

**MALICIOUS**

Classifications:

Downloader

Spyware

Threat Names:

Raccoon v1.7.2

Mal/Generic-S

Trojan.GenericKD.33943728

Generic.Andromeda.9525175B

Verdict Reason: -

Sample Type	Windows Exe (x86-32)
File Name	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe
ID	#968560
MD5	613617e5b41e1031a2d72e07afca8c29
SHA1	a1aaa2b0313898160c5c26b162a17179d4b164bc
SHA256	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2
File Size	463.00 KB
Report Created	2021-09-28 09:32 (UTC+2)
Target Environment	win10_64_th2_en_mso2016   exe

## OVERVIEW

### VMRay Threat Identifiers (14 rules, 73 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
<ul style="list-style-type: none"> <li>Rule "Raccoon_1_7_2" from ruleset "Malware" has matched on a memory dump for (process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe.</li> </ul>				
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
<ul style="list-style-type: none"> <li>Tries to read sensitive data of: Microsoft Outlook, Exodus Cryptocurrency Wallet, Internet Explorer, The Bat!, Internet Explorer / Edge.</li> </ul>				
4/5	Reputation	Known malicious file	1	-
<ul style="list-style-type: none"> <li>Reputation analysis labels the sample itself as "Mal/Generic-S".</li> </ul>				
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
<ul style="list-style-type: none"> <li>Built-in AV detected the downloaded file C:\Users\RDhJ0CNFevzX\AppData\Local\Low\luS0wV5wY9qH3\pB4pD1\B4sD3.zip as "Trojan.GenericKD.33943728".</li> <li>Built-in AV detected a memory dump of (process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe as "Generic.Andromeda.9525175B".</li> </ul>				
3/5	Data Collection	Reads cryptocurrency wallet locations	1	-
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet".</li> </ul>				
2/5	Data Collection	Reads sensitive mail data	2	-
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe tries to read sensitive data of mail application "The Bat!" by file.</li> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.</li> </ul>				
2/5	Data Collection	Reads sensitive browser data	3	-
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.</li> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by registry.</li> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.</li> </ul>				
1/5	Mutex	Creates mutex	1	-
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe creates mutex with name "RDhJ0CNFevzX5L1M3_noturbusiness".</li> </ul>				
1/5	Discovery	Reads system data	1	-
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe reads the cryptographic machine GUID from registry.</li> </ul>				
1/5	Hide Tracks	Creates process with hidden window	1	-
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe starts (process #2) cmd.exe with a hidden window.</li> </ul>				
1/5	Network Connection	Downloads file	1	-
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe downloads file via http from 185.138.164.150//f/GpFGKXwB3dP17Spz7px7/0cd970447812bf123f5959c8b2472008584dfcc4.</li> </ul>				
1/5	Network Connection	Downloads executable	1	Downloader
<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe downloads executable via http from 185.138.164.150//f/GpFGKXwB3dP17Spz7px7/847b96a021595de3ac81bc953e7b3e6c632cb2af.</li> </ul>				
1/5	Execution	Drops PE file	56	-

- Drops file nssdbm3.dll.
- Drops file prldap60.dll.
- Drops file qipcap.dll.
- Drops file softokn3.dll.
- Drops file ucrtbase.dll.
- Drops file vcruntime140.dll.
- Drops file AccessibleHandler.dll.
- Drops file AccessibleMarshal.dll.
- Drops file breakpadinjector.dll.
- Drops file freebl3.dll.
- Drops file IA2Marshal.dll.
- Drops file ldap60.dll.
- Drops file ldif60.dll.
- Drops file lgpllibs.dll.
- Drops file libEGL.dll.
- Drops file MapiProxy.dll.
- Drops file mozglue.dll.
- Drops file mozMapi32.dll.
- Drops file msvcp140.dll.
- Drops file nss3.dll.
- Drops file nssckbi.dll.
- Drops file api-ms-win-core-namedpipe-l1-1-0.dll.
- Drops file api-ms-win-core-processenvironment-l1-1-0.dll.
- Drops file api-ms-win-core-processthreads-l1-1-0.dll.
- Drops file api-ms-win-core-processthreads-l1-1-1.dll.
- Drops file api-ms-win-core-profile-l1-1-0.dll.
- Drops file api-ms-win-core-rtlsupport-l1-1-0.dll.
- Drops file api-ms-win-core-string-l1-1-0.dll.
- Drops file api-ms-win-core-synch-l1-1-0.dll.
- Drops file api-ms-win-core-synch-l1-2-0.dll.
- Drops file api-ms-win-core-sysinfo-l1-1-0.dll.
- Drops file api-ms-win-core-timezone-l1-1-0.dll.
- Drops file api-ms-win-core-util-l1-1-0.dll.
- Drops file api-ms-win-crt-conio-l1-1-0.dll.
- Drops file api-ms-win-crt-convert-l1-1-0.dll.
- Drops file api-ms-win-crt-environment-l1-1-0.dll.
- Drops file api-ms-win-crt-filestream-l1-1-0.dll.
- Drops file api-ms-win-crt-heap-l1-1-0.dll.
- Drops file api-ms-win-crt-locale-l1-1-0.dll.
- Drops file api-ms-win-crt-math-l1-1-0.dll.
- Drops file api-ms-win-crt-multibyte-l1-1-0.dll.
- Drops file api-ms-win-crt-private-l1-1-0.dll.
- Drops file api-ms-win-crt-process-l1-1-0.dll.
- Drops file api-ms-win-crt-runtime-l1-1-0.dll.
- Drops file api-ms-win-crt-stdio-l1-1-0.dll.
- Drops file api-ms-win-crt-string-l1-1-0.dll.
- Drops file api-ms-win-crt-time-l1-1-0.dll.
- Drops file api-ms-win-crt-utility-l1-1-0.dll.
- Drops file api-ms-win-core-file-l1-2-0.dll.
- Drops file api-ms-win-core-file-l2-1-0.dll.
- Drops file api-ms-win-core-handle-l1-1-0.dll.
- Drops file api-ms-win-core-heap-l1-1-0.dll.
- Drops file api-ms-win-core-interlocked-l1-1-0.dll.
- Drops file api-ms-win-core-libraryloader-l1-1-0.dll.
- Drops file api-ms-win-core-localization-l1-2-0.dll.
- Drops file api-ms-win-core-memory-l1-1-0.dll.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-
		<ul style="list-style-type: none"> <li>(Process #1) 889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe resolves 266 API functions by name.</li> </ul>		
-	Trusted	Known clean file	57	-

- Embedded file "nssdbm3.dll" is a known clean file.
- Embedded file "prldap60.dll" is a known clean file.
- Embedded file "qjpcap.dll" is a known clean file.
- Embedded file "softokn3.dll" is a known clean file.
- Embedded file "ucrtdbase.dll" is a known clean file.
- Embedded file "vcruntime140.dll" is a known clean file.
- Embedded file "AccessibleHandler.dll" is a known clean file.
- Embedded file "AccessibleMarshal.dll" is a known clean file.
- Embedded file "breakpadinjector.dll" is a known clean file.
- Embedded file "freebl3.dll" is a known clean file.
- Embedded file "IA2Marshal.dll" is a known clean file.
- Embedded file "ldap60.dll" is a known clean file.
- Embedded file "ldif60.dll" is a known clean file.
- Embedded file "lgpllibs.dll" is a known clean file.
- Embedded file "libEGL.dll" is a known clean file.
- Embedded file "MapiProxy.dll" is a known clean file.
- Embedded file "mozglue.dll" is a known clean file.
- Embedded file "mozMapi32.dll" is a known clean file.
- Embedded file "msvcpl140.dll" is a known clean file.
- Embedded file "nss3.dll" is a known clean file.
- Embedded file "nssckbi.dll" is a known clean file.
- Embedded file "api-ms-win-core-namedpipe-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-processenvironment-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-processthreads-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-processthreads-l1-1-1.dll" is a known clean file.
- Embedded file "api-ms-win-core-profile-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-rtssupport-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-string-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-synch-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-synch-l1-2-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-sysinfo-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-timezone-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-util-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-conio-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-convert-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-environment-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-filestream-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-heap-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-locale-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-math-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-multibyte-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-private-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-process-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-runtime-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-stdio-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-string-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-time-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-crt-utility-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-file-l1-2-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-file-l2-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-handle-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-heap-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-interlocked-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-libraryloader-l1-1-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-localization-l1-2-0.dll" is a known clean file.
- Embedded file "api-ms-win-core-memory-l1-1-0.dll" is a known clean file.
- File "C:\Users\RDhJOCN\Fevz\XAppData\Local\Low\sqlite3.dll" is a known clean file.

Score	Category	Operation	Count	Classification
-	Trusted	Executable has a trusted signature	18	-
<ul style="list-style-type: none"> <li>• Executable nssdbm3.dll has a trusted signature.</li> <li>• Executable prldap60.dll has a trusted signature.</li> <li>• Executable qipcap.dll has a trusted signature.</li> <li>• Executable softokn3.dll has a trusted signature.</li> <li>• Executable AccessibleHandler.dll has a trusted signature.</li> <li>• Executable AccessibleMarshal.dll has a trusted signature.</li> <li>• Executable breakpadinjector.dll has a trusted signature.</li> <li>• Executable freebl3.dll has a trusted signature.</li> <li>• Executable IA2Marshal.dll has a trusted signature.</li> <li>• Executable ldap60.dll has a trusted signature.</li> <li>• Executable ldif60.dll has a trusted signature.</li> <li>• Executable lgpllibs.dll has a trusted signature.</li> <li>• Executable libEGL.dll has a trusted signature.</li> <li>• Executable MapiProxy.dll has a trusted signature.</li> <li>• Executable mozglue.dll has a trusted signature.</li> <li>• Executable mozMapi32.dll has a trusted signature.</li> <li>• Executable nss3.dll has a trusted signature.</li> <li>• Executable nssckbi.dll has a trusted signature.</li> </ul>				

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	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
				#T1045 Software Packing	#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System	#T1105 Remote File Copy		
					#T1003 Credential Dumping	#T1083 File and Directory Discovery					
						#T1217 Browser Bookmark Discovery					

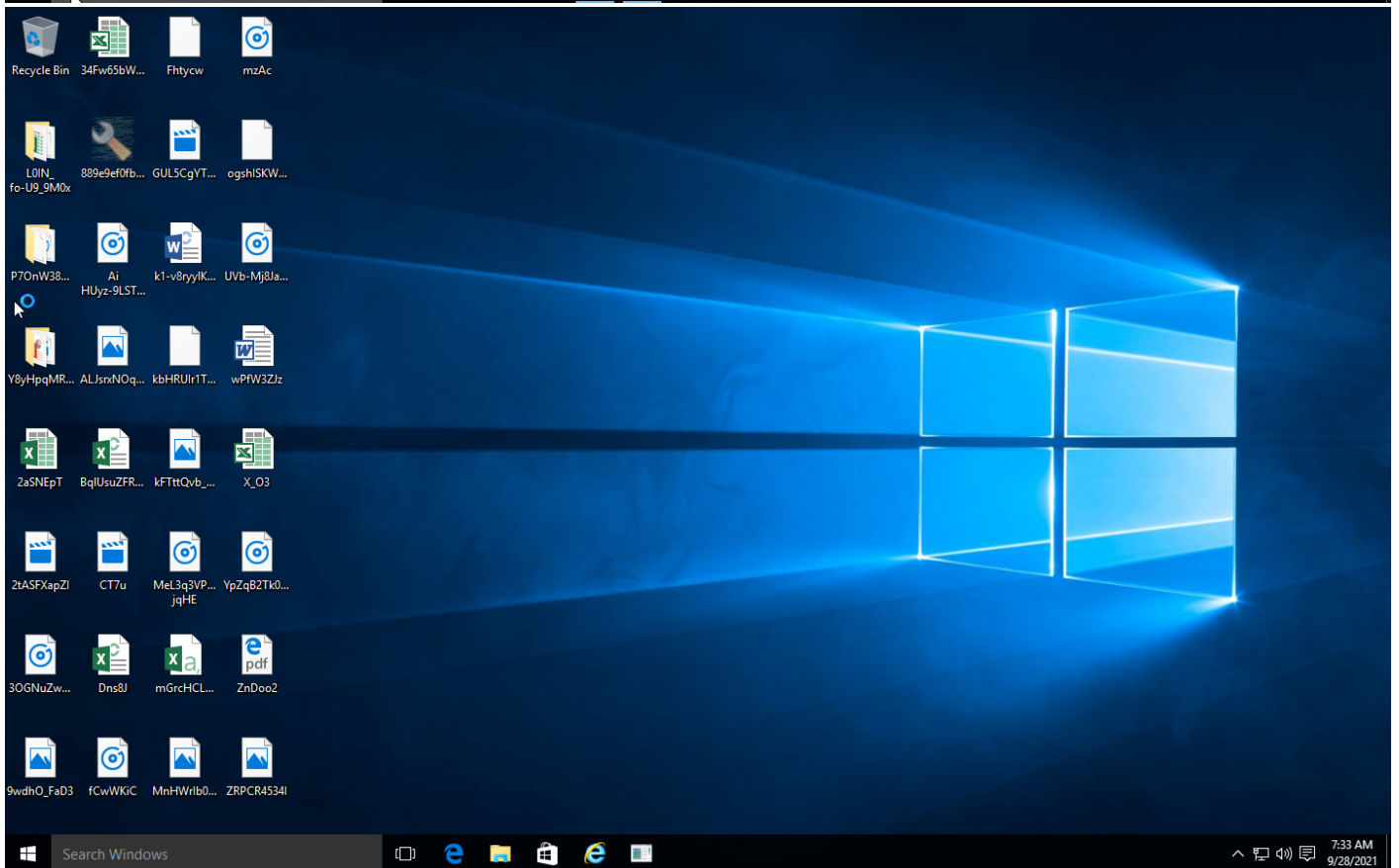
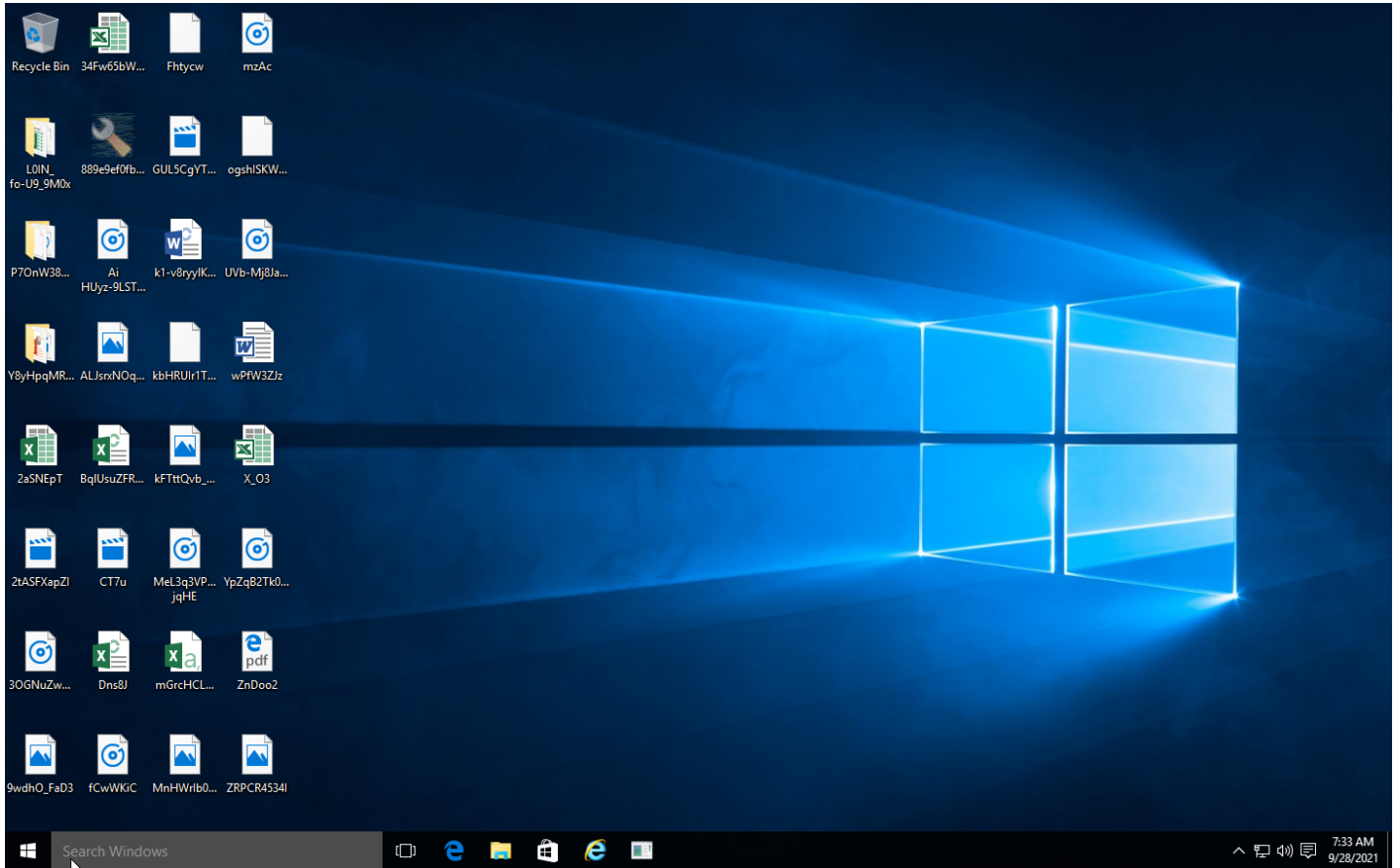
**Sample Information**

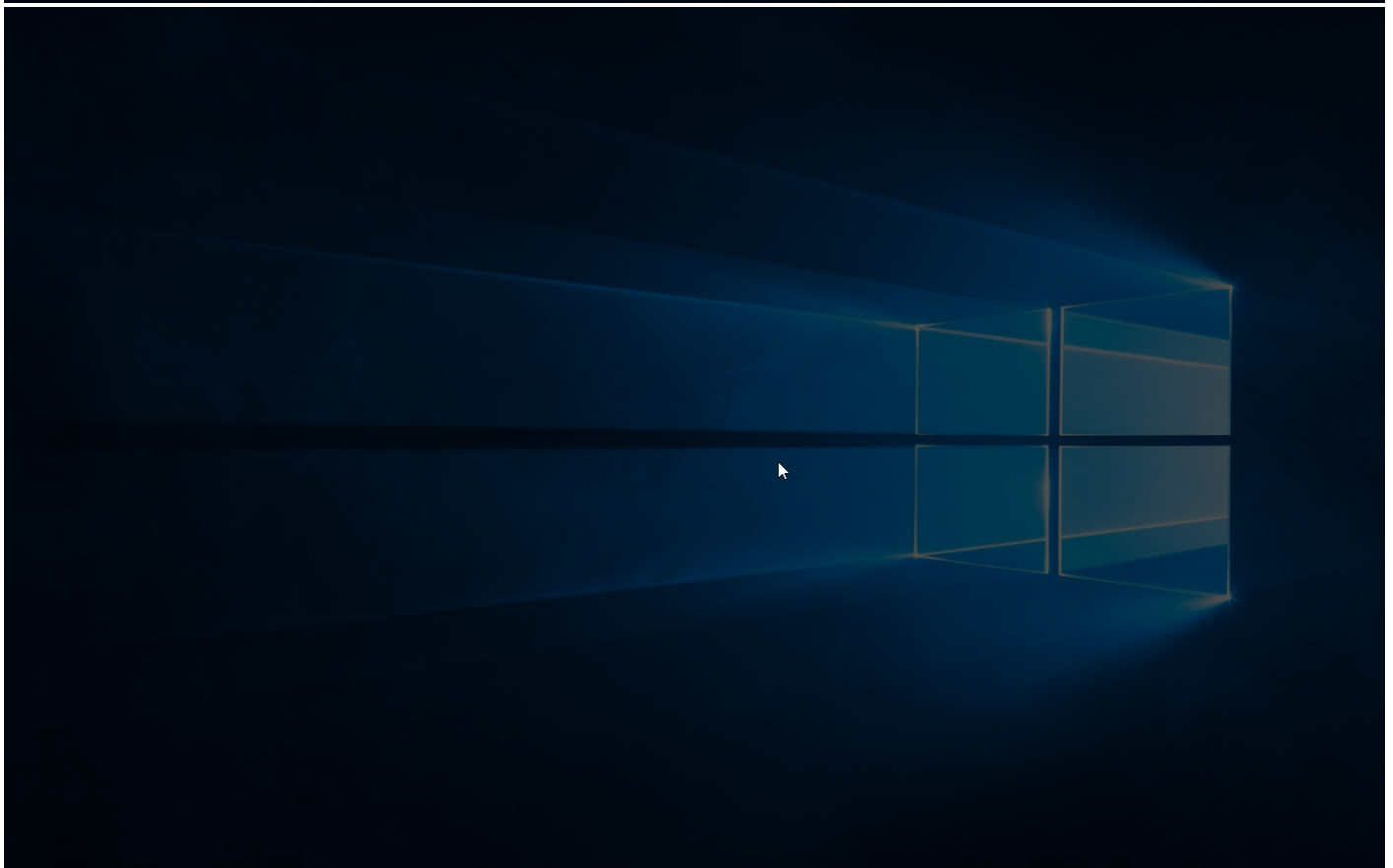
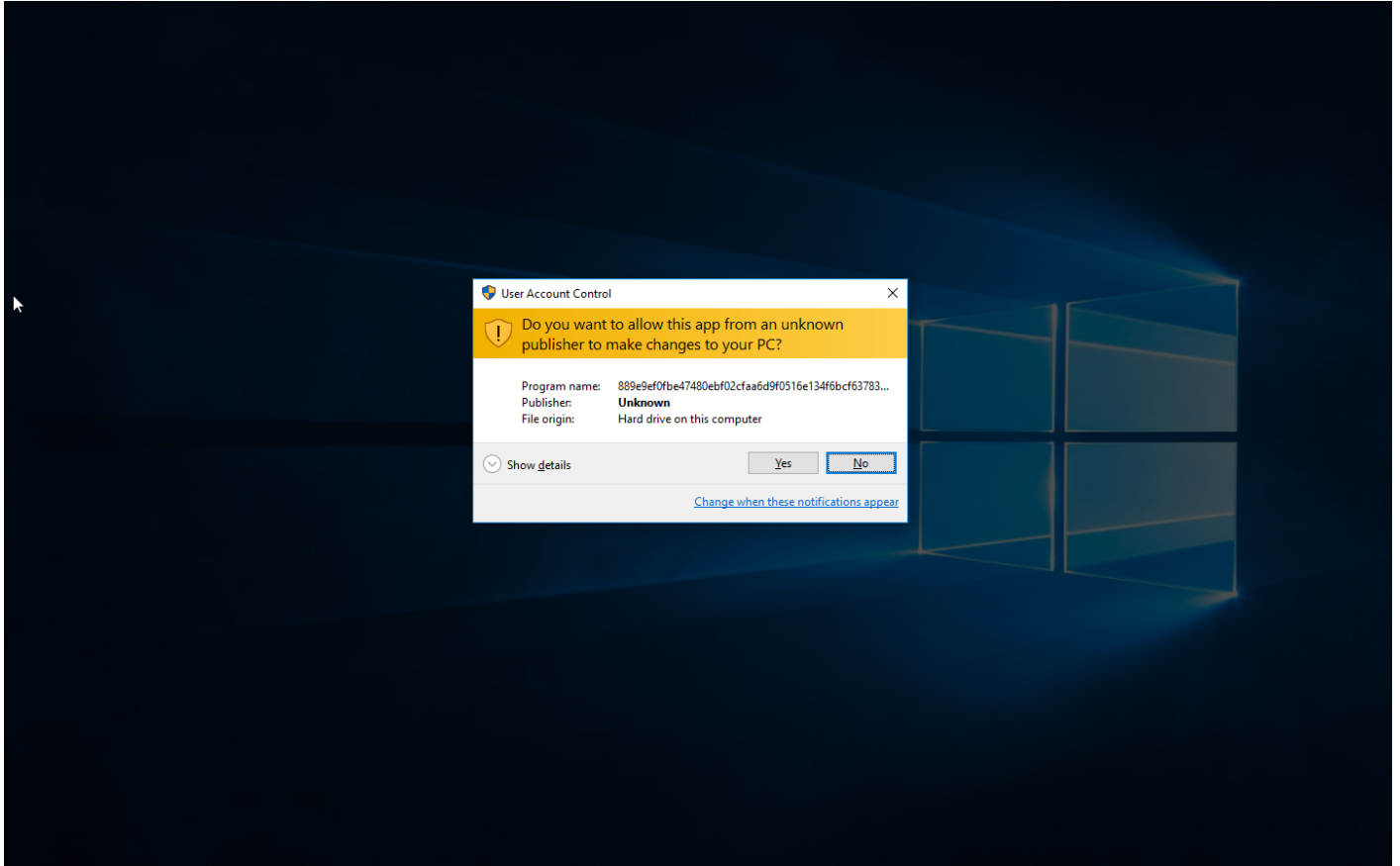
ID	#968560
MD5	613617e5b41e1031a2d72e07afca8c29
SHA1	a1aaa2b0313898160c5c26b162a17179d4b164bc
SHA256	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2
SSDeep	12288:VPr9y5EGqZgz/EHFT2mch8QaVtwjMhBp+I9ABqe:VPI5QZgz/+DE8QEiUMIi9
ImpHash	006a79ea8a61231651632116bf97f2d7
File Name	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe
File Size	463.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

**Analysis Information**

Creation Time	2021-09-28 09:32 (UTC+2)
Analysis Duration	00:01:36
Termination Reason	All processes terminated
Number of Monitored Processes	3
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	2
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	33







Screenshots truncated

## NETWORK

### General

34.65 KB total sent

3778.66 KB total received

2 ports 80, 443

2 contacted IP addresses

0 URLs extracted

2 files downloaded

0 malicious hosts detected

### DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

### HTTP/S

4 URLs contacted, 2 servers

2 sessions, 34.65 KB sent, 3778.66 KB received

### HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	185.138.164.150/	-	-		0 bytes	NA
GET	185.138.164.150////GpFGKXwB3dP17Spz7px7/847b96a021595de3ac81bc953e7b3e6c632cb2af	-	-		0 bytes	NA
GET	185.138.164.150////GpFGKXwB3dP17Spz7px7/0cd970447812bf123f5959c8b2472008584dfcc4	-	-		0 bytes	NA
GET	https://t.me/agrybirdsgamerept	-	-		0 bytes	NA

## BEHAVIOR

### Process Graph



**Process #1: 889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe**

ID	1
File Name	c:\users\rldhj0cnfevz\desktop\889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe
Command Line	"C:\Users\RdHj0CNFeVz\X\Desktop\889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe"
Initial Working Directory	C:\Users\RdHj0CNFeVz\X\Desktop\
Monitor Start Time	Start Time: 61923, Reason: Analysis Target
Unmonitor End Time	End Time: 131961, Reason: Terminated
Monitor duration	70.04s
Return Code	0
PID	1772
Parent PID	1636
Bitness	32 Bit

**Dropped Files (61)**

File Name	File Size	SHA256	YARA Match
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\sqlite3.dll	895.25 KB	83bc57dcf282264f2b00c21ce0339eac20fcb7401f7c5472c0cd0c014844e5f7	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-crt-time-l1-1-0.dll	20.30 KB	69885fd581641b4a680846f93c2dd21e5dd8e3ba37409783bc5b3160a919cb5d	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-crt-utility-l1-1-0.dll	18.30 KB	a1d1d6b0cb0a8421d7c0d1297c4c389c95514493cd0a386b49dc517ac1b9a2b0	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-crt-stdio-l1-1-0.dll	23.80 KB	b1e702b840aeb2e9244cd41512d158a43e6e9516cd2015a84eb962fa3ffb0df7	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-crt-runtime-l1-1-0.dll	22.30 KB	c9bbc07a033bab6a828ecc30648b501121586f6f53346b1cd0649d7b648ea60b	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-core-processenvironment-l1-1-0.dll	18.80 KB	96898930fb338da45497be019ae1adc63c5851141169d3023e53ce4c7a483e	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\mozglue.dll	133.95 KB	a0c6630d4012ae0311ff40f406911bcf1a23f7a4762ce219b8dffa012d188cc	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-crt-file-system-l1-1-0.dll	19.80 KB	7633774effe7c0add6752ffe90104d633fc8262c87871d096c2fc07c20018ed2	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-crt-private-l1-1-0.dll	71.30 KB	65ded8d2ce159b2f5569f55b2caf0e2c90f3694bd88c89de790a15a49d8386b9	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-core-file-l2-1-0.dll	17.80 KB	c85dc081b1964b77d289aac43cc64746e7b141d036f248a731601eb98f827719	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-core-timezone-l1-1-0.dll	17.80 KB	24c9aa0b70e557a49dac159c825a013a71a190df5e7a837bfa047a06bba59eca	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\gpllibs.dll	54.45 KB	7f93b70257d966ea1c1a6038892b19e8360aadd8e8ae58e75ebb0697b9ea8786	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\qipcap.dll	15.95 KB	7a589024cf0eeb59f020f91be4fe7ee0c90694c92918a467d5277574ac25a5a2	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\mozMapi32.dll	81.45 KB	06ef2010b738f99bcdebbf162473a4ee090678bb6862eeb0d4c7a8c3f225bb	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\inssdbm3.dll	90.45 KB	be3987a6cd970ff570a916774eb3d4e1edce675e70edac1bafe2104685610b0	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\api-ms-win-core-processthreads-l1-1-1.dll	18.30 KB	91eeb842973495deb98cef0377240d2f9c3d370ac4cf513fd21585e9f265a6a	✘
C:\Users\RdHj0CNFeVz\X\AppData\Local\Low\us0wv5wY9qH3\AccessibleHandler.dll	120.45 KB	a1a2bb03a7cfcea8944845a8fc12974482f44b44fd20be73298ffd630f65d8d0	✘

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-file-l1-2-0.dll	17.80 KB	c8c499b012d0d63b7afc8b4ca42d6d996b2fc2e8b5f94cacfbec9e6f33e8a03	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\inss3.dll	1215.95 KB	1989526553fd1e1e49b0fea8036822ca062d3d39c4cab4a37846173d0f1753d5	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\msvcpl140.dll	429.80 KB	334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\apiProxy.dll	19.45 KB	bcfb0e397df40aba8c8c5dd23c13c414345decdd3b42df946226be97defbf30	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-handle-l1-1-0.dll	17.80 KB	945cc64ee04b1964c1f9fcdc3124dd83973d332f5cfb696cdf128ca5c4cbd0e5	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-interop-l1-1-0.dll	17.44 KB	deccd75fc3fc2bb31338b6fe26deffbd7914c6cd6a907e76fd4931b7d141718c	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\vruntime140.dll	81.82 KB	c40bb03199a2054dabfc7a8e01d6099e91de7193619effbd0f142a7bf031c14d	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\libEGL.dll	21.95 KB	7b9fc6be34f43d39471c2add872d5b4350853db11cc66a323ef9e0c231542fb9	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\softokn3.dll	141.45 KB	25a4dae37120426ab060ebb39b7030b3e7c1093cc34b087f223b6843b651871	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-profile-l1-1-0.dll	17.30 KB	8eb5270fa99069709c846db38be743a1a80a42aa1a8776131f79e1d07cc411c	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-math-l1-1-0.dll	28.30 KB	bec7b7ab83a5d0ec5c35f0841cbbf413e01ac878550fbb34816ed55185dcfed	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-multibyte-l1-1-0.dll	25.80 KB	66abf3a1147751c95689f5bc6a259e55281ec3d06d3332dd0ba464effa716735	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-processthreads-l1-1-0.dll	18.94 KB	9dab884071b1f7d7a167f9bec94ba2bee875e3365603fa29b31de286c6a97a1d	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-memory-l1-1-0.dll	18.30 KB	bb33a9e906a5863043753c44f6f8165afe4d5edb7e55efa47e6e1ed90778eca	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-synch-l1-1-0.dll	19.80 KB	5dd4ccd63e6ed07ca3987ab5634ca4207d69c47c2544dfefc41935617652820f	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-environment-l1-1-0.dll	18.30 KB	c0d75d1887c32a1b1006b3cfc29df84a0d73c435cdcb40b6964be176a61382	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\breakpadinjector.dll	114.95 KB	87ed943d2f06d9ca8824789405b412e770fe84454950ec7e96105f756d858e52	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-convert-l1-1-0.dll	21.80 KB	3cc1377d495260c380e8d225e5ee889cbb2ed22e79862d4278cfa898e58e44d1	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-namedpipe-l1-1-0.dll	17.80 KB	c4f60911068ab6d7f578d449ba7b5b9969f08fc683fd0ce8e2705bbf061f507	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\idif60.dll	19.95 KB	3aabb0aa86ce8a91e5c49b7de577af73b9889d7f03af919f17f3f315a879b0f	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-string-l1-1-0.dll	22.94 KB	73cc56f20268bfb329ccd891822e2e70dd70fe21fc7101deb3fa30c34a08450c	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-localization-l1-2-0.dll	20.30 KB	03ad57c24ff2cf895b5f533f0ecbd10266fd8634c6b9053cc9c33b814ad5d97	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-string-l1-1-0.dll	17.80 KB	7670fdede524a485c13b11a7c878015e9b0d441b7d8eb15ca675ad6b9c9a7311	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-heap-l1-1-0.dll	18.80 KB	f5cf623ba14b017af4aec6c15eee446c647ab6d2a5dee9d6975adc69994a113d	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\dap60.dll	128.95 KB	2b128b3702f8509f35cad0d657c9a00f0487b93d70336df229f8588fba6ba926	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-sysinfo-l1-1-0.dll	18.80 KB	4b704b36e1672ae02e697efd1b46f11b42d776550ba34a90cd189f6c5c61f92	✘

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\A2Marshal.dll	68.95 KB	621f38bd19f62c9ce6826d492ecd710c00bbdcf1fb4e4815883f29f1431dfda	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-rtlsupport-l1-1-0.dll	17.30 KB	2257fea1e71f7058439b3727ed68ef048bd91dcacd64762eb5c64a9d49df0b57	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\inssckbi.dll	328.45 KB	2481da1c459a2429a933d19ad6ae514bd2ae59818246ddb67b0ef44146ced3d8	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\AccessibleMarshal.dll	25.45 KB	d368eb240106f87188c4f2ae30db793a2d250d9344f0e0267d4f6a58e68152ad	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-util-l1-1-0.dll	17.80 KB	f7d450a0f59151bcefb98d20fcae35f76029df57138002db5651d1b6a33adc86	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\ucrtbase.dll	1115.30 KB	0bb8c77de80acf9c43de59a8fd75e611cc3eb8200c69f11e94389e8af2ceb7a9	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\pridap60.dll	23.45 KB	46b005817868f91cf60baa052ee96436cf6194ce9a61e93260df5037cdfa37a5	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-libraryloader-l1-1-0.dll	18.30 KB	bb25ccf8694d1fcfce85a7159dcf6985fdb54728d29b021cb3d14242f65909ce	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-locale-l1-1-0.dll	18.30 KB	565a2eec5449eeeed68b430f2e9b92507f979174f9c9a71d0c36d58b96051c33	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\freebl3.dll	326.45 KB	9876c53134dbbec4dcca67581f53638eba3fea3a15491aa3cf2526b71032da97	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-synch-l1-2-0.dll	18.30 KB	30d99ce1d732f6c9cf82671e1d9088aa94e720382066b79175e2d16778a3dad1	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-process-l1-1-0.dll	18.80 KB	c03124ba691b187917ba79078c66e12cbf5387a3741203070ba23980aa471e8b	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-core-heap-l1-1-0.dll	17.80 KB	44f6df4280c8ecc9c6e609b1a4bfee041332d337d84679cfe0d6678ce8f2998a	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\api-ms-win-crt-conio-l1-1-0.dll	18.80 KB	9ca21763c528584bdb4efeb914faaf792c9d7360677c87e93bd7ba7bb4367f2	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\us0wV5wY9qH3\pB4pD1B4sD3.zip	2762.03 KB	4cfada7eb51a6c0cb26283f9c86784b2b2587c59c46a5d3dc0f06cad2c55ee97	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\outlook.txt	134 bytes	33897c27a1f9608d3f7f99c801fa58039911fa834c475d9b949baa3fc2d114d8	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\lyH9tY9hO9gL5	998 bytes	ee2dcb8f8e55ad28130d04c44882b1ebd07f562039bb45f322241991d66a505f	✘
C:\Users\RDhJ0CNFeVzX\AppData\Local\Low\6ORbjhpsjA4.zip	961 bytes	9278d1d9f27fa99a64c6e9c0d7909cd7cfd11e8c9b35fb7ec230ca36a4bc1d38	✘

**Host Behavior**

Type	Count
Module	353
File	8429
Environment	52
System	39
User	4
Mutex	2
Process	1
Registry	947
COM	1
-	138

**Network Behavior**

Type	Count
HTTP	4
HTTPS	1
TCP	2



**Process #2: cmd.exe**

ID	2
File Name	c:\windows\system32\cmd.exe
Command Line	cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q "C:\Users\RDhJ0CNFevzX\Desktop\889e9ef0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\LocalLow\
Monitor Start Time	Start Time: 130063, Reason: Child Process
Unmonitor End Time	End Time: 148040, Reason: Terminated
Monitor duration	17.98s
Return Code	0
PID	2124
Parent PID	1772
Bitness	32 Bit

**Host Behavior**

Type	Count
Module	8
Registry	17
File	31
Environment	19
System	1
Process	1

**Process #4: timeout.exe**

ID	4
File Name	c:\windows\syswow64\timeout.exe
Command Line	timeout /T 10 /NOBREAK
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\LocalLow\
Monitor Start Time	Start Time: 136840, Reason: Child Process
Unmonitor End Time	End Time: 148294, Reason: Terminated
Monitor duration	11.45s
Return Code	0
PID	5072
Parent PID	2124
Bitness	32 Bit

**Host Behavior**

Type	Count
Module	2
System	127
File	69

## ARTIFACTS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
889e9ef0f0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2	C:\Users\RDhJ0CNFevzX\Desktop\889e9ef0f0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	Sample File	463.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
4cfada7eb51a6c0cb26283f9c86784b2b2587c59c46a5d3dc0f06cad2c55ee97	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\pB4pD1B4sD3.zip	Downloaded File	2762.03 KB	application/zip	Create, Read, Delete, Write, Access	MALICIOUS
33897c27a1f9608d3f7f99c801fa58039911fa83c475d9b949baa3fc2d114d8	outlook.txt, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\outlook.txt, mails\outlook.txt	Dropped File	134 bytes	text/plain	Write, Read, Create, Access	CLEAN
be3987a6cd970ff570a916774eb3d4e1edce675e70edac1baf5e2104685610b0	nssdbm3.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\nssdbm3.dll	Embedded File	90.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
46b005817868f91cf60baa052ee96436fc6194ce9a61e93260df5037cdfa37a5	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\prldap60.dll, prldap60.dll	Embedded File	23.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
7a589024cf0eeb59f020f91be4fe7ee0c90694c92918a467d5277574ac25a5a2	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\qipcap.dll, qipcap.dll	Embedded File	15.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
25a4dae37120426ab060ebb39b7030b3e7c1093cc34b0877223b6843b651871	softokn3.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\softokn3.dll	Embedded File	141.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
0bb8c77de80ac9c43de59a8fd75e611c3eb8200c69f11e9439e8af2ceb7a9	ucrtbase.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\ucrtbase.dll	Embedded File	1115.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d	vcruntime140.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\vcruntime140.dll	Embedded File	81.82 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
a1a2bb03a7cfea8944845a8fc12974482f44b44fd20be73298ffd630f65d8d0	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\AccessibleHandler.dll, AccessibleHandler.dll	Embedded File	120.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
d368eb240106f87188c4f2ae30db793a2d250d9344f0e0267d4f6a5e688152ad	AccessibleMarshal.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\AccessibleMarshal.dll	Embedded File	25.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
87ed943d2f06d9ca8824789405b412e770fe84454950ec7e96105f756d858e52	breakpadinjector.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\breakpadinjector.dll	Embedded File	114.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
9876c53134dbbec4dcca67581f5363eba3fea3a15491aa3cf2526b71032da97	freebl3.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\freebl3.dll	Embedded File	326.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
621f38bd19f62c9ce6826d492ecd710c00bbdcf1fb4e4815883f29f1431dfda	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\IA2Marshal.dll, IA2Marshal.dll	Embedded File	68.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
2b128b3702f8509f35cad0d657c9a00f0487b93d70336df229f8588fba6ba926	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\ldap60.dll, ldap60.dll	Embedded File	128.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
3aahbe0aa86ce8a91e5c49b7de577af73b9889d7f03af919f17f3f315a879b0f	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\ldif60.dll, ldif60.dll	Embedded File	19.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
7f93b70257d966ea1c1a6038892b19e8360aad8e8ae58e75ebb0697b9ea8786	lgpllibs.dll, C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\lgpllibs.dll	Embedded File	54.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
7b9fc6be34f43d39471c2add872d5b4350853db11cc66a323ef9e0c231542fb9	C:\Users\RDhJ0CNFevzX\AppData\Local\Low\Software\Y9qH3\libEGL.dll, libEGL.dll	Embedded File	21.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
bcb0e397df40aba8c8c5dd23c13c414345decdd3d4b2df946226be97defbf30	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\MapiProxy_InUse.dll, MapiProxy.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\MapiProxy.dll, MapiProxy_InUse.dll	Embedded File	19.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
a0c6630d4012ae0311ff404f06911bc1a23f7a4762ce219b8dfffa012d188cc	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\mozglue.dll, mozglue.dll	Embedded File	133.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
06ef2010b738f99bcdebfb1624734ae090678bb6862eeb0d4c7a8c3f225bb	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\mozMapi32.dll, mozMapi32.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\mozMapi32_InUse.dll	Embedded File	81.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
334e69ac9367f708ce601a6f490ff227d6c206336da5222f148b25831d22e13d4	msvcpl140.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\msvcpl140.dll	Embedded File	429.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
1989526553fd1e1e49b0fea8036822ca062d3d39c4cab4a37846173d0f1753d5	nss3.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\nss3.dll	Embedded File	1215.95 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
2481da1c459a2429a933d19ad6ae514bd2ae59818246ddb67b0ef44146ced3d8	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\nssckbi.dll, nssckbi.dll	Embedded File	328.45 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
c4f60f911068ab6d7f578d449ba7b5b9969f08fc683fd0ce8e2705bbf061f507	api-ms-win-core-namedpipe-l1-1-0.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-namedpipe-l1-1-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
96898930ffb338da45497be019ae1adcd63c5851141169d3023e53ce4c7a483e	api-ms-win-core-processenvironment-l1-1-0.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-processenvironment-l1-1-0.dll	Embedded File	18.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
9dab884071b1f7d7a167f9bec94ba2bee875e3365603fa29b31de286c6a97a1d	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-processthreads-l1-1-0.dll, api-ms-win-core-processthreads-l1-1-0.dll	Embedded File	18.94 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
91eeb842973495deb98cef0377240d2f9c3d370ac4cf513fd215857e9f265a6a	api-ms-win-core-processthreads-l1-1-1.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-processthreads-l1-1-1.dll	Embedded File	18.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
8eb5270fa99069709c846db38be743a1a80a42aa1a88776131f79e1d07cc411c	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-profile-l1-1-0.dll, api-ms-win-core-profile-l1-1-0.dll	Embedded File	17.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
2257fea1e71f7058439b3727ed68ef048bd91dcacd64762eb5c64a9d49df0b57	api-ms-win-core-rtlsupport-l1-1-0.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-rtlsupport-l1-1-0.dll	Embedded File	17.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
7670fdede524a485c13b11a7c878015e9b0d441b7d8eb15ca675ad6b9c9a7311	api-ms-win-core-string-l1-1-0.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-string-l1-1-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
5dd4ccd63e6ed07ca3987ab5634ca4207d69c47c2544dfe4c1935617652820f	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-synch-l1-1-0.dll, api-ms-win-core-synch-l1-1-0.dll	Embedded File	19.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
30d99ce1d732f6c9cf82671e1d9088aa94e720382066b79175e2d16778a3dad1	C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-synch-l1-2-0.dll, api-ms-win-core-synch-l1-2-0.dll	Embedded File	18.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
4b704b36e1672ae02e697efd1bf46f11b42d776550ba34a90cd189f6c5c61f92	api-ms-win-core-sysinfo-l1-1-0.dll, C: \\Users\RDhJ0CNFeVzX\AppData\Local\Low\U50wV5wY9qH3\api-ms-win-core-sysinfo-l1-1-0.dll	Embedded File	18.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
24c9aa0b70e557a49dac159c825a013a71a190df5e7a837bfa047a06bba59eca	C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-core-timezone-l1-1-0.dll, api-ms-win-core-timezone-l1-1-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
f7d450af59151bcefb98d20fcae35f76029df57138002db5651d1b6a33adc86	C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-core-util-l1-1-0.dll, api-ms-win-core-util-l1-1-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
9ca21763c528584bdb4efebe914faaf792c9d7360677c87e93bd7ba7bb4367f2	api-ms-win-crt-conio-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-conio-l1-1-0.dll	Embedded File	18.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
3cc1377d495260c380e8d225e5ee889cbb2ed22e79862d4278cfa898e58e44d1	C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-convert-l1-1-0.dll, api-ms-win-crt-convert-l1-1-0.dll	Embedded File	21.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
c0d75d1887c32a1b1006b3cfc29df84a0d73c435cdcb404b6964be176a61382	api-ms-win-crt-environment-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-environment-l1-1-0.dll	Embedded File	18.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
7633774effe7c0add6752ffe90104d633fc8262c87871d096c2fc07c20018ed2	C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-file-system-l1-1-0.dll, api-ms-win-crt-file-system-l1-1-0.dll	Embedded File	19.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
f5cf623ba14b017af4aec6c15eee446c647ab6d2a5dee9d6975adc69994a113d	C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-heap-l1-1-0.dll, api-ms-win-crt-heap-l1-1-0.dll	Embedded File	18.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
565a2eec5449eeed68b430f2e9b92507979174f9c9a71d0c36d58b96051c33	api-ms-win-crt-locale-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-locale-l1-1-0.dll	Embedded File	18.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
beece7bab83a5d0ec5c35f0841cbbf413e01ac878550fbb34816ed55185dcfed	C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-math-l1-1-0.dll, api-ms-win-crt-math-l1-1-0.dll	Embedded File	28.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
66abf3a1147751c95689f5bc6a259e55281ec3d06d3332dd0ba464effa716735	api-ms-win-crt-multibyte-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-multibyte-l1-1-0.dll	Embedded File	25.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
65ded8d2ce159b2f5569f55b2caf0e2c90f3694bd88c89de790a15a49d8386b9	api-ms-win-crt-private-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-private-l1-1-0.dll	Embedded File	71.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
c03124ba691b187917ba79078c66e12cbf5387a3741203070ba23980aa471e8b	api-ms-win-crt-process-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-process-l1-1-0.dll	Embedded File	18.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
c9bbc07a033bab6a828ecc30648b501121586f6f53346b1cd0649d7b648ea60b	api-ms-win-crt-runtime-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-runtime-l1-1-0.dll	Embedded File	22.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
b1e702b840aeb2e9244cd41512d158a43e6e9516cd2015a84eb962fa3ff0df7	api-ms-win-crt-stdio-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-stdio-l1-1-0.dll	Embedded File	23.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
73cc56f20268bfb329ccd891822e2e70dd70fe21fc7101deb3fa30c34a08450c	api-ms-win-crt-string-l1-1-0.dll, C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-string-l1-1-0.dll	Embedded File	22.94 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
69885fd581641b4a690846f93c2dd21e5dd8e3ba37409783bc5b3160a919cb5d	C: \\Users\RDhJ0CNFevz\XAppData\Local\Low\US0wV5wY9qH3\api-ms-win-crt-time-l1-1-0.dll, api-ms-win-crt-time-l1-1-0.dll	Embedded File	20.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a1d1d6b0cb0a8421d7c0d1297c4c389c95514493cd0a386b49dc517ac1b9a2b0	api-ms-win-crt-utility-l1-1-0.dll, C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-crt-utility-l1-1-0.dll	Embedded File	18.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
c8c499b012d0d63b7afc8b4c43c64746e7b141d036f248acfbec9e6f33e8a03	api-ms-win-core-file-l1-2-0.dll, C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-file-l1-2-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
c85dc081b1964b77d289aac43c64746e7b141d036f248a731601eb98f827719	C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-file-l2-1-0.dll, api-ms-win-core-file-l2-1-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
945cc64ee04b1964c19fcdc3124dd83973d332f5cfb696cdf128ca5c4cbdd0e5	api-ms-win-core-handle-l1-1-0.dll, C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-handle-l1-1-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
44f6df4280c8ecc9c6e609b1a4f6ee041332d332f5cfb696cdf128ca5c4cbdd0e5	api-ms-win-core-heap-l1-1-0.dll, C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-heap-l1-1-0.dll	Embedded File	17.80 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
deccd75fc3fc2bb31338b6fe26defbd7914c6cd6a907e76fd4931b7d141718c	C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-interlocked-l1-1-0.dll, api-ms-win-core-interlocked-l1-1-0.dll	Embedded File	17.44 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
bb25ccf8964d1fcce85a7159dcf6985fdb54728d29b021cb3d14242f65909ce	api-ms-win-core-libraryloader-l1-1-0.dll, C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-libraryloader-l1-1-0.dll	Embedded File	18.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
03ad57c24ff2cf895b5f533f0ebd10266fd8634c6b9053cc9cb33b814ad5d97	C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-localization-l1-2-0.dll, api-ms-win-core-localization-l1-2-0.dll	Embedded File	20.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
bb33a9e906a5863043753c44f6f8165afe4d5edb7e55efa4c7e6e1ed90778eca	api-ms-win-core-memory-l1-1-0.dll, C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\US0wV5wY9qH3\api-ms-win-core-memory-l1-1-0.dll	Embedded File	18.30 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN
9278d1d9f27fa99a64c6e9c0d7909cd7cfd11e8c9b35fb7ec230ca36a4bc1d38	C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\6ORbJhpsJA4.zip	Dropped File	961 bytes	application/zip	Create, Read, Delete, Write, Access	CLEAN
ee2dcb8f8e55ad28130d04c44882b1ebd07f562039bb45f322241991d66a505f	System Info.txt, C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\yH9Y9hO9gLS	Embedded File	998 bytes	text/plain	Create, Read, Delete, Write, Access	CLEAN
83bc57dcf282264f2b00c21ce0339eac20fcb7401f7c5472c0cd0c014844e5f7	C:\Users\RDhJ0CNFevzX\AppDataLocal\Low\sqlite3.dll	Downloaded File	895.25 KB	application/vnd.microsoft.portable-executable	Write, Create, Delete, Access	CLEAN

## Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\889e9ef0fbae47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	Sample File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Low\sqlite3.dll	Downloaded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\atomic	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Binance	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\1password	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bitwarden\data.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Daedalus Mainnet	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\electroncash	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFezX\AppData\Roaming\electrum	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\electrum-LTC	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\Ethereum Wallet	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\Ethereum	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\Exodus\exodus.wallet	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Local\Blockstream	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\Guarda	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\Jaxx\Local Storage	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\com.libertyjaxx	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\Documents\Monerowallets	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\MyMonero	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\WalletWasabi\Client	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\Opera Software	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\ins3.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\Roaming\discord	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\pB4pD1B4sD3.zip	Downloaded File	Create, Read, Delete, Write, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\outlook.txt	Dropped File	Write, Read, Create, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\insdbm3.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\prldap60.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\qipcap.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\softokn3.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\ucrtbase.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\vcrunime140.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\AccessibleHandler.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\AccessibleMarshal.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\breakpadinjector.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFezX\AppData\LocalLow\us0wV5wY9qH3\freebl3.dll	Embedded File	Write, Create, Delete, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\A2Mashal.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\ldap60.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\ldif60.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\lgpllibs.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\libEGL.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\MapiProxy.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\MapiProxy_InUse.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\mozglue.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\mozMapi32.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\mozMapi32_InUse.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\msvcpl140.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\inssckbi.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-namedpipe-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-processenvironment-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-processthreads-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-processthreads-l1-1-1.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-profile-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-rtlsupport-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-string-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-synch-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-synch-l1-2-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-sysinfo-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-timezone-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-util-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFeVzX\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-crt-conio-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN



File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-convert-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-environment-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-file-system-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-heap-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-locale-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-math-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-multibyte-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-private-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-process-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-runtime-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-stdio-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-string-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-time-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-crt-utility-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-file-l1-2-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-file-l2-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-handle-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-heap-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-interlocked-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-libraryloader-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-localization-l1-2-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\us0wv5wY9qH3\api-ms-win-core-memory-l1-1-0.dll	Embedded File	Write, Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\yH9tY9hO9gL5	Dropped File, Embedded File	Create, Read, Delete, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\firefox_urls.txt	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\chrome_urls.txt	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\ie_autofill.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\ie_ftp_data.txt	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\thunderbird.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\foxmail.temp	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Bither\address.db	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\wallets\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\discord_files\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\bitwarden\data.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\_1password	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\6ORbjhpsjA4.zip	Dropped File	Create, Read, Delete, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\CC.txt	Accessed File	Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow\TL4W4xN3sO8	Accessed File	Delete, Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\LocalLow	Accessed File	Access	CLEAN
Nul	Accessed File	Create, Access	CLEAN
C:\Windows\SysWOW64\timeout.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
\\?.C:\Users\RDhJ0CNFevzX\Desktop\889e9ef0f0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	Accessed File	Write, Access	CLEAN

**URL**

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://185.138.164.150	-	185.138.164.150	-	POST	CLEAN
http://185.138.164.150/fffGpFGKXwB3dP17Spz7px7/847b96a021595de3ac81bc953e7b3e6c632cb2af	-	185.138.164.150	-	GET	CLEAN
http://185.138.164.150/fffGpFGKXwB3dP17Spz7px7/0cd970447812bf123f5959c8b2472008584dfcc4	-	185.138.164.150	-	GET	CLEAN
https://t.me/agrybirdsgamerept	-	149.154.167.99	-	GET	CLEAN

**Domain**

Domain	IP Address	Country	Protocols	Verdict
t.me	149.154.167.99	-	HTTPS	CLEAN

**IP**

IP Address	Domains	Country	Protocols	Verdict
149.154.167.99	t.me	United Kingdom	DNS, HTTPS, TCP	CLEAN
185.138.164.150	-	United Kingdom	HTTP, TCP	CLEAN

**Mutex**

Name	Operations	Parent Process Name	Verdict
RDhJ0CNFevzX5L1M3_noturbusiness	access	889e9ef0f0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN

**Registry**

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	889e9ef0f0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	889e9ef0f0be47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Identities	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Account Manager	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Account Manager\Outlook	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\19.0\Outlook\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\18.0\Outlook\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\17.0\Outlook\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Email Address	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Email Address	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Server URL	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HT TP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SM TP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\PO P3 Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SM TP Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMA P Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SM TP Email Address	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SM TP Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\PO P3 Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\PO P3 User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SM TP User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\INN TP Email Address	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\INN TP User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\INN TP Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMA P Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMA P User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Em ail	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HT TP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HT TP Server URL	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\PO P3 User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMA P User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HT TPMail User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea1 35471e147c2.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\HT TMail Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\SMTP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\POP3 Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\IMAP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\NNTP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\HT TMail Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\SMTP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\POP3 Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\IMAP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\NNTP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\HT TMail Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\SMTP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\POP3 Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\SMTP Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\IMAP Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\SMTP Email Address	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\SMTP Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3 Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3 User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\SMTP User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\NNTP Email Address	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\NNT P User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\NNT P Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\Email	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\HTTP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\HTTP Server URL	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3 User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\HTTPMail User Name	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\HTTPMail Server	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\SMTP User	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3 Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\NNT P Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\HTTPMail Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\SMTP Password2	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3 Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\NNT P Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\HTTP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\SMTP Password	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Port	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb08da6869ae8f9d	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\fb6ed2903a4a11cfb57e524153480001	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Outlook\Profiles\Outlook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN



Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NE5BAKEX\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NEData	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NEData\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NMobileOptionPack	access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NMobileOptionPack\DisplayName	read, access	889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	CLEAN

**Reduced dataset**
**Process**

Process Name	Commandline	Verdict
889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe	"C:\Users\RDhJOCNFez\X\Desktop\889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe"	MALICIOUS
cmd.exe	cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q "C:\Users\RDhJOCNFez\X\Desktop\889e9ef0fbe47480ebf02cfaa6d9f0516e134f6bcf63783ee5ea135471e147c2.exe"	CLEAN
timeout.exe	timeout /T 10 /NOBREAK	CLEAN



## Antivirus (2)

File Type	Threat Name	File Name	Verdict
Downloaded File	Trojan.GenericKD.33943728	C: \\Users\RDhJ0CNFevzX\AppData\Local\Low\luS0wV5wY9qH3lpB4pD 11B4sD3.zip	MALICIOUS
Memory Dump	Generic.Andromeda.9525175B	-	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 01:56:46+00:00
Built-in AV Database Records	10476967

### 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	RDhJ0CNFezX
User Profile	C:\Users\RDhJ0CNFezX
Temp Directory	C:\Users\RDhJ0C-1\AppData\Local\Temp
System Root	C:\Windows