MALICIOUS

Classifications: Spyware | Injector

Threat Names: XBinder | XLoader | Mal/Generic-S | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Java Archive**
File Name	**sample.jar**
ID	#2924796
MD5	3c0ab7ca460491b57892aecf093dca97
SHA1	685a7aa5d866c222119a1d4b3d485e2c72a02b9a
SHA256	33ff9bb1a784b8896ab920c2e0fab1f9e9a631d9b5a8b204f0455acece52630e
File Size	706.03 KB
Report Created	2022-01-18 18:38 (UTC+1)
Target Environment	win10_64_th2_en_desktop | java

OVERVIEW

VMRay Threat Identifiers (28 rules, 122 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	-
	• Rule "XBinder" from ruleset "Generic" has matched on the sample itself. • Rule "XLoader_Win32" from ruleset "Malware" has matched on the dropped file "c:\users\rdhj0cnfevzx\appdata\local\temp\cielert.tmp". • Rule "XLoader_Win32" from ruleset "Malware" has matched on a memory dump for (process #3) gikaopzb.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Google Chrome, Internet Explorer, Opera, AbleFTP, Mozilla Firefox.			
4/5	Injection	Writes into the memory of another process	3	Injector
	• (Process #5) gikaopzb.exe modifies memory of (process #6) explorer.exe. • (Process #7) rundll32.exe modifies memory of (process #6) explorer.exe. • (Process #5) gikaopzb.exe modifies memory of (process #7) rundll32.exe.			
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #5) gikaopzb.exe alters context of (process #6) explorer.exe. • (Process #7) rundll32.exe alters context of (process #6) explorer.exe.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels file "C:\Users\RDhJ0CNFevzX\glkAOpZB.exe" as "Mal/Generic-S". • File "c:\users\rdhj0cnfevzx\appdata\local\temp\cielert.tmp" is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	4	-
	• (Process #6) explorer.exe contacted known malicious URL "http://www.cannabeeswax.com/xzes...mlNjP1rKSJg1qQ==&XnjlvN=HFNDqh9Ho". • (Process #6) explorer.exe contacted known malicious URL "http://www.cannabeeswax.com/xzes/". • Reputation analysis labels the URL "http://www.metaverse-coaching.com/...WoiJtbdWFziEewpA==&XnjlvN=HFNDqh9Ho" which was contacted by (process #6) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "http://www.metaverse-coaching.com/xzes/" which was contacted by (process #6) explorer.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Resolves known malicious domain	1	-
	• Resolved domain "www.elsist.online" is a known malicious domain.			
3/5	Input Capture	Captures clipboard data	1	Spyware
	• (Process #6) explorer.exe reads data from clipboard.			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #5) gikaopzb.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #5) gikaopzb.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #7) rundll32.exe has a thread which sleeps more than 5 minutes. • (Process #6) explorer.exe has a thread which sleeps more than 5 minutes.			

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive browser data	5	-

- (Process #7) rundll32.exe tries to read sensitive data of web browser "Mozilla Firefox" by file.
- (Process #7) rundll32.exe tries to read sensitive data of web browser "Google Chrome" by file.
- (Process #11) cmd.exe tries to read sensitive data of web browser "Google Chrome" by file.
- (Process #7) rundll32.exe tries to read sensitive data of web browser "Opera" by file.
- (Process #7) rundll32.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive ftp data	1	-

- (Process #7) rundll32.exe tries to read sensitive data of ftp application "AbleFTP" by file.

Score	Category	Operation	Count	Classification
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-

- (Process #3) gikaopzb.exe modifies memory of (process #5) gikaopzb.exe.

Score	Category	Operation	Count	Classification
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-

- (Process #3) gikaopzb.exe alters context of (process #5) gikaopzb.exe.

Score	Category	Operation	Count	Classification
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	22	-

- (Process #5) gikaopzb.exe makes a direct system call to "NtQuerySystemInformation".
- (Process #5) gikaopzb.exe makes a direct system call to "NtQueryInformationProcess".
- (Process #5) gikaopzb.exe makes a direct system call to "NtAllocateVirtualMemory".
- (Process #5) gikaopzb.exe makes a direct system call to "NtFreeVirtualMemory".
- (Process #5) gikaopzb.exe makes a direct system call to "NtOpenProcessToken".
- (Process #5) gikaopzb.exe makes a direct system call to "NtAdjustPrivilegesToken".
- (Process #5) gikaopzb.exe makes a direct system call to "NtClose".
- (Process #5) gikaopzb.exe makes a direct system call to "NtOpenDirectoryObject".
- (Process #5) gikaopzb.exe makes a direct system call to "NtCreateMutant".
- (Process #5) gikaopzb.exe makes a direct system call to "NtCreateSection".
- (Process #5) gikaopzb.exe makes a direct system call to "NtMapViewOfSection".
- (Process #5) gikaopzb.exe makes a direct system call to "NtOpenProcess".
- (Process #5) gikaopzb.exe makes a direct system call to "NtQueryInformationToken".
- (Process #5) gikaopzb.exe makes a direct system call to "NtProtectVirtualMemory".
- (Process #5) gikaopzb.exe makes a direct system call to "NtCreateFile".
- (Process #5) gikaopzb.exe makes a direct system call to "NtQueryInformationFile".
- (Process #5) gikaopzb.exe makes a direct system call to "NtDelayExecution".
- (Process #5) gikaopzb.exe makes a direct system call to "NtReadVirtualMemory".
- (Process #5) gikaopzb.exe makes a direct system call to "NtOpenThread".
- (Process #5) gikaopzb.exe makes a direct system call to "NtReadFile".
- (Process #5) gikaopzb.exe makes a direct system call to "NtUnmapViewOfSection".
- (Process #5) gikaopzb.exe makes a direct system call to "NtResumeThread".

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

- (Process #1) java.exe starts (process #3) gikaopzb.exe with a hidden window.
- (Process #3) gikaopzb.exe starts (process #5) gikaopzb.exe with a hidden window.
- (Process #6) explorer.exe starts (process #7) rundll32.exe with a hidden window.
- (Process #7) rundll32.exe starts (process #11) cmd.exe with a hidden window.
- (Process #6) explorer.exe starts C:\Program Files (x86)\Xmpxd9\hl-ili.exe with a hidden window.

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	3	-

Score	Category	Operation	Count	Classification
	• (Process #5) gikaopzb.exe creates mutex with name "0M1P2-24V-8B9WJ_". • (Process #7) rundll32.exe creates mutex with name "0M1P2-24V-8B9WJ_". • (Process #7) rundll32.exe creates mutex with name "9PNO-9-W2-I5-33E".			
1/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #5) gikaopzb.exe reads from (process #6) explorer.exe. • (Process #5) gikaopzb.exe reads from (process #7) rundll32.exe.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #7) rundll32.exe adds "C:\Program Files (x86)\Xmpxd9\hl-ili.exe" to Windows startup via registry.			
1/5	System Modification	Modifies application directory	1	-
	• (Process #6) explorer.exe modifies "C:\Program Files (x86)\Xmpxd9".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #7) rundll32.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #7) rundll32.exe tries to gather information about application "Mozilla Firefox" by file.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) java.exe resolves 43 API functions by name.			
1/5	Network Connection	Performs DNS request	30	-

Score	Category	Operation	Count	Classification
		• (Process #6) explorer.exe resolves host name "www.distressedthenblessed.com" to IP "162.241.218.205". • (Process #6) explorer.exe resolves host name "www.cannabeeswax.com" to IP "199.34.228.171". • (Process #6) explorer.exe resolves host name "www.muintel.net" to IP "75.2.85.42". • (Process #6) explorer.exe resolves host name "www.update-mind.com" to IP "-". • (Process #6) explorer.exe resolves host name "www.wilbertluna.com" to IP "208.91.197.91". • (Process #6) explorer.exe resolves host name "www.extrobility.com" to IP "217.70.184.50". • (Process #6) explorer.exe resolves host name "www.communication.services" to IP "-". • (Process #6) explorer.exe resolves host name "www.eleonoritalia.com" to IP "62.149.128.45". • (Process #6) explorer.exe resolves host name "www.cpcacursos.com" to IP "162.241.61.34". • (Process #6) explorer.exe resolves host name "www.mindbodyweightlossmethod.com" to IP "62.233.121.61". • (Process #6) explorer.exe resolves host name "www.dalainstitute.info" to IP "51.77.52.109". • (Process #6) explorer.exe resolves host name "www.joannhydeyoga.com" to IP "66.235.200.145". • (Process #6) explorer.exe resolves host name "www.theravewizards.com" to IP "198.54.117.216". • (Process #6) explorer.exe resolves host name "www.elsist.online" to IP "-". • (Process #6) explorer.exe resolves host name "www.metaverse-coaching.com" to IP "121.254.178.252". • (Process #6) explorer.exe resolves host name "www.mylyk.net" to IP "104.21.94.157". • (Process #6) explorer.exe resolves host name "www.overway.store" to IP "154.16.245.157". • (Process #6) explorer.exe resolves host name "www.7looks-mocha-totalbeauty.com" to IP "183.90.231.50". • (Process #6) explorer.exe resolves host name "www.publiccoins.online" to IP "-". • (Process #6) explorer.exe resolves host name "www.printyourdays.com" to IP "104.21.48.190". • (Process #6) explorer.exe resolves host name "www.knowsyourdream.com" to IP "-". • (Process #6) explorer.exe resolves host name "www.venkataramanagraphics.com" to IP "72.167.127.85". • (Process #6) explorer.exe resolves host name "www.monenee.xyz" to IP "-". • (Process #6) explorer.exe resolves host name "www.beandhira.com" to IP "-". • (Process #6) explorer.exe resolves host name "www.skindefense5.com" to IP "64.190.62.111". • (Process #6) explorer.exe resolves host name "www.healthybalancedliving.com" to IP "3.130.253.23". • (Process #6) explorer.exe resolves host name "www.punkidz.com" to IP "156.234.182.39". • (Process #6) explorer.exe resolves host name "www.lochnas.com" to IP "192.64.119.254". • (Process #6) explorer.exe resolves host name "www.senerants.tech" to IP "-". • (Process #6) explorer.exe resolves host name "www.dashmints.com" to IP "162.0.231.244".		
1/5	Network Connection	Connects to remote host	22	-

Score	Category	Operation	Count	Classification
	• (Process #6) explorer.exe opens an outgoing TCP connection to host "162.241.218.205:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "199.34.228.171:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "75.2.85.42:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "208.91.197.91:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "217.70.184.50:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "62.149.128.45:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "162.241.61.34:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "62.233.121.61:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "51.77.52.109:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "66.235.200.145:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "198.54.117.216:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "121.254.178.252:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "104.21.94.157:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "154.16.245.157:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "183.90.231.50:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "104.21.48.190:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "72.167.127.85:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "64.190.62.111:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "3.130.253.23:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "192.64.119.254:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "156.234.182.39:80". • (Process #6) explorer.exe opens an outgoing TCP connection to host "162.0.231.244:80".		
1/5	Crash	An unmonitored process crashed	1	-
	• Unmonitored process runtimebroker.exe crashed.			
1/5	Execution	Drops PE file	2	-
	• (Process #1) java.exe drops file "C:\Users\RDhJ0CNFevzX\glkAOpZB.exe". • Drops file c:\users\rdhj0cnfevzx\appdata\local\temp\cielert.tmp.			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDhJ0CNFevzX\glkAOpZB.exe".			
-	Trusted	Known clean file	1	-
	• File "C:\Users\RDhJ0CNFevzX\m2rKEl2wJZ.txt" is a known clean file.			

Mitre ATT&CK Matrix

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

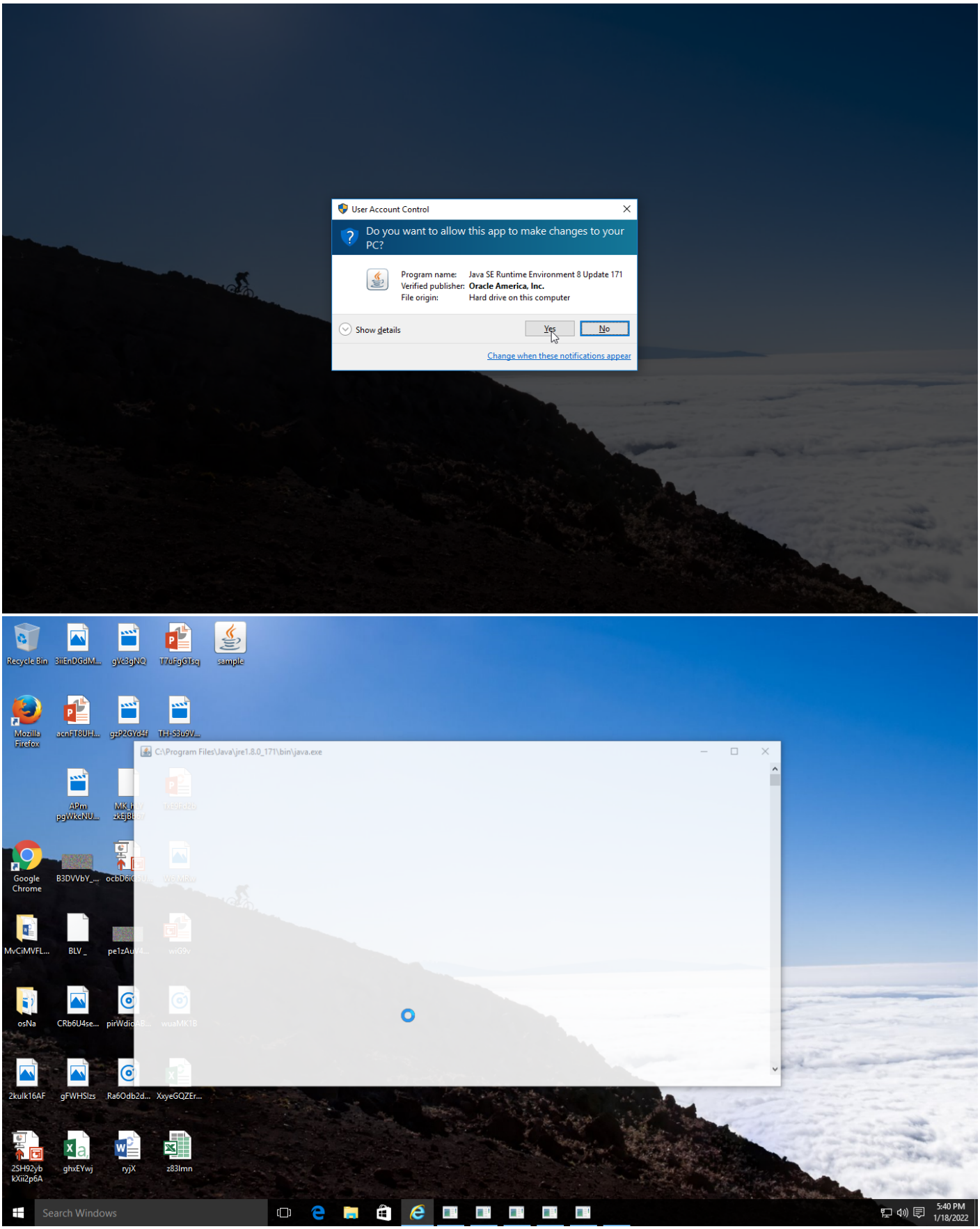
Sample Information

ID	#2924796
MD5	3c0ab7ca460491b57892aecf093dca97
SHA1	685a7aa5d866c222119a1d4b3d485e2c72a02b9a
SHA256	33ff9bb1a784b8896ab920c2e0fab1f9e9a631d9b5a8b204f0455acece52630e
SSDeep	12288:q/wCW2+HpZChZpaDQjZ72kX58jza8TYMrkyWLNGrKp4hJhh3bYdlTa:q/vR+HpZNi7H180MYMrKpohpbYd8a
File Name	sample.jar
File Size	706.03 KB
Sample Type	Java Archive
Has Macros	✓

Analysis Information

Creation Time	2022-01-18 18:38 (UTC+1)
Analysis Duration	00:05:00
Termination Reason	Timeout
Number of Monitored Processes	26
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	3

Recycle Bin
3iiEnDGdM...
gVc3gNQ
T7uFgGTsq
sample
Mozilla Firefox
acnFT8UH...
gzP2GYd4f
TH-S3u9V...
APm pgWkcNU...
MK_hLY zkEjBb67
TxE9Pd2b
Google Chrome
B3DVVbY_...
ocbD6iQ5U...
W6 MRw
MvCiMVFL...
BLV _
pe1zAuV4...
wiG9v
osNa
CRb6U4se...
pirWdioAB...
wuaMK1B
2kulk16AF
gFWHSlzs
Ra6Odb2d...
XxyeGQZEr...
2SH92yb kXii2p6A
ghxEYwj
ryjX
z83Imn
Search Windows
5:39 PM
1/18/2022



Screenshots truncated

NETWORK

General

10020.64 KB total sent

344.22 KB total received

1 ports 80

23 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

55 DNS requests for 30 domains

1 nameservers contacted

25 total requests returned errors

HTTP/S

50 URLs contacted, 22 servers

118 sessions, 3277.32 KB sent, 266.43 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://www.distressedthenblessed.com/xzes/	-	-		0 bytes	NA
GET	http://www.distressedthenblessed.com/xzes/?fPvdTfP=qta2XgLpJD0UJeOmnNNCsYOZQAr8lLiHkRXUM4hponnLum3Sko0HNCnlcBOpo2T9WKQqHA==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
GET	http://www.cannabeeswax.com/xzes/?fPvdTfP=MnkJGqa3tkJYrNwXwf+SQCXqe9xCUdMYZwqCRe5AdpvkdOhCSjAyksY5mlNjP1rKSJg1qQ==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
GET	http://www.muintel.net/xzes/?fPvdTfP=7dPOxqSGMW0L8hlFGu6rm7yNCxvkKFvS/HQycNL3QP0OiVyzun6JwSF5ntRV2TTVU8tbFA==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
POST	http://www.cannabeeswax.com/xzes/	-	-		0 bytes	NA
POST	http://www.muintel.net/xzes/	-	-		0 bytes	NA
GET	http://www.wilbertluna.com/xzes/?fPvdTfP=EU40BBWIyZv+CeoOh9wLC2Sy0USpPHzyDUV4UMwzyT54U54r+rzGbSA1EEvbYTQJ3TREQw==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
GET	http://www.extrobility.com/xzes/?fPvdTfP=pd/4jJ6jLgoCWPH/GHUgj0FHbCU6+qKjd6PN15Ru4R6uBn9glEdMwokePvqp4Tct3DAb4g==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
POST	http://www.wilbertluna.com/xzes/	-	-		0 bytes	NA
POST	http://www.extrobility.com/xzes/	-	-		0 bytes	NA
GET	http://www.eleonoritalia.com/xzes/?fPvdTfP=dGVhXmv/Ev2mORIQnUGskdehpcwp8r0HTFZZz+ISCj08k18P++8BxEjg4Ft4U9K2XKkX4A==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
GET	http://www.cpcacursos.com/xzes/?fPvdTfP=61uYctvZwZ8Sp3djwTs/ePBNtPg20uoPiMbdeJbZ57IZPEYJt69lNO3EZv26EwNfkImL2g==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.mindbodyweightlossmethod.com/xzes/?fPvdTfP=Rvlcq+i7q7kRIhcCci6HzJn3Vgbs8lkZ3qFCamrgyZPpaSwOznlYsQuJhKWwxSWF5imggw==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
GET	http://www.dalainstitute.info/xzes/?fPvdTfP=CPfiPKWK5LZIlly0Y09a8SHSPP5QoGiXgTF+OOq8iYZD4WpEFq03gqLRDF/iG1nWVv660g==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
GET	http://www.metaverse-coaching.com/xzes/?fPvdTfP=mplh2iHN36zwzCvjnuubKHZFR0jd/mTSeFkuMh06lTP5jmZCQ9iS7wWoiJtbdWFziEewpA==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
GET	http://www.mylyk.net/xzes/?fPvdTfP=lZAWFjxlzIo8AvKzM9v0DCjfM8h6xX/Vie0BER185F7DTJN7Gb1m96i9Ww364gmXpwvyaA==&Mx=Wlpl	-	-		0 bytes	NA
POST	http://www.eleonoritalia.com/xzes/	-	-		0 bytes	NA
GET	http://www.eleonoritalia.com/xzes/?fPvdTfP=dGVhXmv/Ev2mORIQnUGskdehpcwp8r0HTFZZz+ISCj08k18P++8BxEjg4Ft4U9K2XKkX4A==&Mx=Wlpl	-	-		0 bytes	NA
GET	http://www.extrobility.com/xzes/?fPvdTfP=pd/4jJ6jLgoCWPH/GHUgj0FHbCU6+qKjd6PN15Ru4R6uBn9glEdMwokePvqp4Tct3DAb4g==&Mx=Wlpl	-	-		0 bytes	NA
GET	http://www.overway.store/xzes/?fPvdTfP=NelJDzsWSz5EVZYy3pWwuAqYTUkdDte6huV8TkEY+SvYHK9zRcBYxeVFWYdVVt/jrxsjsA==&Mx=Wlpl	-	-		0 bytes	NA
POST	http://www.cpcacursos.com/xzes/	-	-		0 bytes	NA
POST	http://www.mindbodyweightlossmethod.com/xzes/	-	-		0 bytes	NA
POST	http://www.dalainstitute.info/xzes/	-	-		0 bytes	NA
POST	http://www.joannhydeyoga.com/xzes/	-	-		0 bytes	NA
GET	http://www.7looks-mocha-totalbeauty.com/xzes/?fPvdTfP=N6kvuAXHq1eVHQ2e8nDxm1bATb9xJ8kGsA5u90v+9KhKcWZ9JLFx/zAPmWa4/jqVMzkOHg==&Mx=Wlpl	-	-		0 bytes	NA
GET	http://www.distressedthenblessed.com/xzes/?fPvdTfP=qta2XgLpJD0UJeOmnNNCsYOZQAr8lLiHkRXUM4hponnLum3Sko0HNCnIcBOpo2T9WKQqHA==&Mx=Wlpl	-	-		0 bytes	NA
GET	http://www.joannhydeyoga.com/xzes/?fPvdTfP=M74vbXdatV6xDvL6/loAkrjESC9Z5XZA/+6NQlBWeUhuvtB2es1cFv1IRip/2lkUNu1/CA==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
POST	http://www.theravewizards.com/xzes/	-	-		0 bytes	NA
GET	http://www.theravewizards.com/xzes/?fPvdTfP=hsby6OJ/fd6ThLUdZbSyJdZ7YeDc2IcIgsMuottqV+UF+OnCYZb0G45wB+nhiN/ricwxiA==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
POST	http://www.metaverse-coaching.com/xzes/	-	-		0 bytes	NA
POST	http://www.overway.store/xzes/	-	-		0 bytes	NA
GET	http://www.printyourdays.com/xzes/?fPvdTfP=WvVdSYbKp96wH048bjEVjLioWRcomDeCwGP5DsGxMK4Q1oFCkmDEchfPL+qbhMw+Vvr/6w==&if8=7nz42h_PfxRhtde	-	-		0 bytes	NA
POST	http://www.7looks-mocha-totalbeauty.com/xzes/	-	-		0 bytes	NA
GET	http://www.venkataramanagraphics.com/xzes/?fPvdTfP=zQCXJP8LggsZoUmXHFz9GWvVffBXhlgfEpXjhYl/bV5XFEUeHH6MpZREokIqHen0Y7wkVg==&if8=7nz42h_PfxRhtde	-	-		0 bytes	NA
GET	http://www.mindbodyweightlossmethod.com/xzes/?fPvdTfP=Rvlcq+i7q7kRIhcCci6HzJn3Vgbs8lkZ3qFCamrgyZPpaSwOznlYsQuJhKWwxSWF5imggw==&if8=7nz42h_PfxRhtde	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://www.mylyk.net/xzes/?fPvdTfP=IZAWFjxlzIo8AvKzM9v0DCjfM8h6xX/Vie0BER185F7DTJN7Gb1m96i9Ww364gmXpwvyaA==&if8=7nz42h_PfxRhtde	-	-		0 bytes	NA
POST	http://www.venkataramanagraphics.com/xzes/	-	-		0 bytes	NA
GET	http://www.skindefense5.com/xzes/?fPvdTfP=nzYmw7PgvXl3RVxY+22S0s66JIboZ9taw8WhBbJqqOeAmHf1Jq6dfLQuQN0DXxF4yypuTw==&s2=wZxpTbThw4ppsl	-	-		0 bytes	NA
GET	http://www.eleonoritalia.com/xzes/?s2=wZxpTbThw4ppsl&fPvdTfP=dGVhXmv/Ev2mORIQnUGskdehpcwp8r0HTFZZz+lSCj08k18P++8BxEjg4Ft4U9K2XKkX4A==	-	-		0 bytes	NA
GET	http://www.healthybalancedliving.com/xzes/?fPvdTfP=Orxi7BqtkIQQhmFsXk66PD0SSSSqk86WkGR6LUZk9NXV5D1XaC2g8Hl8xZwfwmZ8pB0v8Q==&s2=wZxpTbThw4ppsl	-	-		0 bytes	NA
GET	http://www.punkidz.com/xzes/?s2=wZxpTbThw4ppsl&fPvdTfP=rzqcJvicjlO1REHeJYC8xd++pVURv744ENDtGRRvNKzpNTaKu7eGHsB4p2bzaao8N19v3g==	-	-		0 bytes	NA
POST	http://www.skindefense5.com/xzes/	-	-		0 bytes	NA
POST	http://www.healthybalancedliving.com/xzes/	-	-		0 bytes	NA
POST	http://www.punkidz.com/xzes/	-	-		0 bytes	NA
GET	http://www.dashmints.com/xzes/?fPvdTfP=WU+vhYw1FCGUzoOC9mxW//+INZAAC3fdNAegkUfjRfNchOBBzc+toiSaox38c5d0R6zVvA==&XnjlvN=HFNDqh9Ho	-	-		0 bytes	NA
POST	http://www.lochnas.com/xzes/	-	-		0 bytes	NA
GET	http://www.lochnas.com/xzes/?fPvdTfP=stwJlOwy5CWIDHGfLETpAqRwwrDBzTynArbgdcfDkklacgwwr2U0EHUYz568MSnJkjbUVw==&s2=wZxpTbThw4ppsl	-	-		0 bytes	NA
POST	http://www.dashmints.com/xzes/	-	-		0 bytes	NA
GET	http://www.skindefense5.com/xzes/?fPvdTfP=nzYmw7PgvXl3RVxY+22S0s66JIboZ9taw8WhBbJqqOeAmHf1Jq6dfLQuQN0DXxF4yypuTw==&zR-TJ=8phDMLKxmnQDtp60	-	-		0 bytes	NA
POST	http://www.mylyk.net/xzes/	-	-		0 bytes	NA

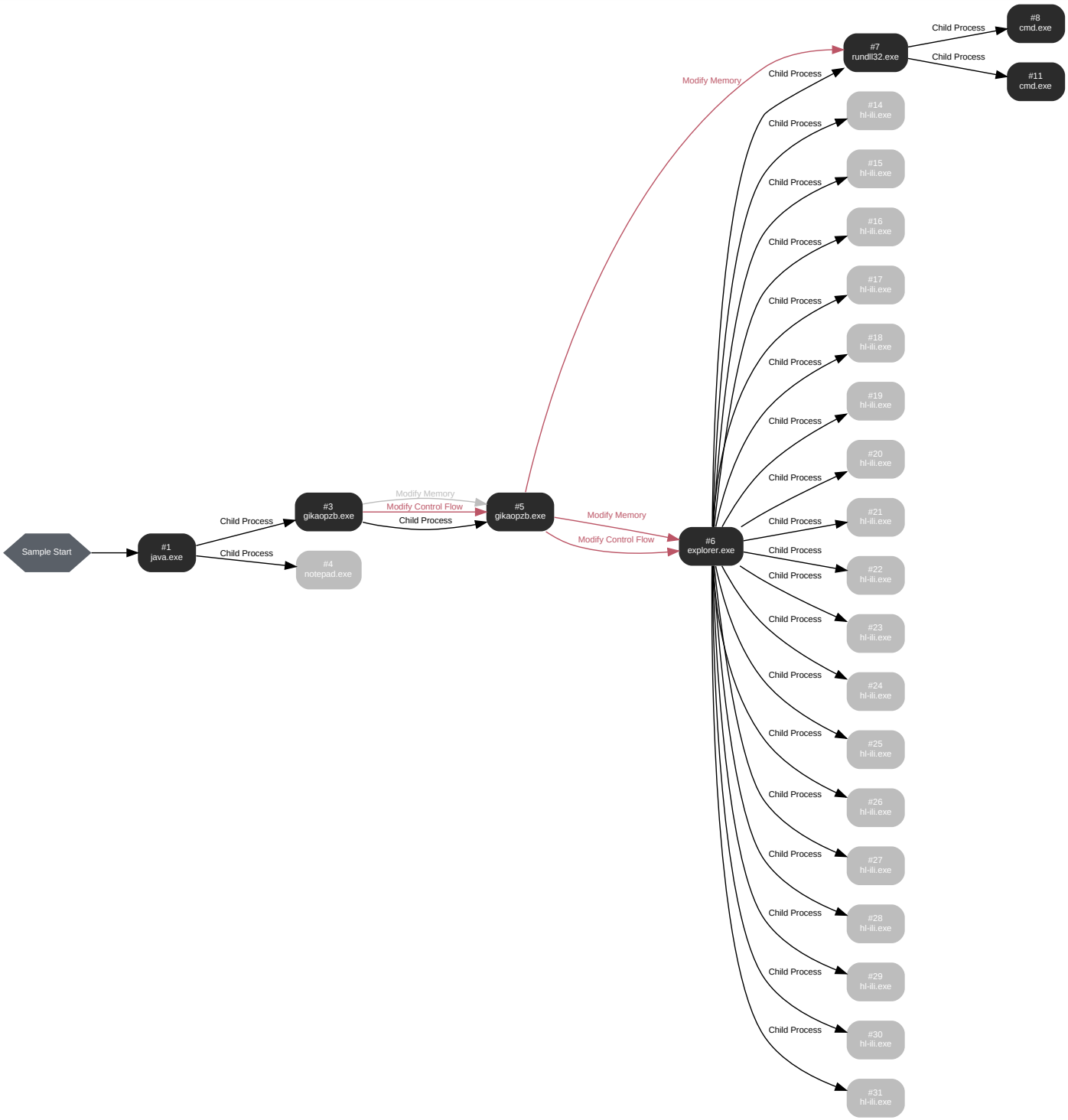
DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.distressedthenblessed.com, distressedthenblessed.com	NoError	162.241.218.205	distressedthenblessed.com	NA
A	www.cannabeeswax.com, cannabeeswax.com	NoError	199.34.228.171	cannabeeswax.com	NA
A	www.muintel.net, muintel.net	NoError	75.2.85.42, 99.83.196.71	muintel.net	NA
A	www.update-mind.com, update-mind.com	NoError		update-mind.com	NA
A	www.wilbertluna.com	NoError	208.91.197.91		NA
A	www.extrobility.com, webredir.vip.gandi.net	NoError	217.70.184.50	webredir.vip.gandi.net	NA
A	www.communication.services	ServFail			NA
A	www.eleonoritalia.com, eleonoritalia.com	NoError	62.149.128.45	eleonoritalia.com	NA
A	www.cpcacursos.com, cpcacursos.com	NoError	162.241.61.34	cpcacursos.com	NA
A	www.mindbodyweightlossmethod.com	NoError	62.233.121.61		NA

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www.dalainstitute.info, dalainstitute.info	NoError	51.77.52.109	dalainstitute.info	NA
A	www.joannhydeyoga.com, joannhydeyoga.com	NoError	66.235.200.145	joannhydeyoga.com	NA
A	www.theravewizards.com, parkingpage.namecheap.com	NoError	198.54.117.216, 198.54.117.211, 198.54.117.212, 198.54.117.217, 198.54.117.210, 198.54.117.218, 198.54.117.215	parkingpage.namecheap.com	NA
A	www.elsist.online	NXDomain			NA
A	www.metaverse-coaching.com	NoError	121.254.178.252		NA
A	www.mylyk.net	NoError	104.21.94.157, 172.67.137.204		NA
A	www.overway.store, overway.store	NoError	154.16.245.157	overway.store	NA
A	www.7looks-mocha-totalbeauty.com	NoError	183.90.231.50		NA
A	www.publiccoins.online	NXDomain			NA
A	www.printyourdays.com	NoError	104.21.48.190, 172.67.156.13		NA
A	www.knowsyourdream.com	ServFail			NA
A	www.venkataramanagraphics.com, venkataramanagraphics.com	NoError	72.167.127.85	venkataramanagraphics.com	NA
A	www.monenee.xyz	NXDomain			NA
A	www.beandhira.com	NXDomain			NA
A	www.skindefense5.com	NoError	64.190.62.111		NA
A	www.healthybalancedliving.com, traff-2.hugedomains.com, hdr-nlb5-4e815dd67a14bf7f.elb.us-east-2.amazonaws.com	NoError	3.130.253.23, 3.130.204.160	traff-2.hugedomains.com, hdr-nlb5-4e815dd67a14bf7f.elb.us-east-2.amazonaws.com	NA
A	www.punkidz.com	NoError	156.234.182.39		NA
A	www.lochnas.com	NoError	192.64.119.254		NA
A	www.senerants.tech	ServFail			NA
A	www.dashmints.com	NoError	162.0.231.244		NA
-	www.update-mind.com	-			NA
-	www.eleonoritalia.com	-	62.149.128.45		NA
-	www.extrobility.com	-	217.70.184.50		NA
-	www.distressedthenblessed.com	-	162.241.218.205		NA

BEHAVIOR

Process Graph



Process #1: java.exe

ID	1
File Name	c:\program files\java\jre1.8.0_171\bin\java.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\java.exe" -jar "C:\Users\RDHJ0C~1\Desktop\sample.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 66965, Reason: Analysis Target
Unmonitor End Time	End Time: 152923, Reason: Terminated
Monitor duration	85.96s
Return Code	0
PID	4688
Parent PID	1488
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\gIkAOpZB.exe	612.00 KB	4216ff4fa7533209a6e50c6f05c5216b8afb456e6a3ab6b65ed9fcbdbd275096	✗
C:\Users\RDhJ0CNFevzX\m2rKEl2wJZ.txt	6 bytes	2b7814d3fca2e99e56c51b6ff2aa313ea6e9da6424804240aa8ad891fdfe0900	✗

Host Behavior

Type	Count
System	32
File	3601
Module	69
Environment	5
-	4
Process	2
Keyboard	4
Registry	2
-	4
Window	1

Process #3: gikaopzb.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\gikaopzb.exe
Command Line	C:\Users\RDhJ0CNFevzX\glkAOpZB.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 121290, Reason: Child Process
Unmonitor End Time	End Time: 177779, Reason: Terminated
Monitor duration	56.49s
Return Code	0
PID	3556
Parent PID	4688
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	163.50 KB	82dd41529ae86f25911df1f4b3b032008b7bc7af33b47c5367863bde1291a410	✗

Host Behavior

Type	Count
System	9
File	11
Environment	1
Module	21
Keyboard	1
Process	2
-	25
-	3

Process #4: notepad.exe

ID	4
File Name	c:\windows\system32\notepad.exe
Command Line	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\RDhJ0CNFevzX\m2rKEl2wJZ.txt
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 149959, Reason: Child Process
Unmonitor End Time	End Time: 317184, Reason: Terminated
Monitor duration	167.22s
Return Code	1073807364
PID	3816
Parent PID	4688
Bitness	64 Bit

Process #5: gikaopzb.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\gikaopzb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\gIkAOpZB.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 174761, Reason: Child Process
Unmonitor End Time	End Time: 183293, Reason: Terminated
Monitor duration	8.53s
Return Code	0
PID	3976
Parent PID	3556
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xde8	0x400000(4194304)	0x29000	✗	1
Modify Control Flow	#3: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xde8 / 0xf8c	0x77a08fe0(2007011296)	-	✓	1
Modify Memory	#3: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xde8	0x3cd008(3985416)	0x4	✓	1

Host Behavior

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

Process #6: explorer.exe

ID	6
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 176596, Reason: Injection
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	201.40s
Return Code	Unknown
PID	1488
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xf8c	0x8d90000(148439040)	0x11b000	✓	1
Modify Control Flow	#5: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xf8c / 0x5d4	0x600000(6291456)	-	✓	1
Modify Control Flow	#5: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xf8c / 0x5d4	0x8e0c909(148949257)	-	✓	1
Modify Memory	#7: c:\windows\syswow64\rundll32.exe	0xf9c	0x10c80000(281542656)	0x1b58000	✓	1
Modify Memory	#7: c:\windows\syswow64\rundll32.exe	0xf9c	0x8eb0000(149618688)	0xe1000	✓	1
Modify Control Flow	#7: c:\windows\syswow64\rundll32.exe	0xf9c / 0x5d4		-	✓	1
Modify Control Flow	#7: c:\windows\syswow64\rundll32.exe	0xf9c / 0x5d4	0x8f0b8f2(149993714)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	612.00 KB	4216ff4fa7533209a6e50c6f05c5216b8afb456e6a3ab6b65ed9fcbdbd275096	✗

Host Behavior

Type	Count
Process	19
Module	3
System	627
File	88
COM	1

Network Behavior

Type	Count
HTTP	118
DNS	55
TCP	183

Process #7: rundll32.exe

ID	7
File Name	c:\windows\syswow64\rundll32.exe
Command Line	"C:\Windows\SysWOW64\rundll32.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 178536, Reason: Child Process
Unmonitor End Time	End Time: 317932, Reason: Terminated
Monitor duration	139.40s
Return Code	1073807364
PID	3992
Parent PID	1488
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xf8c	0x110000(1114112)	0x29000	✓	1
Modify Memory	#5: c:\users\rdhj0cnfevzx\gikaopzb.exe	0xf8c	0x840000(8650752)	0x12000	✓	1

Host Behavior

Type	Count
File	102
-	1
-	1
System	39422
User	1
Mutex	2
Module	16
Registry	363
Process	5
-	6
COM	1
Environment	2
-	2

Process #8: cmd.exe

ID	8
File Name	c:\windows\syswow64\cmd.exe
Command Line	/c del "C:\Users\RDhJ0CNFevzX\glkAOpZB.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 185533, Reason: Child Process
Unmonitor End Time	End Time: 188268, Reason: Terminated
Monitor duration	2.73s
Return Code	0
PID	4076
Parent PID	3992
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	9

Process #11: cmd.exe

ID	11
File Name	c:\windows\syswow64\cmd.exe
Command Line	/c copy "C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\RDHJ0C~1\AppData\Local\Temp\DB1" /V
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 299105, Reason: Child Process
Unmonitor End Time	End Time: 303003, Reason: Terminated
Monitor duration	3.90s
Return Code	0
PID	3424
Parent PID	3992
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\DB1	40.00 KB	eb689f55c70414dda4fc725dd47347bcce902fe9650cfce238af7bf2e95c4674	✖

Host Behavior

Type	Count
Module	8
Registry	17
File	46
Environment	11
System	1
Process	1

Process #14: hl-ili.exe

ID	14
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 317488, Reason: Child Process
Unmonitor End Time	End Time: 319699, Reason: Terminated
Monitor duration	2.21s
Return Code	3221226091
PID	2120
Parent PID	1488
Bitness	32 Bit

Process #15: hl-ili.exe

ID	15
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 317591, Reason: Child Process
Unmonitor End Time	End Time: 319992, Reason: Terminated
Monitor duration	2.40s
Return Code	3221226091
PID	4820
Parent PID	1488
Bitness	32 Bit

Process #16: hl-ili.exe

ID	16
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319027, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.97s
Return Code	Unknown
PID	2688
Parent PID	1488
Bitness	32 Bit

Process #17: hl-ili.exe

ID	17
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319088, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.90s
Return Code	Unknown
PID	620
Parent PID	1488
Bitness	32 Bit

Process #18: hl-ili.exe

ID	18
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319143, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.85s
Return Code	Unknown
PID	3132
Parent PID	1488
Bitness	32 Bit

Process #19: hl-ili.exe

ID	19
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319235, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.76s
Return Code	Unknown
PID	5060
Parent PID	1488
Bitness	32 Bit

Process #20: hl-ili.exe

ID	20
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319333, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.66s
Return Code	Unknown
PID	5064
Parent PID	1488
Bitness	32 Bit

Process #21: hl-ili.exe

ID	21
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319399, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.59s
Return Code	Unknown
PID	3120
Parent PID	1488
Bitness	32 Bit

Process #22: hl-ili.exe

ID	22
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319479, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.51s
Return Code	Unknown
PID	1736
Parent PID	1488
Bitness	32 Bit

Process #23: hl-ili.exe

ID	23
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319542, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.45s
Return Code	Unknown
PID	3536
Parent PID	1488
Bitness	32 Bit

Process #24: hl-ili.exe

ID	24
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319638, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.35s
Return Code	Unknown
PID	1552
Parent PID	1488
Bitness	32 Bit

Process #25: hl-ili.exe

ID	25
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319703, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.29s
Return Code	Unknown
PID	2212
Parent PID	1488
Bitness	32 Bit

Process #26: hl-ili.exe

ID	26
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319768, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.22s
Return Code	Unknown
PID	1728
Parent PID	1488
Bitness	32 Bit

Process #27: hl-ili.exe

ID	27
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319824, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.17s
Return Code	Unknown
PID	1864
Parent PID	1488
Bitness	32 Bit

Process #28: hl-ili.exe

ID	28
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 319943, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	58.05s
Return Code	Unknown
PID	3912
Parent PID	1488
Bitness	32 Bit

Process #29: hl-ili.exe

ID	29
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 320001, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	57.99s
Return Code	Unknown
PID	3580
Parent PID	1488
Bitness	32 Bit

Process #30: hl-ili.exe

ID	30
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 320064, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	57.93s
Return Code	Unknown
PID	2720
Parent PID	1488
Bitness	32 Bit

Process #31: hl-ili.exe

ID	31
File Name	c:\program files (x86)\xmpxd9\hl-ili.exe
Command Line	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 320191, Reason: Child Process
Unmonitor End Time	End Time: 377992, Reason: Terminated by Timeout
Monitor duration	57.80s
Return Code	Unknown
PID	720
Parent PID	1488
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
33ff9bb1a784b8896ab920c2e0fab1f9e9a631d9b5a8b204f0455acece52630e	C:\Users\RDhJ0CNFevzX\Desktop\sample.jar, C:\Users\RDHJ0C~1\Desktop\sample.jar	Sample File	706.03 KB	application/java-archive	Access, Read	MALICIOUS
82dd41529ae86f25911df1f4b3b032008b7bc7af33b47c5367863bde1291a410	c:\users\rdhj0cnfevzx\appdata\local\temp\cielert.tmp	Dropped File	163.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
4216ff4fa7533209a6e50c6f05c5216b8afb456e6a3ab6b65ed9fcbdbd275096	C:\Users\RDhJ0CNFevzX\glkAOpZB.exe	Dropped File	612.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
6192749648567a7382636b4b567a787256a7c98e584aec0e3853c65f12f6dfc6	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Modified File	51 bytes	text/plain	Access, Create, Write	CLEAN
0315dff9329f9a35b194d26d383ab0a1dd07a7d96dc340a1d5ce0e015f78ca69	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
23e5f4241d8a44dd3afd2c98200c7f7e7c298701b23d39df53e9fd59eb4207fe	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Modified File	59.00 KB	application/CDFV2	-	CLEAN
2b7814d3fca2e99e56c51b6ff2aa313ea6e9da6424804240aa8ad891fdfe0900	C:\Users\RDhJ0CNFevzX\m2rKEl2wJZ.txt	Dropped File	6 bytes	text/plain	Access, Create	CLEAN
73b5116552583fdf407582d899f7feac3d251dbed7ec659a8b4584509714a0b9	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\webcache\webcachev01.dat	Dropped File	10240.00 KB	application/x-ms-ese	-	CLEAN
eb689f55c70414dda4fc725dd47347bcce902fe9650cfce238af7bf2e95c4674	C:\Users\RDHJ0C~1\AppData\Local\Temp\DB1, C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Dropped File	40.00 KB	application/x-sqlite3	Access, Create, Write	CLEAN
08963f779e198ed52bef42cf932bbe1921338df156ea876f0907ca05cd58f67e	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Dropped File	58.00 KB	application/CDFV2	-	CLEAN
ae343c2a680c4a2df51c952c986a004efbf00e34693ca20cfe98b58fda7e370f	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Dropped File	59.00 KB	application/CDFV2	-	CLEAN
525c2998c9d31bb06aa869dbf29915c9961ad715318549da3817e3dd901c6557	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\automaticdestinations\f01b4d95cf55d32a.automaticdestinations-ms	Dropped File	59.00 KB	application/CDFV2	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Program Files\Java\jre1.8.0_171\lib\rt.jar	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\server\jvm.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\zip.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\meta-index	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext	Accessed File	Access	CLEAN
C:\Windows\Sun\Java\lib\ext\meta-index	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\access-bridge-64.jar	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Java\jre1.8.0_171\lib\ext\cldrdata.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\dnsns.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\jaccess.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\jfxrt.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\localedata.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\nashorn.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunec.jar	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunjce_provider.jar	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunmscapi.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunpkcs11.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\zipfs.jar	Accessed File	Access	CLEAN
C:\Windows\Sun\Java\lib\ext	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\sample.jar	Sample File	Access, Read	CLEAN
C:\ProgramData\Oracle\Java\usagetracker.properties	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\management\usagetracker.properties	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171	Accessed File	Access	CLEAN
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Modified File	Access, Create, Write	CLEAN
C:\Users\RDHJ0C~1\Desktop\sample.jar	Sample File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\security\java.security	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\resources.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\meta-index	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\sunrsasign.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\jsse.jar	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\jce.jar	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\charsets.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\jfr.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\classes	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\meta-index	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\amd64\sunec.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunec.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\sunec.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\security\US_export_policy.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\security\policy\unlimited\US_export_policy.jar	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Java\jre1.8.0_171\lib\security\policy\unlimited\local_policy.jar	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\net.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\nio.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\security\blacklisted.certs	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\security\cacerts	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\glkAOpZB.exe	Dropped File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\m2rKEl2wJZ.txt	Dropped File	Access, Create	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\awt.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\.accessibility.properties	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\accessibility.properties	Accessed File	Access, Read	CLEAN
\??\C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Create, Read	CLEAN
\??\C:\Users\RDhJ0CNFevzX\glkAOpZB.exe	Accessed File	Access, Create, Read, Write	CLEAN
\??\C:\Windows\system32\ntdll.dll	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\Cielert.tmp	Accessed File	Access, Create, Write	CLEAN
\??\C:\Windows\SysWOW64\rundll32.exe	Accessed File	Access, Create, Read	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\RDhJ0CNFevzX\glkAOpZB.exe	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX	Accessed File	Access	CLEAN
\??\C:\Program Files (x86)\Xmpxd9\hl-ili.exe	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\J9M369S2\J9Mlogrc.ini	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\Xmpxd9	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDHJ0C~1\AppData\Local\Temp\Xmpxd9\hl-ili.exe	Accessed File	Access, Delete, Write	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\J9M369S2\J9Mlogri.ini	Accessed File	Access, Create	CLEAN
C:\Program Files (x86)\Xmpxd9	Accessed File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access, Read	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles\ijfigeuq.default\logins.json	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access, Create	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\AppData\Local\Google\Chrome\User Data\Default\Login Data	Dropped File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\DB1	Dropped File	Access, Create, Write	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access, Create	CLEAN
\??\C:\Program Files (x86)\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN

File Name	Category	Operations	Verdict
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\J9M369S2\J9Mlogrv.ini	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Cookies	Accessed File	Access, Create, Read	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Cookies	Accessed File	Access, Create	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles\ijfigeuq.default\Cookies.sqlite	Accessed File	Access, Create, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.cannabeeswax.com/xzes/?fPvdTfP=MnkJGqa3tkJYrNwXwf+SQCXqe9xCUdMYZwqCRe5AdpvkdOhCSjAyksY5mlNjP1rKSJg1qQ==&XnjlvN=HFNDqh9Ho	-	199.34.228.171	-	GET	MALICIOUS
http://www.cannabeeswax.com/xzes/	-	199.34.228.171	-	POST	MALICIOUS
http://www.metaverse-coaching.com/xzes/?fPvdTfP=mpIh2iHN36zwzCvjnuubKHZFR0jd/mTSeFkuMh06lTP5jmZCQ9iS7wWoiJtbdWFziEewpA==&XnjlvN=HFNDqh9Ho	-	121.254.178.252	-	GET	MALICIOUS
http://www.metaverse-coaching.com/xzes/	-	121.254.178.252	-	POST	MALICIOUS
http://www.distressedthenblessed.com/xzes/	-	162.241.218.205	-	POST	CLEAN
http://www.distressedthenblessed.com/xzes/?fPvdTfP=qta2XgLpJD0UJeOmnNNCsYOZQAr8lLiHkRXUM4hponnLum3Sko0HNCnlcBOpo2T9WKQqHA==&XnjlvN=HFNDqh9Ho	-	162.241.218.205	-	GET	CLEAN
http://www.muintel.net/xzes/?fPvdTfP=7dPOxqSGMW0L8hlFGu6rm7yNCxvkKFvS/HQycNL3QP0OiVyzun6JwSF5ntRV2TTVU8tbFA==&XnjlvN=HFNDqh9Ho	-	75.2.85.42	-	GET	CLEAN
http://www.muintel.net/xzes/	-	75.2.85.42	-	POST	CLEAN
http://www.wilbertluna.com/xzes/?fPvdTfP=EU40BBWlyZv+CeoOh9wLC2Sy0USpPHzyDUV4UMwzyT54U54r+rzGbSA1EEvbYTQJ3TREQw==&XnjlvN=HFNDqh9Ho	-	208.91.197.91	-	GET	CLEAN
http://www.extrobility.com/xzes/?fPvdTfP=pd/4jJ6jLgoCWPH/GHUgj0FHbCU6+qKjd6PN15Ru4R6uBn9glEdMwokePvqp4Tct3DAb4g==&XnjlvN=HFNDqh9Ho	-	217.70.184.50	-	GET	CLEAN
http://www.wilbertluna.com/xzes/	-	208.91.197.91	-	POST	CLEAN
http://www.extrobility.com/xzes/	-	217.70.184.50	-	POST	CLEAN
http://www.eleonoritalia.com/xzes/?fPvdTfP=dGVhXmv/Ev2mORIQnUGskdehpcwp8r0HTFZZz+lSCj08k18P++8BxEjg4Ft4U9K2XKkX4A==&XnjlvN=HFNDqh9Ho	-	62.149.128.45	-	GET	CLEAN
http://www.cpcacursos.com/xzes/?fPvdTfP=61uYctvZwZ8Sp3djwTs/ePBNtPg20uoPiMbdeJbZ57IZPEYJt69INO3EZv26EwNfkImL2g==&XnjlvN=HFNDqh9Ho	-	162.241.61.34	-	GET	CLEAN
http://www.mindbodyweightlossmethod.com/xzes/?fPvdTfP=RvIcq+i7q7kRIhcCci6HzJn3Vgbs8IkZ3qFCamrgyZPpaSwOznlYsQuJhKWwxSWF5imggw==&XnjlvN=HFNDqh9Ho	-	62.233.121.61	-	GET	CLEAN
http://www.dalainstitute.info/xzes/?fPvdTfP=CPfiPKWK5LZIIly0Y09a8SHSPP5QoGiXgTF+OOq8iYZD4WpEFq03gqLRDF/iG1nWVv660g==&XnjlvN=HFNDqh9Ho	-	51.77.52.109	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.mylyk.net/xzes/?fPvdTfP=lZAWFjxlzIo8AvKzM9v0DCjfM8h6xX/Vie0BER185F7DTJN7Gb1m96i9Ww364gmXpwvyaA==&Mx=WIpl	-	104.21.94.157	-	GET	CLEAN
http://www.eleonoritalia.com/xzes/	-	62.149.128.45	-	POST	CLEAN
http://www.eleonoritalia.com/xzes/?fPvdTfP=dGVhXmv/Ev2mORIQnUGskdehpcwp8r0HTFZZz+ISCj08k18P++8BxEjg4Ft4U9K2XKkX4A==&Mx=WIpl	-	62.149.128.45	-	GET	CLEAN
http://www.extrobility.com/xzes/?fPvdTfP=pd/4jJ6jLgoCWPH/GHUgj0FHbCU6+qKjd6PN15Ru4R6uBn9glEdMwokePvqp4Tct3DAb4g==&Mx=WIpl	-	217.70.184.50	-	GET	CLEAN
http://www.overway.store/xzes/?fPvdTfP=NeIJDzsWSz5EVZYy3pWwuAqYTUkdDte6huV8TkEY+SvYHK9zRcBYxeVFWYdVVt/jrxsjsA==&Mx=WIpl	-	154.16.245.157	-	GET	CLEAN
http://www.cpcacursos.com/xzes/	-	162.241.61.34	-	POST	CLEAN
http://www.mindbodyweightlossmethod.com/xzes/	-	62.233.121.61	-	POST	CLEAN
http://www.dalainstitute.info/xzes/	-	51.77.52.109	-	POST	CLEAN
http://www.joannhydeyoga.com/xzes/	-	66.235.200.145	-	POST	CLEAN
http://www.7looks-mocha-totalbeauty.com/xzes/?fPvdTfP=N6kvuAXHq1eVHQ2e8nDxm1bATb9xJ8kGsA5u90v+9KhKcWZ9JLFx/zAPmWa4/jqVMzkOHg==&Mx=WIpl	-	183.90.231.50	-	GET	CLEAN
http://www.distressedthenblessed.com/xzes/?fPvdTfP=qta2XgLpJD0UJeOmnNNCsYOZQAr8lLiHkRXUM4hponnLum3Sko0HNCnlcBOpo2T9WKQqHA==&Mx=WIpl	-	162.241.218.205	-	GET	CLEAN
http://www.joannhydeyoga.com/xzes/?fPvdTfP=M74vbXdatV6xDvL6/loAkrjESC9Z5XZA/+6NQlBWeUhuvtB2es1cFv1IRip/2lkUNu1/CA==&XnjlvN=HFNDqh9Ho	-	66.235.200.145	-	GET	CLEAN
http://www.theravewizards.com/xzes/	-	198.54.117.216	-	POST	CLEAN
http://www.theravewizards.com/xzes/?fPvdTfP=hsby6OJ/fd6ThLUdZbSyJdZ7YeDc2lcIgsMuottqV+UF+OnCYZb0G45wB+nhiN/ricwxiA==&XnjlvN=HFNDqh9Ho	-	198.54.117.216	-	GET	CLEAN
http://www.overway.store/xzes/	-	154.16.245.157	-	POST	CLEAN
http://www.printyourdays.com/xzes/?fPvdTfP=WvVdSYbKp96wH048bjEVjLioWRcomDeCwGP5DsGxMK4Q1oFCkmDEchfPL+qbhMw+Vvr/6w==&if8=7nz42h_PfxRhtde	-	104.21.48.190	-	GET	CLEAN
http://www.7looks-mocha-totalbeauty.com/xzes/	-	183.90.231.50	-	POST	CLEAN
http://www.venkataramanagraphics.com/xzes/?fPvdTfP=zQCXJP8LggsZoUmXHFz9GWvVffBXhlgfEpXjhYl/bV5XFEUeHH6MpZREokIqHen0Y7wkVg==&if8=7nz42h_PfxRhtde	-	72.167.127.85	-	GET	CLEAN
http://www.mindbodyweightlossmethod.com/xzes/?fPvdTfP=Rvlcq+i7q7kRIhcCci6HzJn3Vgbs8lkZ3qFCamrgyZPpaSwOznlYsQuJhKWwxSWF5imggw==&if8=7nz42h_PfxRhtde	-	62.233.121.61	-	GET	CLEAN
http://www.mylyk.net/xzes/?fPvdTfP=lZAWFjxlzIo8AvKzM9v0DCjfM8h6xX/Vie0BER185F7DTJN7Gb1m96i9Ww364gmXpwvyaA==&if8=7nz42h_PfxRhtde	-	104.21.94.157	-	GET	CLEAN
http://www.venkataramanagraphics.com/xzes/	-	72.167.127.85	-	POST	CLEAN
http://www.skindefense5.com/xzes/?fPvdTfP=nzYmw7PgvXl3RVxY+22S0s66JIboZ9taw8WhBbJqqOeAmHf1Jq6dfLQuQN0DXxF4yypuTw==&s2=wZxpTbThw4ppsl	-	64.190.62.111	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://www.eleonoritalia.com/xzes/?s2=wZxpTbThw4ppsl&fPvdTfP=dGVhXmv/Ev2mORIQnUGskdehpcwp8r0HTFZZz+lSCj08k18P++8BxEjg4Ft4U9K2XKkX4A==	-	62.149.128.45	-	GET	CLEAN
http://www.healthybalancedliving.com/xzes/?fPvdTfP=Orxi7BqtkIQQhmFsXk66PD0SSSSqk86WkGR6LUZk9NXV5D1XaC2g8Hl8xZwfwmZ8pB0v8Q==&s2=wZxpTbThw4ppsl	-	3.130.253.23	-	GET	CLEAN
http://www.punkidz.com/xzes/?s2=wZxpTbThw4ppsl&fPvdTfP=rzqcJvicjlO1REHeJYC8xd++pVURv744ENDtGRRvNKzpNTaKu7eGHsB4p2bzaao8N19v3g==	-	156.234.182.39	-	GET	CLEAN
http://www.skindefense5.com/xzes/	-	64.190.62.111	-	POST	CLEAN
http://www.healthybalancedliving.com/xzes/	-	3.130.253.23	-	POST	CLEAN
http://www.punkidz.com/xzes/	-	156.234.182.39	-	POST	CLEAN
http://www.dashmints.com/xzes/?fPvdTfP=WU+vhYw1FCGUzoOC9mxW//+lNZAAC3fdNAegkUfjRfNchOBBzc+toiSaox38c5d0R6zVvA==&XnjlvN=HFNDqh9Ho	-	162.0.231.244	-	GET	CLEAN
http://www.lochnas.com/xzes/	-	192.64.119.254	-	POST	CLEAN
http://www.lochnas.com/xzes/?fPvdTfP=stwJlOwy5CWIDHGfLETpAqRwwrDBzTynArbgdcfDkklacgwwr2U0EHUYz568MSnJkjbUVw==&s2=wZxpTbThw4ppsl	-	192.64.119.254	-	GET	CLEAN
http://www.dashmints.com/xzes/	-	162.0.231.244	-	POST	CLEAN
http://www.skindefense5.com/xzes/?fPvdTfP=nzYmw7PgvXl3RVxY+22S0s66JIboZ9taw8WhBbJqqOeAmHf1Jq6dfLQuQN0DXxF4yypuTw==&zR-TJ=8phDMLKxmnQDtp60	-	64.190.62.111	-	GET	CLEAN
http://www.mylyk.net/xzes/	-	104.21.94.157	-	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.elsist.online	-	-	DNS	MALICIOUS
www.distressedthenblessed.com	162.241.218.205	-	DNS, HTTP	CLEAN
distressedthenblessed.com	162.241.218.205	-	DNS, HTTP	CLEAN
www.cannabeeswax.com	199.34.228.171	-	DNS, HTTP	CLEAN
cannabeeswax.com	199.34.228.171	-	DNS, HTTP	CLEAN
www.muintel.net	75.2.85.42, 99.83.196.71	-	DNS, HTTP	CLEAN
muintel.net	75.2.85.42, 99.83.196.71	-	DNS, HTTP	CLEAN
www.update-mind.com	-	-	DNS	CLEAN
update-mind.com	-	-	DNS	CLEAN
www.wilbertluna.com	208.91.197.91	-	DNS, HTTP	CLEAN
www.extrobility.com	217.70.184.50	-	DNS, HTTP	CLEAN
webredir.vip.gandi.net	217.70.184.50	-	DNS	CLEAN
www.communication.services	-	-	DNS	CLEAN
www.eleonoritalia.com	62.149.128.45	-	DNS, HTTP	CLEAN
eleonoritalia.com	62.149.128.45	-	DNS, HTTP	CLEAN
www.cpcacursos.com	162.241.61.34	-	DNS, HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
cpcacursos.com	162.241.61.34	-	DNS, HTTP	CLEAN
www.mindbodyweightlossmethod.com	62.233.121.61	-	DNS, HTTP	CLEAN
www.dalainstitute.info	51.77.52.109	-	DNS, HTTP	CLEAN
dalainstitute.info	51.77.52.109	-	DNS, HTTP	CLEAN
www.joannhydeyoga.com	66.235.200.145	-	DNS, HTTP	CLEAN
joannhydeyoga.com	66.235.200.145	-	DNS, HTTP	CLEAN
www.theravewizards.com	198.54.117.217, 198.54.117.216, 198.54.117.215, 198.54.117.211, 198.54.117.212, 198.54.117.210, 198.54.117.218	-	DNS, HTTP	CLEAN
parkingpage.namecheap.com	198.54.117.217, 198.54.117.216, 198.54.117.215, 198.54.117.211, 198.54.117.212, 198.54.117.210, 198.54.117.218	-	DNS	CLEAN
www.metaverse-coaching.com	121.254.178.252	-	DNS, HTTP	CLEAN
www.mylyk.net	172.67.137.204, 104.21.94.157	-	DNS, HTTP	CLEAN
www.overway.store	154.16.245.157	-	DNS, HTTP	CLEAN
overway.store	154.16.245.157	-	DNS, HTTP	CLEAN
www.7looks-mocha-totalbeauty.com	183.90.231.50	-	DNS, HTTP	CLEAN
www.publiccoins.online	-	-	DNS	CLEAN
www.printyourdays.com	104.21.48.190, 172.67.156.13	-	DNS, HTTP	CLEAN
www.knowsyourdream.com	-	-	DNS	CLEAN
www.venkataramanagraphics.com	72.167.127.85	-	DNS, HTTP	CLEAN
venkataramanagraphics.com	72.167.127.85	-	DNS, HTTP	CLEAN
www.monenee.xyz	-	-	DNS	CLEAN
www.beandhira.com	-	-	DNS	CLEAN
www.skindefense5.com	64.190.62.111	-	DNS, HTTP	CLEAN
www.healthybalancedliving.com	3.130.204.160, 3.130.253.23	-	DNS, HTTP	CLEAN
traff-2.hugedomains.com	3.130.204.160, 3.130.253.23	-	DNS	CLEAN
hdr-nlb5-4e815dd67a14bf7f.elb.us-east-2.amazonaws.com	3.130.204.160, 3.130.253.23	-	DNS	CLEAN
www.punkidz.com	156.234.182.39	-	DNS, HTTP	CLEAN
www.lochnas.com	192.64.119.254	-	DNS, HTTP	CLEAN
www.senerants.tech	-	-	DNS	CLEAN
www.dashmints.com	162.0.231.244	-	DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
162.241.218.205	www.distressedthenblessed.com, distressedthenblessed.com	United States	TCP, DNS, HTTP	CLEAN
199.34.228.171	www.cannabeeswax.com, cannabeeswax.com	United States	TCP, DNS, HTTP	CLEAN
75.2.85.42	www.muintel.net, muintel.net	United States	TCP, DNS, HTTP	CLEAN

IP Address	Domains	Country	Protocols	Verdict
208.91.197.91	www.wilbertluna.com	Virgin Islands	TCP, DNS, HTTP	CLEAN
217.70.184.50	webredir.vip.gandi.net, www.extrobility.com	France	TCP, DNS, HTTP	CLEAN
62.149.128.45	eleonoritalia.com, www.eleonoritalia.com	Italy	TCP, DNS, HTTP	CLEAN
162.241.61.34	www.cpcacursos.com, cpcacursos.com	United States	TCP, DNS, HTTP	CLEAN
62.233.121.61	www.mindbodyweightlossmethod.com	United Kingdom	TCP, DNS, HTTP	CLEAN
51.77.52.109	dalainstitute.info, www.dalainstitute.info	Poland	TCP, DNS, HTTP	CLEAN
66.235.200.145	www.joannhydeyoga.com, joannhydeyoga.com	United States	TCP, DNS, HTTP	CLEAN
198.54.117.216	parkingpage.namecheap.com, www.theravewizards.com	United States	TCP, DNS, HTTP	CLEAN
121.254.178.252	www.metaverse-coaching.com	S. Korea	TCP, DNS, HTTP	CLEAN
104.21.94.157	www.mylyk.net	-	TCP, DNS, HTTP	CLEAN
154.16.245.157	www.overway.store, overway.store	United States	TCP, DNS, HTTP	CLEAN
183.90.231.50	www.7looks-mocha-totalbeauty.com	Japan	TCP, DNS, HTTP	CLEAN
104.21.48.190	www.printyourdays.com	-	TCP, DNS, HTTP	CLEAN
72.167.127.85	venkataramanagraphics.com, www.venkataramanagraphics.com	United States	TCP, DNS, HTTP	CLEAN
64.190.62.111	www.skindefense5.com	Germany	TCP, DNS, HTTP	CLEAN
3.130.253.23	hdr-nlb5-4e815dd67a14bf7f.elb.us-east-2.amazonaws.com, www.healthybalancedliving.com, traff-2.hugedomains.com	United States	TCP, DNS, HTTP	CLEAN
156.234.182.39	www.punkidz.com	Hong Kong	TCP, DNS, HTTP	CLEAN
192.64.119.254	www.lochnas.com	United States	TCP, DNS, HTTP	CLEAN
162.0.231.244	www.dashmints.com	United States	TCP, DNS, HTTP	CLEAN
99.83.196.71	www.muintel.net, muintel.net	United States	DNS	CLEAN
198.54.117.211	parkingpage.namecheap.com, www.theravewizards.com	United States	DNS	CLEAN
198.54.117.212	parkingpage.namecheap.com, www.theravewizards.com	United States	DNS	CLEAN
198.54.117.217	parkingpage.namecheap.com, www.theravewizards.com	United States	DNS	CLEAN
198.54.117.210	parkingpage.namecheap.com, www.theravewizards.com	United States	DNS	CLEAN
198.54.117.218	parkingpage.namecheap.com, www.theravewizards.com	United States	DNS	CLEAN
198.54.117.215	parkingpage.namecheap.com, www.theravewizards.com	United States	DNS	CLEAN
172.67.137.204	www.mylyk.net	United States	DNS	CLEAN
172.67.156.13	www.printyourdays.com	United States	DNS	CLEAN
3.130.204.160	hdr-nlb5-4e815dd67a14bf7f.elb.us-east-2.amazonaws.com, www.healthybalancedliving.com, traff-2.hugedomains.com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
0M1P2-24V-8B9WJ_	access	gikaopzb.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
9PNO-9-W2-I5-33E	access	rundll32.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows	access	java.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\GDIProcessHandleQuota	access, read	java.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access, create	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\FZEPZLE	access, write	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\15.0\Outlook\Profiles\Outlook\	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access, create	rundll32.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\9375CFF0413111d3B88A00104B2A6676\00000003	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook_2016\	access, create	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661-3990802383-1811730007-1000\SOFTWARE\Microsoft\Internet Explorer\IntelliForms\Storage2	access, create	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\	access, create	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion	access, read	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\39.0 (x86 en-US)\Main	access, create	rundll32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\39.0 (x86 en-US)\Main\Install Directory	access, read	rundll32.exe	CLEAN
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	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\	access, create	rundll32.exe	CLEAN

Process

Process Name	Commandline	Verdict
gikaopzb.exe	C:\Users\RDhJ0CNFevzX\gIkAOpZB.exe	MALICIOUS
gikaopzb.exe	"C:\Users\RDhJ0CNFevzX\gIkAOpZB.exe"	MALICIOUS
hl-ili.exe	"C:\Program Files (x86)\Xmpxd9\hl-ili.exe"	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
rundll32.exe	"C:\Windows\SysWOW64\rundll32.exe"	SUSPICIOUS
cmd.exe	/c copy "C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\RDHJ0C~1\AppData\Local\Temp\DB1" /V	SUSPICIOUS
java.exe	"C:\Program Files\Java\jre1.8.0_171\bin\java.exe" -jar "C:\Users\RDHJ0C~1\Desktop\sample.jar"	CLEAN
notepad.exe	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\RDhJ0CNFevzX\m2rKEl2wJZ.txt	CLEAN
cmd.exe	/c del "C:\Users\RDhJ0CNFevzX\gIkAOpZB.exe"	CLEAN

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	XBinder	Packer used to distribute malware	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\sample.jar	-	5/5
Malware	XLoader_Win32	XLoader Win32	Dropped File	-	Spyware	5/5
Malware	XLoader_Win32	XLoader Win32	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_desktop
Description	win10_64_th2_en_desktop
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	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.1.0 / 2022-01-14 04:00:58
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

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	72.0.3626.81
Firefox Version	39.0
Flash Version	28.0.0.137
Java Version	8.0.1710.11

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