ID: 736953
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 12:25:01
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2

Windows Analysis Report http://ctlinks.wolterskluwer.com/ls/click?upn=-2F-2B5hLiYrr13mMklQzkilNPvE-2BPYo5nhRLT6V-2BqlTi7kpM0RT6onBJ28bgBSAYUbh60t9W3P21gRRyVbLtnTe39-2BUKFAdWE-2F9utgRuUM1WI-2BwvijlKoyye8-2F1lXNbNuywkr9VSIrlzgGsSObiegBJS7X-2FNFxP3asb5ksx5hiqiOe5DLDhLyynO864YG8-2FdOxYumDCcKOeWQMWv-2FQeYeHkTA-3D-3DUnvt_imVlhaP 3

- Overview 3
  - General Information 3
  - Detection 3
  - Signatures 3
  - Classification 3
- Process Tree 3
- Yara Signatures 3
- Sigma Signatures 3
- Snort Signatures 3
- Joe Sandbox Signatures 4
- Mitre Att&ck Matrix 4
- Screenshots 4
  - Thumbnails 4
- Antivirus, Machine Learning and Genetic Malware Detection 5
  - Initial Sample 5
  - Dropped Files 5
  - Unpacked PE Files 5
  - Domains 5
  - URLs 6
- Domains and IPs 6
  - Contacted Domains 6
  - Contacted URLs 6
  - World Map of Contacted IPs 6
    - Public IPs 7
  - Private 8
- General Information 8
  - Warnings 8
- Created / dropped Files 9
- Static File Info 9

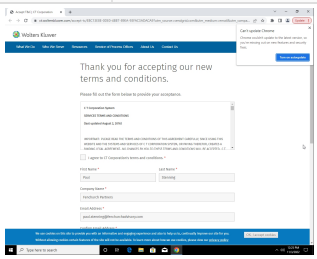
Windows Analysis Report

http://ctlinks.wolterskluwer.com/ls/click?upn=-2F-2B5hLiYrr13mMklQzkilNPvE-2BPYo5nhRLT6V-2Bq...

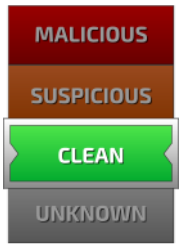
Overview

General Information

Sample URL:	http://ctlinks.wolterskluwer.com/ls/click?upn=-2F-2B5hLiYrr13mMklQzkilNPvE-...21gRRyVbLtnTe39-2BUKFAdWE-2F9utgRuUM1WI-2BwvijlKoyye8-2F1lXNbNuywkr9VSIrlzg
Analysis ID:	736953



Detection

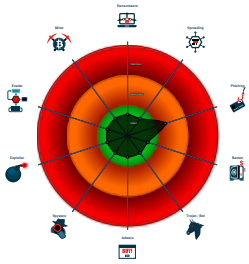


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 5772 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://ctlinks.wolterskluwer.com/ls/click?upn=-2F-2B5hLiYrr13mMklQzkilNPvE-2BPYo5nhRLT6V-2BqlTi7kpM0RT6onBJ28bgBSAYUbh60t9W3P21gRRyVbLtnTe39-2BUKFAdWE-2F9utgRuUM1WI-2BwvijlKoyye8-2F1lXNbNuywkr9VSIrlzgGsSObiegBJS7X-2FNFxP3asb5ksx5hiqiOe5DLDhLyynO864YG8-2FdOxYumDCcKOeWQMWv-2FQeYeHkTA-3D-3DUnvt_imVlhaP3FR-2Fe8ZExGsY6oQnx74nFuNOYPlfTRZidYsSMUOIzqg41MG5lgxasfcocJXJlKP6nRrhJbqXW3TA3nKdUaLxbQjJC-2FDVePYnSDJKtiphyPueYo5ZY-2F0ieEa8XGjp3pPCxqMJsumRw6lmKVm4OnRppS3lvqZxyzClCvozrLe-2Betq383F1LTJph1fLBwzFDHgOFB-2FlTvCP7fRXbrIJeGENSJi0V56PSsw1X1rcEOEPlF5iP-2BzgFTMSSNTG3eeJ-2FbKI8KZKasdXSI2rXfoUo8hHe-2Fl7uQl9ad38-2Ba4bT3Kg5ljsL0aLwRuzzcs0r2UfbAjEtrENgw8bLKnWY6SnnAu-2FcRqPhuVM-2B1V0tJ-2F5-2B3Whx9q5ivCEPorDEmuh7Ykb0Ri6lDrppCPN6TiSATQ-3D-3D MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 4116 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2044 --field-trial-handle=1864,i,11590665349764109 25,8171802982352021328,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

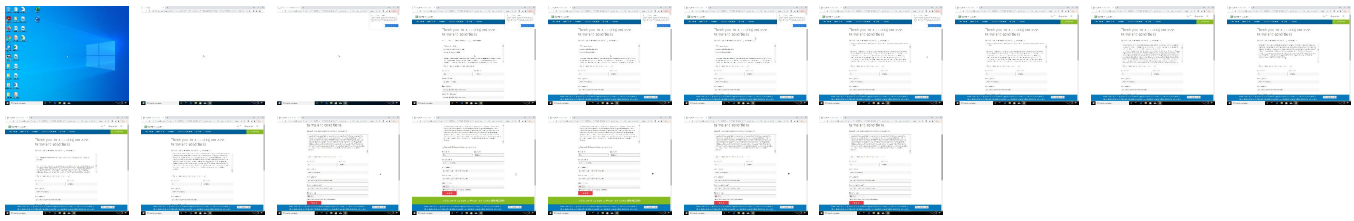
Mitre Att&ck Matrix

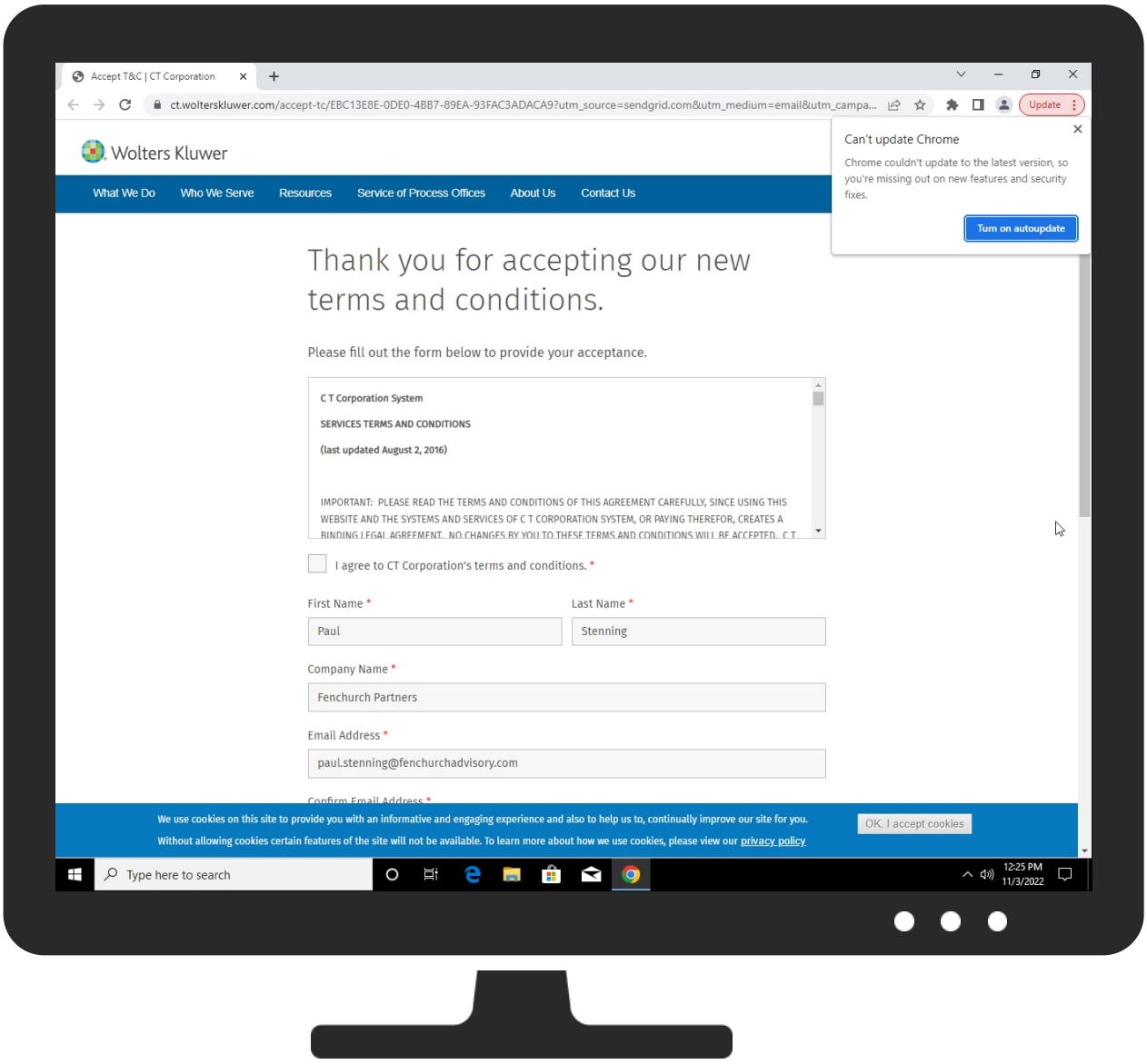
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://ctlinks.wolterskluwer.com/ls/click?upn=-2F-2B5hLiYrr13mMklQzkilNPvE-2BPYo5nhRLT6V-2BqlTi7kpM0RT6onBJ28bgBSAYUbh60t9W3P21gRRyVbLtnTe39-2BUKFAdWE-2F9utgRuUM1WI-2BwvijlKoyye8-2F1IXNbNuywkr9VSIrlzgGsSObiegBJS7X-2FNFxP3asb5ksx5hiqiOe5DLDhLyynO864YG8-2FdOxYumDCcKOeWQMWv-2FQeYeHkTA-3D-3DUnvt_imVlhaP3FR-2Fe8ZExGsY6oQnx74nFuNOYPIfTRZidYsSMUOIzqg41MG5lgxasfcocJXJlKP6nRrhJbqXW3TA3nKdUaLxbQjJC-2FDVePYnSDJKtiphyPueYo5ZY-2F0ieEa8XGjp3pPCxqMJsumRw6ImKVm4OnRppS3lvqZxyzClCvozrLe-2Betq383F1LTJph1fLBwzFDHgOFB-2FlTvCP7fRXbrlJeGENSJi0V56PSsw1X1rcEOEPIF5iP-2BzgFTMSSNTG3eeJ-2FbKI8KZKasdXSl2rXfoUo8hHe-2FI7uQI9ad38-2Ba4bT3Kg5ljsL0aLwRuzzcs0r2UfbAjEtrENgw8bLKnWY6SnnAu-2FcRqPhuVM-2B1V0tJ-2F5-2B3Whx9q5ivCEPorDEmuh7Ykb0Ri6IDrppCPN6TiSATQ-3D-3D	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	157.240.20.35	true	false		high
p01f.t.eloqua.com	142.0.173.26	true	false		high
vc-live-cf.hotjar.io	65.9.66.34	true	false		unknown
accounts.google.com	142.250.185.173	true	false		high
sendgrid.net	167.89.118.52	true	false		high
st1.dialogtech.com	107.22.63.100	true	false		high
stats.g.doubleclick.net	74.125.140.156	true	false		high
vars.hotjar.com	13.227.219.93	true	false		high
adobetarget.data.adobedc.net	13.36.218.177	true	false		unknown
duerzc3hf5let.cloudfront.net	99.86.240.71	true	false		high
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
in-live.live.eks.hotjar.com	52.17.231.22	true	false		high
script.hotjar.com	52.222.236.74	true	false		high
googleads.g.doubleclick.net	172.217.23.98	true	false		high
www.google.com	216.58.212.132	true	false		high
clients.l.google.com	172.217.18.14	true	false		high
cdn.linkedin.oribi.io	108.138.36.102	true	false		high
st2.dialogtech.com	34.226.62.133	true	false		high
www.google.ch	142.250.185.99	true	false		high
d31y97ze264gaa.cloudfront.net	13.225.84.38	true	false		high
wolterskluwer.com.102.122.2o7.net	15.188.95.229	true	false		high
static-cdn.hotjar.com	108.157.4.21	true	false		high
wolterskluwer.tt.omtrdc.net	unknown	unknown	false		unknown
in.hotjar.com	unknown	unknown	false		high
ct.wolterskluwer.com	unknown	unknown	false		high
cdn.tt.omtrdc.net	unknown	unknown	false		unknown
ctlinks.wolterskluwer.com	unknown	unknown	false		high
vc.hotjar.io	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
s676.t.eloqua.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
smetrics.wolterskluwer.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
img.en25.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
bam.nr-data.net	unknown	unknown	false		unknown
snap.licdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://ct.wolterskluwer.com/accept-tc/EBC13E8E-0DE0-4BB7-89EA-93FAC3ADACA9?utm_source=sendgrid.com&utm_medium=email&utm_campaign=website	false		high
https://vars.hotjar.com/box-0feefa1930c964ac6aa4db4e99e8f25f.html	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.99	www.google.ch	United States		15169	GOOGLEUS	false
167.89.118.52	sendgrid.net	United States		11377	SENDGRIDUS	false
107.22.63.100	st1.dialogtech.com	United States		14618	AMAZON-AESUS	false
23.197.8.158	unknown	United States		16625	AKAMAI-ASUS	false
172.217.18.14	clients.l.google.com	United States		15169	GOOGLEUS	false
142.0.173.26	p01f.t.eloqua.com	United States		7160	NETDYNAMICSUS	false
15.188.95.229	wolterskluwer.com.102.122.2o7.net	United States		16509	AMAZON-02US	false
34.226.62.133	st2.dialogtech.com	United States		14618	AMAZON-AESUS	false
172.217.23.98	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
65.9.66.34	vc-live-cf.hotjar.io	United States		16509	AMAZON-02US	false
95.101.54.113	unknown	European Union		34164	AKAMAI-LONGB	false
162.247.241.14	unknown	United States		23467	NEWRELIC-AS-1US	false
52.167.11.129	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
172.217.18.99	unknown	United States		15169	GOOGLEUS	false
142.250.186.136	unknown	United States		15169	GOOGLEUS	false
142.250.184.200	unknown	United States		15169	GOOGLEUS	false
142.250.186.99	unknown	United States		15169	GOOGLEUS	false
52.17.231.22	in-live.live.eks.hotjar.com	United States		16509	AMAZON-02US	false
142.250.186.78	unknown	United States		15169	GOOGLEUS	false
142.250.185.68	unknown	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
13.225.84.38	d31y97ze264gaa.cloudfront.net	United States		16509	AMAZON-02US	false
13.36.218.177	adobetarget.data.adobedc.net	United States		7018	ATT-INTERNET4US	false
13.107.42.14	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
74.125.140.156	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.186.106	unknown	United States		15169	GOOGLEUS	false
151.101.2.137	unknown	United States		54113	FASTLYUS	false
142.250.181.227	unknown	United States		15169	GOOGLEUS	false
185.60.216.19	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
108.157.4.21	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
13.227.219.93	vars.hotjar.com	United States		16509	AMAZON-02US	false
108.138.36.102	cdn.linkedin.oribi.io	United States		16509	AMAZON-02US	false
142.250.185.173	accounts.google.com	United States		15169	GOOGLEUS	false
52.222.236.74	script.hotjar.com	United States		16509	AMAZON-02US	false
99.86.240.71	duerzc3hf5let.cloudfront.net	United States		16509	AMAZON-02US	false
157.240.20.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
88.221.168.237	unknown	European Union		16625	AKAMAI-ASUS	false
142.250.185.98	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736953
Start date and time:	2022-11-03 12:25:01 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://ctlinks.wolterskluwer.com/ls/click?upn=-2F-2B5hLiYrr13mMklQzkilNPvE-2BPYo5nhRLT6V-2BqlTi7kpM0RT6onBJ28bgBSAYUbh60t9W3P21gRRyVbLtnTe39-2BUKFAdWE-2F9utgRuUM1WI-2BwvijlKoyye8-2F1lXNbNuywkr9VSlrlzgGsSObiegBJS7X-2FNFxP3asb5ksx5hiqiOe5DLDhLyynO864YG8-2FdOxYumDCcKOeWQMWv-2FQeYeHkTA-3D-3DUnvt_imVlhaP3FR-2Fe8ZExGsY6oQnx74nFuNOYPlfTRZidYsSMUOIzqg41MG5lgxasfcocJXJlKP6nRrhJbqXW3TA3nKdUaLxbQjJC-2FDVePYnSDJKtiphyPueYo5ZY-2F0ieEa8XGjp3pPCxqMJsumRw6ImKVm4OnRppS3lvqZxyzClCvozrLe-2Betq383F1LTJph1fLBwzFDHgOFB-2FlTvCP7fRXbrlJeGENSJi0V56PSsw1X1rcEOEPlF5iP-2BzgFTMSSNTG3eeJ-2FbKl8KZKasdXSI2rXfoUo8hHe-2Fl7uQl9ad38-2Ba4bT3Kg5ljsL0aLwRuzzcs0r2UfbAjEtrENgw8bLKnWY6SnnAu-2FcRqPhuVM-2B1V0tJ-2F5-2B3Whx9q5ivCEPorDEmuh7Ykb0Ri6lDrppCPN6TiSATQ-3D-3D
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@25/0@32/348

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, usocoreworker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.126.31.69, 40.126.31.73, 20.190.159.23, 20.190.159.71, 20.190.159.0, 20.190.159.73, 40.126.31.67, 20.190.159.4, 142.250.186.99, 52.167.11.129, 34.104.35.123, 88.221.168.237, 142.250.186.136, 142.250.184.200, 95.101.54.113, 95.101.54.122, 13.107.42.14, 142.250.185.98, 142.250.186.106, 142.250.186.138, 172.217.16.138, 142.250.186.42, 142.250.186.74, 172.217.18.10, 172.217.16.202, 142.250.184.202, 216.58.212.170, 172.217.23.106, 142.250.185.74, 142.250.186.170, 142.250.185.106, 142.250.184.234, 142.250.185.202, 142.250.181.234, 142.250.186.78, 151.101.2.137, 151.101.66.137, 151.101.130.137, 151.101.194.137, 23.197.8.158, 162.247.241.14
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, fs.microsoft.com, www.googleadservices.com, content-autofill.googleapis.com, wildcard.en25.com.edgekey.net, www.tm.lg.prod.aadmsa.akadns.net, cn-assets.adobedtm.com.edgekey.net, clientservices.googleapis.com, www.tm.a.prd.aadg.akadns.net, od.linkedin.edgesuite.net, k.sni.global.fastly.net, login.msa.msidentity.com, ssl.google-analytics.com, wk-grc-ct-prod-myct.trafficmanager.net, l-0005.l-msedge.net, prda.aadg.msidentity.com, edgedl.me.gvt1.com, login.live.com, e7808.dscg.akamaiedge.net, www.googletagmanager.com, e5763.g.akamaiedge.net, a1916.dscg2.akamai.net, bam.nr-data.net.cdn.cloudflare.net, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Created / dropped Files

No created / dropped files found

Static File Info

No static file info