WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

DNS Insights behind the JumpCloud Supply Chain Attack

Table of Contents

Executive Report

Even solutions meant to enhance security can sometimes fall prey to the best cyber attackers. That's what happened to JumpCloud, a cloud-based directory service platform designed to centralize and simplify identity access management (IAM).

SentinelOne researchers analyzed the supply chain attacks and published 32 JumpCloud attack indicators of compromise (IoCs). WhoisXML API, in an effort to identify additional artifacts, if any, performed an IoC list expansion that uncovered:

- 145 domains that shared some of the dedicated IP hosts identified as IoCs, one of which has been dubbed malicious based on a bulk malware check
- 392 domains that contained the strings **centos**, **datadog**, and **zscaler** akin to some of the domains identified as IoCs

JumpCloud Supply Chain Attack IoC Facts

The SentinelOne JumpCloud supply chain attack analysis identified 13 domains and 19 IP addresses as IoCs.

As a first step, we subjected the 13 domains to a bulk WHOIS lookup, which revealed that:

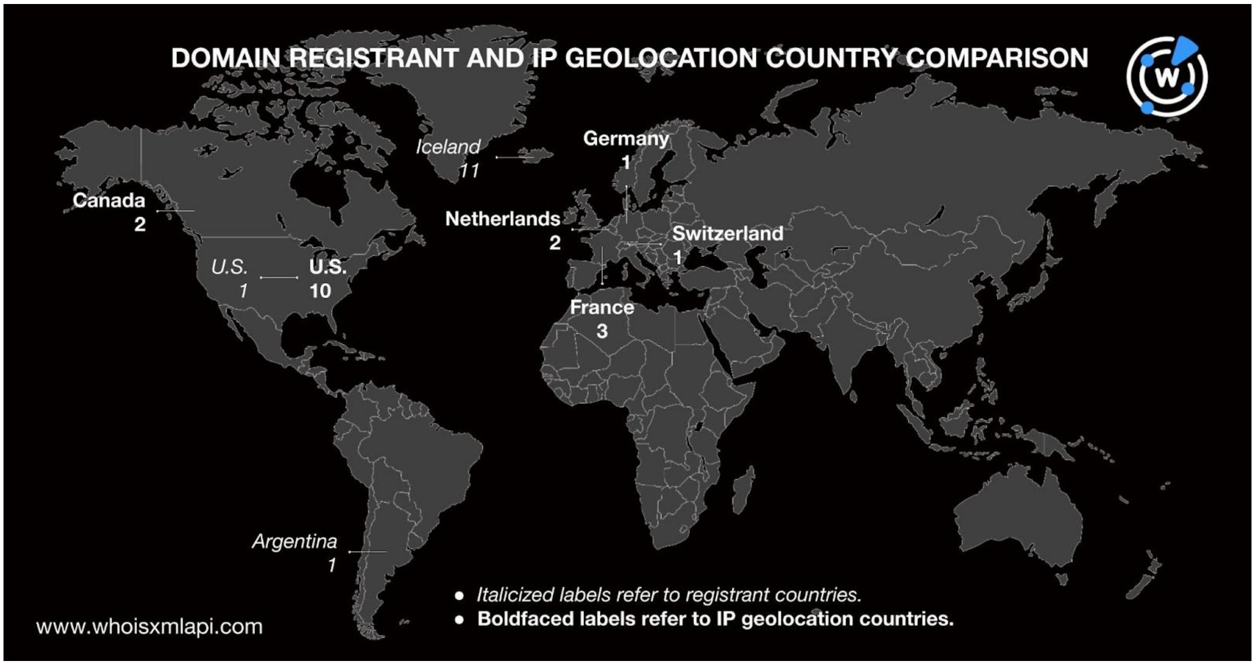
- The IoCs were distributed among three registrars. A majority of them, 11 domains to be exact, were administered by Namecheap. LaunchPad and PDR accounted for one IoC each.
- A majority of the domains were relatively new, as 11 of them were created just this year. The remaining two were a little older, created in 2019 and 2020.
- The domains identified as IoCs were registered in three countries—11 in Iceland and one each in Argentina and the U.S.

It’s also interesting to note that the website categorization lookup results for the domains identified as IoCs classified all 13 as malware sites.

Next, we performed a bulk IP geolocation lookup for the 19 IP addresses identified as IoCs and found that:

- The IoCs were spread across six geolocation countries led by the U.S., which accounted for 10 countries. France came in second, accounting for three IP addresses. Canada and the Netherlands rounded out the top 3, each accounting for two IoCs each.
- Four of the IP addresses were administered by OVH SAS. Fifteen ISPs—Amazon, ColoCrossing, DataCamp, DediPath, Hetzner, Hivelocity, M247, Network Solutions, Private Layer, QuadraNet, Sharktech, Sollutium, The Constant Company, The Optimal Link Corporation, and Unified Layers—managed one IoC each.

The following image compares the domain registrant and IP geolocation countries of the IoCs. Only the U.S. consistently appeared as a registrant and IP geolocation country although the number of IP addresses and domains didn’t match.


DOMAIN REGISTRANT AND IP GEOLOCATION COUNTRY COMPARISON
Iceland 11
Germany 1
Canada 2
Netherlands 2
Switzerland 1
U.S. 1
U.S. 10
France 3
Argentina 1
• Italicized labels refer to registrant countries.
• Boldfaced labels refer to IP geolocation countries.
www.whoisxmlapi.com

JumpCloud Supply Chain Attack IoC List Expansion Findings

We began our DNS deep dive with DNS lookups, which showed that only two of the domains identified as IoCs continued to resolve to one IP address each—toyourownbeat[.]com to

192[.]185[.]5[.]189 and primerosauxiliosperu[.]com to 162[.]241[.]248[.]14. These IP resolutions, however, were already part of SentinelOne’s IoC list.

Next, reverse IP lookups for the 19 IP addresses identified as IoCs revealed that eight of them were dedicated hosts, one was possibly dedicated, and another one was shared. Three didn’t have active resolutions.

Our search also showed that the nine dedicated and possibly dedicated IP hosts were shared by 145 other domains. One of them, now unreachable—npmaudit[.]com—was classified a malware host by a bulk malware check.

A closer look at the domains identified as IoCs allowed us to identify three unique strings—**centos**, **datadog**, and **zscaler**—that coincided with popular brand names shown in the table below.

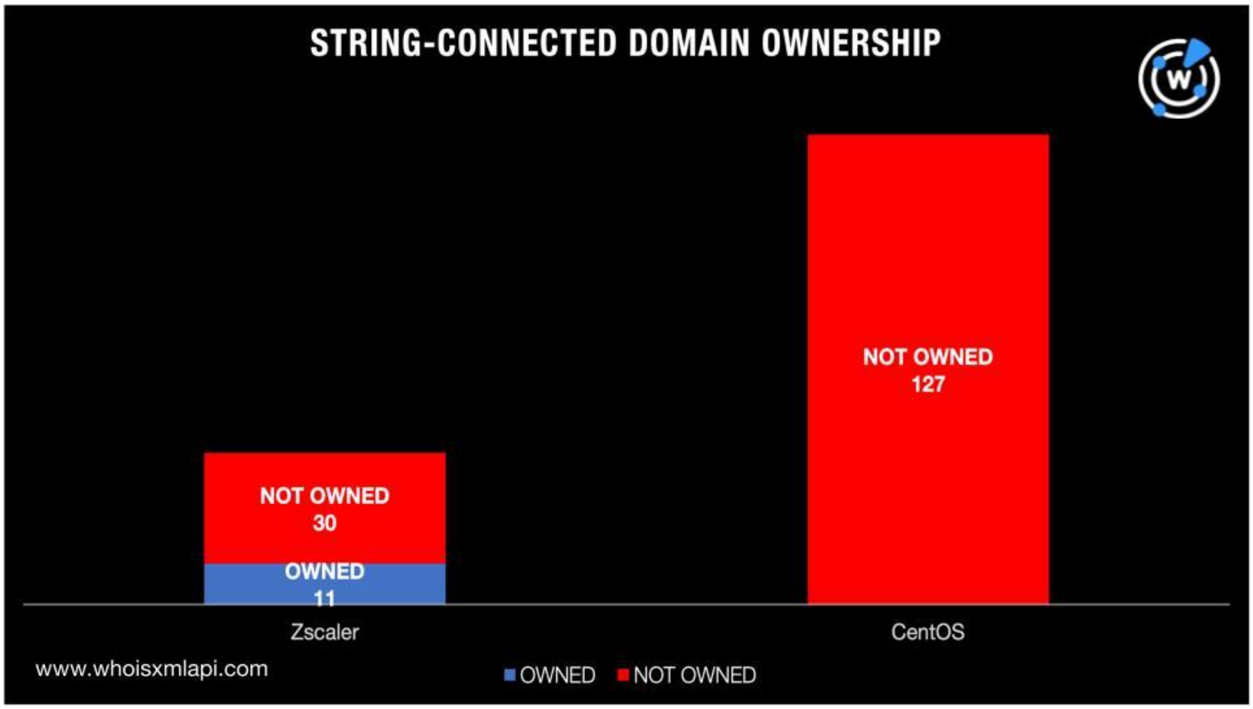
STRING	ASSOCIATED BRAND	DESCRIPTION
centos	CentOS	CentOS is a discontinued free, open-source, and community-supported Linux computing platform functionally compatible with its upstream source—Red Hat Enterprise Linux.
datadog	Datadog	Datadog is an observability service for cloud-scale applications that enables server, database, tool, and service monitoring via a SaaS-based data analytics platform.
zscaler	Zscaler	Zscaler is a cloud security company headquartered in San Jose, California that offers enterprise cloud security services.

We used the above-mentioned strings as Domains & Subdomains Discovery search terms that led to the discovery of 392 domains.

While none of them were categorized as malicious after being subjected to a bulk malware check, many of them couldn't be publicly attributed to the companies. We used the WHOIS record data points in the table below to determine domain ownership. Note that since Datadog's WHOIS record didn't indicate any readily identifiable WHOIS data point, we couldn't make accurate record comparisons for it to determine brand-containing domain ownership.

STRING	COMPANY	OFFICIAL DOMAIN NAME	WHOIS RECORD DETAIL
centos	CentOS	centos[.]org	**Registrant organization:** Red Hat, Inc.
zscaler	Zscaler	zscaler[.]com	**Registrant organization:** Zscaler, Inc.

Our bulk WHOIS lookup and record comparison with the brand name owners' official websites showed that 93% didn't share the same WHOIS record data points, making them publicly unattributable to two of the legitimate companies left on our list. Many of the brand-containing domains could be owned by potential cybersquatters or even cyber attackers waiting for a chance to weaponize them.



—

Our IoC list expansion analysis for the JumpCloud supply chain attacks found that their perpetrators could have 145 IP-connected domains they could weaponize for future campaigns. It also revealed that threat actors could potentially utilize 189 look-alike domains for attacks zooming in on CentOS, Datadog, and Zscaler users or the solution developers themselves, especially since 93% of the **centos**- and **zscaler**-containing domains couldn't be publicly attributed to the solutions developers.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts and IoCs

IoCs SentinelOne Researchers Identified

IP ADDRESS	DOMAIN
51[.]254[.]24[.]19	nomadpkgs[.]com
185[.]152[.]67[.]39	centos-repos[.]org
70[.]39[.]103[.]3	datadog-cloud[.]com
66[.]187[.]75[.]186	toyourownbeat[.]com
104[.]223[.]86[.]8	datadog-graph[.]com
100[.]21[.]104[.]112	centos-pkg[.]org
23[.]95[.]182[.]5	primerosauxiliosperu[.]com
78[.]141[.]223[.]50	zscaler-api[.]org
116[.]202[.]251[.]38	nomadpkg[.]com

89[.]44[.]9[.]202	launchruse[.]com
192[.]185[.]5[.]189	reggedrobin[.]com
162[.]241[.]248[.]14	canolagroove[.]com
179[.]43[.]151[.]196	alwaysckain[.]com
45[.]82[.]250[.]186	
162[.]19[.]3[.]23	
144[.]217[.]92[.]197	
23[.]29[.]115[.]171	
167[.]114[.]188[.]40	
91[.]234[.]199[.]179	

Sample Domains That Shared the Dedicated IP Hosts of Some Domains Identified as IoCs

- astutetrader[.]com
- bhojpuriboys[.]com
- blitzk[.]com
- boqchah[.]com
- brandturbo[.]net
- brookdaleparkdogpark[.]com
- bubaexpress[.]com
- calcsite[.]com
- careerkickinthepants[.]com
- cateringbyteatime[.]com
- chrisking[.]info
- club4x4[.]org[.]au
- comsynmed[.]com
- consultop[.]net
- cookperiodontics[.]com
- cppivmusic[.]com
- cubcakes[.]com
- cybergayani[.]com
- darkhorsestrategies[.]org
- darlingdazzles[.]com
- diabetesdietitian[.]com
- dirtywindshield[.]com
- doubledistortion[.]com
- drawingbydesign[.]net
- electricalinnovationsny[.]com
- evandale[.]info
- glendaleind[.]ca
- glitchguide[.]com
- gracietorres[.]com
- javagroove[.]net
- kpit[.]me
- labashanimation[.]com
- languageadventure[.]net
- lashon[.]net
- lawrenceahoffman[.]com
- leanarticles[.]com
- logisticslist[.]com
- louistorres[.]com
- luxurylimos[.]co[.]nz
- mail[.]astutetrader[.]com

- mail[.]bhojpuriboys[.]com
- mail[.]boqchah[.]com
- mail[.]careerkickinthepants[.]com
- mail[.]comsynmed[.]com
- mail[.]cppivmusic[.]com
- mail[.]cybergayani[.]com
- mail[.]darlingdazzles[.]com
- mail[.]dirtywindshield[.]com
- mail[.]doubledistortion[.]com
- mail[.]drawingbydesign[.]net

Sample Domains That Contained the Strings *centos*, *datadog*, and *zscaler* akin to Some of the Domains Identified as IoCs

- centostar[.]top
- centos777[.]fit
- centos65[.]svn-repos[.]de
- centos1[.]cust[.]dev[.]thingdust[.]io
- centos7[.]paas[.]hosted-by-previder[.]com
- centos-2[.]googlecode[.]com
- centos-test[.]eu[.]meteorapp[.]com
- centos-2[.]website[.]yandexcloud[.]net
- centos777[.]chat
- centosredhat[.]spb[.]ru
- centos63[.]fastly-terrarium[.]com
- centos01[.]ws
- centostar[.]net[.]ng
- centos-2[.]community-pro[.]de
- centosupdates[.]ph
- datadog[.]jpn[.]com
- datadog-agent-qt25[.]onrender[.]com
- datadog-functionapp-tfnsw-ana-ipanalytics-prod[.]azurewebsites[.]net
- datadogshed[.]com
- datadog[.]gotpantheon[.]com
- datadogshq[.]com
- datadog-cloud[.]com
- datadog-agent-pr-979-q090[.]onrender[.]com
- datadog-agent-apfh[.]onrender[.]com
- datadog[.]fin[.]ci
- datadog-agent-staging-m5qg[.]onrender[.]com
- datadog-agent-qqbo[.]onrender[.]com
- datadog-pr-1097[.]onrender[.]com
- datadog-agent-staging-8dcz[.]onrender[.]com
- datadogstore[.]com
- zscalerip[.]io
- zscalerdemosite[.]com
- zscalerbeta[.]vip
- zscalerrecipeforsuccess[.]co[.]uk
- zscalercopilot[.]com
- zscaler-developer-sales[.]live
- zscalermail[.]com
- zscalergscm[.]com
- zscalertwo[.]online
- zscalerpresidentsclub[.]com
- zscaler1[.]co[.]de
- zscalergscm[.]net
- zscalerdrtest[.]pages[.]dev
- zscaler[.]kom
- zscalerzscm[.]org
- zscalerrisk[.]net
- zscalerzscm[.]net
- zscalercareers[.]cloud
- zscalerinfra[.]com
- zscaler-events[.]co[.]de