サプライチェーンのセキュリティ：IconBurstとMaterial Tailwindの攻撃に迫る

目次

要旨

2023年1月初め、ReversingLabsがソフトウェアサプライチェーンにおけるセキュリティの現状に関する調査のレポートを公表しました。レポートでは、npmとPyPIのコードを使った攻撃が過去4年間で合計289%も増加したと報告されています。また、調査では、エビデンスとして「IconBurst」と「Material Tailwind」という2つのnpm攻撃を取り上げています。

ReversingLabsは、組織、特にnpmやPyPIパッケージのユーザに対してネットワークの安全性を高めるよう促しており、その一環として、IconBurstやMaterial Tailwindといった脅威と関連する疑わしい、悪意あるウェブのプロパティへのアクセスをより適切に検出、ブロックするよう推奨しています。

WhoisXML APIの研究者は、この2つの攻撃について、一般に公開されているIoC（セキュリティ侵害インジケーター）のリストをもとに、調査の水平展開を試みました。そして、WHOIS、IPアドレスおよびDNSの情報を徹底的に調べた結果、以下の発見がありました。

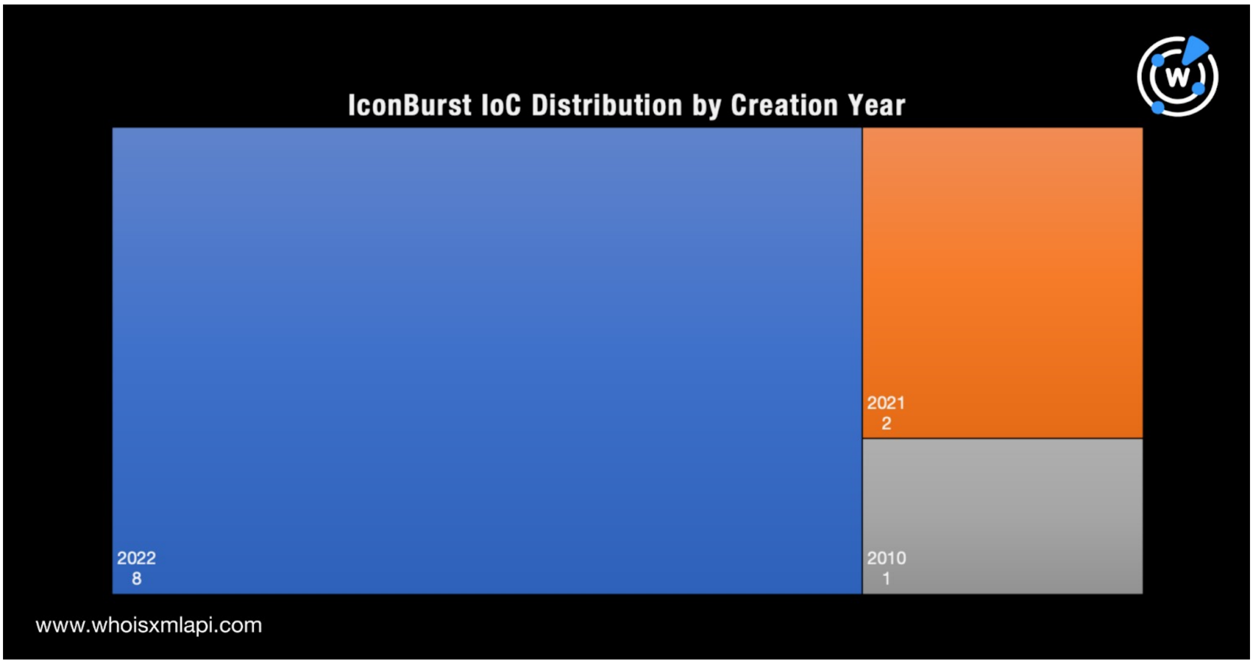
- IoCとして識別されたIconBurstのドメイン名は、15個のIPアドレスに名前解決した。
- 2,401件以上のドメイン名がIconBurstのIoCと同じIPアドレスを使用、そのうち14件のドメイン名は悪意あるものと判定された。
- IconBurstのIoCとされたドメイン名のうち2件については、過去のWHOISレコードに匿名化されていない登録者のメールアドレスが含まれていた。
- 匿名化されていない登録者メールアドレスのうち1つは、別の5件のドメイン名の登録に使用されていた。うち2件のドメイン名は、ReversingLabsの報告書に記載あり。
- Material TailwindのIoCと確認されたIPアドレスのうち1つは、関連する可能性のあるドメイン名を導いた。
- Material TailwindのIoCと見なされたドメインに含まれる「parsee」という文字列が、異なるトップレベルドメイン（TLD）を持つ14のドメイン名で共有されている。

IconBurstのIoCリストをもとに調査を水平展開

IconBurstの攻撃者は、悪意あるnpmモジュールを標的のシステムにインストールし、それらが様々なアプリやウェブサイトから機密データを盗み出すことを可能にします。ReversingLabsでは、以下の13件のドメイン名をIoCとして特定しました。

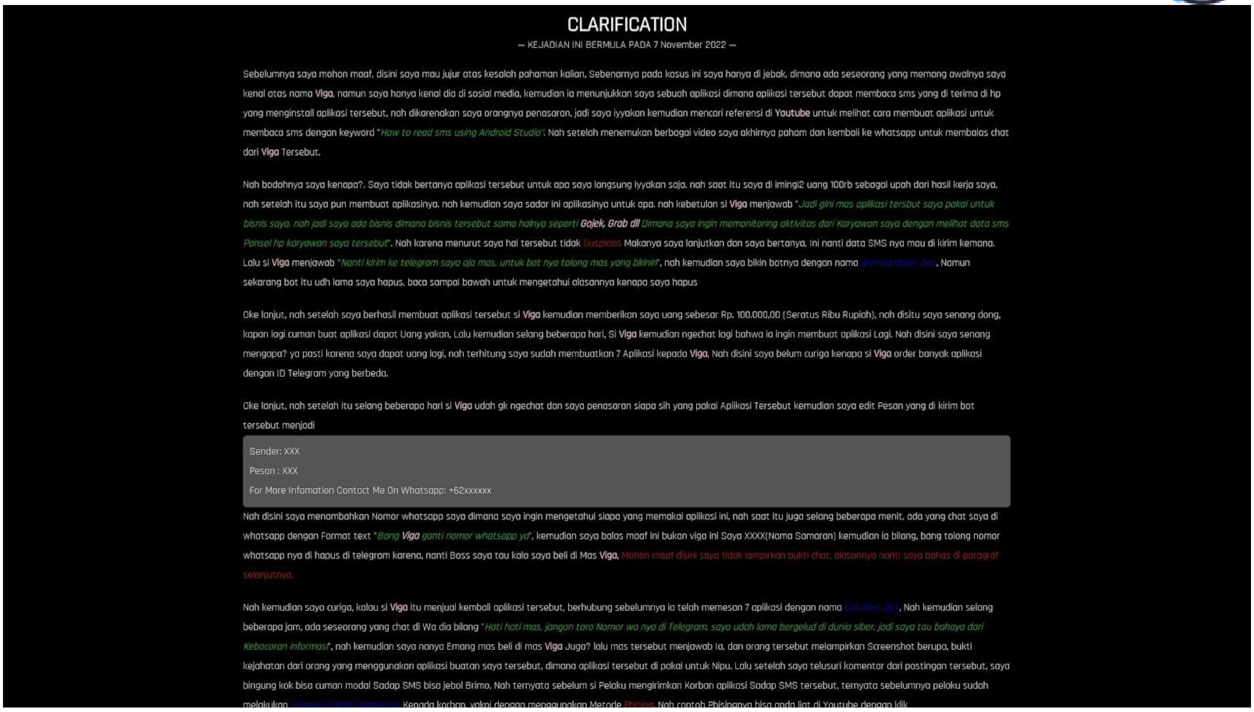
- graph-googleapis[.]com
- ionicio[.]com
- curls[.]safhosting[.]xyz
- arpanrizki[.]my[.]id
- dnster[.]my[.]id
- okep[.]renznesia[.]xyz
- ryucha[.]my[.]id
- panelllgege[.]001www[.]com
- nge[.]scrp[.]my[.]id
- apiii-xyz[.]yogax[.]my[.]id
- panel[.]archodex[.]xyz
- panel[.]curlz[.]online
- api[.]mlbb-x-02[.]ml

これらのドメイン名をまず bulk WHOIS lookup で検索したところ、検索可能な WHOIS レコードを持つドメイン名は 11 件にすぎませんでした。その大部分、8 件は今年に入って新たに登録されたものでした。また、2 件は昨年、1 件は 2010 年に登録されたものです。これらのドメイン名の管理は 8 つのレジストラに分散されています。内訳は、Registrasi Neva Angkasa が 3 件、CV Jogjacamp が 2 件、そして ResellerCamp、WEBCC、Mat Bao Corporation、Web Commerce Communications Ltd.、Hostinger、UAB および Namecheap, Inc.が 1 件ずつです。



登録者の国名が出ていたのは 7 件で、4 件はインドネシア、2 件はマレーシア、1 件はアイスランドでの登録だとわかりました。

当社の screenshot lookup の検索結果では、ionicio[.]com と arpanrizki[.]my[.]id は現在も有効なコンテンツをホストしており、知らないユーザーにはまだリスクがあることを示唆しています。



CLARIFICATION

— KEJADIAN INI BERMULA PADA 7 November 2022 —

Sebelumnya saya mohon maaf, disini saya mau jujur atas kesalah pahaman kalian, Sebenarnya pada kasus ini saya hanya di jebak, dimana ada seseorang yang memang awalnya saya kenal atas nama **Viga**, namun saya hanya kenal dia di sosial media, kemudian ia menunjukkan saya sebuah aplikasi dimana aplikasi tersebut dapat membaca sms yang di terima di hp yang menginstall aplikasi tersebut, nah dikarenakan saya orangnya penasaran, jadi saya iyyakan kemudian mencari referensi di **Youtube** untuk melihat cara membuat aplikasi untuk membaca sms dengan keyword "*How to read sms using Android Studio*", Nah setelah menemukan berbagai video saya akhirnya paham dan kembali ke whatsapp untuk membalas chat dari **Viga** Tersebut.

Nah bodohnya saya kenapa?. Saya tidak bertanya aplikasi tersebut untuk apa saya langsung iyyakan saja. nah saat itu saya di imingi2 uang 100rb sebagai upah dari hasil kerja saya. nah setelah itu saya pun membuat aplikasinya. nah kemudian saya sadar ini aplikasinya untuk apa. nah kebetulan si **Viga** menjawab "*Jadi gini mas aplikasi tersbut saya pakai untuk bisnis saya. nah jadi saya ada bisnis dimana bisnis tersebut sama halnya seperti* ***Gojek, Grab dll*** *Dimana saya ingin memonitoring aktivitas dari Karyawan saya dengan melihat data sms Ponsel hp karyawan saya tersebut*". Nah karena menurut saya hal tersebut tidak Suspicios Makanya saya lanjutkan dan saya bertanya, Ini nanti data SMS nya mau di kirim kemana. Lalu si **Viga** menjawab "*Nanti kirim ke telegram saya aja mas, untuk bot nya tolong mas yang bkinin*", nah kemudian saya bikin botnya dengan nama @smsgrabber_bot, Namun sekarang bot itu udh lama saya hapus, baca sampai bawah untuk mengetahui alasannya kenapa saya hapus

Oke lanjut, nah setelah saya berhasil membuat aplikasi tersebut si **Viga** kemudian memberikan saya uang sebesar Rp. 100.000,00 (Seratus Ribu Rupiah), nah disitu saya senang dong, kapan lagi cuman buat aplikasi dapat Uang yakan, Lalu kemudian selang beberapa hari, Si **Viga** kemudian ngechat lagi bahwa ia ingin membuat aplikasi Lagi. Nah disini saya senang mengapa? ya pasti karena saya dapat uang lagi, nah terhitung saya sudah membuatkan 7 Aplikasi kepada **Viga**, Nah disini saya belum curiga kenapa si **Viga** order banyak aplikasi dengan ID Telegram yang berbeda.

Oke lanjut, nah setelah itu selang beberapa hari si **Viga** udah gk ngechat dan saya penasaran siapa sih yang pakai Aplikasi Tersebut kemudian saya edit Pesan yang di kirim bot tersebut menjadi

Sender: XXX
Pesan : XXX
For More Infomation Contact Me On Whatsapp: +62xxxxxx

Nah disini saya menambahkan Nomor whatsapp saya dimana saya ingin mengetahui siapa yang memakai aplikasi ini, nah saat itu juga selang beberapa menit, ada yang chat saya di whatsapp dengan Format text "*Bang* ***Viga*** *ganti nomor whatsapp ya*", kemudian saya balas maaf ini bukan viga ini Saya XXXX(Nama Samaran) kemudian ia bilang, bang tolong nomor whatsapp nya di hapus di telegram karena, nanti Boss saya tau kalo saya beli di Mas **Viga**, Mohon maaf disini saya tidak lampirkan bukti chat, alasannya nanti saya bahas di paragraf selanjutnya.

Nah kemudian saya curiga, kalau si **Viga** itu menjual kembali aplikasi tersebut, berhubung sebelumnya ia telah memesan 7 aplikasi dengan nama Cek Resi J&T, Nah kemudian selang beberapa jam, ada seseorang yang chat di Wa dia bilang "*Hati hati mas, jangan taro Nomor wa nya di Telegram, saya udah lama bergelud di dunia siber, jadi saya tau bahaya dari Kebocoran informasi*", nah kemudian saya nanya Emang mas beli di mas **Viga** Juga? lalu mas tersebut menjawab Ia, dan orang tersebut melampirkan Screenshot berupa, bukti kejahatan dari orang yang menggunakan aplikasi buatan saya tersebut, dimana aplikasi tersebut di pakai untuk Nipu. Lalu setelah saya telusuri komentar dari postingan tersebut, saya bingung kok bisa cuman modal Sadap SMS bisa jebol Brimo, Nah ternyata sebelum si Pelaku mengirimkan Korban aplikasi Sadap SMS tersebut, ternyata sebelumnya pelaku sudah melakukan Soceng (Social Engineering) Kepada korban, yakni dengan menggunakan Metode Phising, Nah contoh Phisingnya bisa anda liat di Youtube dengan klik

ionicio[.]com のスクリーンショット

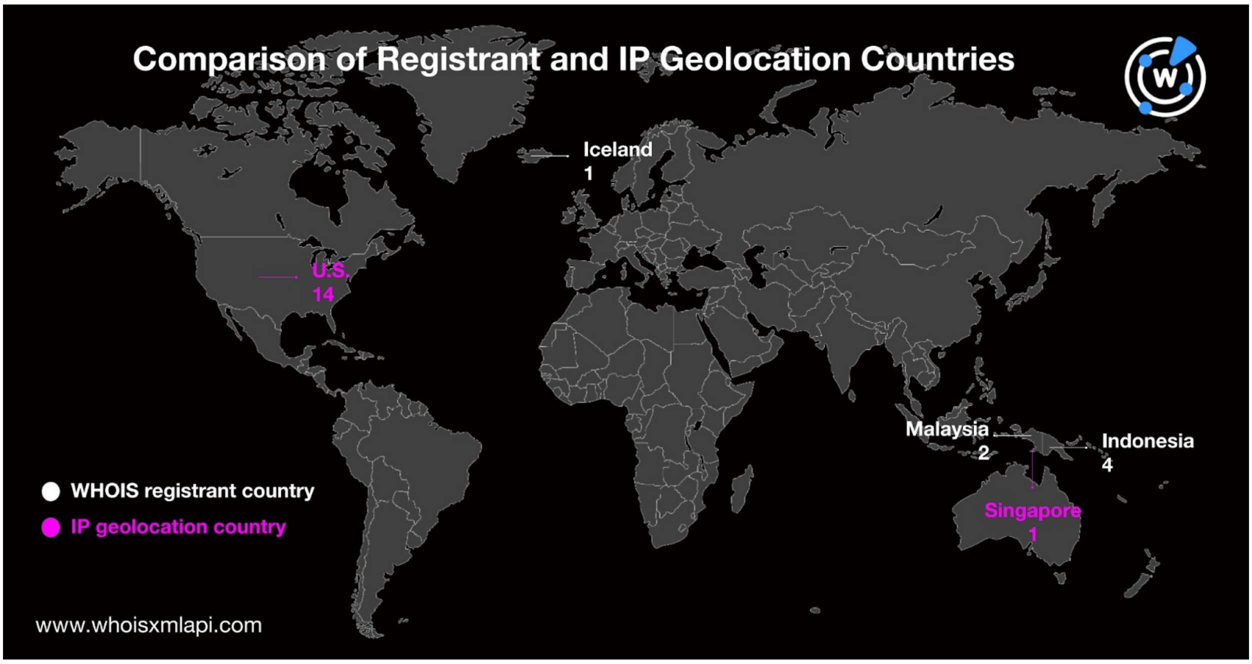
arpanrizki[.]my[.]id のスクリーンショット

それらの IoC を [DNS lookups](#) にかけたところ、15 件の IP アドレスに名前解決することがわか

りました。そのうち8件は以下の通りです。

- 104[.]21[.]33[.]94
- 104[.]21[.]51[.]36
- 104[.]21[.]56[.]91
- 104[.]21[.]76[.]153
- 104[.]21[.]8[.]240
- 104[.]21[.]83[.]223
- 104[.]21[.]9[.]208
- 172[.]67[.]131[.]8

15件のIPアドレスのうち14件が米国、1件がシンガポールで割り当てられたもので、登録者の国とは明らかに異なっています。

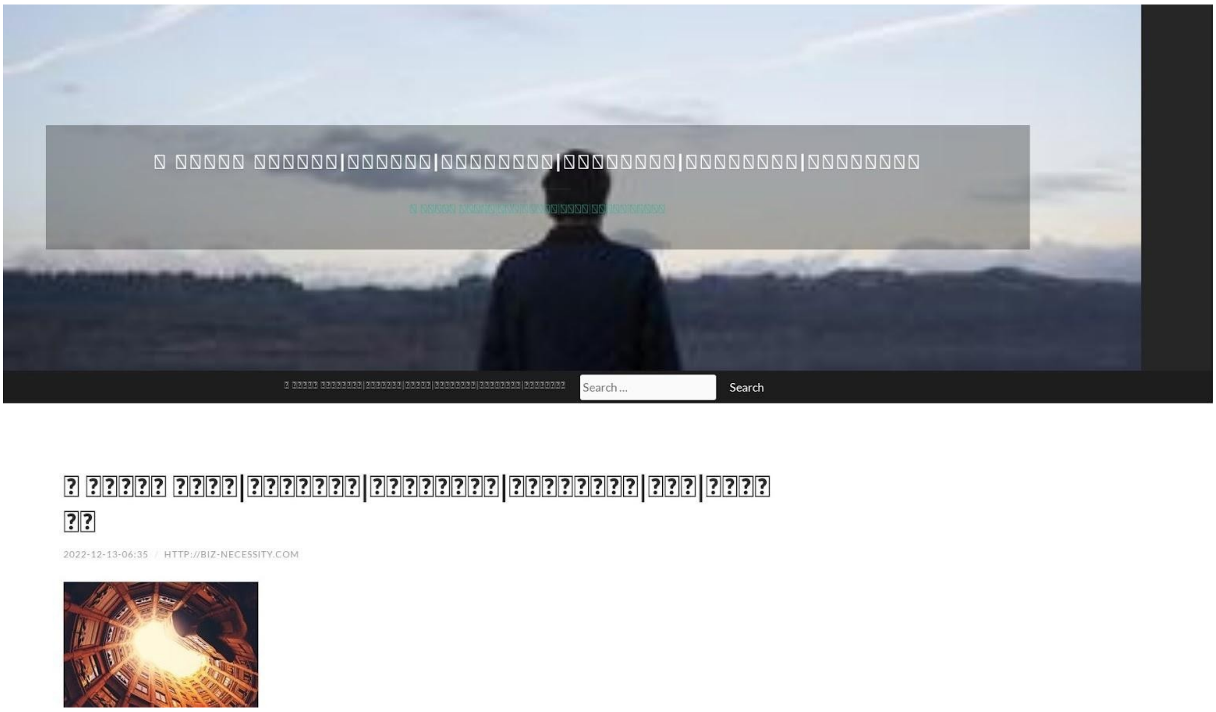


次に IoC の IP アドレスを reverse IP lookups 検索し、関連する可能性のあるドメイン名が 2,400 件近く見つかりました。そのうち 14 件のドメイン名は、様々なマルウェアエンジンによって悪意あるものとして分類されました。その中から特に 7 つを以下に示します。

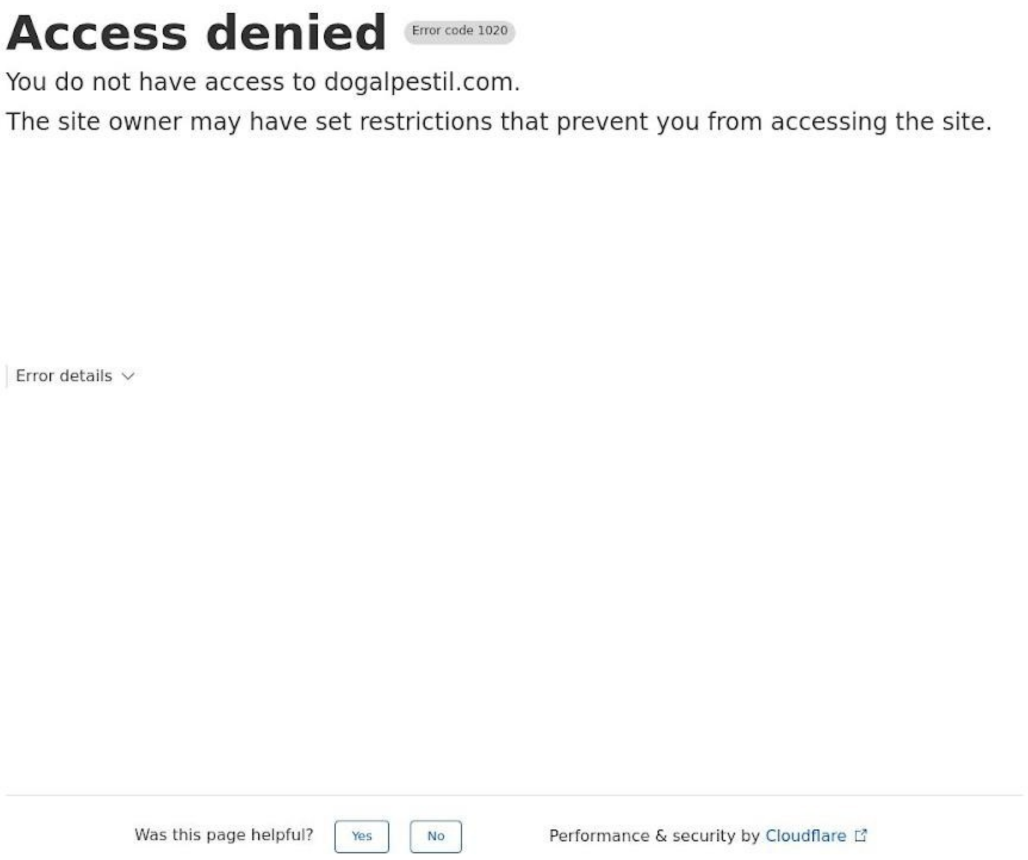
- aaallremain[.]xyz
- achievepatronize[.]top
- archodex[.]xyz
- beorganfamlayer[.]xyz
- biz-necessity[.]com
- bjmcellq[.]net
- claroonline-recargs[.]com

下図の通り、3 件の悪意あるドメイン名は今も有効と思われます：e コマースサイトに見える「beorganfamlayer[.]xyz」、個人ブログに見える「biz-necessity[.]xyz」、そして「dogalpestil[.]com」という制限付きウェブサイト。

beorganfamlayer[.]xyz のスクリーンショット



biz-necessity[.]com のスクリーンショット



Access denied Error code 1020

You do not have access to dogalpestil.com.

The site owner may have set restrictions that prevent you from accessing the site.

dogalpestil[.]com のスクリーンショット

さらにアーティファクトを特定するために IoC の historical WHOIS records(過去の WHOIS レコード)を調べたところ、匿名化されていない２つ登録者メールアドレスが見つかりました。そのうち１つは、公表されている２つの IoC（ionicio[.]com と graph-googleapis[.]com）の登録に使用されたものでした。また、そのメールアドレスで関連づけられた別のドメイン名（api-xyz[.]com）が、さらに別の IoC（apii-xyz[.]yogax[.] my[.] id）に類似しているのは興味深いポイントです。

Material Tailwind の IoC リストをもとに調査を水平展開

他方、Material Tailwind のレポートでは、
85[.]239[.]54[.]17、135[.]125[.]137[.]220、46[.]249[.]58[.]140 という３件の IP アドレスが IoC として列挙されています。

これらの IP アドレスを bulk IP geolocation lookup で検索した結果、３つの国（ドイツ、オランダ、米国）と３社のインターネットサービスプロバイダー（ISP）（BlueVPS OU、OVH SAS、Serverius Holding B.V.）が表示されました。

しかし、IconBurst とは異なり、IoC のひとつにホストされていたのは parsee[.]xyz というドメイン名１件だけでした。「parsee」という文字列を検索語として Domains & Subdomains Discovery を使用したところ、関連する可能性のあるドメイン名が 14 件見つかりました。それらは、.xyz 以外の異なる TLD の下に登録されています。例として７件を以下に示します。

- parsee[.]cn
- parsee[.]uk
- parsee[.]tk
- parsee[.]la
- parsee[.]ru
- parsee[.]ir
- parsee[.]com

いずれのマルウェアエンジンでも悪意があると判断されたものはありませんが、parse[.]xyz に酷似していることから、脅威アクターが論理的に判断して攻撃の道具に追加した可能性があります。

—

IconBurst と Material Tailwind のネットワークの広範な性質と、IoC の調査を当社で水平展開して見つけた追加のアーティファクトから、ソフトウェアのサプライチェーン攻撃はまだ終わっていないと推察できます。とはいえ、兵器化された npm や PyPI パッケージのオープンソースリポジトリをホストしているウェブプロパティからの防御を強化するよう、ReversingLabs は組織に呼びかけ続けています。当社はその呼びかけに賛同します。

同様の調査をご希望のお客様、この調査の完全なデータをご希望のお客様は、当社までお気軽にご連絡ください。

付録：アーティファクトと IoC のサンプル

IconBurst の IoC と同じ IP アドレスを使っているドメイン名のサンプル

- 00htv[.]xyz
- 0990zx[.]com
- 0p[.]fsind[.]site
- 0x11[.]ca
- 1024xb[.]me
- 103newzerkalo1x[.]ru
- 10xfunnel[.]io
- 113113vn[.]com
- 113bar[.]ru
- 119properties[.]com
- a-great-big-data-intl[.]fyi
- a-great-ca-employee-retention-credit[.]zone
- a-great-hoarding-clean-up[.]zone
- a-great-jp-doctor-jobs[.]fyi
- a-great-us-locksmiths[.]fyi
- a-great-w-uk-fb[.]com
- a-prime-investingold-uae[.]zone
- a-prime-nz-goodcredit[.]fyi
- a-snag-creditcard[.]zone
- a-snag-mx-cursos-online[.]fyi
- b-story[.]net
- b1093[.]com
- b4bguide[.]com
- b5ooq[.]me
- baansanrakorganic[.]com
- baby9store[.]com
- bachgbawcallsingforport[.]ml

- back-painsos[.]com
- backhumpcompverpo[.]cf
- backnelaper[.]tk
- c1697629[.]tier1[.]quicns[.]com
- c7[.]fsind[.]site
- ca[.]jjosindustrial[.]com
- cabadcta[.]tk
- cabalattze[.]ru[.]com
- cacedisviohu[.]tk
- cachhuydichchuyentronglol[.]nathaliekrag[.]com
- cacondyricon[.]tk
- cacoudisneotagdo[.]ga
- cacoveredhealth[.]com
- dabbhigcodibilong[.]tk
- dablippscenrousen[.]tk
- dadashmechanic[.]com
- dadpcguide[.]com
- daedalusbinary[.]com
- daev[.]us
- dahcuti[.]com
- dailsyale[.]com
- dailyobjects[.]xyz
- dainamisppe[.]ga
- e-morag[.]pl
- e-mselektrotrinec[.]cz
- e-shigang[.]com
- e[.]jjuanravavr[.]online
- e[.]usetheox[.]com
- e6321[.]com
- eaglesgear[.]com
- eahvpiej[.]tk
- eaiahlgc[.]tk
- ealgsiderky[.]tk
- ffiqih[.]tk-raudhatululum[.]sch[.]id
- finechoicebiscuit[.]id
- foopa[.]my[.]id
- free2fly[.]info
- gazken[.]com
- gervaskas[.]my[.]id
- globalrishivalley[.]com
- globalrishivalley[.]tk-raudhatululum[.]sch[.]id
- gmgusionmlbb[.]my[.]id
- goldenteam888[.]com
- harapanbersatu[.]sch[.]id
- hargovindpublicschool[.]tk-raudhatululum[.]sch[.]id
- hidayatulmubtadiin[.]xyz
- highschoolmen[.]schoolsecondarymss[.]xyz
- highschoolmen[.]xyz
- hobiteknologi[.]com
- hondabjm[.]com
- horoscoponline[.]net
- hundredflowershighersecondaryschool[.]com
- hundredflowershighersecondaryschool[.]tk-raudhatululum[.]sch[.]id
- iecacademy[.]id
- iecbekasi[.]id
- iecbekasi9[.]id
- ilmupengetahuanku[.]com
- ilmupengetahuanku[.]gudangilmuku[.]com
- imanuel[.]sch[.]id
- imanuel[.]tktidiudu[.]sch[.]id
- imerspreneur[.]com
- inayacelluar[.]com
- infodaihatsukarawang[.]com
- jabae[.]my[.]id
- jabae[.]tk-raudhatululum[.]sch[.]id
- jasatamandijogja[.]com
- jasatamanterbaik[.]com
- jasavideoanimasi[.]my[.]id

- jawaharnavodayavidyalaya-nagaland[.]com
- jawaharnavodayavidyalaya-nagaland[.]tk-raudhatululum[.]sch[.]id
- jawaharnavodayavidyalaya[.]com
- jawaharnavodayavidyalaya[.]tk-raudhatululum[.]sch[.]id
- jawaharnavodayavidyalayabhagalpur[.]com