MALICIOUS

Classifications: Spyware, Injector

Threat Names: FormBook, Mal/HTMLGen-A, Trojan.NSISX.Spy.Gen.1, Gen:Variant.Razy.679962

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**PRICE_REQUEST_QUOTATION.exe**
ID	#968763
MD5	85589170af713a03ca622f94429c634a
SHA1	4e0b9dfd13dd6e4b85bca4352be0cec2be9024d7
SHA256	dae6ba220bb0a34de731b57965753391343bfe96f9f3fa4fea48102d3377ccf7
File Size	260.85 KB
Report Created	2021-09-28 10:55 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (28 rules, 161 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "FormBook" from ruleset "Malware" has matched on the function strings for (process #4) cmstp.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: AbleFTP, Google Chrome, Opera, Internet Explorer.			
4/5	Injection	Writes into the memory of another process	6	Injector
	• (Process #2) price_request_quotation.exe modifies memory of (process #3) explorer.exe. • (Process #4) cmstp.exe modifies memory of (process #3) explorer.exe. • (Process #2) price_request_quotation.exe modifies memory of (process #4) cmstp.exe. • (Process #95) -zetrxylspxh.exe modifies memory of (process #96) explorer.exe. • (Process #97) systray.exe modifies memory of (process #96) explorer.exe. • (Process #95) -zetrxylspxh.exe modifies memory of (process #97) systray.exe.			
4/5	Injection	Modifies control flow of another process	4	-
	• (Process #2) price_request_quotation.exe alters context of (process #3) explorer.exe. • (Process #4) cmstp.exe alters context of (process #3) explorer.exe. • (Process #95) -zetrxylspxh.exe alters context of (process #96) explorer.exe. • (Process #97) systray.exe alters context of (process #96) explorer.exe.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	5	-
	• Reputation analysis labels the URL "http://www.nudesalon.digital/rgoe/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "http://www.nudesalon.digital/rgo...pXYVqoNsa8QJw==&THhTxx=yrK4eV4Xxr" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "http://www.rap8b55d.com/rgoe/?Cx...QLIgo6/g==&w8GxJD=efo4sRjxk6y4KP" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "http://www.rap8b55d.com/rgoe/?C...OiZQLIgo6/g==&THhTxx=yrK4eV4Xxr" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "http://www.rap8b55d.com/rgoe/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
4/5	Antivirus	Malicious content was detected by heuristic scan	5	-
	• Built-in AV detected the sample itself as "Trojan.NSISX.Spy.Gen.1". • Built-in AV detected a memory dump of (process #2) price_request_quotation.exe as "Gen:Variant.Razy.679962". • Built-in AV detected a memory dump of (process #1) price_request_quotation.exe as "Gen:Variant.Razy.679962". • Built-in AV detected a memory dump of (process #4) cmstp.exe as "Trojan.NSISX.Spy.Gen.1". • Built-in AV detected a memory dump of (process #95) -zetrxylspxh.exe as "Gen:Variant.Razy.679962".			
3/5	Input Capture	Captures clipboard data	2	Spyware
	• (Process #3) explorer.exe reads data from clipboard. • (Process #96) explorer.exe reads data from clipboard.			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-

Score	Category	Operation	Count	Classification
	• (Process #2) price_request_quotation.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) price_request_quotation.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #4) cmstp.exe has a thread which sleeps more than 5 minutes. • (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Data Collection	Reads sensitive browser data	3	-
	• (Process #4) cmstp.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #4) cmstp.exe tries to read sensitive data of web browser "Opera" by file. • (Process #4) cmstp.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #4) cmstp.exe tries to read sensitive data of ftp application "AbleFTP" by file.			
2/5	Anti Analysis	Creates an unusually large number of processes	1	-
	• Above average number of processes were monitored.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	2	-
	• (Process #1) price_request_quotation.exe modifies memory of (process #2) price_request_quotation.exe. • (Process #94) -zetrxylspxh.exe modifies memory of (process #95) -zetrxylspxh.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	2	-
	• (Process #1) price_request_quotation.exe alters context of (process #2) price_request_quotation.exe. • (Process #94) -zetrxylspxh.exe alters context of (process #95) -zetrxylspxh.exe.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	50	-

Score	Category	Operation	Count	Classification
		• (Process #1) price_request_quotation.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #1) price_request_quotation.exe makes a direct system call to "NtWriteVirtualMemory".		
		• (Process #1) price_request_quotation.exe makes a direct system call to "NtResumeThread".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtQuerySystemInformation".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtQueryInformationProcess".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtAllocateVirtualMemory".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtFreeVirtualMemory".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtOpenProcessToken".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtAdjustPrivilegesToken".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtClose".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtOpenDirectoryObject".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtCreateMutant".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtCreateSection".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtMapViewOfSection".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtOpenProcess".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtQueryInformationToken".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtProtectVirtualMemory".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtCreateFile".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtQueryInformationFile".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtDelayExecution".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtReadVirtualMemory".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtOpenThread".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtReadFile".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #2) price_request_quotation.exe makes a direct system call to "NtResumeThread".		
		• (Process #94) -zetrxylspxh.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #94) -zetrxylspxh.exe makes a direct system call to "NtWriteVirtualMemory".		
		• (Process #94) -zetrxylspxh.exe makes a direct system call to "NtResumeThread".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtQuerySystemInformation".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtQueryInformationProcess".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtAllocateVirtualMemory".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtFreeVirtualMemory".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtOpenProcessToken".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtAdjustPrivilegesToken".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtClose".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtOpenDirectoryObject".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtCreateMutant".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtCreateSection".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtMapViewOfSection".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtOpenProcess".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtQueryInformationToken".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtProtectVirtualMemory".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtCreateFile".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtQueryInformationFile".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtDelayExecution".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtReadVirtualMemory".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtOpenThread".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtReadFile".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtUnmapViewOfSection".		
		• (Process #95) -zetrxylspxh.exe makes a direct system call to "NtResumeThread".		

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

- (Process #1) price_request_quotation.exe starts (process #2) price_request_quotation.exe with a hidden window.
- (Process #3) explorer.exe starts (process #4) cmstp.exe with a hidden window.
- (Process #4) cmstp.exe starts (process #5) cmd.exe with a hidden window.
- (Process #3) explorer.exe starts C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe with a hidden window.
- (Process #94) -zetrxylspxh.exe starts (process #95) -zetrxylspxh.exe with a hidden window.
- (Process #96) explorer.exe starts (process #97) systray.exe with a hidden window.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	6	-

- (Process #1) price_request_quotation.exe reads from (process #2) price_request_quotation.exe.
- (Process #2) price_request_quotation.exe reads from (process #3) explorer.exe.
- (Process #2) price_request_quotation.exe reads from (process #4) cmstp.exe.
- (Process #94) -zetrxylspxh.exe reads from (process #95) -zetrxylspxh.exe.
- (Process #95) -zetrxylspxh.exe reads from (process #96) explorer.exe.
- (Process #95) -zetrxylspxh.exe reads from (process #97) systray.exe.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	2	-

- (Process #1) price_request_quotation.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.
- (Process #94) -zetrxylspxh.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	6	-

- (Process #2) price_request_quotation.exe creates mutex with name "14-ARU9TUYI8wI3z".
- (Process #4) cmstp.exe creates mutex with name "14-ARU9TUYI8wI3z".
- (Process #4) cmstp.exe creates mutex with name "O3-71R46F5CCAG1B".
- (Process #95) -zetrxylspxh.exe creates mutex with name "14-ARU9TUYI8wI3z".
- (Process #97) systray.exe creates mutex with name "14-ARU9TUYI8wI3z".
- (Process #97) systray.exe creates mutex with name "3N5NT194G6EF0HB0".

Score	Category	Operation	Count	Classification
1/5	Persistence	Installs system startup script or application	1	-

- (Process #4) cmstp.exe adds "C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe" to Windows startup via registry.

Score	Category	Operation	Count	Classification
1/5	System Modification	Modifies application directory	1	-

- (Process #3) explorer.exe modifies "C:\Program Files (x86)\Ealwtgnkh".

Score	Category	Operation	Count	Classification
1/5	Discovery	Possibly does reconnaissance	2	-

- (Process #4) cmstp.exe tries to gather information about application "Mozilla Firefox" by registry.
- (Process #4) cmstp.exe tries to gather information about application "Mozilla Firefox" by file.

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

- (Process #1) price_request_quotation.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nspCDFE.tmp\akepwc.dll".

Score	Category	Operation	Count	Classification
1/5	Execution	Executes itself	3	-

- (Process #1) price_request_quotation.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe.
- (Process #3) explorer.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe.
- (Process #94) -zetrxylspxh.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe.

Score	Category	Operation	Count	Classification
1/5	Network Connection	Performs DNS request	27	-

Score	Category	Operation	Count	Classification
		• (Process #3) explorer.exe resolves host name "www.bordandoartes.com" to IP "192.185.213.75".		
		• (Process #3) explorer.exe resolves host name "www.appleluis.host" to IP "-".		
		• (Process #3) explorer.exe resolves host name "www.searchengineeye.com" to IP "160.153.136.3".		
		• (Process #3) explorer.exe resolves host name "www.restate.club" to IP "34.102.136.180".		
		• (Process #3) explorer.exe resolves host name "www.sehatbersama.store" to IP "45.13.133.216".		
		• (Process #3) explorer.exe resolves host name "www.immerseinagro.com" to IP "-".		
		• (Process #3) explorer.exe resolves host name "www.yota.store" to IP "52.58.78.16".		
		• (Process #3) explorer.exe resolves host name "www.thevillageplumbers.com" to IP "34.102.136.180".		
		• (Process #3) explorer.exe resolves host name "www.golfsol.art" to IP "99.86.186.56".		
		• (Process #3) explorer.exe resolves host name "www.nudesalon.digital" to IP "34.102.136.180".		
		• (Process #3) explorer.exe resolves host name "www.iktbn-c01.com" to IP "172.67.189.216".		
		• (Process #3) explorer.exe resolves host name "www.baila.madrid" to IP "31.214.178.54".		
		• (Process #3) explorer.exe resolves host name "www.thejegrouplIc.com" to IP "81.169.145.157".		
		• (Process #3) explorer.exe resolves host name "www.teelandcompany.com" to IP "34.102.136.180".		
		• (Process #3) explorer.exe resolves host name "www.sec-app.pro" to IP "-".		
		• (Process #3) explorer.exe resolves host name "www.thenewtocsin.com" to IP "198.54.117.211".		
		• (Process #3) explorer.exe resolves host name "www.rap8b55d.com" to IP "198.54.112.103".		
		• (Process #3) explorer.exe resolves host name "www.pondokbali.store" to IP "23.227.38.74".		
		• (Process #3) explorer.exe resolves host name "www.sustainablefoodfactory.com" to IP "34.102.136.180".		
		• (Process #3) explorer.exe resolves host name "www.1kingbet.com" to IP "104.21.39.50".		
		• (Process #3) explorer.exe resolves host name "www.shahjahantravel.com" to IP "104.219.248.101".		
		• (Process #3) explorer.exe resolves host name "www.limiteditionft.com" to IP "34.102.136.180".		
		• (Process #3) explorer.exe resolves host name "www.babeshotnud.com" to IP "185.107.56.60".		
		• (Process #3) explorer.exe resolves host name "www.futurodr.com" to IP "154.208.173.139".		
		• (Process #3) explorer.exe resolves host name "www.estanciasanpablo.online" to IP "-".		
		• (Process #3) explorer.exe resolves host name "www.toptaxxi.store" to IP "45.130.41.10".		
		• (Process #96) explorer.exe resolves host name "www.restate.club" to IP "34.102.136.180".		
1/5	Network Connection	Connects to remote host	18	-
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "192.185.213.75:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "160.153.136.3:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "34.102.136.180:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "45.13.133.216:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "52.58.78.16:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "99.86.186.56:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "172.67.189.216:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "31.214.178.54:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "81.169.145.157:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "198.54.117.211:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "198.54.112.103:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "23.227.38.74:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "104.21.39.50:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "104.219.248.101:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "185.107.56.60:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "154.208.173.139:80".		
		• (Process #3) explorer.exe opens an outgoing TCP connection to host "45.130.41.10:80".		
		• (Process #96) explorer.exe opens an outgoing TCP connection to host "34.102.136.180:80".		

Mitre ATT&CK Matrix

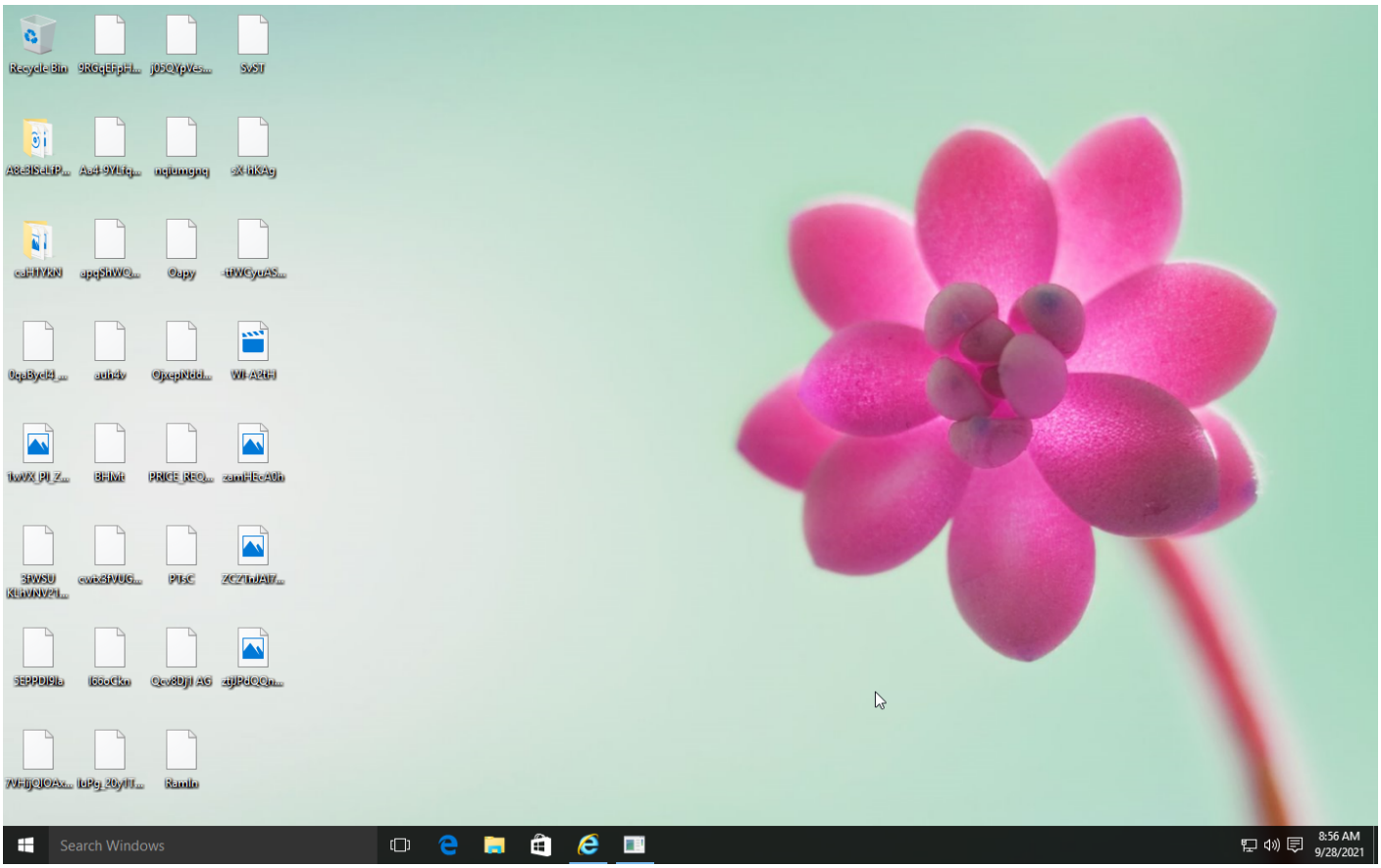
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#T1012 Query Registry		#T1115 Clipboard Data			
				#T1045 Software Packing	#T1003 Credential Dumping	#T1083 File and Directory Discovery		#T1119 Automated Collection			
				#T1112 Modify Registry				#T1005 Data from Local System			

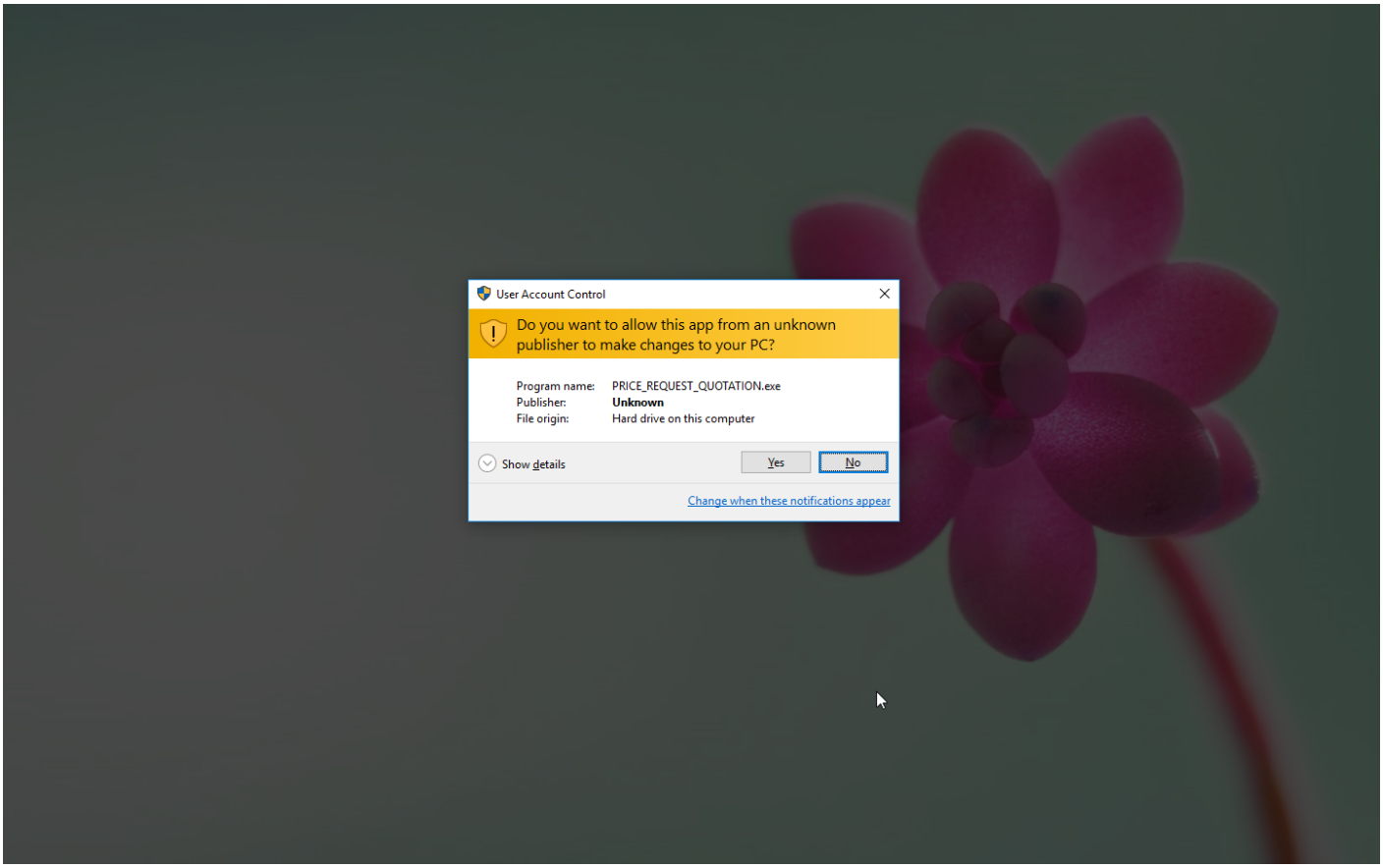
Sample Information

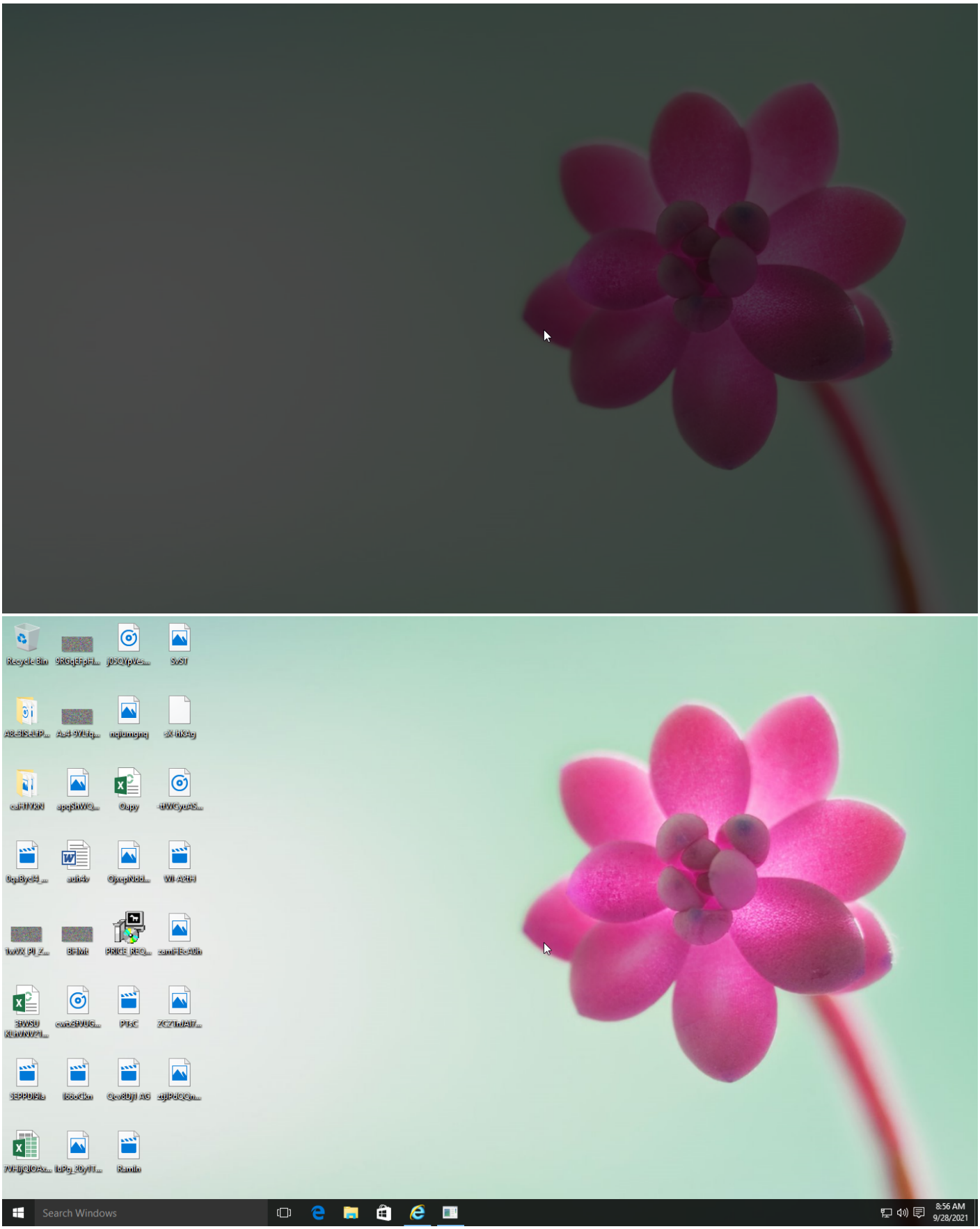
ID	#968763
MD5	85589170af713a03ca622f94429c634a
SHA1	4e0b9dfd13dd6e4b85bca4352be0cec2be9024d7
SHA256	dae6ba220bb0a34de731b57965753391343bfe96f9f3fa4fea48102d3377ccf7
SSDeep	6144:F8LxBsicGu14h0W/c8aRyPwSagdVDgfpnYluQgVd0ka7cDp3:/USWDaRaa6VUBqvr03
ImpHash	b76363e9cb88bf9390860da8e50999d2
File Name	PRICE_REQUEST_QUOTATION.exe
File Size	260.85 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 10:55 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	95
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	6
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


Recycle Bin
Search Windows
8:56 AM
9/28/2021


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



Screenshots truncated

NETWORK

General

82.51 KB total sent

99.96 KB total received

1 ports 80

18 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

40 DNS requests for 26 domains

1 nameservers contacted

10 total requests returned errors

HTTP/S

48 URLs contacted, 17 servers

71 sessions, 66.39 KB sent, 69.47 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://www.bordandoartes.com/rgoe/	-	-		0 bytes	NA
GET	http://www.bordandoartes.com/rgoe/?CxI=IAN+6LZkS+aB/2aiQ72h9+ALXNQwL6dioeeix54bZ9MO84/H7/+jiklTlCiea1o6U5SNkA==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.searchengineeye.com/rgoe/	-	-		0 bytes	NA
GET	http://www.searchengineeye.com/rgoe/?CxI=EXHpTBoivzCZKuB1uj/mQl1CxTx76c7NPbdxHK0a9l8L51JTEvhJv2o6Nk5VUAFXED9xHA==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.restate.club/rgoe/	-	-		0 bytes	NA
GET	http://www.restate.club/rgoe/?CxI=JxGfVlbuMUjpbP2ryp9NqAAUcvSw4xalcvPlMbht+AfdGLaozOMXSMTxw1ejBBSspA9TUA==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.sehatbersama.store/rgoe/	-	-		0 bytes	NA
GET	http://www.sehatbersama.store/rgoe/?CxI=sIXdTxUbKz/96qeCkTgV3Mzc3P/6Etmdy0CNGac80lG7kBMgvgKUgihqHFrjZJ9qD0d1Bg==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.yota.store/rgoe/	-	-		0 bytes	NA
GET	http://www.yota.store/rgoe/?CxI=vDEbv8qQdWhXi00pnoh8UJjCBA7dTpqpRs2jUcgq9SNzcrZBsswg5GW4oy8s4DS6X4nX0g==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.thevillageplumbers.com/rgoe/	-	-		0 bytes	NA
GET	http://www.thevillageplumbers.com/rgoe/?CxI=uoB9N3Y97N7n4fith7cSPcJBcPTqB0g//apWxtglpA+4DlyfKHQX+y6u2ZoMCVv5t8xPig==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.golfsol.art/rgoe/	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.golfsol.art/rgoe/?Cxl=eMTFSmRdy/J8aqp5e0iSmw3xJXULOwGUyVMUAKgY7Af7gubUBsEXILJyEqdeBzu66qQdRg==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.nudesalon.digital/rgoe/	-	-		0 bytes	NA
GET	http://www.nudesalon.digital/rgoe/?Cxl=AcwhRhtx+/5DgHlicgfflNf8LUQZwDIXjd9TWXSB6gbot5lszgiIvjJ67pXYVqoNsa8QJw==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
GET	http://www.iktbn-c01.com/rgoe/?Cxl=9xKKXzDxf4jR9rb9gFXqbZYbfe/mtI21hEgB20jvBm193dN+gRuwcuSlwOYLNp7cLJikRw==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.baila.madrid/rgoe/	-	-		0 bytes	NA
GET	http://www.baila.madrid/rgoe/?Cxl=FZv9m3gLyS4pbbAcIL4wjE/DkmhOUTFyiRpqcFoq7M9qckQiRKdGTqegUN9DDka7aWP55g==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.thejegroupllc.com/rgoe/	-	-		0 bytes	NA
GET	http://www.thejegroupllc.com/rgoe/?Cxl=DsYyhIgFU14uXJAOP6YeNTk5gtpkz9aSQu7fZlWYblSckE14vm83thC+1sq4cjDpXhRiUQ==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.teelandcompany.com/rgoe/	-	-		0 bytes	NA
GET	http://www.teelandcompany.com/rgoe/?Cxl=mDrA6fjGvYH6EvdRXL9JZl5ban60MroB6V8+OSRO0Ae/cJjz84hDdPdymn55tfHVT2xGzg==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
GET	http://www.rap8b55d.com/rgoe/?Cxl=mJVafnjbVaZXnrIEO6aq3UnPXgco9MUciXfkcV/NqCHWEuNhes+RSak/YaSOiZQLlgo6/g==&w8GxJD=efo4sRjxk6y4KP	-	-		0 bytes	NA
GET	http://www.pondokbali.store/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=sDoAOA5OtmLnlX03HdCMDl45v+a30M93mz/qcffau5LNKbK7enTzBZZ7oAoSZDGGtEvZNg==	-	-		0 bytes	NA
GET	http://www.sustainablefoodfactory.com/rgoe/?Cxl=XpHauQK7KC2WjHZdwnq4WMTUpcNEXoZ9uqeg9ayy0mnQx9tbeZVpp7DwWO8PS50hrewzRQ==&w8GxJD=efo4sRjxk6y4KP	-	-		0 bytes	NA
GET	http://www.thejegroupllc.com/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=DsYyhIgFU14uXJAOP6YeNTk5gtpkz9aSQu7fZlWYblSckE14vm83thC+1sq4cjDpXhRiUQ==	-	-		0 bytes	NA
GET	http://www.baila.madrid/rgoe/?Cxl=FZv9m3gLyS4pbbAcIL4wjE/DkmhOUTFyiRpqcFoq7M9qckQiRKdGTqegUN9DDka7aWP55g==&w8GxJD=efo4sRjxk6y4KP	-	-		0 bytes	NA
GET	http://www.1kingbet.com/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=8NZbPdu1i3dUXB0DPU4kzAYblsxeNSXQrC7mh+LsV5Nod9wjyJXKw0SUB0uoW7EPvfFBkQ==	-	-		0 bytes	NA
POST	http://www.iktbn-c01.com/rgoe/	-	-		0 bytes	NA
GET	http://www.shahjahantravel.com/rgoe/?Cxl=d9LWsFuvewb7h/v6EwrCexEPacaTeqblWzYENpEVQ4i2pE2pVH/LcDOAlD5swiUBI2J78g==&w8GxJD=efo4sRjxk6y4KP	-	-		0 bytes	NA
GET	http://www.thenewtocsin.com/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=icL3r7svHZo5uH8Zm6SYIUBWaonuBr/WcR3F0F0+oGeocNnqRdBKeq38Q4roddrx/guvBw==	-	-		0 bytes	NA
GET	http://www.rap8b55d.com/rgoe/?Cxl=mJVafnjbVaZXnrIEO6aq3UnPXgco9MUciXfkcV/NqCHWEuNhes+RSak/YaSOiZQLlgo6/g==&THhTxx=yrK4eV4Xxr	-	-		0 bytes	NA
POST	http://www.rap8b55d.com/rgoe/	-	-		0 bytes	NA
POST	http://www.pondokbali.store/rgoe/	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://www.sustainablefoodfactory.com/rgoe/	-	-		0 bytes	NA
POST	http://www.1kingbet.com/rgoe/	-	-		0 bytes	NA
POST	http://www.shahjahantravel.com/rgoe/	-	-		0 bytes	NA
GET	http://www.golfsol.art/rgoe/?8pJdD=HridIDO&Cxl=eMTFSmRdy/J8aqp5e0iSmw3xJXULOwGUyVMUAKgY7Af7gubUBsEXILJyEqdeBzu66qQdRg==	-	-		0 bytes	NA
GET	http://www.shahjahantravel.com/rgoe/?Cxl=d9LWsFuvewb7h/v6EwrCexEPacaTeqblWzYENpEVQ4i2pE2pVH/LcDOAlD5swiUBI2J78g==&8pJdD=HridIDO	-	-		0 bytes	NA
POST	http://www.limiteditionft.com/rgoe/	-	-		0 bytes	NA
GET	http://www.limiteditionft.com/rgoe/?8pJdD=HridIDO&Cxl=+V4k+VaDQd9kkXtqDVmrj+kvFZmiXxIdf3XwnzRS5bc5p9YIdSzu7Qd7OEO7YBU8bys9Pw==	-	-		0 bytes	NA
GET	http://www.babeshotnud.com/rgoe/?Cxl=qAwo4FiqGQ7vF/RKkBGUgNSCxZXln1VUyos+fVOy+k3yvD0B9CVt/iZeMW8Kxz83olImHw==&8pJdD=HridIDO	-	-		0 bytes	NA
POST	http://www.babeshotnud.com/rgoe/	-	-		0 bytes	NA
POST	http://www.futurodr.com/rgoe/	-	-		0 bytes	NA
GET	http://www.futurodr.com/rgoe/?8pJdD=HridIDO&Cxl=3YB68aMp2Yn/Ksrq43xxGSNHrBeWjD32XiQQxbglw81jxMqzUnRtzjIwk8cYUz/LonKyKg==	-	-		0 bytes	NA
GET	http://www.toptaxxi.store/rgoe/?8pJdD=HridIDO&Cxl=9Ba3zyXU6wZWVfOWx6PLyAS2lxhez7vN5Wx49vUmzMjajZc2jq0x3a89PDLKAravPCI55g==	-	-		0 bytes	NA
POST	http://www.toptaxxi.store/rgoe/	-	-		0 bytes	NA

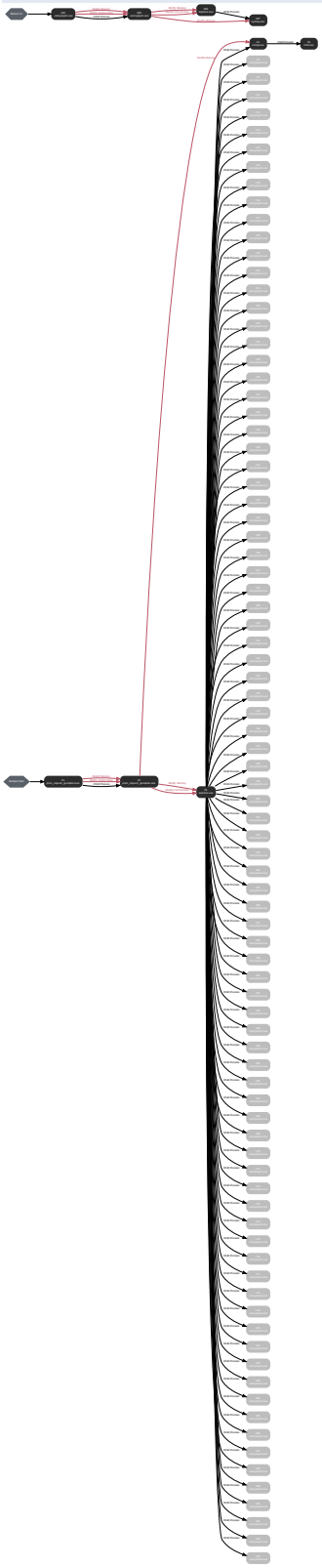
DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.bordandoartes.com, bordandoartes.com	NoError	192.185.213.75	bordandoartes.com	NA
A	www.appleluis.host, appleluis.host	NoError		appleluis.host	NA
A	www.searchengineeye.com, searchengineeye.com	NoError	160.153.136.3	searchengineeye.com	NA
A	www.restate.club, restate.club	NoError	34.102.136.180	restate.club	NA
A	www.sehatbersama.store, sehatbersama.store	NoError	45.13.133.216	sehatbersama.store	NA
A	www.immerseinagro.com	ServFail			NA
A	www.yota.store	NoError	52.58.78.16		NA
A	www.thevillageplumbers.com, thevillageplumbers.com	NoError	34.102.136.180	thevillageplumbers.com	NA
A	www.golfsol.art, dw2vdcfmgkqfo.cloudfront.net	NoError	99.86.186.56, 99.86.186.55, 99.86.186.83, 99.86.186.18	dw2vdcfmgkqfo.cloudfront.net	NA
A	www.nudesalon.digital, nudesalon.digital	NoError	34.102.136.180	nudesalon.digital	NA
A	www.iktbn-c01.com	NoError	172.67.189.216, 104.21.9.250		NA
A	www.baila.madrid, parkingsrv0.dondominio.com	NoError	31.214.178.54	parkingsrv0.dondominio.com	NA
A	www.thejegrouplc.com, thejegrouplc.com	NoError	81.169.145.157	thejegrouplc.com	NA
A	www.teelandcompany.com, teelandcompany.com	NoError	34.102.136.180	teelandcompany.com	NA

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.sec-app.pro	NXDomain			NA
A	www.thenewtocsin.com, parkingpage.namecheap.com	NoError	198.54.117.211, 198.54.117.217, 198.54.117.216, 198.54.117.210, 198.54.117.215, 198.54.117.218, 198.54.117.212	parkingpage.namecheap.com	NA
A	www.rap8b55d.com	NoError	198.54.112.103		NA
A	www.pondokbali.store, shops.myshopify.com	NoError	23.227.38.74	shops.myshopify.com	NA
A	www.sustainablefoodfactory.com, sustainablefoodfactory.com	NoError	34.102.136.180	sustainablefoodfactory.com	NA
A	www.1kingbet.com	NoError	104.21.39.50, 172.67.143.57		NA
A	www.shahjahantravel.com, shahjahantravel.com	NoError	104.219.248.101	shahjahantravel.com	NA
A	www.limiteditionft.com, limiteditionft.com	NoError	34.102.136.180	limiteditionft.com	NA
A	www.babeshotnud.com	NoError	185.107.56.60		NA
A	www.futurodr.com	NoError	154.208.173.139		NA
A	www.estanciasanpablo.online	ServFail			NA
A	www.toptaxxi.store	NoError	45.130.41.10		NA
-	www.thejegroupllc.com	-	81.169.145.157		NA
-	www.baila.madrid	-	31.214.178.54		NA
-	www.golfsol.art	-	99.86.186.56, 99.86.186.55, 99.86.186.83, 99.86.186.18		NA
-	www.shahjahantravel.com	-	104.219.248.101		NA

BEHAVIOR

Process Graph



Process #1: price_request_quotation.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 58153, Reason: Analysis Target
Unmonitor End Time	End Time: 105765, Reason: Terminated
Monitor duration	47.61s
Return Code	0
PID	4736
Parent PID	1636
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\4gyujazywsbdaoe	211.80 KB	ca7d46a32ec12479afeec23562bd199c91d2dc0912462250d1a3811a7e89be83	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\nspCDFE.tmp\akepwc.dll	47.00 KB	19013d7428a659774231fd4b5213a463eeab58a0c347dadfaa95536bd89d3f13	✗

Host Behavior

Type	Count
System	49
Module	32
File	158
Process	1
-	3
-	5

Process #2: price_request_quotation.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 103907, Reason: Child Process
Unmonitor End Time	End Time: 118189, Reason: Terminated
Monitor duration	14.28s
Return Code	0
PID	1676
Parent PID	4736
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0xf78	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0xf78	0x401000(4198400)	0x27c00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0xf78	0x327008(3305480)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0xf78 / 0x7ac	0x772d8fe0(1999474656)	-	✓	1

Host Behavior

Type	Count
File	10
-	1
-	1
System	5
Module	14
User	1
Mutex	1
Environment	1
Process	6
-	8
-	3

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 106358, Reason: Injection
Unmonitor End Time	End Time: 207108, Reason: Terminated
Monitor duration	100.75s
Return Code	1073807364
PID	1636
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0x7ac	0xa6e0000(174981120)	0xed000	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0x7ac / 0x668	0xffffffff(4294967295)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0x7ac / 0x668	0xa72e909(175302921)	-	✓	1
Modify Memory	#4: c:\windows\syswow64\cmstp.exe	0x154	0x106e0000(275644416)	0x1b58000	✓	1
Modify Memory	#4: c:\windows\syswow64\cmstp.exe	0x154	0xaff0000(184483840)	0x144000	✓	1
Modify Control Flow	#4: c:\windows\syswow64\cmstp.exe	0x154 / 0x668		-	✓	1
Modify Control Flow	#4: c:\windows\syswow64\cmstp.exe	0x154 / 0x668	0xb0ae8f2(185264370)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	260.85 KB	dae6ba220bb0a34de731b57965753391343bfe96f9f3fa4fea48102d3377ccf7	✗

Host Behavior

Type	Count
Process	87
Module	3
System	1705
File	268
COM	1

Network Behavior

Type	Count
HTTP	71
DNS	39
TCP	110

Process #4: cmstp.exe

ID	4
File Name	c:\windows\syswow64\cmstp.exe
Command Line	"C:\Windows\SysWOW64\cmstp.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 113674, Reason: Child Process
Unmonitor End Time	End Time: 188827, Reason: Terminated
Monitor duration	75.15s
Return Code	1073807364
PID	1016
Parent PID	1636
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0x7ac	0x110000(1114112)	0x29000	✓	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\price_request_quotation.exe	0x7ac	0x1090000(17367040)	0x17000	✓	1

Host Behavior

Type	Count
File	105
-	1
-	1
System	4365
User	1
Mutex	2
Process	5
Module	14
Registry	1185
-	6
COM	1

Process #5: cmd.exe

ID	5
File Name	c:\windows\syswow64\cmd.exe
Command Line	/c del "C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 121368, Reason: Child Process
Unmonitor End Time	End Time: 124451, Reason: Terminated
Monitor duration	3.08s
Return Code	0
PID	2468
Parent PID	1016
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	18
Environment	11
System	1

Process #8: -zetrxylspxh.exe

ID	8
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189066, Reason: Child Process
Unmonitor End Time	End Time: 192100, Reason: Terminated
Monitor duration	3.03s
Return Code	3221226091
PID	2308
Parent PID	1636
Bitness	32 Bit

Process #9: -zetrxylspxh.exe

ID	9
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189153, Reason: Child Process
Unmonitor End Time	End Time: 192088, Reason: Terminated
Monitor duration	2.94s
Return Code	3221226091
PID	4856
Parent PID	1636
Bitness	32 Bit

Process #10: -zetrxylspxh.exe

ID	10
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189206, Reason: Child Process
Unmonitor End Time	End Time: 192112, Reason: Terminated
Monitor duration	2.91s
Return Code	3221226091
PID	3960
Parent PID	1636
Bitness	32 Bit

Process #11: -zetrxylspxh.exe

ID	11
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189259, Reason: Child Process
Unmonitor End Time	End Time: 192126, Reason: Terminated
Monitor duration	2.87s
Return Code	3221226091
PID	5012
Parent PID	1636
Bitness	32 Bit

Process #12: -zetrxylspxh.exe

ID	12
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189314, Reason: Child Process
Unmonitor End Time	End Time: 192133, Reason: Terminated
Monitor duration	2.82s
Return Code	3221226091
PID	4976
Parent PID	1636
Bitness	32 Bit

Process #13: -zetrxylspxh.exe

ID	13
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189374, Reason: Child Process
Unmonitor End Time	End Time: 192142, Reason: Terminated
Monitor duration	2.77s
Return Code	3221226091
PID	5068
Parent PID	1636
Bitness	32 Bit

Process #14: -zetrxylspxh.exe

ID	14
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189432, Reason: Child Process
Unmonitor End Time	End Time: 192143, Reason: Terminated
Monitor duration	2.71s
Return Code	3221226091
PID	4992
Parent PID	1636
Bitness	32 Bit

Process #15: -zetrxylspxh.exe

ID	15
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189491, Reason: Child Process
Unmonitor End Time	End Time: 192152, Reason: Terminated
Monitor duration	2.66s
Return Code	3221226091
PID	5092
Parent PID	1636
Bitness	32 Bit

Process #16: -zetrxylspxh.exe

ID	16
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189559, Reason: Child Process
Unmonitor End Time	End Time: 192121, Reason: Terminated
Monitor duration	2.56s
Return Code	3221226091
PID	5084
Parent PID	1636
Bitness	32 Bit

Process #17: -zetrxylspxh.exe

ID	17
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189673, Reason: Child Process
Unmonitor End Time	End Time: 192166, Reason: Terminated
Monitor duration	2.49s
Return Code	3221226091
PID	5020
Parent PID	1636
Bitness	32 Bit

Process #18: -zetrxylspxh.exe

ID	18
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189815, Reason: Child Process
Unmonitor End Time	End Time: 192165, Reason: Terminated
Monitor duration	2.35s
Return Code	3221226091
PID	4800
Parent PID	1636
Bitness	32 Bit

Process #19: -zetrxylspxh.exe

ID	19
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 189877, Reason: Child Process
Unmonitor End Time	End Time: 192168, Reason: Terminated
Monitor duration	2.29s
Return Code	3221226091
PID	2120
Parent PID	1636
Bitness	32 Bit

Process #20: -zetrxylspxh.exe

ID	20
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191196, Reason: Child Process
Unmonitor End Time	End Time: 196569, Reason: Terminated
Monitor duration	5.37s
Return Code	3221226091
PID	2116
Parent PID	1636
Bitness	32 Bit

Process #21: -zetrxylspxh.exe

ID	21
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191245, Reason: Child Process
Unmonitor End Time	End Time: 195795, Reason: Terminated
Monitor duration	4.55s
Return Code	3221226091
PID	2064
Parent PID	1636
Bitness	32 Bit

Process #22: -zetrxylspxh.exe

ID	22
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191300, Reason: Child Process
Unmonitor End Time	End Time: 196609, Reason: Terminated
Monitor duration	5.31s
Return Code	3221226091
PID	3156
Parent PID	1636
Bitness	32 Bit

Process #23: -zetrxylspxh.exe

ID	23
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191349, Reason: Child Process
Unmonitor End Time	End Time: 198430, Reason: Terminated
Monitor duration	7.08s
Return Code	3221226091
PID	2192
Parent PID	1636
Bitness	32 Bit

Process #24: -zetrxylspxh.exe

ID	24
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191394, Reason: Child Process
Unmonitor End Time	End Time: 196298, Reason: Terminated
Monitor duration	4.90s
Return Code	3221226091
PID	4676
Parent PID	1636
Bitness	32 Bit

Process #25: -zetrxylspxh.exe

ID	25
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191433, Reason: Child Process
Unmonitor End Time	End Time: 198436, Reason: Terminated
Monitor duration	7.00s
Return Code	3221226091
PID	2072
Parent PID	1636
Bitness	32 Bit

Process #26: -zetrxylspxh.exe

ID	26
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191479, Reason: Child Process
Unmonitor End Time	End Time: 198552, Reason: Terminated
Monitor duration	7.07s
Return Code	3221226091
PID	4772
Parent PID	1636
Bitness	32 Bit

Process #27: -zetrxylspxh.exe

ID	27
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191523, Reason: Child Process
Unmonitor End Time	End Time: 198565, Reason: Terminated
Monitor duration	7.04s
Return Code	3221226091
PID	4672
Parent PID	1636
Bitness	32 Bit

Process #28: -zetrxylspxh.exe

ID	28
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191575, Reason: Child Process
Unmonitor End Time	End Time: 198866, Reason: Terminated
Monitor duration	7.29s
Return Code	3221226091
PID	2176
Parent PID	1636
Bitness	32 Bit

Process #29: -zetrxylspxh.exe

ID	29
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191640, Reason: Child Process
Unmonitor End Time	End Time: 198883, Reason: Terminated
Monitor duration	7.24s
Return Code	3221226091
PID	2060
Parent PID	1636
Bitness	32 Bit

Process #30: -zetrxylspxh.exe

ID	30
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191697, Reason: Child Process
Unmonitor End Time	End Time: 198894, Reason: Terminated
Monitor duration	7.20s
Return Code	3221226091
PID	5032
Parent PID	1636
Bitness	32 Bit

Process #31: -zetrxylspxh.exe

ID	31
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191748, Reason: Child Process
Unmonitor End Time	End Time: 198902, Reason: Terminated
Monitor duration	7.15s
Return Code	3221226091
PID	2068
Parent PID	1636
Bitness	32 Bit

Process #32: -zetrxylspxh.exe

ID	32
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191808, Reason: Child Process
Unmonitor End Time	End Time: 198906, Reason: Terminated
Monitor duration	7.10s
Return Code	3221226091
PID	5028
Parent PID	1636
Bitness	32 Bit

Process #33: -zetrxylspxh.exe

ID	33
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191872, Reason: Child Process
Unmonitor End Time	End Time: 198945, Reason: Terminated
Monitor duration	7.07s
Return Code	3221226091
PID	1168
Parent PID	1636
Bitness	32 Bit

Process #34: -zetrxylspxh.exe

ID	34
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 191943, Reason: Child Process
Unmonitor End Time	End Time: 199094, Reason: Terminated
Monitor duration	7.15s
Return Code	3221226091
PID	5004
Parent PID	1636
Bitness	32 Bit

Process #35: -zetrxylspxh.exe

ID	35
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192001, Reason: Child Process
Unmonitor End Time	End Time: 199098, Reason: Terminated
Monitor duration	7.10s
Return Code	3221226091
PID	2344
Parent PID	1636
Bitness	32 Bit

Process #36: -zetrxylspxh.exe

ID	36
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192070, Reason: Child Process
Unmonitor End Time	End Time: 199109, Reason: Terminated
Monitor duration	7.04s
Return Code	3221226091
PID	2172
Parent PID	1636
Bitness	32 Bit

Process #37: -zetrxylspxh.exe

ID	37
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192145, Reason: Child Process
Unmonitor End Time	End Time: 199109, Reason: Terminated
Monitor duration	6.96s
Return Code	3221226091
PID	2300
Parent PID	1636
Bitness	32 Bit

Process #38: -zetrxylspxh.exe

ID	38
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192240, Reason: Child Process
Unmonitor End Time	End Time: 199224, Reason: Terminated
Monitor duration	6.98s
Return Code	3221226091
PID	1816
Parent PID	1636
Bitness	32 Bit

Process #39: -zetrxylspxh.exe

ID	39
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192302, Reason: Child Process
Unmonitor End Time	End Time: 199221, Reason: Terminated
Monitor duration	6.92s
Return Code	3221226091
PID	2376
Parent PID	1636
Bitness	32 Bit

Process #40: -zetrxylspxh.exe

ID	40
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192356, Reason: Child Process
Unmonitor End Time	End Time: 199221, Reason: Terminated
Monitor duration	6.87s
Return Code	3221226091
PID	2352
Parent PID	1636
Bitness	32 Bit

Process #41: -zetrxylspxh.exe

ID	41
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192411, Reason: Child Process
Unmonitor End Time	End Time: 198873, Reason: Terminated
Monitor duration	6.46s
Return Code	3221226091
PID	2180
Parent PID	1636
Bitness	32 Bit

Process #42: -zetrxylspxh.exe

ID	42
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192524, Reason: Child Process
Unmonitor End Time	End Time: 199212, Reason: Terminated
Monitor duration	6.69s
Return Code	3221226091
PID	2700
Parent PID	1636
Bitness	32 Bit

Process #43: -zetrxylspxh.exe

ID	43
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192648, Reason: Child Process
Unmonitor End Time	End Time: 199212, Reason: Terminated
Monitor duration	6.56s
Return Code	3221226091
PID	2804
Parent PID	1636
Bitness	32 Bit

Process #44: -zetrxylspxh.exe

ID	44
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192720, Reason: Child Process
Unmonitor End Time	End Time: 199203, Reason: Terminated
Monitor duration	6.48s
Return Code	3221226091
PID	3952
Parent PID	1636
Bitness	32 Bit

Process #45: -zetrxylspxh.exe

ID	45
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192786, Reason: Child Process
Unmonitor End Time	End Time: 199201, Reason: Terminated
Monitor duration	6.42s
Return Code	3221226091
PID	864
Parent PID	1636
Bitness	32 Bit

Process #46: -zetrxylspxh.exe

ID	46
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192936, Reason: Child Process
Unmonitor End Time	End Time: 199193, Reason: Terminated
Monitor duration	6.26s
Return Code	3221226091
PID	3948
Parent PID	1636
Bitness	32 Bit

Process #47: -zetrxylspxh.exe

ID	47
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192997, Reason: Child Process
Unmonitor End Time	End Time: 199190, Reason: Terminated
Monitor duration	6.19s
Return Code	3221226091
PID	2552
Parent PID	1636
Bitness	32 Bit

Process #48: -zetrxylspxh.exe

ID	48
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 193057, Reason: Child Process
Unmonitor End Time	End Time: 199189, Reason: Terminated
Monitor duration	6.13s
Return Code	3221226091
PID	3908
Parent PID	1636
Bitness	32 Bit

Process #49: -zetrxylspxh.exe

ID	49
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 193136, Reason: Child Process
Unmonitor End Time	End Time: 199503, Reason: Terminated
Monitor duration	6.37s
Return Code	3221226091
PID	1004
Parent PID	1636
Bitness	32 Bit

Process #50: -zetrxylspxh.exe

ID	50
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194362, Reason: Child Process
Unmonitor End Time	End Time: 199504, Reason: Terminated
Monitor duration	5.14s
Return Code	3221226091
PID	4788
Parent PID	1636
Bitness	32 Bit

Process #51: -zetrxylspxh.exe

ID	51
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194419, Reason: Child Process
Unmonitor End Time	End Time: 199522, Reason: Terminated
Monitor duration	5.10s
Return Code	3221226091
PID	4476
Parent PID	1636
Bitness	32 Bit

Process #52: -zetrxylspxh.exe

ID	52
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194475, Reason: Child Process
Unmonitor End Time	End Time: 199561, Reason: Terminated
Monitor duration	5.09s
Return Code	3221226091
PID	4496
Parent PID	1636
Bitness	32 Bit

Process #53: -zetrxylspxh.exe

ID	53
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194664, Reason: Child Process
Unmonitor End Time	End Time: 199526, Reason: Terminated
Monitor duration	4.86s
Return Code	3221226091
PID	4504
Parent PID	1636
Bitness	32 Bit

Process #54: -zetrxylspxh.exe

ID	54
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194729, Reason: Child Process
Unmonitor End Time	End Time: 199557, Reason: Terminated
Monitor duration	4.83s
Return Code	3221226091
PID	4668
Parent PID	1636
Bitness	32 Bit

Process #55: -zetrxylspxh.exe

ID	55
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194780, Reason: Child Process
Unmonitor End Time	End Time: 199553, Reason: Terminated
Monitor duration	4.77s
Return Code	3221226091
PID	4112
Parent PID	1636
Bitness	32 Bit

Process #56: -zetrxylspxh.exe

ID	56
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194836, Reason: Child Process
Unmonitor End Time	End Time: 199535, Reason: Terminated
Monitor duration	4.70s
Return Code	3221226091
PID	4508
Parent PID	1636
Bitness	32 Bit

Process #57: -zetrxylspxh.exe

ID	57
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194895, Reason: Child Process
Unmonitor End Time	End Time: 199539, Reason: Terminated
Monitor duration	4.64s
Return Code	3221226091
PID	4472
Parent PID	1636
Bitness	32 Bit

Process #58: -zetrxylspxh.exe

ID	58
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 199927, Reason: Child Process
Unmonitor End Time	End Time: 201938, Reason: Terminated
Monitor duration	2.01s
Return Code	3221226091
PID	1920
Parent PID	1636
Bitness	32 Bit

Process #59: -zetrxylspxh.exe

ID	59
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 199972, Reason: Child Process
Unmonitor End Time	End Time: 202073, Reason: Terminated
Monitor duration	2.10s
Return Code	3221226091
PID	1300
Parent PID	1636
Bitness	32 Bit

Process #60: -zetrxylspxh.exe

ID	60
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 200032, Reason: Child Process
Unmonitor End Time	End Time: 202083, Reason: Terminated
Monitor duration	2.05s
Return Code	3221226091
PID	1252
Parent PID	1636
Bitness	32 Bit

Process #61: -zetrxylspxh.exe

ID	61
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 200076, Reason: Child Process
Unmonitor End Time	End Time: 202092, Reason: Terminated
Monitor duration	2.02s
Return Code	3221226091
PID	2152
Parent PID	1636
Bitness	32 Bit

Process #62: -zetrxylspxh.exe

ID	62
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 200118, Reason: Child Process
Unmonitor End Time	End Time: 202072, Reason: Terminated
Monitor duration	1.95s
Return Code	3221226091
PID	1840
Parent PID	1636
Bitness	32 Bit

Process #63: -zetrxylspxh.exe

ID	63
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 200173, Reason: Child Process
Unmonitor End Time	End Time: 202099, Reason: Terminated
Monitor duration	1.93s
Return Code	3221226091
PID	4864
Parent PID	1636
Bitness	32 Bit

Process #64: -zetrxylspxh.exe

ID	64
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 200274, Reason: Child Process
Unmonitor End Time	End Time: 202199, Reason: Terminated
Monitor duration	1.93s
Return Code	3221226091
PID	3152
Parent PID	1636
Bitness	32 Bit

Process #65: -zetrxylspxh.exe

ID	65
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201227, Reason: Child Process
Unmonitor End Time	End Time: 205755, Reason: Terminated
Monitor duration	4.53s
Return Code	3221226091
PID	3508
Parent PID	1636
Bitness	32 Bit

Process #66: -zetrxylspxh.exe

ID	66
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201273, Reason: Child Process
Unmonitor End Time	End Time: 207008, Reason: Terminated
Monitor duration	5.74s
Return Code	3221226091
PID	2148
Parent PID	1636
Bitness	32 Bit

Process #67: -zetrxylspxh.exe

ID	67
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201336, Reason: Child Process
Unmonitor End Time	End Time: 207008, Reason: Terminated
Monitor duration	5.67s
Return Code	3221226091
PID	3656
Parent PID	1636
Bitness	32 Bit

Process #68: -zetrxylspxh.exe

ID	68
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201393, Reason: Child Process
Unmonitor End Time	End Time: 207008, Reason: Terminated
Monitor duration	5.62s
Return Code	3221226091
PID	2216
Parent PID	1636
Bitness	32 Bit

Process #69: -zetrxylspxh.exe

ID	69
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201450, Reason: Child Process
Unmonitor End Time	End Time: 207061, Reason: Terminated
Monitor duration	5.61s
Return Code	3221226091
PID	452
Parent PID	1636
Bitness	32 Bit

Process #70: -zetrxylspxh.exe

ID	70
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201503, Reason: Child Process
Unmonitor End Time	End Time: 207008, Reason: Terminated
Monitor duration	5.50s
Return Code	3221226091
PID	3684
Parent PID	1636
Bitness	32 Bit

Process #71: -zetrxylspxh.exe

ID	71
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201558, Reason: Child Process
Unmonitor End Time	End Time: 206976, Reason: Terminated
Monitor duration	5.42s
Return Code	3221226091
PID	3692
Parent PID	1636
Bitness	32 Bit

Process #72: -zetrxylspxh.exe

ID	72
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201615, Reason: Child Process
Unmonitor End Time	End Time: 207000, Reason: Terminated
Monitor duration	5.38s
Return Code	3221226091
PID	3548
Parent PID	1636
Bitness	32 Bit

Process #73: -zetrxylspxh.exe

ID	73
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201669, Reason: Child Process
Unmonitor End Time	End Time: 206096, Reason: Terminated
Monitor duration	4.43s
Return Code	3221226091
PID	3436
Parent PID	1636
Bitness	32 Bit

Process #74: -zetrxylspxh.exe

ID	74
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201718, Reason: Child Process
Unmonitor End Time	End Time: 207072, Reason: Terminated
Monitor duration	5.35s
Return Code	3221226091
PID	5116
Parent PID	1636
Bitness	32 Bit

Process #75: -zetrxylspxh.exe

ID	75
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201773, Reason: Child Process
Unmonitor End Time	End Time: 207061, Reason: Terminated
Monitor duration	5.29s
Return Code	3221226091
PID	3404
Parent PID	1636
Bitness	32 Bit

Process #76: -zetrxylspxh.exe

ID	76
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201826, Reason: Child Process
Unmonitor End Time	End Time: 207060, Reason: Terminated
Monitor duration	5.23s
Return Code	3221226091
PID	3784
Parent PID	1636
Bitness	32 Bit

Process #77: -zetrxylspxh.exe

ID	77
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201903, Reason: Child Process
Unmonitor End Time	End Time: 207072, Reason: Terminated
Monitor duration	5.17s
Return Code	3221226091
PID	1204
Parent PID	1636
Bitness	32 Bit

Process #78: -zetrxylspxh.exe

ID	78
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201997, Reason: Child Process
Unmonitor End Time	End Time: 207060, Reason: Terminated
Monitor duration	5.06s
Return Code	3221226091
PID	4132
Parent PID	1636
Bitness	32 Bit

Process #79: -zetrxylspxh.exe

ID	79
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202084, Reason: Child Process
Unmonitor End Time	End Time: 207072, Reason: Terminated
Monitor duration	4.99s
Return Code	3221226091
PID	4116
Parent PID	1636
Bitness	32 Bit

Process #80: -zetrxylspxh.exe

ID	80
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202136, Reason: Child Process
Unmonitor End Time	End Time: 207060, Reason: Terminated
Monitor duration	4.92s
Return Code	3221226091
PID	4148
Parent PID	1636
Bitness	32 Bit

Process #81: -zetrxylspxh.exe

ID	81
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202194, Reason: Child Process
Unmonitor End Time	End Time: 207059, Reason: Terminated
Monitor duration	4.87s
Return Code	3221226091
PID	4140
Parent PID	1636
Bitness	32 Bit

Process #82: -zetrxylspxh.exe

ID	82
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202245, Reason: Child Process
Unmonitor End Time	End Time: 207007, Reason: Terminated
Monitor duration	4.76s
Return Code	3221226091
PID	4156
Parent PID	1636
Bitness	32 Bit

Process #83: -zetrxylspxh.exe

ID	83
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202295, Reason: Child Process
Unmonitor End Time	End Time: 207059, Reason: Terminated
Monitor duration	4.76s
Return Code	3221226091
PID	4236
Parent PID	1636
Bitness	32 Bit

Process #84: -zetrxylspxh.exe

ID	84
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202345, Reason: Child Process
Unmonitor End Time	End Time: 207007, Reason: Terminated
Monitor duration	4.66s
Return Code	3221226091
PID	4228
Parent PID	1636
Bitness	32 Bit

Process #85: -zetrxylspxh.exe

ID	85
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202509, Reason: Child Process
Unmonitor End Time	End Time: 207059, Reason: Terminated
Monitor duration	4.55s
Return Code	3221226091
PID	3672
Parent PID	1636
Bitness	32 Bit

Process #86: -zetrxylspxh.exe

ID	86
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202613, Reason: Child Process
Unmonitor End Time	End Time: 207058, Reason: Terminated
Monitor duration	4.45s
Return Code	3221226091
PID	4260
Parent PID	1636
Bitness	32 Bit

Process #87: -zetrxylspxh.exe

ID	87
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202672, Reason: Child Process
Unmonitor End Time	End Time: 207058, Reason: Terminated
Monitor duration	4.39s
Return Code	3221226091
PID	4204
Parent PID	1636
Bitness	32 Bit

Process #88: -zetrxylspxh.exe

ID	88
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202724, Reason: Child Process
Unmonitor End Time	End Time: 207058, Reason: Terminated
Monitor duration	4.33s
Return Code	3221226091
PID	4244
Parent PID	1636
Bitness	32 Bit

Process #89: -zetrxylspxh.exe

ID	89
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202777, Reason: Child Process
Unmonitor End Time	End Time: 207057, Reason: Terminated
Monitor duration	4.28s
Return Code	3221226091
PID	4252
Parent PID	1636
Bitness	32 Bit

Process #90: -zetrxylspxh.exe

ID	90
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202841, Reason: Child Process
Unmonitor End Time	End Time: 207057, Reason: Terminated
Monitor duration	4.22s
Return Code	3221226091
PID	2160
Parent PID	1636
Bitness	32 Bit

Process #91: -zetrxylspxh.exe

ID	91
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202914, Reason: Child Process
Unmonitor End Time	End Time: 207057, Reason: Terminated
Monitor duration	4.14s
Return Code	3221226091
PID	4660
Parent PID	1636
Bitness	32 Bit

Process #92: -zetrxylspxh.exe

ID	92
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202977, Reason: Child Process
Unmonitor End Time	End Time: 207056, Reason: Terminated
Monitor duration	4.08s
Return Code	3221226091
PID	4340
Parent PID	1636
Bitness	32 Bit

Process #93: -zetrxylspxh.exe

ID	93
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 203048, Reason: Child Process
Unmonitor End Time	End Time: 207056, Reason: Terminated
Monitor duration	4.01s
Return Code	3221226091
PID	5016
Parent PID	1636
Bitness	32 Bit

Process #94: -zetrxylspxh.exe

ID	94
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 267993, Reason: Autostart
Unmonitor End Time	End Time: 278415, Reason: Terminated
Monitor duration	10.42s
Return Code	0
PID	3236
Parent PID	1660
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nscE967.tmp\akepwc.dll	47.00 KB	19013d7428a659774231fd4b5213a463eeab58a0c347dadfaa95536bd89d3f13	✖

Host Behavior

Type	Count
System	49
Module	32
File	159
Process	1
-	3
-	5

Process #95: -zetrxylspxh.exe

ID	95
File Name	c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe
Command Line	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 276182, Reason: Child Process
Unmonitor End Time	End Time: 282892, Reason: Terminated
Monitor duration	6.71s
Return Code	0
PID	3336
Parent PID	3236
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#94: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xca8	0x400000(4194304)	0x200	✓	1
Modify Memory	#94: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xca8	0x401000(4198400)	0x27c00	✓	1
Modify Memory	#94: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xca8	0x228008(2261000)	0x4	✓	1
Modify Control Flow	#94: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xca8 / 0xd0c	0x77d58fe0(2010484704)	-	✓	1

Host Behavior

Type	Count
File	10
-	1
-	1
System	5
Module	14
User	1
Mutex	1
Environment	1
Process	6
-	8
-	3

Process #96: explorer.exe

ID	96
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 278199, Reason: Injection
Unmonitor End Time	End Time: 300693, Reason: Terminated by Timeout
Monitor duration	22.49s
Return Code	Unknown
PID	1660
Parent PID	1636
Bitness	64 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#95: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xd0c	0x81b0000(135987200)	0xe8000	✓	1
Modify Control Flow	#95: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xd0c / 0x680		-	✓	1
Modify Control Flow	#95: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xd0c / 0x680	0x81f9909(136288521)	-	✓	1
Modify Memory	#97: c:\windows\syswow64\systray.exe	0xd18	0xe4a0000(239730688)	0x1b58000	✓	1
Modify Memory	#97: c:\windows\syswow64\systray.exe	0xd18	0x7d00000(131072000)	0xa2000	✓	1
Modify Control Flow	#97: c:\windows\syswow64\systray.exe	0xd18 / 0x680	0xcfa58(850520)	-	✓	1
Modify Control Flow	#97: c:\windows\syswow64\systray.exe	0xd18 / 0x680	0x7d1c8f2(131188978)	-	✓	1

Host Behavior

Type	Count
Process	1
Module	3
System	2

Network Behavior

Type	Count
DNS	1
TCP	1

Process #97: systray.exe

ID	97
File Name	c:\windows\syswow64\systray.exe
Command Line	"C:\Windows\SysWOW64\systray.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 278547, Reason: Child Process
Unmonitor End Time	End Time: 300693, Reason: Terminated by Timeout
Monitor duration	22.15s
Return Code	Unknown
PID	3348
Parent PID	1660
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#95: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xd0c	0x110000(1114112)	0x29000	✓	1
Modify Memory	#95: c:\program files (x86)\ealwtgnkh\-zetrxylspxh.exe	0xd0c	0xbc0000(12320768)	0x6000	✓	1

Host Behavior

Type	Count
File	11
-	1
-	1
System	16
Module	11
User	1
Mutex	2
Registry	4
Process	4
-	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dae6ba220bb0a34de731b57965753391343bfe96f9f3fa4fea48102d3377ccf7	C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe, C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe	Sample File	260.85 KB	application/vnd.microsoft.portable-executable	Read, Access	MALICIOUS
1517ab5489988fd256f9420a9f3eb1285d0c262d274bd7eb30d986d610fec28b	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Modified File	51.50 KB	application/CDFV2	-	CLEAN
ca7d46a32ec12479afeec23562bd199c91d2dc0912462250d1a3811a7e89be83	C:\Users\RDHJ0C~1\AppData\Local\Temp\4gyujazywsbdaoe	Dropped File	211.80 KB	application/octet-stream	Write, Read, Create, Access	CLEAN
19013d7428a659774231fd4b5213a463eeab58a0c347dadfaa95536bd89d3f13	C:\Users\RDHJ0C~1\AppData\Local\Temp\nscE967.tmp\akepwc.dll, C:\Users\RDHJ0C~1\AppData\Local\Temp\nspCDFE.tmp\akepwc.dll	Dropped File	47.00 KB	application/vnd.microsoft.portable-executable	Write, Create, Access	CLEAN
4a7839716f95d3bb2dd07172f2afedd6d440f370444f35e0eb1b7885d4177a93	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Dropped File	50.62 KB	application/CDFV2	-	CLEAN
6ca5cdce3c66a07ad6c83572f2d006b18c44be92b509c3e9a3430f024add1e3b	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Dropped File	51.50 KB	application/CDFV2	-	CLEAN
1a7c1aa751f133eb2f7b823b5c1a92de0d906bec4174b85af7de382ed03e0cd8	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Dropped File	51.50 KB	application/CDFV2	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nspC235.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe	Sample File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nspCDFE.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\4gyujazywsbdaoe	Dropped File	Write, Read, Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nspCDFE.tmp\akepwc.dll	Dropped File	Write, Create, Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Read, Access	CLEAN
\??\C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Read, Create, Access	CLEAN
\??\C:\Windows\SysWOW64\cmstp.exe	Accessed File	Read, Create, Access	CLEAN

File Name	Category	Operations	Verdict
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Desktop\PRICE_REQUEST_QUOTATION.exe	Accessed File	Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe	Accessed File	Write, Read, Create, Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows\System32	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
\??\C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe	Accessed File	Read, Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\4N7P3RR-\4N7logrc.ini	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\Ealwtgnkh	Accessed File	Create, Access	CLEAN
\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\Ealwtgnkh\-zetrxylspxh.exe	Accessed File	Write, Delete, Access	CLEAN
C:\Program Files (x86)\Ealwtgnkh	Accessed File	Write, Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\4N7P3RR-\4N7logri.ini	Accessed File	Create, Access	CLEAN
\??\C:\Program Files (x86)\Mozilla Firefox\Firefox.exe	Accessed File	Create, Access	CLEAN
\??\C:\Program Files\Mozilla Firefox\Firefox.exe	Accessed File	Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\4N7P3RR-\4N7logrv.ini	Accessed File	Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Cookies	Accessed File	Create, Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Cookies	Accessed File	Create, Access	CLEAN
\??\C:\Cookies.sqlite	Accessed File	Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nswE85C.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe	Sample File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nscE967.tmp	Accessed File	Create, Delete, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nscE967.tmp\akepwc.dll	Dropped File	Write, Create, Access	CLEAN
\??\C:\Windows\SysWOW64\systray.exe	Accessed File	Read, Create, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.nudesalon.digital/rgoe/	-	34.102.136.180	-	POST	MALICIOUS
http://www.nudesalon.digital/rgoe/?Cxl=AcwhRhtx+/5DgHlicgffINf8LUQZwDlXjd9TWXSB6gbot5IszgiIvjJ67pXYVqoNsa8QJw==&THhTxx=yrK4eV4Xxr	-	34.102.136.180	-	GET	MALICIOUS
http://www.rap8b55d.com/rgoe/?Cxl=mJVafnjbVaZXnrIEO6aq3UnPXgco9MUciXfkcV/NqCHWEuNhes+RSak/YaSOiZQLlgo6/g==&w8GxJD=efo4sRjxk6y4KP	-	198.54.112.103	-	GET	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.rap8b55d.com/rgoe/?Cxl=mJVafnjbVaZXnrIEO6aq3UnPXgco9MUciXfkcV/NqCHWEuNhes+RSak/YaSOiZQLlgo6/g==&THhTxx=yrK4eV4Xxr	-	198.54.112.103	-	GET	MALICIOUS
http://www.rap8b55d.com/rgoe/	-	198.54.112.103	-	POST	MALICIOUS
http://www.bordandoartes.com/rgoe/	-	192.185.213.75	-	POST	CLEAN
http://www.bordandoartes.com/rgoe/?Cxl=lAN+6LZkS+aB/2aiQ72h9+ALXNQwL6dioeeix54bZ9MO84/H7/+jiklTlCiea1o6U5SNkA==&THhTxx=yrK4eV4Xxr	-	192.185.213.75	-	GET	CLEAN
http://www.searchengineeye.com/rgoe/	-	160.153.136.3	-	POST	CLEAN
http://www.searchengineeye.com/rgoe/?Cxl=EXHpTBoivzCZKuB1uj/mQl1CxTx76c7NPbdxHK0a9l8L51JTEvhJv2o6Nk5VUAFXED9xHA==&THhTxx=yrK4eV4Xxr	-	160.153.136.3	-	GET	CLEAN
http://www.restate.club/rgoe/	-	34.102.136.180	-	POST	CLEAN
http://www.restate.club/rgoe/?Cxl=JxGfVlbuMUjpbP2ryp9NqAAUcvSw4xalcvPlMbht+AfdGLaozOMXSMTxw1ejBBSspA9TUA==&THhTxx=yrK4eV4Xxr	-	34.102.136.180	-	GET	CLEAN
http://www.sehatbersama.store/rgoe/	-	45.13.133.216	-	POST	CLEAN
http://www.sehatbersama.store/rgoe/?Cxl=sIXdTxUbKz/96qeCkTgV3Mzc3P/6Etmdy0CNGac80lG7kBMgvgKUgihqHFrjZJ9qD0d1Bg==&THhTxx=yrK4eV4Xxr	-	45.13.133.216	-	GET	CLEAN
http://www.yota.store/rgoe/	-	52.58.78.16	-	POST	CLEAN
http://www.yota.store/rgoe/?Cxl=vDEbv8qQdWhXi00pnoh8UJjCBA7dTpqpRs2jUcgq9SNzcrZBsswg5GW4oy8s4DS6X4nX0g==&THhTxx=yrK4eV4Xxr	-	52.58.78.16	-	GET	CLEAN
http://www.thevillageplumbers.com/rgoe/	-	34.102.136.180	-	POST	CLEAN
http://www.thevillageplumbers.com/rgoe/?Cxl=uoB9N3Y97N7n4fith7cSPcJBcPTqB0g//apWxtglpA+4DIyfKHQX+y6u2ZoMCVv5t8xPig==&THhTxx=yrK4eV4Xxr	-	34.102.136.180	-	GET	CLEAN
http://www.golfsol.art/rgoe/	-	99.86.186.56	-	POST	CLEAN
http://www.golfsol.art/rgoe/?Cxl=eMTFSmRdy/J8aqp5e0iSmw3xJXULOwGUyVMUAKgY7Af7gubUBsEXILJyEqdeBzu66qQdRg==&THhTxx=yrK4eV4Xxr	-	99.86.186.56	-	GET	CLEAN
http://www.iktbn-c01.com/rgoe/?Cxl=9xKKXzDxf4jR9rb9gFXqbZYbfe/mtI21hEgB20jvBm193dN+gRuwcuSlwOYLNp7cLJikRw==&THhTxx=yrK4eV4Xxr	-	172.67.189.216	-	GET	CLEAN
http://www.baila.madrid/rgoe/	-	31.214.178.54	-	POST	CLEAN
http://www.baila.madrid/rgoe/?Cxl=FZv9m3gLyS4pbbAcIL4wjE/DkmhOUTFyiRpqcFoq7M9qckQiRKdGTqegUN9DDka7aWP55g==&THhTxx=yrK4eV4Xxr	-	31.214.178.54	-	GET	CLEAN
http://www.thejegroupllc.com/rgoe/	-	81.169.145.157	-	POST	CLEAN
http://www.thejegroupllc.com/rgoe/?Cxl=DsYyhlgFU14uXJAOP6YeNTk5gtpkz9aSQu7fZIWYblSckE14vm83thC+1sq4cjDpXhRiUQ==&THhTxx=yrK4eV4Xxr	-	81.169.145.157	-	GET	CLEAN
http://www.teelandcompany.com/rgoe/	-	34.102.136.180	-	POST	CLEAN
http://www.teelandcompany.com/rgoe/?Cxl=mDrA6fjGvYH6EvdRXL9JZI5ban60MroB6V8+OSRO0Ae/cJjz84hDdPdymn55tfHVT2xGzg==&THhTxx=yrK4eV4Xxr	-	34.102.136.180	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.pondokbali.store/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=sDoAOA5OtmLnlX03HdCMDI45v+a30M93mz/qcffau5LNKbK7enTzBZZ7oAoSZDGGtEvZNg==	-	23.227.38.74	-	GET	CLEAN
http://www.sustainablefoodfactory.com/rgoe/?Cxl=XpHauQK7KC2WjHZdwnq4WMTUpcNEXoZ9uqeg9ayy0mnQx9tbeZVpp7DwWO8PS50hrewzRQ==&w8GxJD=efo4sRjxk6y4KP	-	34.102.136.180	-	GET	CLEAN
http://www.thejegroupllc.com/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=DsYyhlgFU14uXJAOP6YeNTk5gtpkz9aSQu7fZIWYblSckE14vm83thC+1sq4cjDpXhRiUQ==	-	81.169.145.157	-	GET	CLEAN
http://www.baila.madrid/rgoe/?Cxl=FZv9m3gLyS4pbbAcIL4wjE/DkmhOUTFyiRpqcFoq7M9qckQiRKdGTqegUN9DDka7aWP55g==&w8GxJD=efo4sRjxk6y4KP	-	31.214.178.54	-	GET	CLEAN
http://www.1kingbet.com/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=8NZbPdu1i3dUXB0DPU4kzAYblsxeNSXQrC7mh+LsV5Nod9wjyJXKw0SUB0uoW7EPvfFBkQ==	-	104.21.39.50	-	GET	CLEAN
http://www.iktbn-c01.com/rgoe/	-	172.67.189.216	-	POST	CLEAN
http://www.shahjahantravel.com/rgoe/?Cxl=d9LWsFuvewb7h/v6EwrCexEPacaTeqblWzYENpEVQ4i2pE2pVH/LcDOAID5swiUBI2J78g==&w8GxJD=efo4sRjxk6y4KP	-	104.219.248.101	-	GET	CLEAN
http://www.thenewtocsin.com/rgoe/?w8GxJD=efo4sRjxk6y4KP&Cxl=icL3r7svHZo5uH8Zm6SYIUBWaonuBr/WcR3F0F0+oGeocNnqRdBKeq38Q4roddrx/guvBw==	-	198.54.117.211	-	GET	CLEAN
http://www.pondokbali.store/rgoe/	-	23.227.38.74	-	POST	CLEAN
http://www.sustainablefoodfactory.com/rgoe/	-	34.102.136.180	-	POST	CLEAN
http://www.1kingbet.com/rgoe/	-	104.21.39.50	-	POST	CLEAN
http://www.shahjahantravel.com/rgoe/	-	104.219.248.101	-	POST	CLEAN
http://www.golfsol.art/rgoe/?8pJdD=HridIDO&Cxl=eMTFSmRdy/J8aqp5e0iSmw3xJXULOwGUyVMUAKgY7Af7gubUBsEXILJyEqdeBzu66qQdRg==	-	99.86.186.56	-	GET	CLEAN
http://www.shahjahantravel.com/rgoe/?Cxl=d9LWsFuvewb7h/v6EwrCexEPacaTeqblWzYENpEVQ4i2pE2pVH/LcDOAID5swiUBI2J78g==&8pJdD=HridIDO	-	104.219.248.101	-	GET	CLEAN
http://www.limiteditionft.com/rgoe/	-	34.102.136.180	-	POST	CLEAN
http://www.limiteditionft.com/rgoe/?8pJdD=HridIDO&Cxl=+V4k+VaDQd9kkXtqDVmrj+kvFZmiXxldf3XwnzRS5bc5p9YIdSzu7Qd7OEO7YBU8bys9Pw==	-	34.102.136.180	-	GET	CLEAN
http://www.babeshotnud.com/rgoe/?Cxl=qAwo4FiqGQ7vF/RKkBGUgNSCxZXln1VUyos+fVOy+k3yvD0B9CVt/iZeMW8Kxz83olImHw==&8pJdD=HridIDO	-	185.107.56.60	-	GET	CLEAN
http://www.babeshotnud.com/rgoe/	-	185.107.56.60	-	POST	CLEAN
http://www.futurodr.com/rgoe/	-	154.208.173.139	-	POST	CLEAN
http://www.futurodr.com/rgoe/?8pJdD=HridIDO&Cxl=3YB68aMp2Yn/Ksrq43xxGSNHrBeWjD32XiQQxbglw81jxMqzUnRtzjIwk8cYUz/LonKyKg==	-	154.208.173.139	-	GET	CLEAN
http://www.toptaxxi.store/rgoe/?8pJdD=HridIDO&Cxl=9Ba3zyXU6wZWVfOWx6PLyAS2Ixhez7vN5Wx49vUmzMjajZc2jq0x3a89PDLKAravPCI55g==	-	45.130.41.10	-	GET	CLEAN
http://www.toptaxxi.store/rgoe/	-	45.130.41.10	-	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.bordandoartes.com	192.185.213.75	-	DNS, HTTP	CLEAN
bordandoartes.com	192.185.213.75	-	DNS, HTTP	CLEAN
www.appleluis.host	-	-	DNS	CLEAN
appleluis.host	-	-	DNS	CLEAN
www.searchengineeye.com	160.153.136.3	-	DNS, HTTP	CLEAN
searchengineeye.com	160.153.136.3	-	DNS, HTTP	CLEAN
www.restate.club	34.102.136.180	-	DNS, HTTP	CLEAN
restate.club	34.102.136.180	-	DNS, HTTP	CLEAN
www.sehatbersama.store	45.13.133.216	-	DNS, HTTP	CLEAN
sehatbersama.store	45.13.133.216	-	DNS, HTTP	CLEAN
www.immerseinagro.com	-	-	DNS	CLEAN
www.yota.store	52.58.78.16	-	DNS, HTTP	CLEAN
www.thevillageplumbers.com	34.102.136.180	-	DNS, HTTP	CLEAN
thevillageplumbers.com	34.102.136.180	-	DNS, HTTP	CLEAN
www.golfsol.art	99.86.186.56, 99.86.186.83, 99.86.186.55, 99.86.186.18	-	DNS, HTTP	CLEAN
dw2vdcfmgkqfo.cloudfront.net	99.86.186.56, 99.86.186.83, 99.86.186.55, 99.86.186.18	-	DNS	CLEAN
www.nudesalon.digital	34.102.136.180	-	DNS, HTTP	CLEAN
nudesalon.digital	34.102.136.180	-	DNS, HTTP	CLEAN
www.iktbn-c01.com	172.67.189.216, 104.21.9.250	-	DNS, HTTP	CLEAN
www.baila.madrid	31.214.178.54	-	DNS, HTTP	CLEAN
parkingsrv0.dondominio.com	31.214.178.54	-	DNS	CLEAN
www.thejegroupllc.com	81.169.145.157	-	DNS, HTTP	CLEAN
thejegroupllc.com	81.169.145.157	-	DNS, HTTP	CLEAN
www.teelandcompany.com	34.102.136.180	-	DNS, HTTP	CLEAN
teelandcompany.com	34.102.136.180	-	DNS, HTTP	CLEAN
www.sec-app.pro	-	-	DNS	CLEAN
www.thenewtocsin.com	198.54.117.210, 198.54.117.216, 198.54.117.218, 198.54.117.211, 198.54.117.215, 198.54.117.217, 198.54.117.212	-	DNS, HTTP	CLEAN
parkingpage.namecheap.com	198.54.117.210, 198.54.117.216, 198.54.117.218, 198.54.117.211, 198.54.117.215, 198.54.117.217, 198.54.117.212	-	DNS	CLEAN
www.rap8b55d.com	198.54.112.103	-	DNS, HTTP	CLEAN
www.pondokbali.store	23.227.38.74	-	DNS, HTTP	CLEAN
shops.myshopify.com	23.227.38.74	-	DNS	CLEAN
www.sustainablefoodfactory.com	34.102.136.180	-	DNS, HTTP	CLEAN
sustainablefoodfactory.com	34.102.136.180	-	DNS, HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www.1kingbet.com	172.67.143.57, 104.21.39.50	-	DNS, HTTP	CLEAN
www.shahjahantravel.com	104.219.248.101	-	DNS, HTTP	CLEAN
shahjahantravel.com	104.219.248.101	-	DNS, HTTP	CLEAN
www.limiteditionft.com	34.102.136.180	-	DNS, HTTP	CLEAN
limiteditionft.com	34.102.136.180	-	DNS, HTTP	CLEAN
www.babeshotnud.com	185.107.56.60	-	DNS, HTTP	CLEAN
www.futurodr.com	154.208.173.139	-	DNS, HTTP	CLEAN
www.estanciasanpablo.online	-	-	DNS	CLEAN
www.toptaxxi.store	45.130.41.10	-	DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.185.213.75	www.bordandoartes.com, bordandoartes.com	United States	DNS, HTTP, TCP	CLEAN
192.168.0.1	-	-	UDP, DNS	CLEAN
160.153.136.3	searchengineeye.com, www.searchengineeye.com	Netherlands	DNS, HTTP, TCP	CLEAN
34.102.136.180	www.restate.club, thevillageplumbers.com, teelandcompany.com, www.limiteditionft.com, www.thevillageplumbers.com, nudesalon.digita... ...ionft.com, sustainablefoodfactory.com, www.sustainablefoodfactory.com, www.nudesalon.digital, www.teelandcompany.com, restate.club	United States	DNS, HTTP, TCP	CLEAN
45.13.133.216	sehatbersama.store, www.sehatbersama.store	Cyprus	DNS, HTTP, TCP	CLEAN
52.58.78.16	www.yota.store	Germany	DNS, HTTP, TCP	CLEAN
99.86.186.56	www.golfsol.art, dw2vdcfmgkqfo.cloudfront.net	United States	DNS, HTTP, TCP	CLEAN
172.67.189.216	www.iktbn-c01.com	United States	DNS, HTTP, TCP	CLEAN
31.214.178.54	parkingsrv0.dondominio.com, www.baila.madrid	Spain	DNS, HTTP, TCP	CLEAN
81.169.145.157	www.thejegroupllc.com, thejegroupllc.com	Germany	DNS, HTTP, TCP	CLEAN
198.54.117.211	www.thenewtocsin.com, parkingpage.namecheap.com	United States	DNS, HTTP, TCP	CLEAN
198.54.112.103	www.rap8b55d.com	United States	DNS, HTTP, TCP	CLEAN
23.227.38.74	shops.myshopify.com, www.pondokbali.store	Canada	DNS, HTTP, TCP	CLEAN
104.21.39.50	www.1kingbet.com	-	DNS, HTTP, TCP	CLEAN
104.219.248.101	www.shahjahantravel.com, shahjahantravel.com	United States	DNS, HTTP, TCP	CLEAN
185.107.56.60	www.babeshotnud.com	United Kingdom	DNS, HTTP, TCP	CLEAN
154.208.173.139	www.futurodr.com	Hong Kong	DNS, HTTP, TCP	CLEAN
45.130.41.10	www.toptaxxi.store	Russia	DNS, HTTP, TCP	CLEAN
99.86.186.55	www.golfsol.art, dw2vdcfmgkqfo.cloudfront.net	United States	DNS	CLEAN
99.86.186.83	www.golfsol.art, dw2vdcfmgkqfo.cloudfront.net	United States	DNS	CLEAN
99.86.186.18	www.golfsol.art, dw2vdcfmgkqfo.cloudfront.net	United States	DNS	CLEAN
104.21.9.250	www.iktbn-c01.com	-	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
198.54.117.217	www.thenewtocsin.com, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.216	www.thenewtocsin.com, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.210	www.thenewtocsin.com, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.215	www.thenewtocsin.com, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.218	www.thenewtocsin.com, parkingpage.namecheap.com	United States	DNS	CLEAN
198.54.117.212	www.thenewtocsin.com, parkingpage.namecheap.com	United States	DNS	CLEAN
172.67.143.57	www.1kingbet.com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
14-ARU9TUYI8wI3z	access	price_request_quotation.exe	CLEAN
O3-71R46F5CCAG1B	access	cmstp.exe	CLEAN
3N5NT194G6EF0HB0	access	systray.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	create, access	systray.exe, cmstp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	systray.exe, cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GJVLGF	write, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\15.0\Outlook\Profiles\Outlook\	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	create, access	cmstp.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook_2016\	create, access	cmstp.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Internet Explorer\IntelliForms\Storage2	create, access	cmstp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\	create, access	cmstp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\	create, access	cmstp.exe	CLEAN

Process

Process Name	Commandline	Verdict
price_request_quotation.exe	"C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe"	MALICIOUS
-zetrxylspxh.exe	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"	MALICIOUS
-zetrxylspxh.exe	"C:\Program Files (x86)\Ealwtgnkh\-zetrxylspxh.exe"	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
cmstp.exe	"C:\Windows\SysWOW64\cmstp.exe"	SUSPICIOUS
systray.exe	"C:\Windows\SysWOW64\systray.exe"	SUSPICIOUS
cmd.exe	/c del "C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe"	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	FormBook	FormBook	Function Strings	function_strings_process_4.txt	Spyware	5/5

Antivirus (6)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.NSISX.Spy.Gen.1	C:\Users\RDhJ0CNFevzX\Desktop\PRICE_REQUEST_QUOTATION.exe	MALICIOUS
Memory Dump	Gen:Variant.Razy.679962	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.679962	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.679962	-	MALICIOUS
Memory Dump	Trojan.NSISX.Spy.Gen.1	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.679962	-	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	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows