MALICIOUS

Classifications: Backdoor | Keylogger

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**cagrt.exe**
ID	#10314621
MD5	60160e5c59102cdfd7506d7d106fc029
SHA1	d44460fe999e4838fd507b0abba3f12ed599d4bd
SHA256	0f0f8f3babd10779dac4805595ef2141ad4dee809a140c3262c2cb729149ceb2
File Size	3172.00 KB
Report Created	2024-04-27 09:44 (UTC)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (22 rules, 184 matches)

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Bypasses Windows User Account Control (UAC)	4	-
	• (Process #1) cagrt.exe disables UAC dialog via registry. • (Process #1) cagrt.exe tries to disable UAC prompt for local administrators. • (Process #4) wjhuwcp.exe tries to disable UAC prompt for local administrators. • (Process #5) wjhuwcp.exe tries to disable UAC prompt for local administrators.			
4/5	System Modification	Disables a crucial system tool	1	-
	• (Process #1) cagrt.exe disables the Registry Editor via registry.			
4/5	Defense Evasion	Tries to disable antivirus software	1	-
	• (Process #4) wjhuwcp.exe stops a service related to Windows Defender via ControlService (API).			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	System Modification	Disables a crucial system service	5	-
	• (Process #4) wjhuwcp.exe stops Windows Firewall service by ControlService API. • (Process #4) wjhuwcp.exe stops Windows Security Center service by ControlService API. • (Process #4) wjhuwcp.exe stops Internet Connection Sharing service by ControlService API. • (Process #4) wjhuwcp.exe stops Windows Update service by ControlService API. • (Process #4) wjhuwcp.exe disables Windows Update service by ChangeServiceConfigA API.			
2/5	Hide Tracks	Hides files	12	-
	• (Process #4) wjhuwcp.exe hides the file "C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Users\OqXZRaykm\AppData\Local\irlusudcijqrearuzovqqztca.lkq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Windows\irlusudcijqrearuzovqqztca.lkq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Users\OQXZRA~1\AppData\Local\Temp\irlusudcijqrearuzovqqztca.lkq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "irlusudcijqrearuzovqqztca.lkq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Windows\system32\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Program Files (x86)\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Users\OqXZRaykm\AppData\Local\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Windows\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "C:\Users\OQXZRA~1\AppData\Local\Temp\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" by setting its "hidden" attribute. • (Process #4) wjhuwcp.exe hides the file "nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" by setting its "hidden" attribute.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #4) wjhuwcp.exe has a thread which sleeps more than 5 minutes.			
2/5	Network Connection	Sets up server that accepts incoming connections	1	Backdoor
	• (Process #4) wjhuwcp.exe starts a TCP server listening on port 23558.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-

Score	Category	Operation	Count	Classification
	• Tries to detect VirtualPC via vpcext instruction at "0xb073f0f".			
1/5	Mutex	Creates mutex	3	-
	• (Process #1) cagrt.exe creates mutex with name "ilzcuqtmmhidkalihqrgadr". • (Process #4) wjhuwcp.exe creates mutex with name "yzlmcwxomfexcqzuryxkc". • (Process #5) wjhuwcp.exe creates mutex with name "pregxsumlffzfueayggunp".			
1/5	Persistence	Installs system startup script or application	61	-

- (Process #1) cagrt.exe adds "Explorer.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "wvfeskjyulizcovojol.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "wvfeskjyulizcovojol.exe ." to Windows startup via registry.
- (Process #1) cagrt.exe adds "czheqgdqkzujkuzqj.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "vryufuqcvjdrraeu.exe ." to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\yzlmcwxomfexcqzuryxkc.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\yzlmcwxomfexcqzuryxkc.exe ." to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\wvfeskjyulizcovojol.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\jjuujccsphfxbowqmsqc.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\vryufuqcvjdrraeu.exe ." to Windows startup via registry.
- (Process #1) cagrt.exe adds "yzlmcwxomfexcqzuryxkc.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "jjuujccsphfxbowqmsqc.exe ." to Windows startup via registry.
- (Process #1) cagrt.exe adds "vryufuqcvjdrraeu.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\ljsqdusgbrndfqwoim.exe ." to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\ljsqdusgbrndfqwoim.exe" to Windows startup via registry.
- (Process #1) cagrt.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\vryufuqcvjdrraeu.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "Explorer.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "Explorer.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "czheqgdqkzujkuzqj.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "vryufuqcvjdrraeu.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "wvfeskjyulizcovojol.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "ljsqdusgbrndfqwoim.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "yzlmcwxomfexcqzuryxkc.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "czheqgdqkzujkuzqj.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "ljsqdusgbrndfqwoim.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "ljsqdusgbrndfqwoim.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "yzlmcwxomfexcqzuryxkc.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\vryufuqcvjdrraeu.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\yzlmcwxomfexcqzuryxkc.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\vryufuqcvjdrraeu.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\ljsqdusgbrndfqwoim.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\wvfeskjyulizcovojol.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\wvfeskjyulizcovojol.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\czheqgdqkzujkuzqj.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\yzlmcwxomfexcqzuryxkc.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\czheqgdqkzujkuzqj.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "vryufuqcvjdrraeu.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "vryufuqcvjdrraeu.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "jjuujccsphfxbowqmsqc.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "ljsqdusgbrndfqwoim.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "jjuujccsphfxbowqmsqc.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\wvfeskjyulizcovojol.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\czheqgdqkzujkuzqj.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\yzlmcwxomfexcqzuryxkc.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\ljsqdusgbrndfqwoim.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "wvfeskjyulizcovojol.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "wvfeskjyulizcovojol.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "wvfeskjyulizcovojol.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "czheqgdqkzujkuzqj.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\jjuujccsphfxbowqmsqc.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\jjuujccsphfxbowqmsqc.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\vryufuqcvjdrraeu.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "jjuujccsphfxbowqmsqc.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "yzlmcwxomfexcqzuryxkc.exe ." to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\jjuujccsphfxbowqmsqc.exe" to Windows startup via registry.
- (Process #4) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\ljsqdusgbrndfqwoim.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\vryufuqcvjdrraeu.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "yzlmcwxomfexcqzuryxkc.exe" to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\wvfeskjyulizcovojol.exe ." to Windows startup via registry.
- (Process #5) wjhuwcp.exe adds "C:\Users\OQXZRA~1\AppData\Local\Temp\jjuujccsphfxbowqmsqc.exe" to Windows startup via registry.

Score	Category	Operation	Count	Classification
1/5	System Modification	Modifies operating system directory	6	-
	• (Process #4) wjhuwcp.exe creates file "C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq" in the OS directory. • (Process #4) wjhuwcp.exe creates file "C:\Windows\irlusudcijqrearuzovqqztca.lkq" in the OS directory. • (Process #4) wjhuwcp.exe creates file "C:\Windows\system32\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" in the OS directory. • (Process #4) wjhuwcp.exe creates file "C:\Windows\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq" in the OS directory. • (Process #4) wjhuwcp.exe modifies file "C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq" in the OS directory. • (Process #4) wjhuwcp.exe modifies file "C:\Windows\irlusudcijqrearuzovqqztca.lkq" in the OS directory.		
1/5	System Modification	Modifies application directory	2	-
	• (Process #4) wjhuwcp.exe modifies "C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq". • (Process #4) wjhuwcp.exe modifies "C:\Program Files (x86)\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq".		
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #4) wjhuwcp.exe enables process privilege "SeDebugPrivilege".		
1/5	Discovery	Enumerates running processes	1	-
	• (Process #4) wjhuwcp.exe enumerates running processes.		
1/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #4) wjhuwcp.exe frequently reads the state of a keyboard key by API.		
1/5	Network Connection	Performs DNS request	67	-

- (Process #4) wjhuwcp.exe fails to resolve hostname "ovuvuioxnd.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "zpkyqy.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "ngaktnaw.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "bebshzesxvh.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "wkouaxsl.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "amdwrt.net"
- (Process #4) wjhuwcp.exe resolves hostname "www.whatismyip.com" to IP "104.27.207.92".
- (Process #4) wjhuwcp.exe fails to resolve hostname "qmkuidndfwv.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "wmiosyoyoa.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "jlcfzvgtso.info"
- (Process #4) wjhuwcp.exe resolves hostname "www.baidu.com" to IP "103.235.46.40".
- (Process #4) wjhuwcp.exe resolves hostname "www.showmyipaddress.com" to IP "188.114.96.3".
- (Process #4) wjhuwcp.exe fails to resolve hostname "bqcanilwnuj.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "nqnnvzbygeb.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "uwidfnhb.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "www.whatismyip.ca"
- (Process #4) wjhuwcp.exe fails to resolve hostname "tikydyz.net"
- (Process #4) wjhuwcp.exe resolves hostname "www.wikipedia.org" to IP "185.15.59.224".
- (Process #4) wjhuwcp.exe fails to resolve hostname "qatqtsqesmd.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "eymwsewwok.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "vabpled.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "jbbfbnlpzo.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "dkitrpodbn.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "whatismyip.everdot.org"
- (Process #4) wjhuwcp.exe fails to resolve hostname "ttfbgn.net"
- (Process #4) wjhuwcp.exe resolves hostname "iwuwem.org" to IP "162.249.65.164".
- (Process #4) wjhuwcp.exe fails to resolve hostname "gumcwcyskm.org"
- (Process #4) wjhuwcp.exe resolves hostname "www.youtube.com" to IP "142.250.191.142".
- (Process #4) wjhuwcp.exe fails to resolve hostname "yypaiqkwokz.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "zypdwsbniw.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "asykget.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "lozylvzsn.org"
- (Process #4) wjhuwcp.exe fails to resolve hostname "ggybyqnvrq.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "eqoiqe.org"
- (Process #4) wjhuwcp.exe fails to resolve hostname "yejspkr.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "exzihifb.info"
- (Process #4) wjhuwcp.exe resolves hostname "whatismyipaddress.com" to IP "104.19.223.79".
- (Process #4) wjhuwcp.exe fails to resolve hostname "bicsnsjoe.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "cfjvdxggxy.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "bwdyfxd.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "kmhcfkjhs.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "wozqja.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "jqdsgajcjyv.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "lynojqbnm.org"
- (Process #4) wjhuwcp.exe fails to resolve hostname "pmnbndfev.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "faysxbmq.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "yaeqsu.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "pmpcryg.org"
- (Process #4) wjhuwcp.exe fails to resolve hostname "bwzemcsali.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "iqpqduz.info"
- (Process #4) wjhuwcp.exe resolves hostname "www.showmyipaddress.com" to IP "104.21.74.56".
- (Process #4) wjhuwcp.exe fails to resolve hostname "rlszzbk.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "bqduqyvvo.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "kquceeau.com"
- (Process #4) wjhuwcp.exe fails to resolve hostname "llcuscfm.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "dzfiafodymkx.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "wwjmyst.info"
- (Process #4) wjhuwcp.exe fails to resolve hostname "nxbmxjdftdbe.net"
- (Process #4) wjhuwcp.exe fails to resolve hostname "ludmhagmqrb.org"
- (Process #4) wjhuwcp.exe fails to resolve hostname "yemboiwya.info"

Score	Category	Operation	Count	Classification
1/5	Network Connection	Connects to remote host	8	-

- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "188.114.96.3:80".
- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "104.19.223.79:80".
- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "104.27.207.92:80".
- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "104.21.74.56:80".
- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "103.235.46.40:80".
- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "185.15.59.224:80".
- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "162.249.65.164:80".
- (Process #4) wjhuwcp.exe opens an outgoing TCP connection to host "142.250.191.142:80".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Obfuscates control flow	1	-

- Modifies exception handler (e.g., the instruction pointer is modified within an exception handler filter).

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	3	-

- (Process #1) cagrt.exe resolves 139 API functions by name.
- (Process #4) wjhuwcp.exe resolves 139 API functions by name.
- (Process #5) wjhuwcp.exe resolves 139 API functions by name.

Score	Category	Operation	Count	Classification
1/5	Discovery	Checks external IP address	2	-

- (Process #4) wjhuwcp.exe checks external IP by asking IP info service at "http://whatismyipaddress.com".
- (Process #4) wjhuwcp.exe checks external IP by asking IP info service at "http://www.whatismyip.com".

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

- Executes dropped file "C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe".

Mitre ATT&CK Matrix

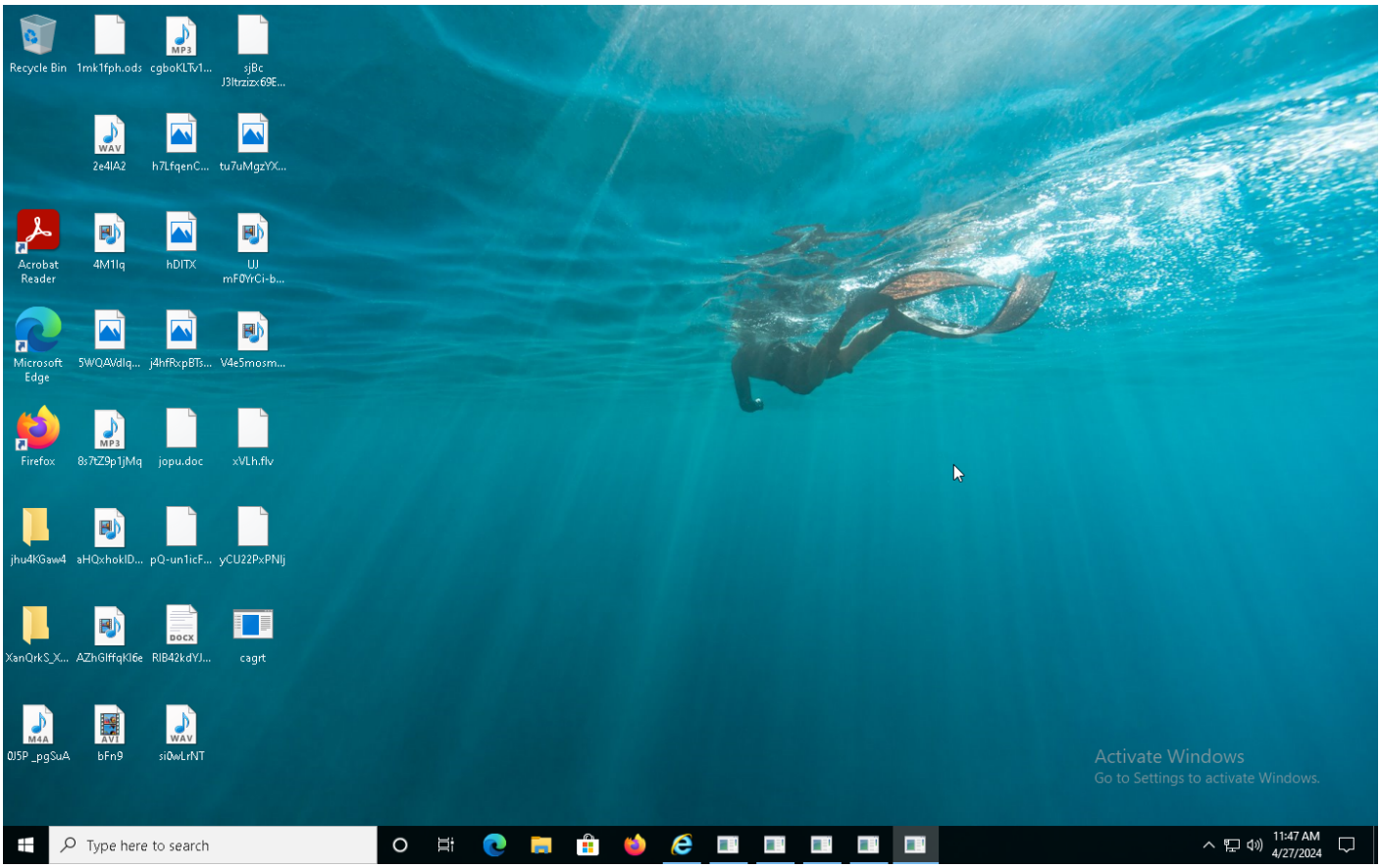
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder	#T1088 Bypass User Account Control	#T1112 Modify Registry	#T1056 Input Capture	#T1057 Process Discovery		#T1056 Input Capture			#T1489 Service Stop
		#T1158 Hidden Files and Directories		#T1088 Bypass User Account Control		#T1016 System Network Configuration Discovery					
				#T1158 Hidden Files and Directories		#T1497 Virtualization/ Sandbox Evasion					
				#T1089 Disabling Security Tools							
				#T1045 Software Packing							
				#T1027 Obfuscated Files or Information							
				#T1497 Virtualization/ Sandbox Evasion							

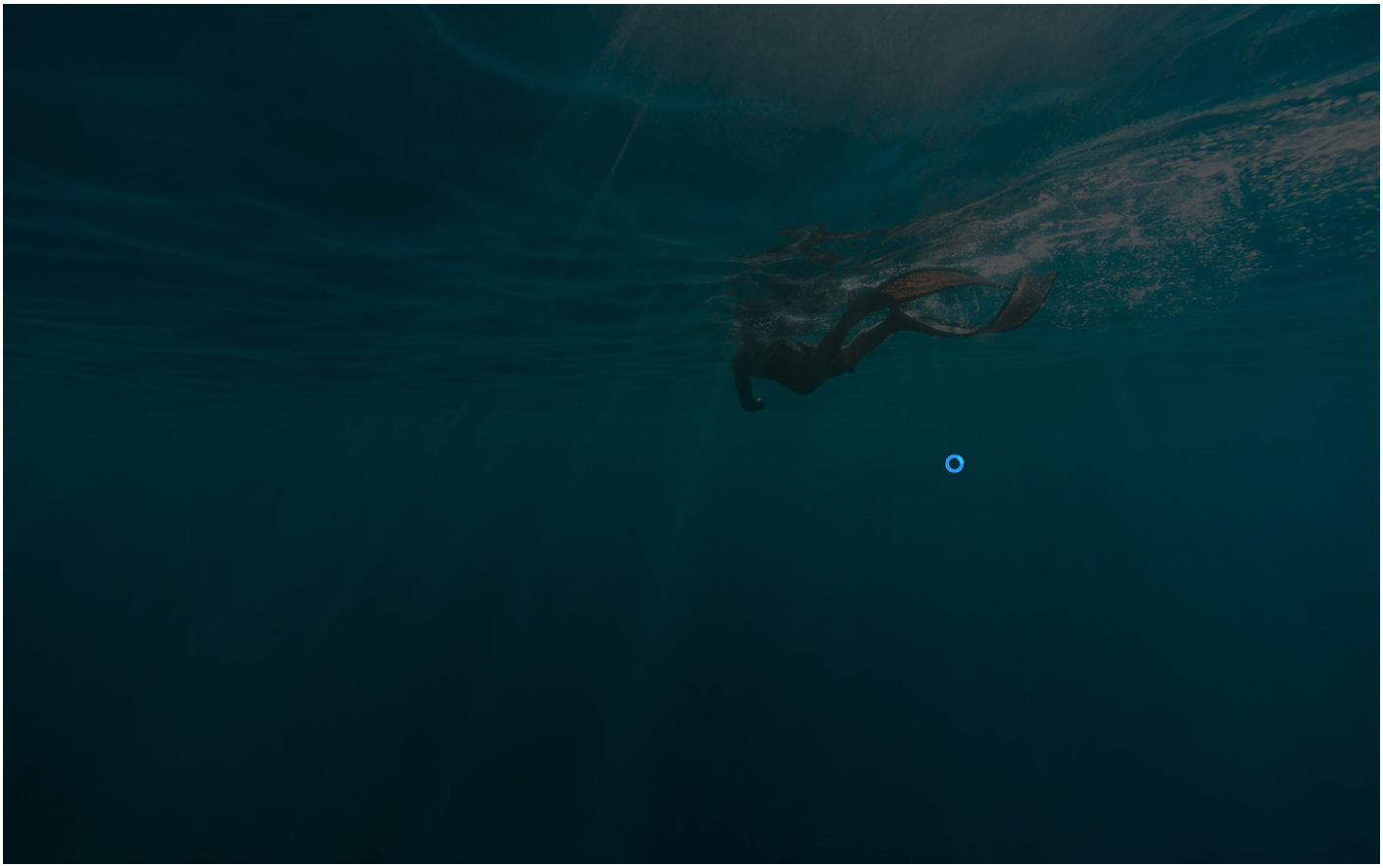
Sample Information

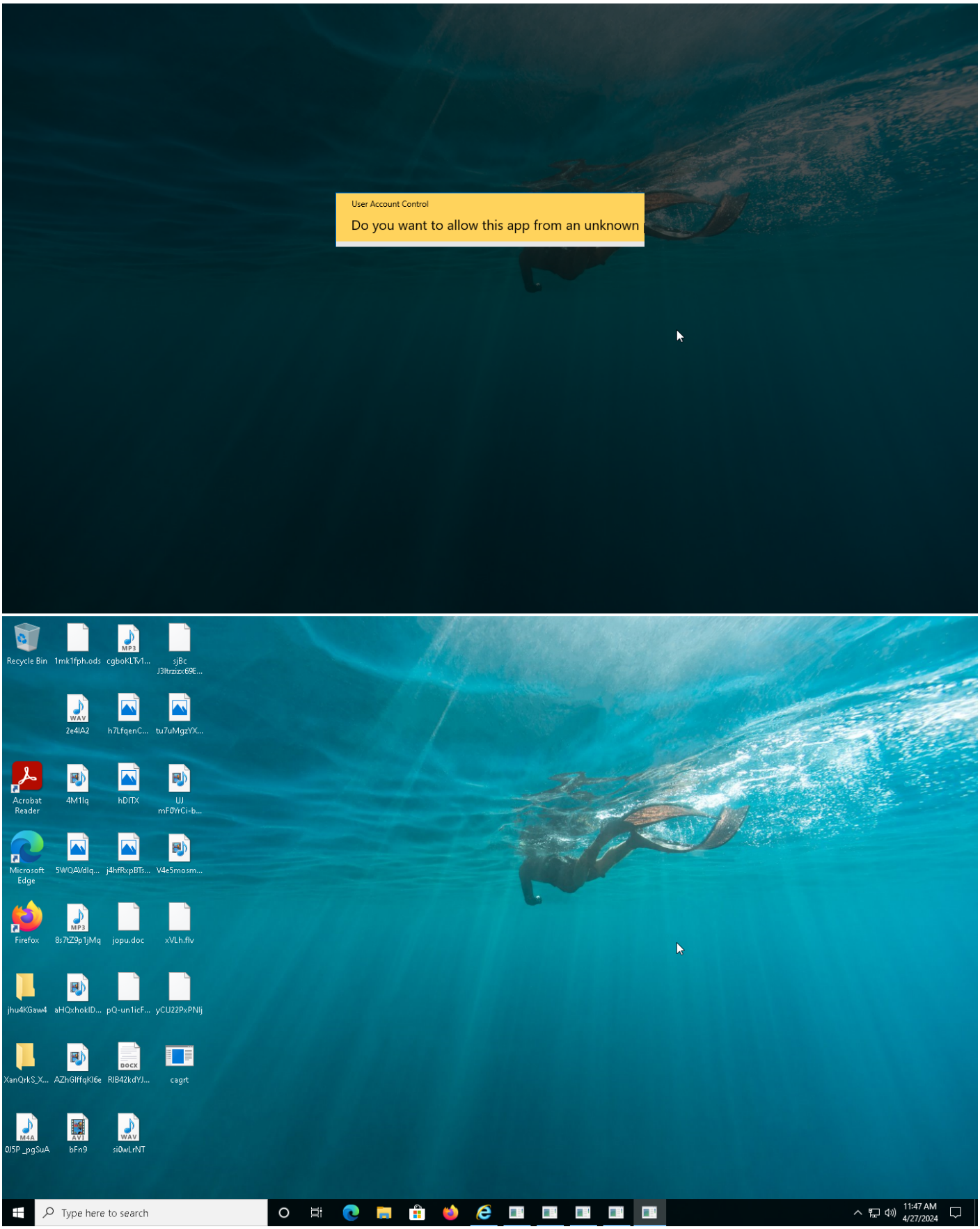
ID	#10314621
MD5	60160e5c59102cdfd7506d7d106fc029
SHA1	d44460fe999e4838fd507b0abba3f12ed599d4bd
SHA256	0f0f8f3babd10779dac4805595ef2141ad4dee809a140c3262c2cb729149ceb2
SSDeep	6144:33ue8ySm8hQAAIfFrRXuEE+0l97mKwKKqHVV/mx86JQPDHDdx/Qtqa:F/zkFF+EExZmKbKuV9IPJQPDHvd
ImpHash	d67c205451cfa889d29c6c8718886c08
File Name	cagrt.exe
File Size	3172.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-04-27 09:44 (UTC)
Analysis Duration	00:03:24
Termination Reason	Timeout
Number of Monitored Processes	3
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	0


Recycle Bin
1mk1fph.ods
cgboKLTv1...
sjBc
J3ltrzizx69E...
2e4lA2
h7LfqenC...
tu7uMgzYX...
Acrobat Reader
4M1lq
hDITX
UJ
mF0YrCi-b...
Microsoft Edge
5WQAVdlq...
j4hfRxpBTs...
V4e5mosm...
Firefox
8s7tZ9p1jMq
jopu.doc
xVLh.flv
jhu4KGaw4
aHQxhokID...
pQ-un1icF...
yCU22PxPNlj
XanQrkS_X...
AZhGlffqKl6e
RIB42kdYJ...
cagrt
0J5P _pgSuA
bFn9
si0wLrNT
Activate Windows
Go to Settings to activate Windows.
Type here to search
11:47 AM
4/27/2024





Screenshots truncated

NETWORK

General

12.82 KB total sent

404.53 KB total received

2 ports 80, 53

9 contacted IP addresses

51 URLs extracted

7 files downloaded

0 malicious hosts detected

DNS

82 DNS requests for 66 domains

1 nameservers contacted

72 total requests returned errors

HTTP/S

6 URLs contacted, 7 servers

18 sessions, 7.74 KB sent, 393.54 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://dss1[.]bdstatic[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://fanyi[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://pss[.]bdstatic[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://dss0[.]bdstatic[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://xueshu[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://news[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://ss1[.]bdstatic[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://image[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://e[.]baidu[.]com/ebaidu/home?refer=887	-	-	-	0 bytes	CLEAN
GET	hxxp://sp0[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://tieba[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://map[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://music[.]taihe[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://sp2[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://sp1[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com/img/flexible/logo/pc/result@2.png	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com/s?wd=%E7%99%BE%E5%BA%A6%E7%83%AD%E6%90%9C&sa=ire_dl_gh_logo_texing&rsv_dl=igh_logo_pcs	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://www[.]baidu[.]com/more/	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com/img/PCtm_d9c8750bed0b3c7d089fa7d55720d6cf.png	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com/img/PCfb_5bf082d29588c07f842ccde3f97243ea.png	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com/img/flexible/logo/pc/result.png	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com/img/flexible/logo/pc/peak-result.png	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com/baidu.html?from=noscript	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]showmyipaddress[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]whatismyip[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://whatismyipaddress[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]wikipedia[.]org	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]youtube[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://haokan[.]baidu[.]com/?sfrom=baidu-top	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newfanyi-da0cea8f7e.png	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newjiankang-f03b804b4b.png	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/yingxiaoicon-612169cc36.png	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newbaike-889054f349.png	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newzhibo-a6a0831ecd.png	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newzhidao-da1cf444b0.png	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newxueshuicon-a5314d5c83.png	-	-	-	0 bytes	CLEAN
GET	hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newyinyue-03ecd1e9b9.png	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]cloudflare[.]com/5xx-error-landing	-	-	-	0 bytes	CLEAN
GET	hxxps://baike[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://jiankang[.]baidu[.]com/widescreen/home	-	-	-	0 bytes	CLEAN
GET	hxxps://zhidao[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://passport[.]baidu[.]com/v2/?login&tpl=mn&u=http%3A%2F%2Fwww.baidu.com%2F&sms=5	-	-	-	0 bytes	CLEAN
GET	hxxps://top[.]baidu[.]com/board?platform=pc&sa=pcindex_entry	-	-	-	0 bytes	CLEAN
GET	hxxps://psstatic[.]cdn[.]bcebos[.]com/video/wiseindex/aa6eef91f8b5b1a33b454c401_1660835115000.png	-	-	-	0 bytes	CLEAN
GET	hxxps://wenku[.]baidu[.]com/?fr=bdpcindex	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]hao123[.]com/?src=from_pc	-	-	-	0 bytes	CLEAN
GET	hxxps://pan[.]baidu[.]com/?from=1026962h	-	-	-	0 bytes	CLEAN
GET	hxxps://sp1[.]baidu[.]com/5b1ZeDe5KgQFm2e88IuM_a/mwb2.gif	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://live[.]baidu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]baidu[.]com/s?wd=%E5%BC%80%E5%88%9B%E8%A5%BF%E9%83%A8%E5%A4%A7%E5%BC%80%E5%8F%91%E6%96%B0%E6%A0%BC%E5%B1%80&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]baidu[.]com/s?wd=6%E5%B2%81%E7%94%B7%E7%AB%A5%E9%A2%85%E9%AA%A8%E5%AF%84%E5%85%BB%E8%85%B9%E9%83%A81%E4%B8%AA%E5%8D%8A%E6%9C%88&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]baidu[.]com/s?wd=%E5%B9%BF%E5%B7%9E%E5%87%BA%E7%8E%B0%E9%BE%99%E5%8D%B7%E9%A3%8E&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]baidu[.]com/s?wd=%E5%8D%97%E6%98%8C%E7%81%AB%E7%81%BE%E8%87%B43%E6%AD%BB+%E5%A5%B3%E5%AD%90%E5%85%A8%E8%BA%AB%E7%86%... ...%E9%BB%91%E9%80%83%E7%94%9F&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]baidu[.]com/s?wd=%E3%80%8A%E5%A5%94%E8%B7%91%E5%90%A7%E3%80%8B%E7%BB%99%E8%89%BA%E4%BA%BAP%E5%AE%89%E5%85%A8%E5%B8%A6&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]baidu[.]com/s?wd=%E5%A4%AA%E7%A9%BA%E5%86%8D%E8%81%9A%E9%A6%96+%E9%97%AE%E5%A4%A9%E6%97%A0%E6%AD%A2%E5%A2%83&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]baidu[.]com/favicon.ico	-	-	-	0 bytes	CLEAN

DNS Requests

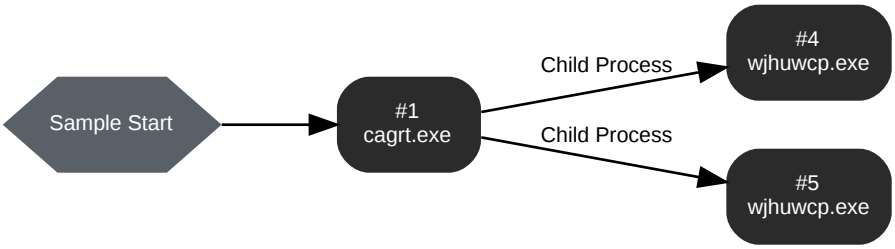
Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	ovuvuioxnd[.]info	NX_DOMAIN	-	-	CLEAN
A	zpkyqy[.]info	NX_DOMAIN	-	-	CLEAN
A	bebshzesxvh[.]net	NX_DOMAIN	-	-	CLEAN
A	ngaktnaw[.]info	NX_DOMAIN	-	-	CLEAN
A	wkouaxsl[.]info	NX_DOMAIN	-	-	CLEAN
A	amdwrt[.]net	NX_DOMAIN	-	-	CLEAN
A	www[.]whatismyip[.]com	NO_ERROR	104.27.207.92, 104.27.206.92	-	CLEAN
A	qmkuidndfwv[.]net	NX_DOMAIN	-	-	CLEAN
A	wmiosyoyoa[.]com	NX_DOMAIN	-	-	CLEAN
A	jlcfzvgtso[.]info	NX_DOMAIN	-	-	CLEAN
A	www[.]baidu[.]com, www[.]a[.]shifen[.]com, www[.]wshifen[.]com	NO_ERROR	103.235.46.40	www[.]a[.]shifen[.]com, www[.]wshifen[.]com	CLEAN
A	www[.]showmyipaddress[.]com	NO_ERROR	188.114.96.3, 188.114.97.3	-	CLEAN
A	bqcanilwnuj[.]com	NX_DOMAIN	-	-	CLEAN
A	nqnnvzbygeb[.]com	NX_DOMAIN	-	-	CLEAN

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	uwidfnhb[.]info	NX_DOMAIN	-	-	CLEAN
A	www[.]whatismyip[.]ca	NX_DOMAIN	-	-	CLEAN
A	tikydyz[.]net	NX_DOMAIN	-	-	CLEAN
A	www[.]wikipedia[.]org, dyna[.]wikimedia[.]org	NO_ERROR	185.15.59.224	dyna[.]wikimedia[.]org	CLEAN
A	qatqtsqesmd[.]net	NX_DOMAIN	-	-	CLEAN
A	eymwsewwok[.]com	NX_DOMAIN	-	-	CLEAN
A	vabpled[.]info	NX_DOMAIN	-	-	CLEAN
A	jbbfbnlpzo[.]net	NX_DOMAIN	-	-	CLEAN
A	rlszzbk[.]net	NX_DOMAIN	-	-	CLEAN
A	dkitrpodbn[.]net	NX_DOMAIN	-	-	CLEAN
A	whatismyip[.]everdot[.]org	NX_DOMAIN	-	-	CLEAN
A	ttfbgn[.]net	NX_DOMAIN	-	-	CLEAN
A	iwuwem[.]org	NO_ERROR	162.249.65.164	-	CLEAN
A	gumcwcyskm[.]org	NO_ERROR	-	-	CLEAN
A	www[.]youtube[.]com, youtube-ui[.]l[.]google[.]com	NO_ERROR	142.250.191.142, 142.250.191.174, 142.250.191.206, 142.250.191.238, 172.217.0.174, 172.217.1.110, 172.217.2.46, 172.217.4.78, 142.250.190.14, 142.250.190.46, 142.250.190.78, 142.250.190.110, 142.250.190.142, 142.250.191.110	youtube-ui[.]l[.]google[.]com	CLEAN
A	yypaiqkwokz[.]net	NX_DOMAIN	-	-	CLEAN
A	zypdwsbniw[.]net	NX_DOMAIN	-	-	CLEAN
A	kquceeau[.]com	NX_DOMAIN	-	-	CLEAN
A	asykget[.]net	NX_DOMAIN	-	-	CLEAN
A	lozylvzsn[.]org	NX_DOMAIN	-	-	CLEAN
A	ggybyqnvrq[.]info	NX_DOMAIN	-	-	CLEAN
A	eqoiqe[.]org	NX_DOMAIN	-	-	CLEAN
A	yejspkr[.]net	NX_DOMAIN	-	-	CLEAN
A	exzihifb[.]info	NX_DOMAIN	-	-	CLEAN
A	whatismyipaddress[.]com	NO_ERROR	104.19.223.79, 104.19.222.79	-	CLEAN
A	bicsnsjoe[.]info	NX_DOMAIN	-	-	CLEAN
A	cfjvdxggxy[.]info	NX_DOMAIN	-	-	CLEAN
A	bwdyfxd[.]net	NX_DOMAIN	-	-	CLEAN
A	kmhcfkjhs[.]net	NX_DOMAIN	-	-	CLEAN
A	wozqja[.]info	NX_DOMAIN	-	-	CLEAN
A	imakzxrvpl[.]info	NX_DOMAIN	-	-	CLEAN

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	jqdsgajcjyv[.]com	NX_DOMAIN	-	-	CLEAN
A	lynojqbnm[.]org	NX_DOMAIN	-	-	CLEAN
A	pmnbndfev[.]com	NX_DOMAIN	-	-	CLEAN
A	faysxbmq[.]info	NX_DOMAIN	-	-	CLEAN
A	yaeqsu[.]com	NX_DOMAIN	-	-	CLEAN
A	pmpcryg[.]org	NX_DOMAIN	-	-	CLEAN
A	bwzemcsali[.]info	NX_DOMAIN	-	-	CLEAN
A	iqpqduz[.]info	NX_DOMAIN	-	-	CLEAN
A	bqduqyvvo[.]info	NX_DOMAIN	-	-	CLEAN
A	llcuscfm[.]info	NX_DOMAIN	-	-	CLEAN
A	dzfiafodymkx[.]net	NX_DOMAIN	-	-	CLEAN
A	wwjmyst[.]info	NX_DOMAIN	-	-	CLEAN
A	nxbmxjdftdbe[.]net	NX_DOMAIN	-	-	CLEAN
A	ludmhagmqrb[.]org	NX_DOMAIN	-	-	CLEAN
A	oembvhyvje[.]info	NX_DOMAIN	-	-	CLEAN
A	oaguoiccuswc[.]com	NX_DOMAIN	-	-	CLEAN
A	yicwsqsq[.]com	NX_DOMAIN	-	-	CLEAN
A	bkvjdstb[.]info	NX_DOMAIN	-	-	CLEAN
A	nshqdmtabpw[.]net	NX_DOMAIN	-	-	CLEAN
A	bkpytkqvec[.]net	NX_DOMAIN	-	-	CLEAN
A	jgggrkswl[.]info	NX_DOMAIN	-	-	CLEAN

BEHAVIOR

Process Graph



Process #1: cagrt.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\cagrt.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\cagrt.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 218336, Reason: Analysis Target
Unmonitor End Time	End Time: 259218, Reason: Terminated
Monitor duration	40.88s
Return Code	0
PID	3140
Parent PID	-
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe	3172.00 KB	0f0f8f3babd10779dac4805595ef2141ad4dee809a140c3262c2cb729149ceb2	✖
C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe	4448.00 KB	3942ef3732b4fbb8282e015b7f1860fc524a4e33f3b3f6bcd5ed892116805a60	✖

Host Behavior

Type	Count
System	115
Module	158
File	54
Environment	1
Mutex	7
Registry	87
Process	3

Process #4: wjhuwcp.exe

ID	4
File Name	c:\users\oqxzraykm\appdata\local\temp\wjhuwcp.exe
Command Line	"C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe" "-"
Initial Working Directory	C:\Users\OQXZRA~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 245313, Reason: Child Process
Unmonitor End Time	End Time: 421452, Reason: Terminated by timeout
Monitor duration	176.14s
Return Code	Unknown
PID	5036
Parent PID	3140
Bitness	32 Bit

Dropped Files (6)

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq	272 bytes	6e517960f7acf2e91cb6742715e62ea4bd11c5fe0e0fb333aab2b39ce4e6ff07	✖
C:\Windows\system32\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq	3.99 KB	2d6312967c650a828e7d9286f8ef5573762419dbeefbca98ec79279f3f538c89	✖
C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq	272 bytes	1ef6c6138c50e5ed75a327b478e3f3325de9b612c762a0369137474c9ce511da	✖
C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq	272 bytes	0e7f6e0126fc3fdedc7046f184ea924d828524be871d60a9b8d861be29d9e847	✖
C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq	272 bytes	f94284e6ba48dffcd9d95c0675630048f34a0e70ee833509b3a278480f57647c	✖
C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq	272 bytes	e983f16a67f3c4f3e10028cb477fdb02d0768ee00d55cce1162104587a8b0ab8	✖

Host Behavior

Type	Count
System	1742
Module	159
File	372
Environment	1
Mutex	11
Registry	236
-	72
User	1
-	85
Process	4
Keyboard	7462

Network Behavior

Type	Count
HTTP	18
DNS	73

Type	Count
TCP	27

Process #5: wjhuwcp.exe

ID	5
File Name	c:\users\oqxzraykm\appdata\local\temp\wjhuwcp.exe
Command Line	"C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe" "-"
Initial Working Directory	C:\Users\OQXZRA~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 246073, Reason: Child Process
Unmonitor End Time	End Time: 421452, Reason: Terminated by timeout
Monitor duration	175.38s
Return Code	Unknown
PID	5232
Parent PID	3140
Bitness	32 Bit

Host Behavior

Type	Count
System	535
Module	157
File	40
Environment	1
Mutex	24
Registry	228
Process	7

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0f0f8f3babd10779dac4805595ef2141ad4dee809a140c3262c2cb729149ceb2	C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe, C:\Users\OqXZRaykm\Desktop\cagrt.exe	Dropped File	3172.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
3942ef3732b4fbb8282e015b7f1860fc524a4e33f3b3f6bcd5ed892116805a60	C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe	Dropped File	4448.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
446a6087825fa73eadb045e5a2e9e2adf7df241b571228187728191d961dda1f	-	Downloaded File	167 bytes	text/html	-	CLEAN
554eb24659837260c3c28a16f48eb667113fe665cee24dce288f982fe375b14e	-	Downloaded File	4.42 KB	text/html	-	CLEAN
74346794663292753090ea3611e0fc7afe1e7cea857aefa2515133d8a7651fc	-	Downloaded File	4.42 KB	text/html	-	CLEAN
4a4bed98893c9bf4bde2ad59f51ed85eb9590a6b2416b24b2e61d3eaae09732b	-	Downloaded File	4.42 KB	text/html	-	CLEAN
23f6e8febfc3692506d61e29ad765ccb5356a90aa227cfa9a0405c547fe27f29	-	Downloaded File	4.42 KB	text/html	-	CLEAN
7a3d46a11dc411965815a92d5f9ee9e91f7bcfb8a0271c213a5e289da9732ecb	-	Downloaded File	4.42 KB	text/html	-	CLEAN
fba44daf9492c5e066646cd3c17196efeae1e1c0698ab0a6d0bd80efec0e03b7	-	Downloaded File	331.18 KB	text/html	-	CLEAN
e983f16a67f3c4f3e10028cb477fdb02d0768ee00d55cce1162104587a8b0ab8	C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq, irlusudcijqrearuzovqqztca.lkq, C:\Users\OQXZRA~1\AppData\Local\Temp\irlusudc... ...a\Local\irlusudcijqrearuzovqqztca.lkq, C:\Windows\irlusudcijqrearuzovqqztca.lkq, C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq	Dropped File	272 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
2d6312967c650a828e7d9286f8ef5573762419dbeefbca98ec79279f3f538c89	C:\Windows\system32\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq, C:\Users\OqXZRaykm\AppData\Local\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmo... ...C:\Users\OQXZRA~1\AppData\Local\Temp\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq, C:\Windows\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq	Dropped File	3.99 KB	application/octet-stream	Access, Create, Write	CLEAN
f94284e6ba48dffcd9d95c0675630048f34a0e70ee833509b3a278480f57647c	C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq, irlusudcijqrearuzovqqztca.lkq, C:\Users\OQXZRA~1\AppData\Local\Temp\irlusudc... ...a\Local\irlusudcijqrearuzovqqztca.lkq, C:\Windows\irlusudcijqrearuzovqqztca.lkq, C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq	Dropped File	272 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
0e7f6e0126fc3fdedc7046f184ea924d828524be871d60a9b8d861be29d9e847	C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq, irlusudcijqrearuzovqqztca.lkq, C:\Users\OQXZRA~1\AppData\Local\Temp\irlusudc... ...a\Local\irlusudcijqrearuzovqqztca.lkq, C:\Windows\irlusudcijqrearuzovqqztca.lkq, C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq	Dropped File	272 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1ef6c6138c50e5ed75a327b478e3f3325de9b612c762a0369137474c9ce511da	C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq, irlusudcijqrearuzovqqztca.lkq, C:\Users\OQXZRA~1\AppData\Local\Temp\irlusudc... ...a\Local\irlusudcijqrearuzovqqztca.lkq, C:\Windows\irlusudcijqrearuzovqqztca.lkq, C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq	Dropped File	272 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
6e517960f7acf2e91cb6742715e62ea4bd11c5fe0e0fb333aab2b39ce4e6ff07	C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq, irlusudcijqrearuzovqqztca.lkq, C:\Users\OQXZRA~1\AppData\Local\Temp\irlusudc... ...a\Local\irlusudcijqrearuzovqqztca.lkq, C:\Windows\irlusudcijqrearuzovqqztca.lkq, C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq	Dropped File	272 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\cagrt.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
C:\Windows\system32\irlusudcijqrearuzovqqztca.lkq	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Program Files (x86)\irlusudcijqrearuzovqqztca.lkq	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\OqXZRaykm\AppData\Local\irlusudcijqrearuzovqqztca.lkq	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Windows\irlusudcijqrearuzovqqztca.lkq	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
irlusudcijqrearuzovqqztca.lkq	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Windows\system32\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Program Files (x86)\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\OqXZRaykm\AppData\Local\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq	Accessed File, Dropped File	Access, Create, Write	CLEAN
nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmoc.skq	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\jvsefk	Accessed File	Access, Create	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\jvsefk\nhmgpcwgxjbnls	Accessed File	Access, Create	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\jvsefk\	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\\vryufuqcvjdrraeu.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\\czheqgdqkzujkuzqj.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\\ljsqdusgbrndfqwoim.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\wvfeskjyulizcovojol.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\\jjuujccsphfxbowqmsqc.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\\yzlmcwxomfexcqzuryxkc.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\\pregxsumlffzfueayggunp.exe	Accessed File	Access	CLEAN
C:\Windows\system32\vryufuqcvjdrraeu.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\\czheqgdqkzujkuzqj.exe	Accessed File	Access	CLEAN
C:\Windows\system32\\ljsqdusgbrndfqwoim.exe	Accessed File	Access	CLEAN
C:\Windows\system32\\wvfeskjyulizcovojol.exe	Accessed File	Access	CLEAN
C:\Windows\system32\\jjuujccsphfxbowqmsqc.exe	Accessed File	Access	CLEAN
C:\Windows\system32\yzlmcwxomfexcqzuryxkc.exe	Accessed File	Access	CLEAN
C:\Windows\system32\pregxsumlffzfueayggunp.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\mfjckwpyozqbyefshgxcmfjckwpyozqbyef.hgx	Accessed File	Access	CLEAN
C:\Windows\system32\mfjckwpyozqbyefshgxcmfjckwpyozqbyef.hgx	Accessed File	Access	CLEAN
C:\Program Files (x86)\mfjckwpyozqbyefshgxcmfjckwpyozqbyef.hgx	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Local\mfjckwpyozqbyefshgxcmfjckwpyozqbyef.hgx	Accessed File	Access	CLEAN
C:\Windows\mfjckwpyozqbyefshgxcmfjckwpyozqbyef.hgx	Accessed File	Access	CLEAN
vryufuqcvjdrraeumoiqdzgcncykdrlzzimcuw.ylh	Accessed File	Access	CLEAN
C:\Windows\system32\vryufuqcvjdrraeumoiqdzgcncykdrlzzimcuw.ylh	Accessed File	Access	CLEAN
C:\Program Files (x86)\vryufuqcvjdrraeumoiqdzgcncykdrlzzimcuw.ylh	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Local\vryufuqcvjdrraeumoiqdzgcncykdrlzzimcuw.ylh	Accessed File	Access	CLEAN
C:\Windows\vryufuqcvjdrraeumoiqdzgcncykdrlzzimcuw.ylh	Accessed File	Access	CLEAN
czheqgdqkzujkuzqjmhqebjgsifsmbwlmwbsloj.gdl	Accessed File	Access	CLEAN
C:\Windows\system32\czheqgdqkzujkuzqjmhqebjgsifsmbwlmwbsloj.gdl	Accessed File	Access	CLEAN
C:\Program Files (x86)\czheqgdqkzujkuzqjmhqebjgsifsmbwlmwbsloj.gdl	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Local\czheqgdqkzujkuzqjmhqebjgsifsmbwlmwbsloj.gdl	Accessed File	Access	CLEAN
C:\Windows\czheqgdqkzujkuzqjmhqebjgsifsmbwlmwbsloj.gdl	Accessed File	Access	CLEAN
C:\Program Files (x86)\\WinRAR\rar.exe	Accessed File	Access	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\jvsefk\vlmchqgmzh.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\\Common Files\Adobe\ARM\1.0\AdobeARM.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	Accessed File	Access	CLEAN
Explorer.exe	Miscellaneous File	-	CLEAN
wvfeskjyulizcovojol.exe	Miscellaneous File	-	CLEAN
wvfeskjyulizcovojol.exe .	Miscellaneous File	-	CLEAN
czheqgdqkzujkuzqj.exe	Miscellaneous File	-	CLEAN
vryufuqcvjdrraeu.exe .	Miscellaneous File	-	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\yzlmcwxomfexcqzuryxkc.exe .	Miscellaneous File	-	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\vryufuqcvjdrraeu.exe .	Miscellaneous File	-	CLEAN

File Name	Category	Operations	Verdict
yzlmcwxomfexcqzuryxkc.exe	Miscellaneous File	-	CLEAN
jjuujccsphfxbowqmsqc.exe .	Miscellaneous File	-	CLEAN
vryufuqcvjdrraeu.exe	Miscellaneous File	-	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\ljsqdusgbrndfqwoim.exe .	Miscellaneous File	-	CLEAN
ljsqdusgbrndfqwoim.exe .	Miscellaneous File	-	CLEAN
ljsqdusgbrndfqwoim.exe	Miscellaneous File	-	CLEAN
yzlmcwxomfexcqzuryxkc.exe .	Miscellaneous File	-	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\czheqgdqkzujkuzqj.exe .	Miscellaneous File	-	CLEAN
jjuujccsphfxbowqmsqc.exe	Miscellaneous File	-	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\wvfeskjyulizcovojol.exe .	Miscellaneous File	-	CLEAN
czheqgdqkzujkuzqj.exe .	Miscellaneous File	-	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\jjuujccsphfxbowqmsqc.exe .	Miscellaneous File	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://www[.]showmyipaddress[.]com	Contacted, Extracted	104.21.74.56, 172.67.155.175, 188.114.96.3, 188.114.97.3	United States, The Netherlands	GET	CLEAN
hxxp://whatismyipaddress[.]com	Contacted, Extracted	104.19.222.79, 104.19.223.79	-	GET	CLEAN
hxxp://www[.]whatismyip[.]com	Contacted, Extracted	104.27.207.92, 104.27.206.92	-	GET	CLEAN
hxxp://www[.]youtube[.]com	Contacted, Extracted	172.217.1.110, 142.250.190.46, 142.250.190.142, 142.250.190.110, 172.217.4.78, 142.250.191.110, 172.217.2.46, 142.250.190.78, 142.250.191.142, 142.250.191.174, 142.250.191.206, 142.250.190.14, 172.217.0.174, 142.250.191.238	United States	GET	CLEAN
hxxp://www[.]wikipedia[.]org	Contacted, Extracted	185.15.59.224	United States	GET	CLEAN
hxxp://www[.]baidu[.]com	Contacted, Extracted	103.235.46.40	Hong Kong	GET	CLEAN
hxxps://www[.]cloudflare[.]com/5xx-error-landing	Extracted	-	-	-	CLEAN
hxxps://www[.]baidu[.]com/favicon.ico	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxp://dss0[.]bdstatic[.]com	Extracted	-	-	-	CLEAN
hxxp://dss1[.]bdstatic[.]com	Extracted	-	-	-	CLEAN
hxxp://ss1[.]bdstatic[.]com	Extracted	-	-	-	CLEAN
hxxp://sp0[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxp://sp1[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxp://sp2[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxp://pss[.]bdstatic[.]com	Extracted	-	-	-	CLEAN
hxxps://psstatic[.]cdn[.]bcebos[.]com/video/wiseindex/aa6eef91f8b5b1a33b454c401_1660835115000.png	Extracted	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://passport[.]baidu[.]com/v2/?login&tpl=mn&u=http%3A%2F%2Fwww.baidu.com%2F&sms=5	Extracted	-	-	-	CLEAN
hxxp://news[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxps://www[.]hao123[.]com/?src=from_pc	Extracted	-	-	-	CLEAN
hxxp://map[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxp://tieba[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxps://haokan[.]baidu[.]com/?sfrom=baidu-top	Extracted	-	-	-	CLEAN
hxxp://image[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxps://pan[.]baidu[.]com/?from=1026962h	Extracted	-	-	-	CLEAN
hxxps://wenku[.]baidu[.]com/?fr=bdpcindex	Extracted	-	-	-	CLEAN
hxxp://www[.]baidu[.]com/more/	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxp://fanyi[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxp://xueshu[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxps://baike[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxps://zhidao[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxps://jiankang[.]baidu[.]com/widescreen/home	Extracted	-	-	-	CLEAN
hxxp://e[.]baidu[.]com/ebaidu/home?refer=887	Extracted	-	-	-	CLEAN
hxxps://live[.]baidu[.]com	Extracted	-	-	-	CLEAN
hxxp://music[.]taihe[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]baidu[.]com/s?wd=%E7%99%BE%E5%BA%A6%E7%83%AD%E6%90%9C&sa=ire_dl_gh_logo_texing&rsv_dl=igh_logo_pcs	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxps://top[.]baidu[.]com/board?platform=pc&sa=pcindex_entry	Extracted	-	-	-	CLEAN
hxxps://www[.]baidu[.]com/s?wd=%E5%BC%80%E5%88%9B%E8%A5%BF%E9%83%A8%E5%A4%A7%E5%BC%80%E5%8F%91%E6%96%B0%E6%A0%BC%E5%B1%80&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxps://www[.]baidu[.]com/s?wd=%E5%A4%AA%E7%A9%BA%E5%86%8D%E8%81%9A%E9%A6%96+%E9%97%AE%E5%A4%A9%E6%97%A0%E6%AD%A2%E5%A2%83&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxps://www[.]baidu[.]com/s?wd=%E5%8D%97%E6%98%8C%E7%81%AB%E7%81%BE%E8%87%B43%E6%AD%BB+%E5%A5%B3%E5%AD%90%E5%85%A8%E8%BA%AB%E7%86%... ...%E9%BB%91%E9%80%83%E7%94%9F&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxps://www[.]baidu[.]com/s?wd=%E5%B9%BF%E5%B7%9E%E5%87%BA%E7%8E%B0%E9%BE%99%E5%8D%B7%E9%A3%8E&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	Extracted	103.235.46.40	Hong Kong	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://www[.]baidu[.]com/s?wd=%E3%80%8A%E5%A5%94%E8%B7%91%E5%90%A7%E3%80%8B%E7%BB%99%E8%89%BA%E4%BA%BA%E5%AE%89%E5%85%A8%E5%B8%A6&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxps://www[.]baidu[.]com/s?wd=6%E5%B2%81%E7%94%B7%E7%AB%A5%E9%A2%85%E9%AA%A8%E5%AF%84%E5%85%BB%E8%85%B9%E9%83%A81%E4%B8%AA%E5%8D%8A%E6%9C%88&sa=fyb_n_homepage&rsv_dl=fyb_n_homepage&from=super&cl=3&tn=baidutop10&fr=top1000&rsv_idx=2&hisfilter=1	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newfanyi-da0cea8f7e.png	Extracted	-	-	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newxueshuicon-a5314d5c83.png	Extracted	-	-	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newbaike-889054f349.png	Extracted	-	-	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newzhidao-da1cf444b0.png	Extracted	-	-	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newjiankang-f03b804b4b.png	Extracted	-	-	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/yingxiaoicon-612169cc36.png	Extracted	-	-	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newzhibo-a6a0831ecd.png	Extracted	-	-	-	CLEAN
hxxps://dss0[.]bdstatic[.]com/5aV1bjqh_Q23odCf/static/superman/img/topnav/newyinyue-03ecd1e9b9.png	Extracted	-	-	-	CLEAN
hxxp://www[.]baidu[.]com/img/PCtm_d9c8750bed0b3c7d089fa7d55720d6cf.png	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxp://www[.]baidu[.]com/img/PCfb_5bf082d29588c07f842ccde3f97243ea.png	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxp://www[.]baidu[.]com/img/flexible/logo/pc/result.png	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxp://www[.]baidu[.]com/img/flexible/logo/pc/result@2.png	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxp://www[.]baidu[.]com/img/flexible/logo/pc/peak-result.png	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxp://www[.]baidu[.]com/baidu.html?from=noscript	Extracted	103.235.46.40	Hong Kong	-	CLEAN
hxxps://sp1[.]baidu[.]com/5b1ZeDe5KgQFm2e88IuM_a/mwb2.gif	Extracted	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www[.]showmyipaddress[.]com	104.21.74.56, 172.67.155.175, 188.114.96.3, 188.114.97.3	United States, The Netherlands	TCP, DNS, HTTP	CLEAN
whatismyipaddress[.]com	104.19.222.79, 104.19.223.79	-	TCP, DNS, HTTP	CLEAN
www[.]whatismyip[.]com	104.27.207.92, 104.27.206.92	-	TCP, DNS, HTTP	CLEAN
www[.]youtube[.]com	172.217.1.110, 142.250.190.46, 142.250.190.142, 142.250.190.110, 172.217.4.78, 142.250.191.110, 172.217.2.46, 142.250.190.78, 142.250.191.142, 142.250.191.174, 142.250.191.206, 142.250.190.14, 172.217.0.174, 142.250.191.238	United States	TCP, DNS, HTTP	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www[.]wikipedia[.]org	185.15.59.224	United States	TCP, DNS, HTTP	CLEAN
www[.]baidu[.]com	103.235.46.40	Hong Kong	TCP, DNS, HTTP	CLEAN
www[.]cloudflare[.]com	-	-	-	CLEAN
dss0[.]bdstatic[.]com	-	-	-	CLEAN
dss1[.]bdstatic[.]com	-	-	-	CLEAN
ss1[.]bdstatic[.]com	-	-	-	CLEAN
sp0[.]baidu[.]com	-	-	-	CLEAN
sp1[.]baidu[.]com	-	-	-	CLEAN
sp2[.]baidu[.]com	-	-	-	CLEAN
pss[.]bdstatic[.]com	-	-	-	CLEAN
psstatic[.]cdn[.]bcebos[.]com	-	-	-	CLEAN
passport[.]baidu[.]com	-	-	-	CLEAN
news[.]baidu[.]com	-	-	-	CLEAN
www[.]hao123[.]com	-	-	-	CLEAN
map[.]baidu[.]com	-	-	-	CLEAN
tieba[.]baidu[.]com	-	-	-	CLEAN
haokan[.]baidu[.]com	-	-	-	CLEAN
image[.]baidu[.]com	-	-	-	CLEAN
pan[.]baidu[.]com	-	-	-	CLEAN
wenku[.]baidu[.]com	-	-	-	CLEAN
fanyi[.]baidu[.]com	-	-	-	CLEAN
xueshu[.]baidu[.]com	-	-	-	CLEAN
baike[.]baidu[.]com	-	-	-	CLEAN
zhidao[.]baidu[.]com	-	-	-	CLEAN
jiankang[.]baidu[.]com	-	-	-	CLEAN
e[.]baidu[.]com	-	-	-	CLEAN
live[.]baidu[.]com	-	-	-	CLEAN
music[.]taihe[.]com	-	-	-	CLEAN
top[.]baidu[.]com	-	-	-	CLEAN
www[.]whatismyip[.]ca	-	-	-	CLEAN
whatismyip[.]everdot[.]org	-	-	-	CLEAN
youtube-ui[.]l[.]google[.]com	172.217.1.110, 142.250.190.46, 142.250.190.142, 142.250.190.110, 172.217.4.78, 142.250.191.110, 172.217.2.46, 142.250.190.78, 142.250.191.142, 142.250.191.174, 142.250.191.206, 142.250.190.14, 172.217.0.174, 142.250.191.238	United States	TCP, DNS, HTTP	CLEAN
iwuwem[.]org	162.249.65.164	United States	TCP, DNS	CLEAN
ggybyqnvrq[.]info	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
qmkuidndfwv[.]net	-	-	-	CLEAN
faysxbmq[.]info	-	-	-	CLEAN
bicsnsjoe[.]info	-	-	-	CLEAN
lynojqbnm[.]org	-	-	-	CLEAN
qatqtsqesmd[.]net	-	-	-	CLEAN
wmiosyoyoa[.]com	-	-	-	CLEAN
dkitrpodbn[.]net	-	-	-	CLEAN
eymwsewwok[.]com	-	-	-	CLEAN
bkpytkqvec[.]net	-	-	-	CLEAN
bqcanilwnuj[.]com	-	-	-	CLEAN
dzfiafodymkx[.]net	-	-	-	CLEAN
jlcfzvgtso[.]info	-	-	-	CLEAN
eqoiqe[.]org	-	-	-	CLEAN
dyna[.]wikimedia[.]org	185.15.59.224	United States	TCP, DNS, HTTP	CLEAN
iqpqduz[.]info	-	-	-	CLEAN
jbbfbnlpzo[.]net	-	-	-	CLEAN
pmnbndfev[.]com	-	-	-	CLEAN
wkouaxsl[.]info	-	-	-	CLEAN
www[.]a[.]shifen[.]com	103.235.46.40	Hong Kong	TCP, DNS, HTTP	CLEAN
www[.]wshifen[.]com	103.235.46.40	Hong Kong	TCP, DNS, HTTP	CLEAN
lozylvzsn[.]org	-	-	-	CLEAN
jgggrkswl[.]info	-	-	-	CLEAN
nxbmxjdftdbe[.]net	-	-	-	CLEAN
bkvjdstb[.]info	-	-	-	CLEAN
imakzxrvpl[.]info	-	-	-	CLEAN
wozqja[.]info	-	-	-	CLEAN
gumcwcyskm[.]org	-	-	-	CLEAN
ttfbgn[.]net	-	-	-	CLEAN
kquceeau[.]com	-	-	-	CLEAN
llcuscfm[.]info	-	-	-	CLEAN
oembvhyvje[.]info	-	-	-	CLEAN
nshqdmtabpw[.]net	-	-	-	CLEAN
cfjvdxggxy[.]info	-	-	-	CLEAN
uwidfnhb[.]info	-	-	-	CLEAN
zpkyqy[.]info	-	-	-	CLEAN
oaguoiccuswc[.]com	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
bqduqyvvo[.]info	-	-	-	CLEAN
yypaiqkwokz[.]net	-	-	-	CLEAN
yaeqsu[.]com	-	-	-	CLEAN
bwdyfxd[.]net	-	-	-	CLEAN
ludmhagmqrb[.]org	-	-	-	CLEAN
kmhcfkjhs[.]net	-	-	-	CLEAN
nqnnvzbygeb[.]com	-	-	-	CLEAN
wwjmyst[.]info	-	-	-	CLEAN
asykget[.]net	-	-	-	CLEAN
exzihifb[.]info	-	-	-	CLEAN
ngaktnaw[.]info	-	-	-	CLEAN
ovuvuioxnd[.]info	-	-	-	CLEAN
jqdsgajcjyv[.]com	-	-	-	CLEAN
amdwrt[.]net	-	-	-	CLEAN
bwzemcsali[.]info	-	-	-	CLEAN
yejspkr[.]net	-	-	-	CLEAN
pmpcryg[.]org	-	-	-	CLEAN
vabpled[.]info	-	-	-	CLEAN
tikydyz[.]net	-	-	-	CLEAN
zypdwsbniw[.]net	-	-	-	CLEAN
yicwsqsq[.]com	-	-	-	CLEAN
bebshzesxvh[.]net	-	-	-	CLEAN
rlszzbk[.]net	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
188.114.96.3	www[.]showmyipaddress[.]com	The Netherlands	TCP, DNS, HTTP	CLEAN
104.19.223.79	whatismyipaddress[.]com	-	TCP, DNS, HTTP	CLEAN
104.27.207.92	www[.]whatismyip[.]com	-	TCP, DNS, HTTP	CLEAN
162.249.65.164	iwuwem[.]org	United States	TCP, DNS	CLEAN
142.250.191.142	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	TCP, DNS, HTTP	CLEAN
185.15.59.224	www[.]wikipedia[.]org, dyna[.]wikimedia[.]org	United States	TCP, DNS, HTTP	CLEAN
103.235.46.40	www[.]wshifen[.]com, www[.]a[.]shifen[.]com, www[.]baidu[.]com	Hong Kong	TCP, DNS, HTTP	CLEAN
104.21.74.56	www[.]showmyipaddress[.]com	-	TCP, DNS, HTTP	CLEAN
188.114.97.3	www[.]showmyipaddress[.]com	The Netherlands	DNS	CLEAN
104.19.222.79	whatismyipaddress[.]com	-	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
104.27.206.92	www[.]whatismyip[.]com	-	DNS	CLEAN
142.250.191.174	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.191.206	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.191.238	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
172.217.0.174	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
172.217.1.110	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
172.217.2.46	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
172.217.4.78	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.190.14	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.190.46	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.190.78	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.190.110	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.190.142	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
142.250.191.110	youtube-ui[.]l[.]google[.]com, www[.]youtube[.]com	United States	DNS	CLEAN
172.67.155.175	www[.]showmyipaddress[.]com	United States	DNS	CLEAN
0.0.0.0	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
ilzcuqtmmhidkalihqrgadr	access	cagrt.exe	CLEAN
yzlmcwxomfexcqzuryxkc	access	cagrt.exe, wjhuwcp.exe	CLEAN
pregxsumlffzfueayggunp	access	cagrt.exe, wjhuwcp.exe	CLEAN
dblessugkcdblessugkcdbless	access	cagrt.exe, wjhuwcp.exe	CLEAN
hhtoegkyeybbniyaesysvvhcsuym	access	wjhuwcp.exe	CLEAN
nhmgpcwgxjbnlsuiyyqwhbgajwqardvhfmocsskqbvaudqkulxpbzgiwmmekvpuoxk	access	wjhuwcp.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	read, write, access	cagrt.exe, wjhuwcp.exe	MALICIOUS
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools	write, access	cagrt.exe, wjhuwcp.exe	MALICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	write, access	cagrt.exe, wjhuwcp.exe	MALICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\jvsefk	write, access	cagrt.exe, wjhuwcp.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\wjhuwcp	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\lzympwko	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\crrgkshmy	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\vImchqgmzh	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\nfiahskshrhr	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\qhjagqhocla	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\yjfqq	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\jvsefk	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\wjhuwcp	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableInstallerDetection	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableSecureUIAPaths	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ValidateAdminCodeSignatures	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL	create, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Security Center	create, access	cagrt.exe, wjhuwcp.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SecurityCenter\AntiVirusOverride	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SecurityCenter\FirewallOverride	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SecurityCenter\UacDisableNotify	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SecurityCenter\AntiVirusDisableNotify	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SecurityCenter\FirewallDisableNotify	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SecurityCenter\UpdatesDisableNotify	write, access	cagrt.exe, wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot	delete, access	wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjects\{FD6905CE-952F-41F1-9A6F-135D9C6622CC}	delete, access	wjhuwcp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows Defender	delete, access	wjhuwcp.exe	CLEAN

Process

Process Name	Commandline	Verdict
cagrt.exe	"C:\Users\OqXZRaykm\Desktop\cagrt.exe"	MALICIOUS
wjhuwcp.exe	"C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe" "-"	MALICIOUS
wjhuwcp.exe	"C:\Users\OQXZRA~1\AppData\Local\Temp\wjhuwcp.exe" "-"	MALICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_20h1_en_base
Description	windows 10 (64bit 20H1 -EN-)
Architecture	x86 64-bit
Operating System	Windows 10 20H1
Kernel Version	10.0.19041.208 (dc9233f8-5819-e3d0-929a-7bde0b87f0b9)
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	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.207.19041.0
Chrome Version	Not installed
Firefox Version	108.0
Flash Version	Not installed
Java Version	8.0.3610.9

System Information

Sample Directory	C:\Users\OqXZRaykm\Desktop
Computer Name	PXTHFFRYO7
User Domain	PXTHFFRYO7
User Name	OqXZRaykm
User Profile	C:\Users\OqXZRaykm
Temp Directory	C:\Users\OQXZRA~1\AppData\Local\Temp

System Root	C:\Windows