JumpCloudサプライチェーン攻撃の痕跡をDNSで発見

目次

要旨

セキュリティ強化を目的としたソリューションであっても、時としてサイバー攻撃者の餌食になることがあります。それが、Identity Access Management （IAM）を一元化・簡素化するために設計されたクラウドベースのディレクトリサービス「JumpCloud」に起こったことです。

SentinelOneの研究者は先般、JumpCloudのサプライチェーン攻撃を分析し、攻撃に関与した32個のセキュリティ侵害インジケーター（IoC）を公開しました。これを受け、WhoisXML APIでは、さらなるアーティファクトを特定するためにそのIoCリストの拡張を試みました。その結果、以下を発見しました。

- IoCとして特定された専用IPホストの一部を共用する145個のドメイン名。そのうちの1個はマルウェアの一括チェックにより悪意あるドメイン名と判明
- IoCとして特定された一部のドメイン名と同様に**centos**、**datadog**または**zscaler**という文字列を含む392個のドメイン名

JumpCloudサプライチェーン攻撃のIoC

SentinelOneによるJumpCloudサプライチェーン攻撃の分析では、13個のドメイン名と19個のIPアドレスがIoCとして特定されました。当社ではまず、その13個のドメイン名をBulk WHOIS Lookupで検索しました。そして、以下を検出しました。

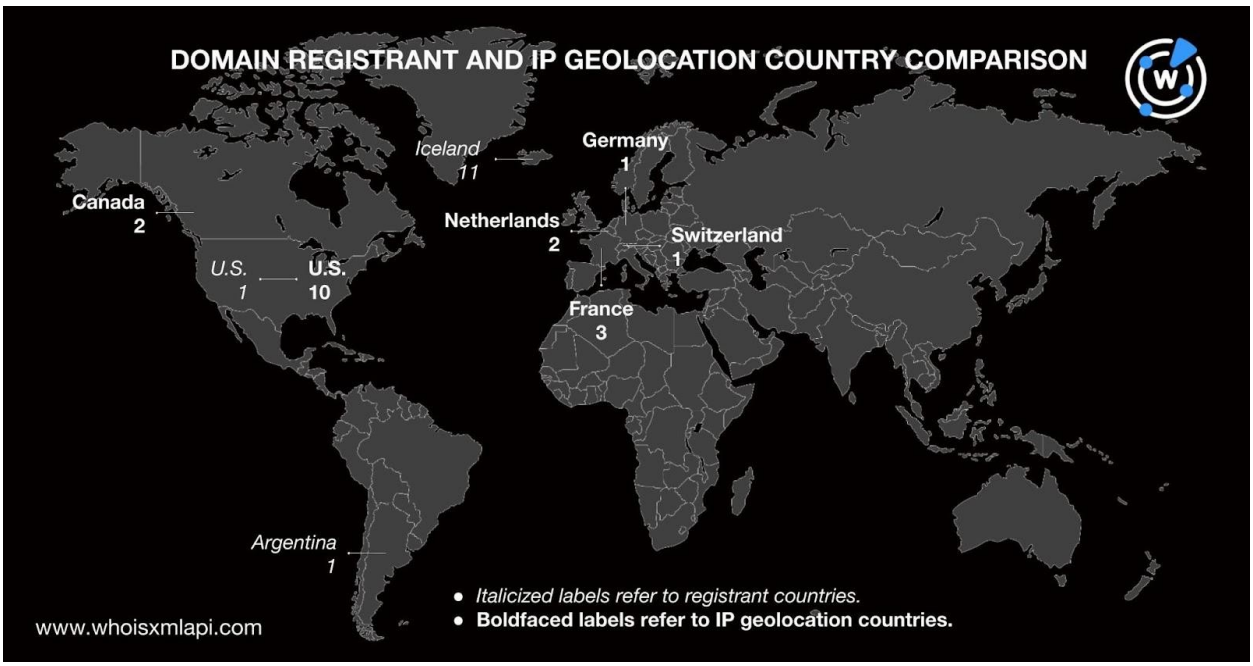
- IoCのドメイン名の管理レジストラ3社。Namecheapが11個、LaunchPadとPDRがそれぞれ1個のドメイン名を管理。
- 13個のうち11個は今年に入って新規登録されたドメイン名。残りの2つはそれぞれ2019年と2020年に登録。
- 11個のドメイン名はアイスランドで登録。アルゼンチン、米国でそれぞれ1個登録。

また、IoCのドメイン名13個をWebsite Categorization Lookupにかけたところ、その全てがマルウェアサイトに分類されました。

次に、IoCとして特定された19個のIPアドレスをBulk IP Geolocation Lookupで検索しました。その結果、以下が明らかになりました。

- ジオロケーションは6カ国に分散。最多の10個が米国に位置。次に多かったのは3個が位置していたフランス。これに、2個ずつ位置していたカナダとオランダが続く。
- OVH SASが最多の4アドレスを管理。その他、15社のISP（Amazon、ColoCrossing、DataCamp, DediPath、Hetzner、Hivelocity、M247、Network Solutions、Private Layer、QuadraNet、Sharktech、Sollutium、The Constant Company、The Optimal Link CorporationおよびUnified Layers）がそれぞれ1個を管理。

以下は、IoCのドメイン名登録者およびIPアドレスのジオロケーションを地図上で示したものです。ドメイン名登録者とIPアドレスの両方の所在国として挙がっているのは米国のみです。



JumpCloudサプライチェーン攻撃IoCリストの拡張

DNS Lookupを使ってDNSをさらに深掘りしたところ、IoCとして特定されたドメイン名のうち2個（oyourownbeat[.]comとprimerosauxiliosperu[.]com）が、それぞれ1個のIPアドレス（192[.]185[.]5[.]189と162[.]241[.]248[.]14）に名前解決しました。なお、この2つのIPアドレスは、すでにSentinelOneのIoCリストに含まれています。

次に、IoCとされた19個のIPアドレスをReverse IP Lookupで検索しました。その結果、8個は専用ホスト、1個はおそらく専用ホスト、1個は共用ホストであることがわかりました。また、3個はドメイン名と関連づけられていませんでした。

専用およびおそらく専用と分類された合計9個のIPアドレスは、145個の別のドメイン名に共用されていました。そのうちの1個で、現在は到達不能となっているnpmaudit[.]comは、一括マルウェアチェックでマルウェアホストに分類されました。

IoCとして特定されたドメイン名さらに見ていくと、下表のように、人気ブランド名に対応した**centos**、**datadog**、**zscaler**という固有の文字列が浮かび上がってきました。

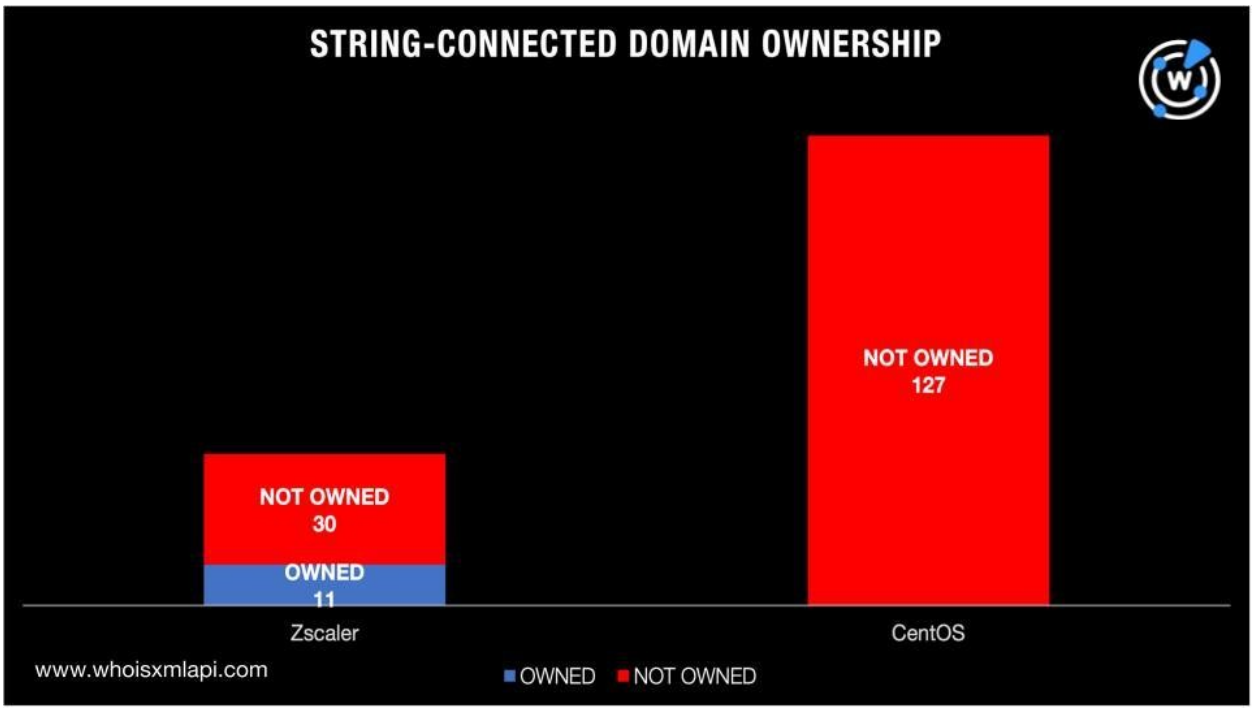
文字列	関連ブランド	概要
centos	CentOS	CentOS は、Red Hat Enterprise Linuxと互換性のある、無料、オープンソースのLinux コンピューティングプラットフォーム。現在は提供されていない。
datadog	Datadog	Datadogは、SaaS型データ分析プラットフォームを介してサーバー、データベース、ツールおよびサービスを監視するクラウドアプリケーション向けのモニタリングサービス。
zscaler	Zscaler	Zscalerは、カリフォルニア州サンノゼを本拠とするクラウドベースのセキュリティサービス。

上記の3つの文字列をキーワードとしてDomains & Subdomains Discoveryで検索したところ、392個のドメイン名がマッチしました。

それらを一括マルウェアチェックにかけたところ、悪意があると分類されたドメイン名はありませんでした。しかし、その多くは、CentOS、DatadogまたはZscalerへの帰属を公開情報から確認できませんでした。以下の表は、WHOISレコードの情報からドメイン名の所有者を確認した結果です。なお、Datadogについては、WHOISレコードに識別可能な情報が含まれておらず、ドメイン名の所有者を特定できませんでした。

文字列	会社名	公式ドメイン名	WHOISレコード
centos	CentOS	centos[.]org	**Registrant organization:** Red Hat, Inc.
zscaler	Zscaler	zscaler[.]com	**Registrant organization:** Zscaler, Inc.

今回Domains & Subdomains Discoveryで検出したドメイン名をWHOIS一括検索にかけ、ブランド所有者の公式ドメイン名のレコードと比較したところ、93%のWHOISレコードは公式ドメイン名のそれと一致せず、CentOSおよびZscalerと無関係であることがわかりました。こうしたブランドを含むドメイン名の多くは、サイバースクワッターまたはサイバー攻撃者が悪用目的で所有している可能性があります。



—

JumpCloudサプライチェーン攻撃のIoCリスト拡張分析では、特定のIPアドレスを共用する145個のドメイン名が犯人によって所有されている可能性があることがわかりました。それらのドメイン名は、今後悪用されるかもしれません。また、CentOS、DatadogおよびZscalerのユーザーまたはソリューション開発者を標的とした攻撃のために、見た目の似た189個のドメインを脅威アクターが利用する可能性があることも明らかになりました。そして、**centos**または**zscaler**という文字列を含むドメイン名の93%は、各ソリューション提供者への帰属を確認できませんでした。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項：*当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

SentinelOneが特定したIoC

IPアドレス	ドメイン名
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	

一部のIoCドメイン名のIPホストを共用していたドメイン名の例

- 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

一部のIoCドメイン名と同様にcentos、datadog、zscalerを含むドメイン名の例

- 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