e-58a9-0531358e4e63}".
- (Process #9) explorer.exe creates mutex with name "{a4165b4a-bfe7-c4c5-3fb8-0a45db645781}".
- (Process #9) explorer.exe creates mutex with name "{6d23ed51-38ca-5cb0-6eab-e5ee861c8501}".
- (Process #9) explorer.exe creates mutex with name "{74cce2f8-af0d-c651-67a5-40d9130ec8dd}".
- (Process #9) explorer.exe creates mutex with name "{71bd3620-3609-45a6-a2d2-d17d970bb0}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #2) juujetlws.exe reads from (process #9) explorer.exe. • (Process #10) juujetlws.exe reads from (process #9) explorer.exe.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #9) explorer.exe resolves 26 API functions by name.			

Mitre ATT&CK Matrix

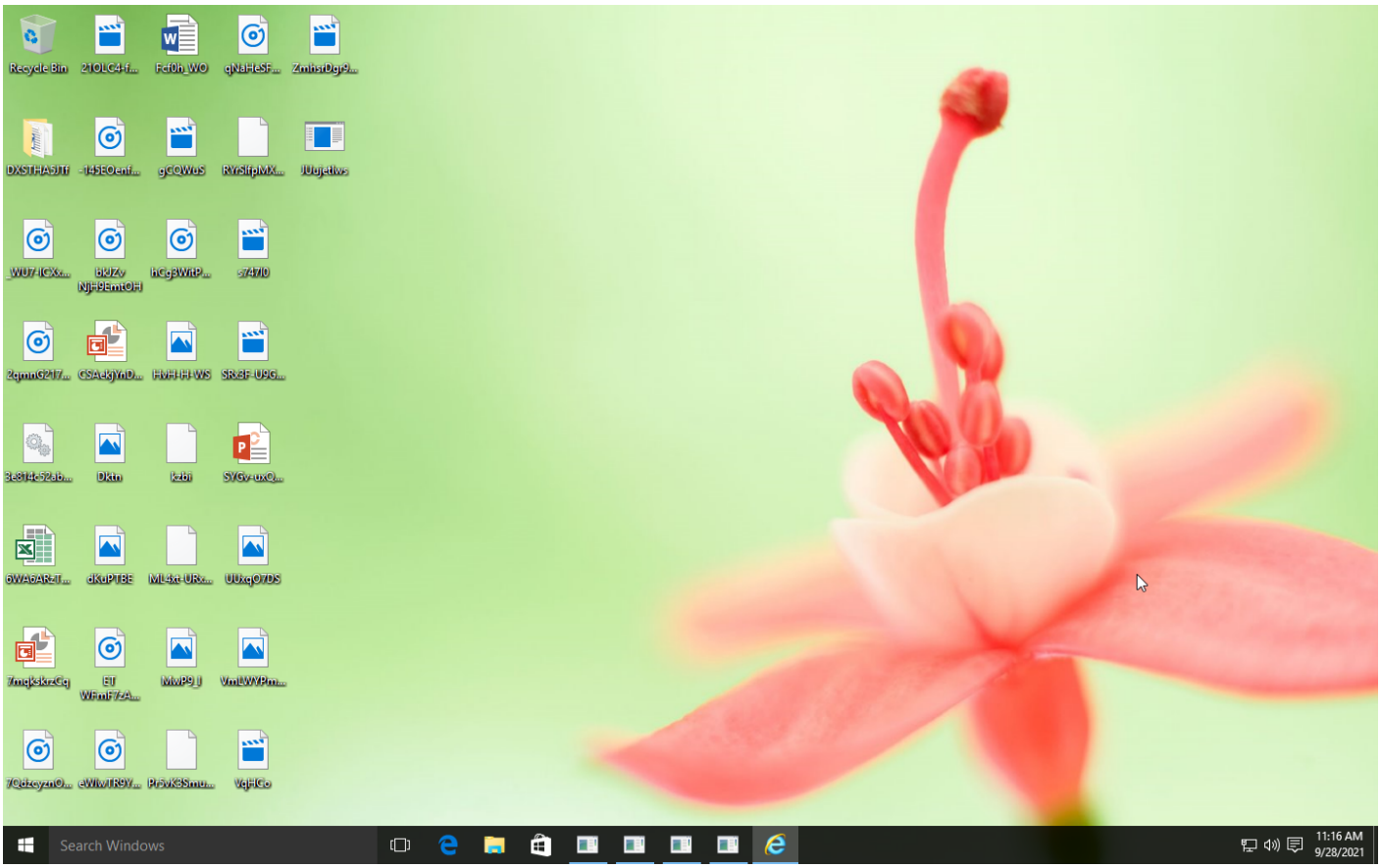
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing		#T1082 System Information Discovery					
						#T1012 Query Registry					

Sample Information

ID	#2782721
MD5	2ab698a4e7608708ae2a693966194322
SHA1	300f4d7d2f462dac7e6ab333d8783bab4f371316
SHA256	3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572
SSDeep	12288:wVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1Cp3A:1fP7fWsK5z9A+WGAW+V5SB6Ct4bnbW
ImpHash	6668be91e2c948b183827f040944057f
File Name	3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll
File Size	2200.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 13:15 (UTC+2)
Analysis Duration	00:03:54
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	16
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
Search Windows
11:16 AM
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

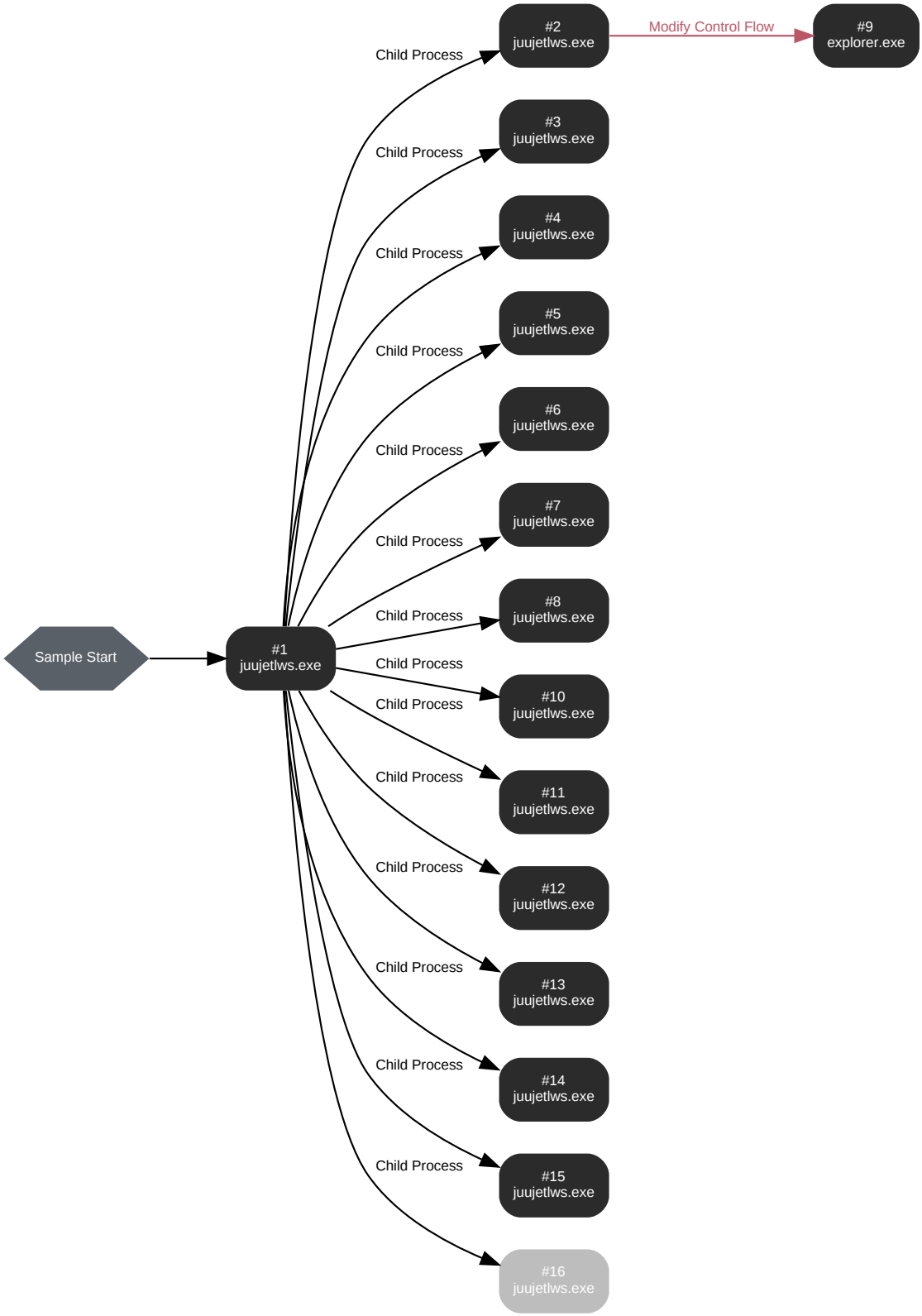
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: juujetlws.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp16ohnict" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 65018, Reason: Analysis Target
Unmonitor End Time	End Time: 300314, Reason: Terminated by Timeout
Monitor duration	235.30s
Return Code	Unknown
PID	4924
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	15

Process #2: juujetlws.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a0698... ... 3a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 86582, Reason: Child Process
Unmonitor End Time	End Time: 122475, Reason: Terminated
Monitor duration	35.89s
Return Code	0
PID	3272
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	35
Environment	2
Registry	789
Mutex	6
Process	2
-	44
-	32
-	112

Process #3: juujetlws.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 88754, Reason: Child Process
Unmonitor End Time	End Time: 101502, Reason: Terminated
Monitor duration	12.75s
Return Code	0
PID	680
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	769
Mutex	7

Process #4: juujetlws.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 90317, Reason: Child Process
Unmonitor End Time	End Time: 107889, Reason: Terminated
Monitor duration	17.57s
Return Code	0
PID	1360
Parent PID	4924
Bitness	64 Bit

Host Behavior

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

Process #5: juujetlws.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VInvokeProvider@DirectUI@@UIInvokeProvider@@$0A@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 92663, Reason: Child Process
Unmonitor End Time	End Time: 113261, Reason: Terminated
Monitor duration	20.60s
Return Code	0
PID	2824
Parent PID	4924
Bitness	64 Bit

Host Behavior

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

Process #6: juujetlws.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VRangeValueProvider@DirectUI@@UIRangeValueProvider@@$03@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 95497, Reason: Child Process
Unmonitor End Time	End Time: 115024, Reason: Terminated
Monitor duration	19.53s
Return Code	0
PID	2884
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	769
Mutex	7

Process #7: juujetlws.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VScrollItemProvider@DirectUI@@UIScrollItemProvider@@$05@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 99003, Reason: Child Process
Unmonitor End Time	End Time: 120136, Reason: Terminated
Monitor duration	21.13s
Return Code	0
PID	1072
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	4
Environment	2
Registry	768
Mutex	7

Process #8: juujetlws.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VScrollProvider@DirectUI@@UIScrollProvider@@$04@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 102147, Reason: Child Process
Unmonitor End Time	End Time: 122463, Reason: Terminated
Monitor duration	20.32s
Return Code	0
PID	336
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	654
Mutex	7

Process #9: explorer.exe

ID	9
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 103335, Reason: Injection
Unmonitor End Time	End Time: 300314, Reason: Terminated by Timeout
Monitor duration	196.98s
Return Code	Unknown
PID	1600
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (70)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x758	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x7bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xe58	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xe88	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xed4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xfbc	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x4c4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x1c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0xe14	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x1288	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x1320	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x1380	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb28bab580(140716696843648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\juujetlws.exe	0x12cc / 0x69c	0x7ffb2626ee40(140716653604416)	-	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✘
-	1.42 KB	e7625d14c9f93f70cf91f2e95cd9b6aac327763aa2abd14c206086bdaa212008	✘
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✘
-	1.42 KB	41bf31dedd494d47870ee949ca5595303cd6c2d3fa679edc0a3a25626d592e5d	✘

Host Behavior

Type	Count
Module	48
File	118
System	381
Process	113
Registry	23960
Environment	1
-	22
Mutex	1382

Process #10: juujetlws.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VSelectionItemProvider@DirectUI@@UISelectionItemProvider@@$06@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 105365, Reason: Child Process
Unmonitor End Time	End Time: 300314, Reason: Terminated by Timeout
Monitor duration	194.95s
Return Code	Unknown
PID	1840
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	7
Environment	2
Registry	789
Mutex	5
Process	2
-	2
-	1

Process #11: juujetlws.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VSelectionProvider@DirectUI@@UISelectionProvider@@$07@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 108788, Reason: Child Process
Unmonitor End Time	End Time: 204941, Reason: Terminated
Monitor duration	96.15s
Return Code	0
PID	1944
Parent PID	4924
Bitness	64 Bit

Host Behavior

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

Process #12: juujetlws.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VTableItemProvider@DirectUI@@UITableItemProvider@@$09@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 113645, Reason: Child Process
Unmonitor End Time	End Time: 231002, Reason: Terminated
Monitor duration	117.36s
Return Code	0
PID	2688
Parent PID	4924
Bitness	64 Bit

Host Behavior

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

Process #13: juujetlws.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117756, Reason: Child Process
Unmonitor End Time	End Time: 300314, Reason: Terminated by Timeout
Monitor duration	182.56s
Return Code	Unknown
PID	2832
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #14: juujetlws.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VToggleProvider@DirectUI@@UIToggleProvider@@$0L@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 125197, Reason: Child Process
Unmonitor End Time	End Time: 300314, Reason: Terminated by Timeout
Monitor duration	175.12s
Return Code	Unknown
PID	1496
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	8

Process #15: juujetlws.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $PatternProvider@VValueProvider@DirectUI@@UIValueProvider@@$0M@@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 242955, Reason: Child Process
Unmonitor End Time	End Time: 300314, Reason: Terminated by Timeout
Monitor duration	57.36s
Return Code	Unknown
PID	3036
Parent PID	4924
Bitness	64 Bit

Host Behavior

Type	Count
Module	15
File	38
Environment	1

Process #16: juujetlws.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\juujetlws.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C: \Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0? $SafeArrayAccessor@H@DirectUI@@QEAA@XZ
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 281450, Reason: Child Process
Unmonitor End Time	End Time: 300314, Reason: Terminated by Timeout
Monitor duration	18.86s
Return Code	Unknown
PID	4168
Parent PID	4924
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572	C:\Users\RDhJ0CNFevzX\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll, C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll	Sample File	2200.00 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
e7625d14c9f93f70cf91f2e95cd9b6aac327763aa2abd14c206086bdaa212008	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
41bf31dedd494d47870ee949ca5595303cd6c2d3fa679edc0a3a25626d592e5d	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\JUujetlws.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp16ohnict	Accessed File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Program Files\Windows Photo Viewer\outlook.exe	Accessed File	Access, Read	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	juujetlws.exe	CLEAN
{54137ce8-d76d-e7fc-dec3-c85f290e5b98}	access	juujetlws.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}	access	explorer.exe	CLEAN
{e8353f60-b296-77d3-712c-682bf3e23f29}	access	explorer.exe	CLEAN
{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}	access	explorer.exe	CLEAN
{298ddcca-efe5-2f07-cbb5-e91e37797537}	access	explorer.exe	CLEAN
{3efe96e0-aada-6cdc-4854-db5a860aa498}	access	explorer.exe	CLEAN
{0969e291-b21e-da66-8a27-2c05635de7c1}	access	explorer.exe	CLEAN
{ca617e03-c43b-e689-fb55-6daa5ee7afd0}	access	explorer.exe	CLEAN
{794d917c-1834-7d66-daf9-60090b7d143f}	access	explorer.exe	CLEAN
{20ac3a9e-af78-6300-0f8d-4f83854bc2ae}	access	explorer.exe	CLEAN
{e232db4a-6058-9dc3-05c2-f08eab1aff8b}	access	explorer.exe	CLEAN
{d16d5bd5-a9e5-3451-c896-a81deb35e494}	access	explorer.exe	CLEAN
{2d42d2db-a175-1095-da60-d7c547321259}	access	explorer.exe	CLEAN
{ffd3ea5a-0bdc-be0c-871f-c2fe4aa06898}	access	explorer.exe	CLEAN
{4eb5ef4a-8c84-962c-99cb-f08513493246}	access	explorer.exe	CLEAN
{4784410d-e3f9-554d-7932-46a2951b1a14}	access	explorer.exe	CLEAN
{7a6d2748-578c-61de-d634-d36a39ae9499}	access	explorer.exe	CLEAN
{0b7ba948-3cca-a9ee-ef68-bca12f0e84a2}	access	explorer.exe	CLEAN
{5bffd7b8-454a-d897-55b3-ba9b73e0f7e8}	access	explorer.exe	CLEAN
{fe886e8c-a23d-7a39-eb2b-a2f6429f4e23}	access	explorer.exe	CLEAN
{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}	access	explorer.exe	CLEAN
{56890943-b990-1d76-48d6-16063e4d02b0}	access	explorer.exe	CLEAN
{2909efc7-e828-45b2-19c5-01ec2ef0c97b}	access	explorer.exe	CLEAN
{e697b08b-6228-db49-1b5f-122d452e86b1}	access	explorer.exe	CLEAN
{9ffb2102-4ed7-3d87-65ab-805271e438f1}	access	explorer.exe	CLEAN
{16770cb7-b91c-ef6e-e0ce-9944b6f847e9}	access	explorer.exe	CLEAN
{bc738eef-d34f-5290-c271-80f802b0874e}	access	explorer.exe	CLEAN
{076cdbc3-53e2-4ed4-7b49-76a741cb0f92}	access	explorer.exe	CLEAN
{ed9037cf-84b5-6f0c-01db-1f89943b4ec1}	access	explorer.exe	CLEAN
{1bc6a851-4ae7-d17d-9611-affa9e1d58b2}	access	explorer.exe	CLEAN
{2835d429-2a00-0fb6-5c11-3e59c353659a}	access	explorer.exe	CLEAN
{daa370fa-1379-7113-c11a-e30a38c99e5d}	access	explorer.exe	CLEAN
{01f24baa-a48c-b675-d94f-c4d185fa1b74}	access	explorer.exe	CLEAN
{7e5d2be3-0634-bb96-47ee-3083eb9bef97}	access	explorer.exe	CLEAN
{ad578bd5-3c50-f523-98ef-c00bb2e8cdcd}	access	explorer.exe	CLEAN
{3c33918e-27da-9f35-2586-b9f012933134}	access	explorer.exe	CLEAN
{ac72e331-225f-a96a-c143-d364da64ed30}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{a1090343-24c0-16c8-e547-9b6fb6d0166b}	access	explorer.exe	CLEAN
{6fe25233-3c10-d1be-fd07-8467d220e8d6}	access	explorer.exe	CLEAN
{583163e6-97f6-ca24-26b7-ae90d9895822}	access	explorer.exe	CLEAN
{2b88fe55-b6c3-eb01-2f71-f3795770c574}	access	explorer.exe	CLEAN
{fcd273ea-02e9-5a8a-4a8b-7848d0895772}	access	explorer.exe	CLEAN
{ede07ea5-2e12-7d74-5185-75bb288d7c70}	access	explorer.exe	CLEAN
{fc948bb7-3cee-2bf7-f8c9-909cf6db89de}	access	explorer.exe	CLEAN
{b707c8db-10a1-da7e-58a9-0531358e4e63}	access	explorer.exe	CLEAN
{a4165b4a-bfe7-c4c5-3fb8-0a45db645781}	access	explorer.exe	CLEAN
{6d23ed51-38ca-5cb0-6eab-e5ee861c8501}	access	explorer.exe	CLEAN
{74cce2f8-af0d-c651-67a5-40d9130ec8dd}	access	explorer.exe	CLEAN
{71bb662b-e609-45a6-82d2-d177df9706bc}	access	explorer.exe	CLEAN
{5448aec8-10c2-e89b-6654-58a5f2a67f29}	access	explorer.exe	CLEAN
{35809dca-c072-ec81-460e-44a0ad984eb0}	access	explorer.exe	CLEAN
{ca10318d-d43e-d7f4-54ae-2e3b621216b5}	access	explorer.exe	CLEAN
{66f88062-bc56-b7bd-5e68-f476f8966290}	access	explorer.exe	CLEAN
{867eeaaa-9095-7d70-5174-9d6e7d728884}	access	explorer.exe	CLEAN
{c67f77d2-b29e-8c6f-4220-6b09eca9dfe4}	access	explorer.exe	CLEAN
{f9e73e00-f006-b49c-1dcf-ff85215b0c68}	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
{204ccede-cf27-6aa3-cbb0-8bee83f524ea}	access	explorer.exe	CLEAN
{3186325a-99af-5690-ae74-778f6719bfc6}	access	explorer.exe	CLEAN
{b281d02b-064a-3f84-6ef7-c8378066af34}	access	explorer.exe	CLEAN
{d4fcd5f8-e7e4-8c73-c2e5-9dea809ffc9a}	access	explorer.exe	CLEAN
{7e9a67be-6bc8-6efe-dfff-b8807a425eef}	access	explorer.exe	CLEAN
{c9ea2fd6-41ea-b3e1-465f-c2b9b5d4d63e}	access	explorer.exe	CLEAN
{0fe620b0-69ae-dee7-2d6b-018cf8c7d19c}	access	explorer.exe	CLEAN
{be160789-1fd9-ee8b-3528-3c09aeed0e96}	access	explorer.exe	CLEAN
{d06416aa-46f7-f2c8-b304-9c261b189ee2}	access	explorer.exe	CLEAN
{614957d1-9bd1-e6ec-a276-c7f895abc543}	access	explorer.exe	CLEAN
{8c76a6e0-72e3-69cc-59af-d17071d0a7cb}	access	explorer.exe	CLEAN
{347cb4ac-d8ec-8808-bfcc-71576c6e3697}	access	explorer.exe	CLEAN
{8a31dfcb-2499-d52f-4464-6ddc62174e03}	access	explorer.exe	CLEAN
{5f513df2-c20f-5892-1dd6-f1bae3c29d19}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{45aa54b3-d256-0e16-2dca-cd6a35e5748d}	access	explorer.exe	CLEAN
{81d9bf30-a216-0e27-dbf6-ebc8695c8b50}	access	explorer.exe	CLEAN
{36aa0111-0a7d-9e3f-1f71-8b96c427c3d4}	access	explorer.exe	CLEAN
{cf924d6b-f0ec-fa7c-dff1-5332943fee0c}	access	explorer.exe	CLEAN
{0a4368b8-e95a-fe20-db65-b49262453eeb}	access	explorer.exe	CLEAN
{fba4da96-9e57-83ee-faf0-926ce4409cca}	access	explorer.exe	CLEAN

Registry

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

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8C45A918-B075-FEF6-0DED-B5C899623EB0}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{026F08C5-341A-9406-8117-0A9B26B9732B}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98DFD738-1E78-D107-2616-FA30049BD427}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1384CAC3-17AC-E069-EB5C-4E613FCC6FE4}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5E441BBB-4FA0-7A47-C898-77D45B377F36}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{28ABA520-2C1D-6C61-C0C7-A14CF6B906F1}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{62E4E317-0062-79DE-48F0-1E0765BB0FBB}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3588360E-206F-AD4B-5FE2-CA87B137A0AE}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD715941-4DC5-0356-AE8C-CD7DA56A3E36}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2576763A-EFDC-256B-2964-9C5E743B0B1B}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{92405BE0-7F95-9DE5-BB58-67AC75F6DB46}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder\{EAFCF446-1636-61F3-C2B6-05DEB6DE54E6}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{E258F9C2-639B-989C-87B2-698B749CE389}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A13D7EA4-5D34-8684-2E14-FDAFDFB3E2D8}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4D2056E1-92AF-EC5C-2615-AA80579018DA}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{368B1D7B-EAC9-2EB9-9178-5819EFDD132A}\ShellFolder	access, create	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9D74D8D1-A2C2-8A4E-2A5F-EBAAE5390403}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\DisplayVersion	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008F-0000-1000-0000000FF1CE}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{929FBD26-9020-399B-9A7A-751D61F0B942}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EEA66967-97E2-4561-A999-5C22E3CDE428}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN

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\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	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmp16ohnict" /s	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a0698... ...3a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VInvokeProvider@DirectUI@@UIInvokeProvider@@$0A@@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VRangeValueProvider@DirectUI@@UIRangeValueProvider@@$03@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VScrollItemProvider@DirectUI@@UIScrollItemProvider@@$05@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VScrollProvider@DirectUI@@UIScrollProvider@@$04@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VSelectionItemProvider@DirectUI@@UISelectionItemProvider@@$06@DirectUI@@QEAA@XZ	CLEAN

Process Name	Commandline	Verdict
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VSelectionProvider@DirectUI@@UISelectionProvider@@$07@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VTableItemProvider@DirectUI@@UITableItemProvider@@$09@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VTableProvider@DirectUI@@UITableProvider@@$08@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VToggleProvider@DirectUI@@UIToggleProvider@@$0L@@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$PatternProvider@VValueProvider@DirectUI@@UIValueProvider@@$0M@@DirectUI@@QEAA@XZ	CLEAN
juujetlws.exe	"C:\Users\RDhJ0CNFevzX\Desktop\JUujetlws.exe" /dll="C:\Users\RDHJ0C~1\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll" /fn_id=??0?$SafeArrayAccessor@H@DirectUI@@QEAA@XZ	CLEAN

YARA / AV

Antivirus (5)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.Generic.30199792	C:\Users\RDhJ0CNFevzX\Desktop\3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

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

Anti Virus Information

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

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows