**JUMPSEC PCAP Incident Analysis Report**

Author: Abdurr Patel

Note: The Appendix is organized to reflect the natural progression of the investigation, supported with logical reasoning and corresponding screenshots.

Sample Name: Malicious Network Traffic.pcap

Date of Analysis: 04/05/2025 – 06/05/2025

Analysis Tools: Network Miner v3.0, Wireshark v4.2.5

Intelligence Sources: Virus Total, AlienVault OTX, WHOIS, Splunk Threat Research, MITRE

Investigation Environment: VirtualBox running Kali Linux

**Assessment Outcome**

**Impact Summary:**  
The incident resulted in the compromise of sensitive data specifically credentials and cookies, likely via an executable delivered through phishing. The malware established a covert command and control channel and exfiltrated data through FTP, indicating a significant breach of network integrity and unknown level of persistence. Research into the malware shows that the attack leveraged known malware families (Snake Keylogger/VIP Recovery).

MITRE ATT&CK TTP's:

* + T1566.001 – Phishing Attachment (High Confidence)
  + T1204.002 - User Execution: Malicious File (High Confidence)
  + T1016.001 – System Network Configuration Discovery: Internet Connection Discovery
  + T1102.002 – Web Service: Bidirectional Communication
  + T1555.003 – Credentials from Web Browsers
  + T1048.002 – Exfiltration Over Alternative Protocol: Exfiltration Over FTP

Discovery of these TTP’s can be found within the Incident Findings section.

**Mitigation Recommendations**

The recommendations provided will be split into short term and long-term mitigation to maximise risk reduction.

|  |  |  |  |
| --- | --- | --- | --- |
| **Short Term Mitigation Strategies** | | **Long Term Mitigation Strategies** | |
| Isolate the Affected Host | Immediately disconnect the compromised system (10.9.17.101) from the network to prevent further data exfiltration and potential lateral movement. | User Intelligence:  Identity Threat Detection and Response / User Behaviour Analytics. | Collect as much identity related intelligence and long-term user behaviour data to be alerted on anomalous actions early. |
| Block Malicious Infrastructure | Implement blacklisting for known malicious entities including Executables, IP addresses, Emails and Domains observed in the PCAP and from Cyber Intelligence. See Attacker Domain and Infrastructure Analysis section and Appendix 27. | Threat Intelligence:  Up to date IOC/ Threat Intelligence via TAXII into the SIEM. | Ensure the continuous update of security tools with the latest CTI feeds, with indicators of compromise (IOCs). Given the date 17/09/2024 of this attack type first appearing, automated response should have prevented this attack. |
| Session and Credential Reset | Reset Cookies and change Passwords for the accounts compromised. A full list can be found in Appendix 28,29 | Client intelligence:  Phishing Simulations | Engaging client’s continuously through simulated phishing campaigns ensures that clients can subconsciously learn the tactics used in phishing emails. Running within the natural working environment improves awareness and provides quantitative feedback on results. |

**Incident Findings**

This Incident overview will focus on malicious activity observed in the PCAP sample, which provides visibility on Command and Control (C2) and Actions / Objectives phases in the perspective of the Cyber Kill Chain. As the investigation developed a full picture was built to include high probability Delivery and Installation techniques.

**PCAP Overview**  
The capture consisted of 896 packets over a two-minute interval, with most of the communication traffic being between the victim (10.9.17.101) and attacker infrastructure at (216.252.233.118)specificallyFTP-DATA [Appendix 1, 2, 3].

**Initial Access via Phishing | T1566.001 , T1204.002**  
The initial access likely occurred through a phishing email delivering a trojan pdf carrying the executable (Hesaphareketi-01.exe) [Appendix 23,24,25]. It is associated with the Snake Keylogger (VIP Recovery variant) which is further corroborated by Virus Total when searching the attackers FTP server username and VIP signature within the txt files. [Appendix 5,20].

**Network Discovery via Geolocation and IP | T1016.001**  
Once executed, the malware performed public IP and geolocation discovery by querying external services:

* **checkip.dyndns.org** was contacted to expose the victim’s public IP [Appendix 7, 8].
* **reallyfreegeoip.org** was queried for geolocation details, potentially triggering further actions [Appendix 9,10].

**Command and Control (C2) via Telegram | T1102.002**  
The malware established a C2 channel by beaconing to api.telegram.org over HTTPS, using encryption certificates (GoDaddy and references to Google PKI) [Appendix 11,12].

**Exfiltration via FTP | T1048.002 , T1555.003**  
Analysis of FTP and FTP-DATA traffic revealed:

* An FTP connection from 10.9.17.101 to 216.252.233.118 (ftp.lifechangerscare.com) [Appendix 15].
* File transfers included stolen cookies and credentials, confirmed by detailed ASCII stream analysis showing persistent data updates [Appendix 16, 17, 18].

**Data Compromise and Malware Attribution**  
The investigation uncovered two files containing stolen credentials and cookies, marked with a “VIP Recovery” signature [ Appendix 19, 20, 21]. Threat intelligence (VirusTotal, AlienVault OTX) and malware analysis paper (Splunk analysis) verified that **Hesaphareketi-01.exe** is linked to known Snake Keylogger and VIPKeylogger malware families, further correlating with external bundled files and associated executables. Additional threat data supports the legitimacy of the observed sender address [Appendix 22, 23, 24, 25, 26,27].

**Timeline of Events**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Time UTC +00** | **Client Host** | **Server Host** | **Port** | **Context** |
| 2024-09-17 20:06:53 | 10.9.17.101 | 158.101.44.242 checkip.dyndns.com | 80 | Public IP Exposure:  The malware queries DynDNS to retrieve the victim's public IP. |
| 2024-09-17 20:06:56 | 10.9.17.101 | 104.21.67.152 reallyfreegeoip.org | 443 | Geolocation Exposure:  The malware uses this service to geolocate the victim |
| 2024-09-17 20:07:05 | 10.9.17.101 | 149.154.167.220 api.telegram.org | 443 | Command & Control (C2) Beacon:  Encrypted connection to Telegram's API to send instructions |
| 2024-09-17 20:07:17 | 10.9.17.101 | 216.252.233.118 ftp.lifechangerscare.com | 21 | FTP Login Attempt:  Initiates a connection using Chuks@ credentials [Appendix 5] |
| 2024-09-17 20:07:19 | 10.9.17.101 | 216.252.233.118 ftp.lifechangerscare.com | 56347 | FTP Passive Data Channel:  FTP enters passive mode, which allows easier firewall traversal. |
| 2024-09-17 20:07:21 | 10.9.17.101 | 216.252.233.118 ftp.lifechangerscare.com | 62759 | Exfiltration Begins:  Stolen credentials and cookies are transmitted to the attacker's FTP server |
| 2024-09-17  20:08:10 | 10.9.17.101 | 158.101.44.242 checkip.dyndns.com | 80 | Repeated Public IP Check:  IP validation |
| 2024-09-17 20:08:45 | 10.9.17.101 | 104.21.67.152 reallyfreegeoip.org | 443 | Repeated Geolocation Check:  Location validation |
| 2024-09-17 20:08:46 | 10.9.17.101 | 149.154.167.220 api.telegram.org | 443 | Persistent C2 Communication:  Trigger transfer or awaiting further instructions |

This timeline has been compiled with the support of Network Miner’s Session Data and Wireshark’s Flow Graph, to provide a high degree of accuracy in of event times and context.

**Attacker Domain and Infrastructure Analysis**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Verdict** | **Description and Usage** | **OSINT Info** | **Sources** |
| checkip.dyndns.com  IP Addresses: 132.226.247.73  132.226.8.169  158.101.44.242  193.122.130.0  193.122.6.168 | Suspicious  Security Vendor Score:  1/97 | Supporting Attacker Infrastructure  Owned by Oracle this service is not inherently malicious however it has a history of being abused for network discovery.  Whilst benign singularly, it is a core part of the attack chain by exposing the public IP for attacker IP to latch on to. | Verdict:  Whitelisted  Registrar:  TUCOWS, INC  Creation Date:  Sep 24, 1996 | AlienVault OTX  [Whois](http://whois.domaintools.com/reallyfreegeoip.org),  [UrlVoid](http://www.urlvoid.com/scan/reallyfreegeoip.org),  [VirusTotal](https://www.virustotal.com/gui/domain/reallyfreegeoip.org/details/) |
| reallyfreegeoip.org  IP Addresses: 104.21.112.1  104.21.16.1  104.21.32.1  104.21.48.1  104.21.64.1  104.21.67.152 | Suspicious  Security Vendor Score:  6/97 | Supporting Attacker infrastructure  Free public IP location API that is commonly abused in attacks downgrading its reputation.  Given the context of the attack being an info stealer, geolocation may indicate value / quality of potential data if it’s a developed area. | Verdict:  Not Listed  Registrar:  Cloudflare, Inc    Creation Date:  Oct 20, 2018 | AlienVault OTX [Whois](http://whois.domaintools.com/reallyfreegeoip.org),  [UrlVoid](http://www.urlvoid.com/scan/reallyfreegeoip.org),  [VirusTotal](https://www.virustotal.com/gui/domain/reallyfreegeoip.org/details/) |
| api.telegram.org  IP Addresses:  149.154.167.220 | Suspicious  Security Vendor Score:  2/94 | Primary Attacker Infrastructure  Secure messenger service that has its API Bot service commonly abused for C2 communication. Ensures that the malware stays active and is persistent with periodic checks. | Verdict:  Whitelisted  Registrar:  GoDaddy.com  Creation Date:  Dec 15, 2003 | AlienVault OTX [Whois](http://whois.domaintools.com/reallyfreegeoip.org),  [UrlVoid](http://www.urlvoid.com/scan/reallyfreegeoip.org),  [VirusTotal](https://www.virustotal.com/gui/domain/reallyfreegeoip.org/details/) |
| lifechangerscare.com  IP Addresses:  No Resolution  (216.252.233.118) | Malicious  Security Vendor Score:  1/94 | Primary Attacker Infrastructure  Identified in association with phishing activities with a speciality in deploying info stealers. Also worth noting that the domain looks to mimic a legitimate site called lifechangecare.co.uk. Its short-lived operation is another common indicator. | Verdict:  Not Listed  Registrar:  NameSilo, LLC    Creation Date:  Nov 3, 2023 | AlienVault OTX [Whois](http://whois.domaintools.com/reallyfreegeoip.org),  [UrlVoid](http://www.urlvoid.com/scan/reallyfreegeoip.org),  [VirusTotal](https://www.virustotal.com/gui/domain/reallyfreegeoip.org/details/) |

**Appendix**

**Appendix 1: PCAP Metadata**

A screenshot of a computer

AI-generated content may be incorrect.Examining the PCAP provides an overview of the number of frames (896 packets) and timeframe of under two minutes in this capture.

**Appendix 2: Endpoints**

Overview of the endpoints involved. Two class A addresses and four public addresses. Notably 10.9.17.101 and 216.252.233.118 hold a lot of packets.

A screenshot of a computer screen

AI-generated content may be incorrect.

**Appendix 3: Conversations**

Further inspection shows that 10.9.17.101 has a considerable amount of communication with this external entity of 216.252.233.118 with an approximately even number of packets being sent and received by both parties.

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 4: Protocol Hierarchy**

Going into what protocols are being used highlights HTTP, HTTPS,DNS and FTP. A large amount of data and bytes are shown to be held in FTP – Data. This potentially relates to exfil type activity.

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 5: Logins**

This is the login credentials used to establish the FTP connection. The username has been flagged in relation to a malware called “vipkeylogger”



**Appendix 6: Sessions**

This indicates a timeline of events and will direct the order of analysis. On first look the malware exposed the public IP and location details. C2 connection via telegram was then made available and FTP communication commenced.

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 7: HTTP Packet Analysis**

Communication to Oracle Public Cloud who own checkip.dyndns.org (158.101.44.242). 20 packets (2.2% of total capture)

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 8: HTTP TCP Stream**

Multiple requests to checkip.dyndns.org to expose 10.9.17.101 public IP being 173.166.146.112

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 9: HTTPS Packet Analysis – IP Discovery**

A screenshot of a computer

AI-generated content may be incorrect.Communication to reallyfreegeoip.org. Potential C2 trigger after geo is found given its reputation from Virus Total and AlienVault OTX. 52 packets (5.8% of total capture)

**Appendix 10: HTTPS IP Discovery TCP Stream**

HTTPS stream shows the encrypted communication with references to google PKI and reallyfreegeoip.org.

A screenshot of a computer program

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.Appendix 11: HTTPS Packet Analysis - C2 Connection**

api.telegram has verified connection to 10.9.17.101 binding via port 443

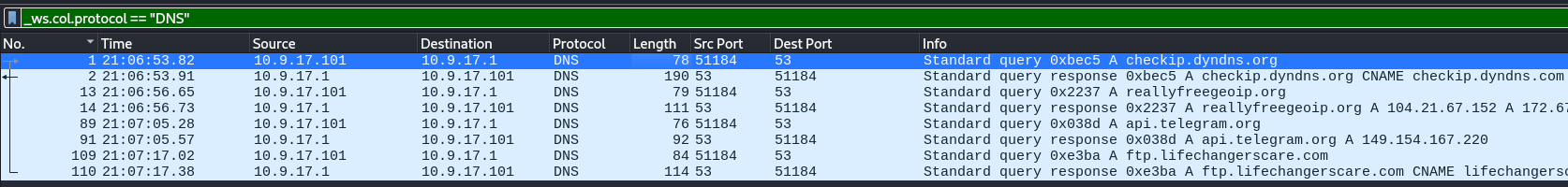
**Appendix 12: HTTPS C2 Connection TCP Stream**

GoDaddy encryption certificate used for api.telegram

A screenshot of a computer

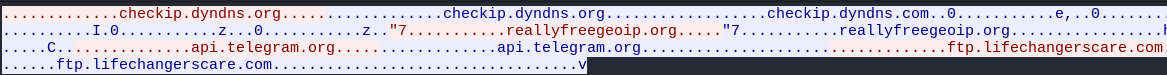
AI-generated content may be incorrect.

**Appendix 13: DNS Packets**

Domains and sub domains requested by 10.9.17.101.

**Appendix 14: DNS UDP Stream**

A further look into the DNS stream shows the multiple IPs referenced in frame 14 are associated with Oracle Cloud who own DynDNS.



**Appendix 15: FTP Packets**

A screenshot of a computer

AI-generated content may be incorrect.Establishing FTP connection from 10.9.17.101 to 216.252.233.118 (lifechangerscare.com). Consisting of 21 packets (2.3% of total capture)

**Appendix 16: FTP TCP Stream**

A screenshot of a computer screen

AI-generated content may be incorrect.Following FTP stream in ASCII format. Cookie and Credential txt files being transferred. Passive mode may be used to circumvent firewall rules to maintain connection.

**Appendix 17: FTP – DATA Packets**

A screenshot of a computer

AI-generated content may be incorrect.A large amount of data relating to cookie and credentials is being collected and transferred to 216.252.233.118. 355 packets (39,6% of total capture). Credentials are collected in a single frame, however the cookie file is updated constantly with each frame being incomplete when reviewing the line based data.

**Appendix 18: FTP – DATA TCP Stream**

Following FTP stream in ASCII format shows 10.9.17.101 exposed by device and location with recovered credentials from various sites. See Appendix for full list.

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 19: Collected Files**

These are all the files contained in the PCAP with the associated host. The last two hold cookie and credential information with cookies holding a majority of that data,

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 20: Stolen Credentials File**

Opened txt file shows stolen site credentials including email with a signature “VIP Recovery”

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 21: Stolen Cookies File**

Opened txt file shows stolen cookies from sites with a signature “VIP Recovery”

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 22: Virus Total Inspection**

Searching for 216.252.233.118 we find that the malware associated with the domain are commonly classified as be trojans as evident by the fake pdf files. A common executable listed is Hesaphareketi-01.exe.

phareketi-01.exeA screenshot of a computer

AI-generated content may be incorrect.

**Appendix 23: Hesaphareketi-01.exe Malware inspection**

A screenshot of a computer

AI-generated content may be incorrect.Delving deeper into Hesaphareketi-01.exe confirms trojans, phishing but also two spyware hits specifically related to a snake key logger by Malwarebytes and Ikarus

**Appendix 24: Related IOC’s and Executables**

We also find a related entity called 2024-09-17-malware-zip-archive.zip which match many of the domains contacted within the current investigation.

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 25: Bundled Files**

Hesaphareketi-01.exe has been identified as a malicious executable associated with multiple keylogging malware families, including VIPKeylogger, SnakeKeylogger. A reference to “VIP Recovery” within the txt files.

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 26: Snake Keylogger Reverse Engineering by Splunk**

Splunk research paper dissecting the code and along with MITRE ATT&CK techniques used. From what is described, and corroborated from multiple sources the Snake Keylogger is a credential stealer that appeared in 2020. A “VIP Recovery” variant was discovered on 16/09/2024 that used SMTP. The one we are dealing with looks to be another variant that uses FTP instead found on the 17/09/2024.

A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 27: AlienVault OTX – lifechangerscare.com**

We get some more information regarding the potential sender address from this attack.

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

**Appendix 28: Compromised Credentials**

Password information has been redacted.

Recovered From: Outlook

URL: mx.win11rulez.academy

E-Mail: win11user1@win11rulez.academy

Recovered From: Edge Chromium

Host: https://funtime.tv/

USR: win11user123

---------------------------------

Recovered From: Edge Chromium

Host: https://sillysite.ai/

USR: win11user123

---------------------------------

Recovered From: Edge Chromium

Host: https://win11fanatic.com/

USR: win11user123

---------------------------------

**Appendix 29: Extracted Hosts that have compromised cookies**

|  |  |  |
| --- | --- | --- |
| .1rx.io | .casalemedia.com | .hogville.net |
| .33across.com | .cbsnews.com | .hybrid.ai |
| .360yield.com | .ccgateway.net | .ib.mookie1.com |
| .3lift.com | .cdn.dxkulture.com | .id5-sync.com |
| .507b28fb-2ef1-4c34-8bda-ba32030bb199.prmutv.co | .cdnwidget.com | .im-apps.net |
| .5d79bce7-5d2b-427e-a6c4-b89b6c7bf048.prmutv.co | .civicscience.com | .impact-ad.jp |
| .a-mo.net | .clarity.ms | .imrworldwide.com |
| .a-mx.com | .cleveland19.com | .imtwjwoasak.com |
| .a.usbrowserspeed.com | .clickagy.com | .in.treasuredata.com |
| .a55a84b3-9632-4869-b625-3d8ef43ed18d.prmutv.co | .clientgear.com | .indeed.com |
| .abc.co.uk | .clinch.co | .independent.co.uk |
| .abc.com | .cm.lotlinx.com | .infolinks.com |
| .abcnews.go.com | .cnbc.com | .inmobi.com |
| .ad-stir.com | .cnn.com | .innovid.com |
| .ad.gt | .cnn.io | .insightexpressai.com |
| .addthis.com | .colossusssp.com | .instagram.com |
| .adentifi.com | .company-target.com | .intentiq.com |
| .adfarm1.adition.com | .connatix.com | .ipredictive.com |
| .adform.net | .connexity.net | .ispot.tv |
| .adgrx.com | .contextweb.com | .jivox.com |
| .adhaven.com | .cootlogix.com | .jsrdn.com |
| .adingo.jp | .cpx.to | .kargo.com |
| .adkernel.com | .creative-serving.com | .kark.com |
| .admanmedia.com | .creativecdn.com | .kiro7.com |
| .admixer.net | .criteo.com | .knotch.it |
| .adnxs.com | .crwdcntrl.net | .krushmedia.com |
| .adotmob.com | .csync.loopme.me | .kueezrtb.com |
| .adrta.com | .ctnsnet.com | .ladsp.com |
| .ads.avads.net | .cxense.com | .liadm.com |
| .ads.pubmatic.com | .d6691a17-6fdb-4d26-85d6-b3dd27f55f08.prmutv.co | .lijit.com |
| .ads.stickyadstv.com | .deepintent.com | .linkedin.com |
| .ads.yieldmo.com | .demdex.net | .linksynergy.com |
| .adsby.bidtheatre.com | .democratandchronicle.com | .lunamedia.live |
| .adsrvr.org | .dianomi.com | .marketiq.com |
| .adstanding.com | .digger.com | .mathtag.com |
| .adventori.com | .disqus.com | .media.net |
| .advertising.com | .dlx.addthis.com | .media6degrees.com |
| .adx.opera.com | .dmp.3lift.com | .mediago.io |
| .agkn.com | .dnacdn.net | .mediawallahscript.com |
| .aidemsrv.com | .dotmetrics.net | .mfadsrvr.com |
| .ainews.com | .dotomi.com | .mgid.com |
| .alcmpn.com | .doubleclick.net | .mgm.demdex.net |
| .amazon-adsystem.com | .dpm.demdex.net | .microsoft.com |
| .analytics.yahoo.com | .dxkulture.com | .minutemedia-prebid.com |
| .aniview.com | .e-planning.net | .ml314.com |
| .apnews.com | .e488cdb0-e7cb-4d91-9648-60d437d8e491.prmutv.co | .mookie1.com |
| .apolloprogram.io | .edgeservices.bing.com | .mountain.com |
| .app.link | .eloqua.com | .msn.com |
| .aralego.com | .emxdgt.com | .mxptint.net |
| .audrte.com | .eqads.com | .myaccount.nytimes.com |
| .betweendigital.com | .et.nytimes.com | .nbcnews.com |
| .bfmio.com | .everesttech.net | .nbcu.demdex.net |
| .bidr.io | .ex.co | .news.google.com |
| .bidswitch.net | .exelator.com | .newscgp.com |
| .bing.com | .extremereach.io | .newsmemory.com |
| .blismedia.com | .eyeota.net | .nr-data.net |
| .bluecava.com | .flashtalking.com | .nrich.ai |
| .bluekai.com | .foxnews.com | .nytimes.com |
| .bounceexchange.com | .france24.com | .omnitagjs.com |
| .brand-display.com | .fwmrm.net | .onaudience.com |
| .brandmetrics.com | .getpublica.com | .onetag-sys.com |
| .brightcove.net | .gm.demdex.net | .openx.net |
| .bttrack.com | .go.com | .ortb.net |
| .bumlam.com | .go.sonobi.com | .outbrain.com |
| .c.appier.net | .gobankingrates.com | .ow.pubmatic.com |
| .c.bing.com | .google.com | .owneriq.net |
| .c.msn.com | .googleadservices.com | .p.flipp.com |
| .c1.microsoft.com | .googlesyndication.com |  |
| .c3tag.com | .gumgum.com |  |

|  |  |  |
| --- | --- | --- |
| .pbs.yahoo.com | .teads.tv | blue.thehill.com |
| .piano.io | .tealiumiq.com | bob.dmpxs.com |
| .pippio.com | .technoratimedia.com | business.bing.com |
| .placed.com | .the-ozone-project.com | cdn.gsght.com |
| .pointmediatracker.com | .thehill.com | cm.mgid.com |
| .politico.com | .thenew4ever.com | collector.cdp.cnn.com |
| .politico.eu | .thrtle.com | edgeservices.bing.com |
| .postrelease.com | .thv11.com | edigitalsurvey.com |
| .prebid.a-mo.net | .tpmn.co.kr | elb.the-ozone-project.com |
| .primis.tech | .tpmn.io | gsght.com |
| .pro-market.net | .travelaudience.com | gtrace.mediago.io |
| .proper.io | .traversedlp.com | hogville.net |
| .pub.network | .tremorhub.com | i.liadm.com |
| .pubmatic.com | .tribalfusion.com | io.narrative.io |
| .pxdrop.lijit.com | .trkn.us | krk2.kargo.com |
| .pxl.iqm.com | .truoptik.com | learn.microsoft.com |
| .quantserve.com | .turn.com | live.rezync.com |
| .realestate.com.au | .tvpixel.com | m.stripe.com |
| .resetdigital.co | .twitter.com | news.google.com |
| .reson8.com | .tynt.com | nexstar.blueconic.net |
| .reuters.com | .udmserve.net | ntp.msn.com |
| .rezync.com | .undertone.com | openrtb-us-east-1.axonix.com |
| .rfi.fr | .upi.com | pbs.at.cbsi.com |
| .rfihub.com | .us7-bcdn.newsmemory.com | pbs.nextmillmedia.com |
| .richaudience.com | .usatoday.com | pix.cdnwidget.com |
| .rkdms.com | .usatodayspecial-va.newsmemory.com | pixel.mtrcs.samba.tv |
| .rlcdn.com | .w55c.net | pool.admedo.com |
| .rmp.rakuten.com | .warnermediacdn.com | prebid-s2s.media.net |
| .rqtrk.eu | .washingtonpost.com | prebid.media.net |
| .rtb.mx | .wayfair.com | s2s.t13.io |
| .rtbsystem.com | .weather.com | s2s.yieldlove-ad-serving.net |
| .rubiconproject.com | .wpsdlocal6.com | static.foxnews.com |
| .s3xified.com | .wsj.com | sync.aniview.com |
| .samplicio.us | .wsod.com | sync.srv.stackadapt.com |
| .schwab.com | .www.abc.com | thehill.com |
| .scorecardresearch.com | .www.cnbc.com | tl.foxnews.com |
| .semasio.net | .www.cnn.com | tracking.lifestylejournal.com |
| .servedbyadbutler.com | .www.digger.com | trc.taboola.com |
| .server.cpmstar.com | .www.kark.com | user.democratandchronicle.com |
| .serverbid.com | .www.linkedin.com | vpb-server.jwplayer.com |
| .sharethis.com | .www.nytimes.com | weather.com |
| .sharethrough.com | .www.politico.com | widgets.outbrain.com |
| .simpli.fi | .www.thv11.com | www.abc.com |
| .sitescout.com | .www.ugdturner.com | www.cbsnews.com |
| .smaato.net | .yahoo.co.jp | www.clarity.ms |
| .smadex.com | .yahoo.com | www.cleveland19.com |
| .smartadserver.com | .yellowblue.io | www.cnbc.com |
| .snapchat.com | .yieldmo.com | www.cnn.com |
| .socdm.com | .yieldoptimizer.com | www.democratandchronicle.com |
| .sportradarserving.com | .ymmobi.com | www.foxnews.com |
| .spot.im | .youtube.com | www.france24.com |
| .spotim.market | .zemanta.com | www.google.com |
| .springserve.com | .zeotap.com | www.independent.co.uk |
| .srv.stackadapt.com | a.clickcertain.com | www.kark.com |
| .ssp.wknd.ai | a.nytimes.com | www.kiro7.com |
| .storygize.net | a.remarketstats.com | www.microsoft.com |
| .subaruofamerica.demdex.net | abcnews.go.com | www.nbcnews.com |
| .sundaysky.com | ads.brandcdn.com | www.politico.com |
| .suntcontent.se | ads.resetsrv.com | www.reuters.com |
| .surveywall-api.survata.com | ads.travelaudience.com | www.rfi.fr |
| .sxp.smartclip.net | adservices.brandcdn.com | www.thenew4ever.com |
| .sync.inmobi.com | aorta.clickagy.com | www.thv11.com |
| .t.co | ap.blueconic.net | www.ultptrk.com |
| .taboola.com | apcdp.ainews.com | www.usatoday.com |
| .taboolamedia.com | apnews.com | www.wpsdlocal6.com |
| .tagger.opecloud.com | assets.msn.com | www.wsj.com |
| .tapad.com | beacon.lynx.cognitivlabs.com | xproxy.api.abc.com |
| .taptapnetworks.com | bh.contextweb.com |  |
| .targeting.unrulymedia.com | blue.kark.com |  |