MALICIOUS

Classifications: Spyware | Downloader

Threat Names: Stealc | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**vwnxa.exe**
ID	#7601410
MD5	c8ee28a45cccf35fbbb6364414412ba6
SHA1	4713a14226020ac7802768f8f6a5de9cd8ea9228
SHA256	660f62a2f0eb7ccae6170ec09629ade73d1874486027f22dddd92326a8e0b18e
File Size	257.50 KB
Report Created	2023-05-03 16:22 (UTC+2)
Target Environment	win7_32_sp1 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 38 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Stealc configuration was extracted	1	Spyware
	• A configuration for Stealc was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	5	Spyware
	• YARA detected "Stealc" from ruleset "Stealc" in memory dump data from (process #1) vwnxa.exe. • YARA detected "Stealc" from ruleset "Stealc" in the sample file C:\Users\EEBsYm5\Desktop\vwnxa.exe. • YARA detected "Stealc_fstrings" from ruleset "Malware" in function strings data from (process #1) vwnxa.exe. • YARA detected "Stealc" from ruleset "Stealc" in function strings data from (process #1) vwnxa.exe. • YARA detected "Stealc_fstrings" from ruleset "Stealc" in function strings data from (process #1) vwnxa.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Google Chrome, Microsoft Outlook, Mozilla Firefox.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #1) vwnxa.exe takes screenshots and potentially exfiltrates data.			
4/5	Reputation	Contacts known malicious URL	8	-
	• Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/nss3.dll" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/freebl3.dll" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/vcruntime140.dll" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/mozglue.dll" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/softokn3.dll" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/msvcp140.dll" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/82de66e9459cdb5f.php" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/sqlite3.dll" which was contacted by (process #1) vwnxa.exe as Mal/HTMLGen-A.			
3/5	Data Collection	Takes screenshot	1	-
	• (Process #1) vwnxa.exe takes a screenshot using BitBlt API.			
3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
	• (Process #1) vwnxa.exe uploads 488.686KB data using HTTP POST.			
2/5	Data Collection	Reads sensitive browser data	2	-
	• (Process #1) vwnxa.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #1) vwnxa.exe tries to read sensitive data of web browser "Mozilla Firefox" by file.			
2/5	Discovery	Searches for senstive browser data	2	-
	• (Process #1) vwnxa.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #1) vwnxa.exe searches for sensitive data of web browser "Mozilla Firefox" by file.			
2/5	Discovery	Searches for cryptocurrency wallet locations	3	-

Score	Category	Operation	Count	Classification
	• (Process #1) vwnxa.exe searches for the cryptocurrency wallet "Bitcoin" for "BTC". • (Process #1) vwnxa.exe searches for the cryptocurrency wallet "Ethereum" for "ETH". • (Process #1) vwnxa.exe searches for the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC".			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #1) vwnxa.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Discovery	Searches for senstive application data	1	-
	• (Process #1) vwnxa.exe searches for sensitive data of application "Pidgin" by file.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) vwnxa.exe enumerates running processes.			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #1) vwnxa.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #1) vwnxa.exe tries to gather information about application "Steam" by registry.			
1/5	Network Connection	Downloads executable	7	Downloader
	• (Process #1) vwnxa.exe downloads Windows executable via http from hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/nss3.dll. • (Process #1) vwnxa.exe downloads Windows executable via http from hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/vcruntime140.dll. • (Process #1) vwnxa.exe downloads Windows executable via http from hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/sqlite3.dll. • (Process #1) vwnxa.exe downloads Windows executable via http from hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/mozglue.dll. • (Process #1) vwnxa.exe downloads Windows executable via http from hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/msvcp140.dll. • (Process #1) vwnxa.exe downloads Windows executable via http from hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/softokn3.dll. • (Process #1) vwnxa.exe downloads Windows executable via http from hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/freebl3.dll.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) vwnxa.exe resolves 191 API functions by name.			
-	Trusted	Known clean file	8	-
	• Embedded file "C:\ProgramData\freebl3.dll" is a known clean file. • Embedded file "" is a known clean file. • Embedded file "C:\ProgramData\vcruntime140.dll" is a known clean file. • Embedded file "C:\ProgramData\nss3.dll" is a known clean file. • File "C:\Users\EEBsYm5\AppData\Roaming\Mozilla\Firefox\Profiles\h231daer.default\cookies.sqlite-shm" is a known clean file. • Embedded file "C:\ProgramData\softokn3.dll" is a known clean file. • Embedded file "C:\ProgramData\mozglue.dll" is a known clean file. • Embedded file "C:\ProgramData\msvcp140.dll" is a known clean file.			
-	Trusted	Executable has a trusted signature	4	-
	• Executable C:\ProgramData\freebl3.dll has a trusted signature. • Executable C:\ProgramData\nss3.dll has a trusted signature. • Executable C:\ProgramData\softokn3.dll has a trusted signature. • Executable C:\ProgramData\mozglue.dll has a trusted signature.			

Malware Configuration: Stealc

Metadata	Key	Extracted Value
Encryption Key	Key Algorithm	NDYzNTI0MDA3NDU5NjY4MTQwNjA= RC4
URL	Url	http://176.113.115.26/1e46dcfeff07ca0e/82de66e9459cdb5f.php
Other: Expiration Date	Value	2023-05-19

Mitre ATT&CK Matrix

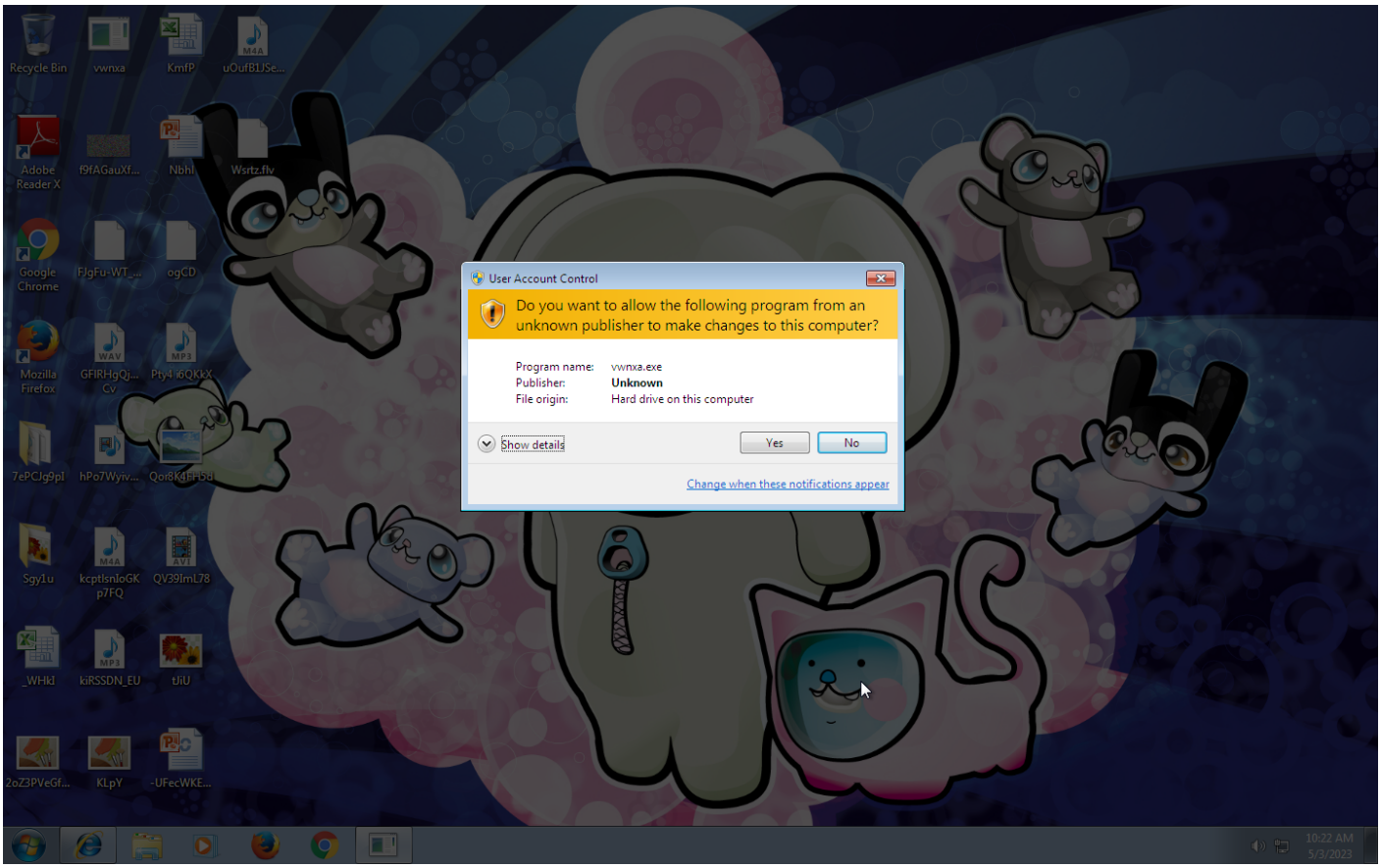
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing	#T1081 Credentials in Files	#T1057 Process Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
					#T1214 Credentials in Registry	#T1083 File and Directory Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
					#T1056 Input Capture	#T1012 Query Registry		#T1113 Screen Capture			
								#T1056 Input Capture			

Sample Information

ID	#7601410
MD5	c8ee28a45cccf35fbbb6364414412ba6
SHA1	4713a14226020ac7802768f8f6a5de9cd8ea9228
SHA256	660f62a2f0eb7ccae6170ec09629ade73d1874486027f22dddd92326a8e0b18e
SSDeep	1536:TTPrKkVttb0nBtc8riV8avsqAVGHL37hhTStjhOxxtain:TTPrKkVttbx82VHkZ2L373TS4Ui
ImpHash	c2e4487f461edff82f81a902e3e4f0b5
File Name	vwnxa.exe
File Size	257.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-05-03 16:22 (UTC+2)
Analysis Duration	00:00:30
Termination Reason	All processes terminated
Number of Monitored Processes	1
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	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	7


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

NETWORK

General

508.41 KB total sent

5272.50 KB total received

1 ports 80

1 contacted IP addresses

1 URLs extracted

41 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

8 URLs contacted, 1 servers

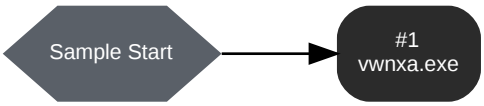
1 sessions, 12201.77 KB sent, 126539.91 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/nss3.dll	-	-	-	0 bytes	MALICIOUS
GET	hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/vcruntime140.dll	-	-	-	0 bytes	MALICIOUS
POST	hxxp://176[.]113[.]115[.]26/82de66e9459cdb5f.php	-	-	-	0 bytes	MALICIOUS
GET	hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/sqlite3.dll	-	-	-	0 bytes	MALICIOUS
GET	hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/mozglue.dll	-	-	-	0 bytes	MALICIOUS
GET	hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/msvcp140.dll	-	-	-	0 bytes	MALICIOUS
GET	hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/softokn3.dll	-	-	-	0 bytes	MALICIOUS
GET	hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/freebl3.dll	-	-	-	0 bytes	MALICIOUS

BEHAVIOR

Process Graph



Process #1: vwnxa.exe

ID	1
File Name	c:\users\eebsym5\desktop\vwnxa.exe
Command Line	"C:\Users\EEBsYm5\Desktop\vwnxa.exe"
Initial Working Directory	C:\Users\EEBsYm5\Desktop\
Monitor Start Time	Start Time: 35771, Reason: Analysis Target
Unmonitor End Time	End Time: 55684, Reason: Terminated
Monitor duration	19.91s
Return Code	0
PID	4004
Parent PID	1460
Bitness	32 Bit

Dropped Files (16)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\GDGHIDBKJEGIECBGIEHCGIDBAA	10240.00 KB	884367f3f05e23a8399be58029222d2cfa343b08387b9d872467dac362f2513a	✖
-	78.98 KB	8934aaeb65b6e6d253dfe72dea5d65856bd871e989d5d3a2a35edfe867bb4825	✖
nM8rm6.doc	9.93 KB	a0cd0667aa850470cbaff1704680d79a2b07d6c9c50ca9a4394a78ad3c793650	✖
-	251.83 KB	74ebbac956e519e16923abdc5ab8912098a4f64e38ddcb2eae23969f306afe5a	✖
C:\ProgramData\GDGDHJJDGHCAAAKEHIJKEBAEGH	7.00 KB	32812d196066c99bf3852fad78b00063dc68e6cc5fb26ae6c862c8c5777d51b0	✖
eG-e_J.doc	32.66 KB	75eccb764d6e872d85ad8e6689fb0fea63fd0b4b119e69210744412f4fa8b756	✖
-	669.33 KB	edd043f2005dbd5902fc421eabb9472a7266950c5cbaca34e2d590b17d12f5fa	✖
C:\ProgramData\AAEHIDAKECFIEBGDHJEB	18.00 KB	c381401ea96dfe9b926126dcbbc0dd6ab541dbf549732cc6c66f20096b1f663e	✖
C:\Users\EEBsYm5\AppData\Roaming\Mozilla\Firefox\Profiles\h231daer.default\cookies.sqlite-shm	32.00 KB	fd4c9fda9cd3f9ae7c962b0ddf37232294d55580e1aa165aa06129b8549389eb	✖
s2y-1 48pOM9j.doc	44.76 KB	e418a7f395ea245a176305c66ac51124cc00cce703134d1390ed0582516456de	✖
C:\ProgramData\IIECFHDB	68.00 KB	81251896048c480249f0c9379e88c5ab97a99a7e0d2f847cc59758cf68609f08	✖
-	439.48 KB	5136a49a682ac8d7f1ce71b211de8688fce42ed57210af087a8e2dbc8a934062	✖
C:\Users\EEBsYm5\AppData\Roaming\Mozilla\Firefox\Profiles\h231daer.default\cookies.sqlite-wal	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\ProgramData\FHJEGIIEGIDGIDHJDAKFCBKEHI	512.00 KB	42696770a5842f7e1a629b40075d599df14f2fed5f97b8ff8608420d6ef9dd09	✖
C:\ProgramData\nss3.dll	1998.33 KB	ac5c92fe6c51cfa742e475215b83b3e11a4379820043263bf50d4068686c6fa5	✖
-	593.83 KB	ba06a6ee0b15f5be5c4e67782eec8b521e36c107a329093ec400fe0404eb196a	✖

Host Behavior

Type	Count
Module	226

Type	Count
System	41
User	2
-	1
Registry	379
Keyboard	2
Process	95
File	1045
Environment	2

Network Behavior

Type	Count
HTTP	24

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3da62c15bfe69a27cecfcc357c07619018f180cd318884d583c1b4dfea449bdf	-	Memory Dump	2212.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
dcf9cf2362e45f2cb56d04b9d767c0f59f8fc4eb54bead63d90753c8e6e122fa	-	Memory Dump	2212.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
9806aabdd04018319576749d79d3da362b02146be52be3f741e4b5e124c2c920	-	Memory Dump	2212.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
660f62a2f0eb7ccae6170ec09629ade73d1874486027f22dddd92326a8e0b18e	C:\Users\EEBsYm5\Desktop\vwnxa.exe	Sample File	257.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
6ce7dfc2f16f05c77561b8fa1551b0705c5e3ed4a25fe38d4ce72d4f34b707cc	-	Downloaded File	43.54 KB	text/plain	-	CLEAN
96c425a343e52c10809c9ebb914978bbe79f16b589c77ae423ea466d2ce0f17f	-	Downloaded File	20 bytes	text/plain	-	CLEAN
8fc0a97c5941255e61be513c46fda9e307bc86cedce6c626ecd37ff6d5f80eda	-	Downloaded File	22 bytes	text/plain	-	CLEAN
2de501ae4b72c94d362d646553db3dc0cd05b00331e9adc661037beacd83d990	-	Downloaded File	60 bytes	text/plain	-	CLEAN
9c7351b7cdd0d3f2d085a0952e2c3407a3e07ead2f7e31c792ac39eeff5252c5	-	Downloaded File	72 bytes	text/plain	-	CLEAN
b2ad4e60b74781102e9452c58a729eaca884fce9540d1f3a4c0508bb7728545b	-	Downloaded File	20 bytes	text/plain	-	CLEAN
884367f3f05e23a8399be58029222d2cfa343b08387b9d872467dac362f2513a	C:\ProgramData\GDGHIDBKJEGIECBGIEHCGIDBAA	Dropped File	10240.00 KB	application/x-sqlite3	Access, Create, Delete, Write	CLEAN
4d6406d078e609d647ea9bc5d2bce9469109de85e0f5e36c28b72697161097a3	-	Downloaded File	1.31 KB	text/plain	-	CLEAN
8934aaeb65b6e6d253dfe72dea5d65856bd871e989d5d3a2a35edfe867bb4825	C:\ProgramData\vcruntime140.dll, c:\users\eebsym5\appdata\local\microsoft\windows\temporary internet files\content.ie5\i81wo4ad\vcruntime140[1].dll	Downloaded File	78.98 KB	application/vnd.microsoft.portable-executable	Access, Create	CLEAN
a0cd0667aa850470cbaff1704680d79a2b07d6c9c50ca9a4394a78ad3c793650	nM8rm6.doc	Dropped File	9.93 KB	application/CDFV2	Access, Create, Delete, Read, Write	CLEAN
88dc357fda1e78806ae1670353be57ecb686d2d61f2d86cdcbf9b181441534ea	-	Downloaded File	28 bytes	text/plain	-	CLEAN
312055727f6078c4fc6c209fe766990d3988be33b59cd2507a64ec50803aeb53	-	Downloaded File	376 bytes	text/plain	-	CLEAN
74ebbac956e519e16923abdc5ab8912098a4f64e38ddcb2eae23969f306afe5a	C:\ProgramData\softokn3.dll, c:\users\eebsym5\appdata\local\microsoft\windows\temporary internet files\content.ie5\i81wo4ad\softokn3[1].dll	Downloaded File	251.83 KB	application/vnd.microsoft.portable-executable	Access, Create	CLEAN
9fdbc2321b330f72d01d484a488f21f437ed5df2e2a6aee0210bbc992b115292	-	Downloaded File	20 bytes	text/plain	-	CLEAN
32812d196066c99bf3852fad78b00063dc68e6cc5fb26ae6c862c8c5777d51b0	C:\ProgramData\GDGDHJJDGHCAAAKEHIJKEBAEGH	Dropped File	7.00 KB	application/x-sqlite3	Access, Create, Delete, Read, Write	CLEAN
29528238f8a951b1de959f0eabc94710400fadd43ba9cda07be9fbb166895c14	-	Downloaded File	28 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6944001df848fbac8e05351598ad0b7d0d2e3284b494a24436bb1b89e778554d	-	Downloaded File	36 bytes	text/plain	-	CLEAN
f7850ac28ba4f5b6f9c35dcfdc39025a0489c376b133153781d44056fae7e245	-	Downloaded File	44 bytes	text/plain	-	CLEAN
75eccb764d6e872d85ad8e6689fb0fea63fd0b4b119e69210744412f4fa8b756	eG-e_J.doc	Dropped File	32.66 KB	application/CDFV2	Access, Create, Delete, Read, Write	CLEAN
edd043f2005dbd5902fc421eabb9472a7266950c5cbaca34e2d590b17d12f5fa	C:\ProgramData\freebl3.dll, c:\users\eebsym5\appdata\local\microsoft\windows\temporary internet files\content.ie5\i81wo4ad\freebl3[1].dll	Downloaded File	669.33 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
617401590e4d67d5cbf79d45256208f4b25b3dea05c75b1226f4b6f27367f57a	-	Downloaded File	250.75 KB	text/plain	-	CLEAN
c381401ea96dfe9b926126dcbbc0dd6ab541dbf549732cc6c66f20096b1f663e	C:\ProgramData\AAEHIDAKECFIEBGDHJEB	Dropped File	18.00 KB	application/x-sqlite3	Access, Create, Delete, Read, Write	CLEAN
f04a245445864fc3bb22c3a219d97fcd948d627677eb32ca0e8d1161c67521aa	-	Downloaded File	148 bytes	text/plain	-	CLEAN
2ea50eb652fb93a1625c83dfa7daeac964a93b4bbde393f9d37807b2e4079548	-	Downloaded File	13.24 KB	text/plain	-	CLEAN
fd4c9fda9cd3f9ae7c962b0ddf37232294d55580e1aa165aa06129b8549389eb	C:\Users\EEBsYm5\AppData\Roaming\Mozilla\Firefox\Profiles\h231daer.default\cookies.sqlite-shm, C:\Users\EEBsYm5\AppData\Roaming\Mozilla\Firefox\Profiles\h231daer.default\places.sqlite-shm	Dropped File	32.00 KB	application/octet-stream	Access, Create, Delete	CLEAN
efd6d146f1aa1f21622bf2a18171ee1a9d6e6ae46da80bf4c7448e5a4a03141a	-	Downloaded File	52 bytes	text/plain	-	CLEAN
e418a7f395ea245a176305c66ac51124cc00cce703134d1390ed0582516456de	s2y-1 48pOM9j.doc	Dropped File	44.76 KB	application/CDFV2	Access, Create, Delete, Read, Write	CLEAN
497074b2f5afcda331a9fb57a6e79b47d3d5425fc8037e6c2e702d96934460bb	-	Downloaded File	4.94 KB	text/plain	-	CLEAN
a05437837cc03bcb5cc153cdf580b2e12c8c668130b37e2bf3c1e6cdf7faddc8	-	Downloaded File	7.09 KB	text/plain	-	CLEAN
81251896048c480249f0c9379e88c5ab97a99a7e0d2f847cc59758cf68609f08	C:\ProgramData\IIECFHDB	Dropped File	68.00 KB	application/x-sqlite3	Access, Create, Delete, Read, Write	CLEAN
55e03d7b027bf0841f98b32a44c8f2e13075710176c471ff11554794c11a49ae	-	Downloaded File	90.67 KB	text/plain	-	CLEAN
5136a49a682ac8d7f1ce71b211de8688fce42ed57210af087a8e2dbc8a934062	C:\ProgramData\msvcp140.dll, c:\users\eebsym5\appdata\local\microsoft\windows\temporary internet files\content.ie5\i81wo4ad\msvcp140[1].dll	Downloaded File	439.48 KB	application/vnd.microsoft.portable-executable	Access, Create	CLEAN
1fd4ef08ff23481d6a334b77bfd98a65287e8c625008a3e57ec388cfb0e319ba	-	Downloaded File	8 bytes	text/plain	-	CLEAN
a4c3ed04a95a3da14a9d235c83d868bed7c0f45cf7f3faa751ee8f50598d2211	-	Downloaded File	4 bytes	text/plain	-	CLEAN
2d333fa52eff4a256ba814ccb742f4f6128c4265b47c358f38e59972dd33de9a	-	Downloaded File	36 bytes	text/plain	-	CLEAN
dbb985ef1ea6dff788a36f8fe2f28d623180af0a35c61b9a8a4f82c2be3588c1	-	Downloaded File	1.63 KB	text/plain	-	CLEAN
ed8d95a36eaf0417ad5682aafd358275431abd83c84bbcaa3c64fbfa539a5558	-	Downloaded File	3.72 KB	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
37a8eec1ce19687d132fe29051dca629d164e2c4958ba141d5f4133a33f0688f	-	Downloaded File	7 bytes	text/plain	-	CLEAN
4841020c8bd06b08fde6e44cbe2e2ab33439e1c8368e936ec5b00dc0584f7260	-	Downloaded File	1081.05 KB	application/vnd.microsoft.portable-executable	-	CLEAN
42696770a5842f7e1a629b40075d599df14f2fed5f97b8ff8608420d6ef9dd09	C:\ProgramData\FHJEGIIEGIDGIDHJDAKFCBKEHI	Dropped File	512.00 KB	application/x-sqlite3	Access, Create, Delete, Write	CLEAN
fb2f451e9652d7e36eb298b9e172b5268b0d67687f5e486f0e377b8914fe625b	-	Downloaded File	1.00 KB	text/plain	-	CLEAN
074a91666f3a2a86ebe6dce98640908083bc73c172c5cc6f5ac18a63cef63e33	-	Downloaded File	60 bytes	text/plain	-	CLEAN
9acc092ec9a45382e1a2e8b4910c10b9ea73ef825a5a06eb61833f270e34b89f	-	Downloaded File	272 bytes	text/plain	-	CLEAN
4085118690b6b24a58e8b9a2e26a15a31f2dfbd9e6280752a04af70e3a5389cc	-	Downloaded File	7 bytes	text/plain	-	CLEAN
52ee5a777eae2f4d35d5c1ba70a71217e068d4a1ad38331e712d3f38bb1682bf	-	Downloaded File	1.43 KB	text/plain	-	CLEAN
92cd10e6b8b068a931196d1d73a032543d5ca1a5bf445e27a1af74258254517c	-	Downloaded File	7 bytes	text/plain	-	CLEAN
3d7db37d08f9140fd09f12b9621cd0954b6d56a9d2f357fb2c7f5d62636d2fd1	-	Downloaded File	5 bytes	text/plain	-	CLEAN
ac5c92fe6c51cfa742e475215b83b3e11a4379820043263bf50d4068686c6fa5	C:\ProgramData\nss3.dll, c:\users\eebsym5\appdata\local\microsoft\windows\temporary internet files\content.ie5\i81wo4ad\nss3[1].dll	Downloaded File	1998.33 KB	application/vnd.microsoft.portable-executable	Access, Create	CLEAN
248ab483acb6c38d681236a10a55027f3d5fcb5b2e85366932e0cd9021e7ebcd	-	Downloaded File	59.68 KB	text/plain	-	CLEAN
ba06a6ee0b15f5be5c4e67782eec8b521e36c107a329093ec400fe0404eb196a	C:\ProgramData\mozglue.dll, c:\users\eebsym5\appdata\local\microsoft\windows\temporary internet files\content.ie5\i81wo4ad\mozglue[1].dll	Downloaded File	593.83 KB	application/vnd.microsoft.portable-executable	Access, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\EEBsYm5\Desktop\vwnxa.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Crashpad\Local Extension Settings\cjelfplplebdjjenllpjcblmjkfcffne\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0\manifest.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Top Sites\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\lt\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\sl\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\el\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extension State\CURRENT\Network\Cookies	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\pnacl\Local Extension Settings\ibnejdfjmmkpcnlpebklmnkoeoihofec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\es_419\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SSLErrorAssistant\Local Extension Settings\ibnejdfjmmkpcnlpebklmnkoeoihofec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\CertificateTransparency\Local Extension Settings\kncchdigobghenbbaddojjnnaogfppfj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\pt_BR\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\vi\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SSLErrorAssistant\Local Extension Settings\fnjhmkhhmkbjkkabndcnnogagogbneec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\Local Extension Settings\nhnkbkgjikgcigadomkphalanndcapjk\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Local State\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Crashpad\Local Extension Settings\cphhlgmgameodnhkjdmkpanlelnlohao\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\sl\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\First Run\Local Extension Settings\fhbohimaelbohpjbbldcngcnapndodjp\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\PepperFlash\Local Extension Settings\ibnejdfjmmkpcnlpebklmnkoeoihofec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\History	Accessed File	Access, Create, Read	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.0.0.6_0\icon_16.png\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\hpglfhgfnhbgpjdenjgmdgoeiappafln\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\bg\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\ru\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Current Tabs\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Origin Bound Certs-journal\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\hi\Network\Cookies	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\es\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\ar\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\EVWhitelist\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Web Data	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\EVWhitelist\Local Extension Settings\cphhlgmgameodnhkjdmkpanlelnlohao\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\fr\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\ja\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\WidevineCdm\Local Extension Settings\ejbalbakoplchlghecdalmeeeajnimhm\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SwiftShader\IndexedDB\chrome-extension_hnfanknocfeofbddgcijnmhnfnkdnaad_0.indexeddb.leveldb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\ru\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\First Run\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\First Run\Local Extension Settings\ibnejdfjmmkpcnlpebklmnkoeoihofec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\da\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\en_GB\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\ca\Network\Cookies	Accessed File	Access	CLEAN
c:\users\eebsym5\appdata\local\microsoft\windows\temporary internet files\content.ie5\i81wo4ad\mozglue[1].dll	Downloaded File, Extracted File	-	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\First Run\Local Extension Settings\kpfopkelmapcoipemfendmdcghnegimn\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\da\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\First Run\Local Extension Settings\cphhlgmgameodnhkjdmkpanlelnlohao\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\MANIFEST-000001\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\es_419\messages.json\Network\Cookies	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\WidevineCdm\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\CertificateTransparency\Local Extension Settings\hpglfhgfnhbgpjdenjgmdgoeiappafln\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_metadata\computed_hashes.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\First Run\Local Extension Settings\ffnbelfdoeiohenkjibnmadjiehjhajb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\sv\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\en_US\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\History-wal	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\cs\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\el\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\vi\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\previews_opt_out.db\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\Documents\\s2y-1 48pOM9j.doc	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SwReporter\Local Extension Settings\ffnbelfdoeiohenkjibnmadjiehjhajb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\Local Extension Settings\cjelfplplebdjjenllpjcblmjkfcffne\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SwReporter\Local Extension Settings\nlbmnnijcnlegkjjpcfjclmcfggfefdm\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\lt\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\fil\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\History-journal	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\et\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\IndexedDB\chrome-extension_hnfanknocfeofbddgcijnmhnfnkdnaad_0.indexeddb.leveldb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\EVWhitelist\Local Extension Settings\fhbohimaelbohpjbbldcngcnapndodjp\CURRENT	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\EVWhitelist\Local Extension Settings\fnjhmkhhmkbjkkabndcnnogagogbneec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\el\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\PepperFlash\Local Extension Settings\hnfanknocfeofbddgcijnmhnfnkdnaad\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\Local Extension Settings\nanjmdknhkinifnkgdcggcfnhdaammmj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\FileTypePolicies\Local Extension Settings\ibnejdfjmmkpcnlpebklmnkoeoihofec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_aohghmighlieiainnegkcijnfilokake\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\pl\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\he\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\EVWhitelist\Local Extension Settings\hnfanknocfeofbddgcijnmhnfnkdnaad\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\ejbalbakoplchlghecdalmeeeajnimhm\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\Local Extension Settings\ffnbelfdoeiohenkjibnmadjiehjhajb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SSLErrorAssistant\Local Extension Settings\djclckkglechooblngghdinmeemkbgci\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\First Run\Local Extension Settings\nhnkbkgjikgcigadomkphalanndcapjk\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\CertificateTransparency\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\ghbmnnjooekpmoecnnniInnbdlolhkhi\MANIFEST-000001\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_metadata\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\JumpListIcons\BBA7.tmp\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Roaming\Mozilla\Firefox\Profiles\h231daer.default\places.sqlite-wal	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\PepperFlash\Local Extension Settings\nanjmdknhkinifnkgdcggcfnhdaammmj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\nanjmdknhkinifnkgdcggcfnhdaammmj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\FileTypePolicies\Local Extension Settings\ejbalbakoplchlghecdalmeeeajnimhm\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\he\Network\Cookies	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\hu\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Crashpad\Local Extension Settings\kncchdigobghenbbaddojjnnaogfppfj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\ca\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\uk\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\WidevineCdm\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\EVWhitelist\Local Extension Settings\nlbmnnijcnlegkjjpcfjclmcfggfefdm\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\FileTypePolicies\Local Extension Settings\fhbohimaelbohpjbbldcngcnapndodjp\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\FileTypePolicies\Local Extension Settings\fnjhmkhhmkbjkkabndcnnogagogbneec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SSLErrorAssistant\Local Extension Settings\cphhlgmgameodnhkjdmkpanlelnlohao\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\pnacl\Local Extension Settings\nhnkbkgjikgcigadomkphalanndcapjk\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000001\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Local State\Local Extension Settings\hnfanknocfeofbddgcijnmhnfnkdnaad\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SwiftShader\Local Extension Settings\hnfanknocfeofbddgcijnmhnfnkdnaad\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\it\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SwiftShader\Local Extension Settings\nanjmdknhkinifnkgdcggcfnhdaammmj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\Local Extension Settings\nlbmnnijcnlegkjjpcfjclmcfggfefdm\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\en_US\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\sv\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\ar\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\OriginTrials\Local Extension Settings\kncchdigobghenbbaddojjnnaogfppfj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Local State\Local Extension Settings\kncchdigobghenbbaddojjnnaogfppfj\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles\..\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\freebl3.dll	Accessed File, Downloaded File, Extracted File	Access, Create, Write	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\CertificateTransparency\Local Extension Settings\fhbohimaelbohpjbbldcngcnapndodjp\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\previews_opt_out.db-journal\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SwReporter\Local Extension Settings\ibnejdfjmmkpcnlpebklmnkoeoihofec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\CertificateTransparency\Local Extension Settings\cjelfplplebdjjenllpjcblmjkfcffne\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\th\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\pl\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0_locales\es\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\PepperFlash\Local Extension Settings\fnjhmkhhmkbjkkabndcnnogagogbneec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.9_0\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\tr\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\PepperFlash\Local Extension Settings\ffnbelfdoeiohenkjibnmadjiehjhajb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\EVWhitelist\Local Extension Settings\hpglfhgfnhbgpjdenjgmdgoeiappafln\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\pnacl\Local Extension Settings\cjelfplplebdjjenllpjcblmjkfcffne\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\kncchdigobghenbbaddojjnnaogfppfj\CURRENT	Accessed File	Access	CLEAN
C:\ProgramData\mozglue.dll	Accessed File, Downloaded File, Extracted File	Access, Create	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\pnacl\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\CertificateTransparency\Local Extension Settings\fnjhmkhhmkbjkkabndcnnogagogbneec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\nl\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\fhbohimaelbohpjbbldcngcnapndodjp\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\PepperFlash\IndexedDB\chrome-extension_hnfanknocfeofbddgcijnmhnfnkdnaad_0.indexeddb.leveldb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\WidevineCdm\Local Extension Settings\fnjhmkhhmkbjkkabndcnnogagogbneec\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0_locales\bg\messages.json\Network\Cookies	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Crashpad\IndexedDB\chrome-extension_hnfanknocfeofbddgcijnmhnfnkdnaad_0.indexeddb.leveldb\CURRENT	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\14.1_0_locales\cs\messages.json\Network\Cookies	Accessed File	Access	CLEAN
C:\Users\EEBsYm5\AppData\Local\Google\Chrome\User Data\SSLErrorAssistant\Local Extension Settings\nlbmnnijcnlegkjjpcfjclmcfggfefdm\CURRENT	Accessed File	Access	CLEAN
C:\ProgramData\GDGDHJJDGHCAAAKEHIJKEBAEGH-wal	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/nss3.dll	Contacted, Extracted	176.113.115.26	Hong Kong	GET	MALICIOUS
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/freebl3.dll	Contacted, Extracted	176.113.115.26	Hong Kong	GET	MALICIOUS
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/vcruntime140.dll	Contacted, Extracted	176.113.115.26	Hong Kong	GET	MALICIOUS
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/mozglue.dll	Contacted, Extracted	176.113.115.26	Hong Kong	GET	MALICIOUS
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/softokn3.dll	Contacted, Extracted	176.113.115.26	Hong Kong	GET	MALICIOUS
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/82de66e9459cdb5f.php	Extracted	176.113.115.26	Hong Kong	-	MALICIOUS
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/msvcp140.dll	Contacted, Extracted	176.113.115.26	Hong Kong	GET	MALICIOUS
hxxp://176[.]113[.]115[.]26/82de66e9459cdb5f.php	Contacted, Extracted	176.113.115.26	Hong Kong	POST	MALICIOUS
hxxp://176[.]113[.]115[.]26/1e46dcfeff07ca0e/sqlite3.dll	Contacted, Extracted	176.113.115.26	Hong Kong	GET	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
176.113.115.26	-	Hong Kong	HTTP, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0C0A-0000-0000000FF1CE}_Office14.PRJPROR_{DEA87BE2-FFCC-4F33-9946-FCBE55A1E998}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0016-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	vwnxa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\oftware\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676\00000003	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0054-0409-0000-0000000FF1CE}_Office14.VISIOR_{CDC4310F-8189-485F-B47D-D972217CE173}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{99ACCA38-6DD3-48A8-96AE-A283C9759279}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{582EA838-9199-3518-A05C-DB09462F68EC}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-002C-0409-0000-0000000FF1CE}_Office14.PRJPROR_{7CA93DF4-8902-449E-A42E-4C5923CFBDE3}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0115-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{4560037C-E356-444A-A015-D21F487D809E}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0016-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-00B4-0409-0000-0000000FF1CE}_Office14.PRJPROR_{18A0C151-8F8A-4B68-A960-60C464B94329}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0115-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{4560037C-E356-444A-A015-D21F487D809E}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-040C-0000-0000000FF1CE}_Office14.PRJPROR_{46298F6A-1E7E-4D4A-B5F5-106A4F0E48C6}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{AC76BA86-7AD7-FFFF-7B44-AA0000000001}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 25.0 (x86 en-US)\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-00B4-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{68306422-7C57-373F-8860-D26CE4BA2A15}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-0057-0000-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-006E-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{4560037C-E356-444A-A015-D21F487D809E}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-006E-0409-0000-0000000FF1CE}_Office14.PRJPROR_{4560037C-E356-444A-A015-D21F487D809E}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0015-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0C0A-0000-0000000FF1CE}_Office14.PROPLUSR_{DEA87BE2-FFCC-4F33-9946-FCBE55A1E998}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-00BA-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83217045FF}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0C0A-0000-0000000FF1CE}_Office14.PROPLUSR_{DEA87BE2-FFCC-4F33-9946-FCBE55A1E998}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-002C-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-002C-0409-0000-0000000FF1CE}_Office14.PRJPROR_{7CA93DF4-8902-449E-A42E-4C5923CFBDE3}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-040C-0000-0000000FF1CE}_Office14.PROPLUSR_{46298F6A-1E7E-4D4A-B5F5-106A4F0E48C6}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0044-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-040C-0000-0000000FF1CE}_Office14.PROPLUSR_{46298F6A-1E7E-4D4A-B5F5-106A4F0E48C6}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001B-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	vwnxa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0018-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001A-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{68306422-7C57-373F-8860-D26CE4BA2A15}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-002C-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{444C5574-6BE0-323E-9BDD-922F6C3C4A04}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001B-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0016-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-003B-0000-0000-0000000FF1CE}_Office14.PRJPROR_{8A8F117F-8EDB-440D-B679-F08909D729F7}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-00A1-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-006E-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{444C5574-6BE0-323E-9BDD-922F6C3C4A04}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0115-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{f325f05b-f963-4640-a43b-c8a494cdda0f}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0054-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0054-0409-0000-0000000FF1CE}_Office14.VISIOR_{CDC4310F-8189-485F-B47D-D972217CE173}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-006E-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{4560037C-E356-444A-A015-D21F487D809E}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-006E-0409-0000-0000000FF1CE}_Office14.PRJPROR_{4560037C-E356-444A-A015-D21F487D809E}	access	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\oftware\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676\00000004	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office14.PRJPROR\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-003B-0000-0000-0000000FF1CE}_Office14.PRJPROR_{8A8F117F-8EDB-440D-B679-F08909D729F7}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0019-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0117-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0409-0000-0000000FF1CE}_Office14.PRJPROR_{99ACCA38-6DD3-48A8-96AE-A283C9759279}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-0057-0000-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0C0A-0000-0000000FF1CE}_Office14.PRJPROR_{DEA87BE2-FFCC-4F33-9946-FCBE55A1E998}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{582EA838-9199-3518-A05C-DB09462F68EC}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0015-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-0057-0000-0000-0000000FF1CE}_Office14.VISIOR_{01D8AE4B-A04D-47E5-81BF-E3F98B81B8C3}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-00B4-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-002C-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{7CA93DF4-8902-449E-A42E-4C5923CFBDE3}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{99ACCA38-6DD3-48A8-96AE-A283C9759279}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-0057-0000-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001A-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-002C-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{AC76BA86-7AD7-FFFF-7B44-AA0000000001}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0115-0409-0000-0000000FF1CE}_Office14.PRJPROR_{4560037C-E356-444A-A015-D21F487D809E}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{AC76BA86-7AD7-FFFF-7B44-AA0000000001}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-040C-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player Plugin\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0044-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{f325f05b-f963-4640-a43b-c8a494cdda0f}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0115-0409-0000-0000000FF1CE}_Office14.PRJPROR_{4560037C-E356-444A-A015-D21F487D809E}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-006E-0409-0000-0000000FF1CE}_Office14.PRJPROR_{4560037C-E356-444A-A015-D21F487D809E}\DisplayName	access, read	vwnxa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{99ACCA38-6DD3-48A8-96AE-A283C9759279}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0115-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0409-0000-0000000FF1CE}_Office14.PRJPROR_{99ACCA38-6DD3-48A8-96AE-A283C9759279}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0015-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0409-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-006E-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001B-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-00B4-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0018-0409-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{444C5574-6BE0-323E-9BDD-922F6C3C4A04}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office14.PRJPROR	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-00B4-0409-0000-0000000FF1CE}_Office14.PRJPROR_{18A0C151-8F8A-4B68-A960-60C464B94329}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Office14.VISIOR	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0C0A-0000-0000000FF1CE}_Office14.PRJPROR_{DEA87BE2-FFCC-4F33-9946-FCBE55A1E998}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	vwnxa.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-0115-0409-0000-0000000FF1CE}_Office14.PROPLUSR_{4560037C-E356-444A-A015-D21F487D809E}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001F-0C0A-0000-0000000FF1CE}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91140000-003B-0000-0000-0000000FF1CE}\DisplayName	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	access, read	vwnxa.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90140000-001A-0409-0000-0000000FF1CE}\DisplayVersion	access, read	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MozillaMaintenanceService	access	vwnxa.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	vwnxa.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
vwnxa.exe	"C:\Users\EEBsYm5\Desktop\vwnxa.exe"	MALICIOUS

YARA / AV

YARA (7)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Stealc	Stealc	Stealc Stealer	Memory Dump	-	Spyware	5/5
Stealc	Stealc	Stealc Stealer	Memory Dump	-	Spyware	5/5
Stealc	Stealc	Stealc Stealer	Memory Dump	-	Spyware	5/5
Stealc	Stealc	Stealc Stealer	Sample File	C:\Users\EEBsYm5\Desktop\vwnxa.exe	Spyware	5/5
Malware	Stealc_fstrings	Stealc Stealer function strings	Function Strings	-	Spyware	5/5
Stealc	Stealc	Stealc Stealer	Function Strings	-	Spyware	5/5
Stealc	Stealc_fstrings	Stealc Stealer function strings	Function Strings	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_32_sp1
Description	-
Architecture	x86 32-bit PAE
Operating System	Windows 7
Kernel Version	6.1.7601.17514 (684da42a-30cc-450f-81c5-35b4d18944b1)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.2.0
Dynamic Engine Version	2023.2.0 / 04/13/2023 04:20
Static Engine Version	2023.2.0.0 / 2023-04-13 03:00:20
AV Exceptions Version	2023.2.1.4 / 2023-04-17 18:38:13
Link Detonation Heuristics Version	2023.2.1.4 / 2023-04-17 18:38:13
Smart Memory Dumping Rules Version	2023.2.1.4 / 2023-04-17 18:38:13
Config Extractors Version	2023.2.1.7 / 2023-04-27 22:55:34
Signature Trust Store Version	2023.2.1.4 / 2023-04-17 18:38:13
VMRay Threat Identifiers Version	2023.2.1.7 / 2023-04-27 22:55:34
YARA Built-in Ruleset Version	2023.2.1.7

Software Information

Adobe Acrobat Reader Version	10.0.0
Microsoft Office	2010
Microsoft Office Version	14.0.4762.1000
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	58.0.3029.110
Firefox Version	25.0
Flash Version	10.3.183.90
Java Version	7.0.450.18

System Information

Sample Directory	C:\Users\EEBsYm5\Desktop
Computer Name	CRH2YWU7
User Domain	CRH2YWU7
User Name	EEBsYm5
User Profile	C:\Users\EEBsYm5
Temp Directory	C:\Users\EEBsYm5\AppData\Local\Temp

System Root	C:\Windows