Supply Chain Security: A Closer Look at the IconBurst and Material Tailwind Attacks

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

Earlier this month, ReversingLabs published a report on the current state of software supply chain security. They stated that the volume of such attacks using npm and PyPI code have increased by a combined 289% in the past four years. The research also cited two npm attacks as evidence—IconBurst and Material Tailwind.

ReversingLabs urges organizations, specifically npm and PyPI package users, to double down on securing their networks, and part of that could be better detection and blocking of access to suspicious and malicious web properties related to threats like IconBurst and Material Tailwind.

WhoisXML API researchers sought to expand the publicly available lists of indicators of compromise (IoCs) for both attacks. Our more in-depth foray aided by exhaustive WHOIS, IP, and DNS intelligence led to the following findings:

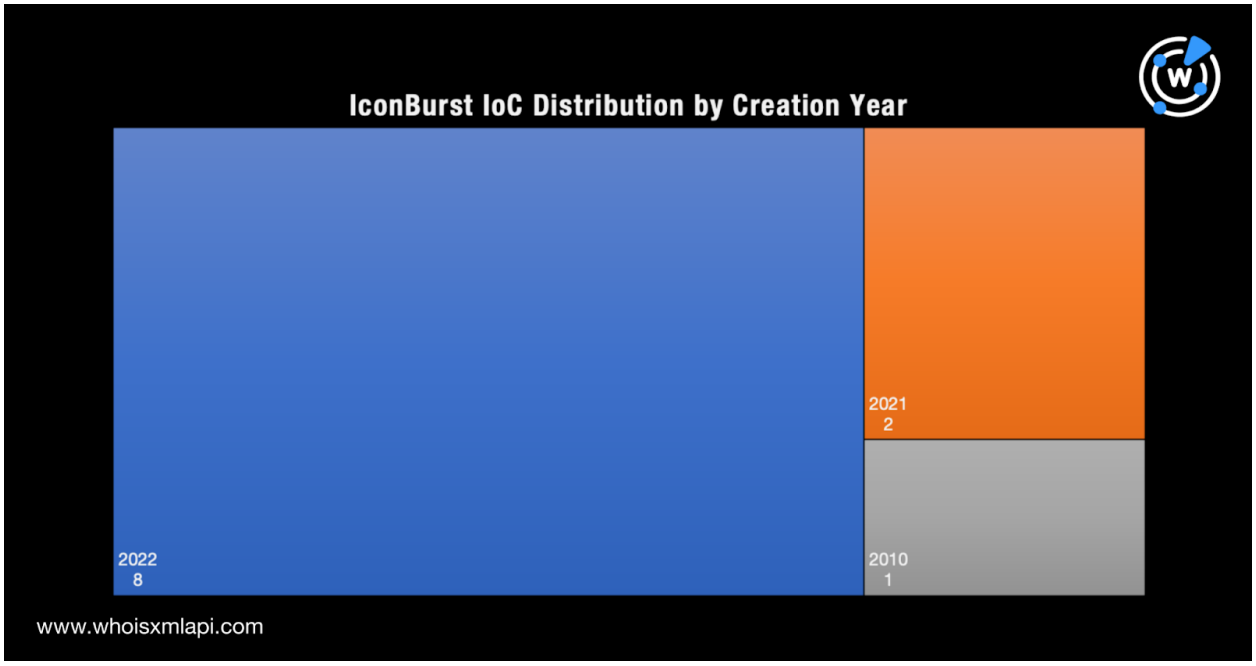
- The IconBurst domains identified as IoCs resolved to 15 IP addresses.
- At least 2,401 domains shared the IconBurst IoCs' IP hosts, 14 of which turned out to be malicious.
- Two of the domains identified as IconBurst IoCs had unredacted email addresses in some of their historical WHOIS records.
- One of the IconBurst IoCs' unredacted registrant email addresses was used to register five other domains, two of which ReversingLabs named in their report.
- One of the IP addresses identified as a Material Tailwind IoC led to a possibly connected domain.
- The string "parsee" that can be found in the Material Tailwind domain considered as an artifact was shared by 14 other domains sporting different top-level domain (TLD) extensions.

IconBurst IoC List Expansion

The IconBurst attackers installed malicious npm modules into target systems, allowing them to steal sensitive data from various apps and websites. ReversingLabs identified 13 domains as IoCs, namely:

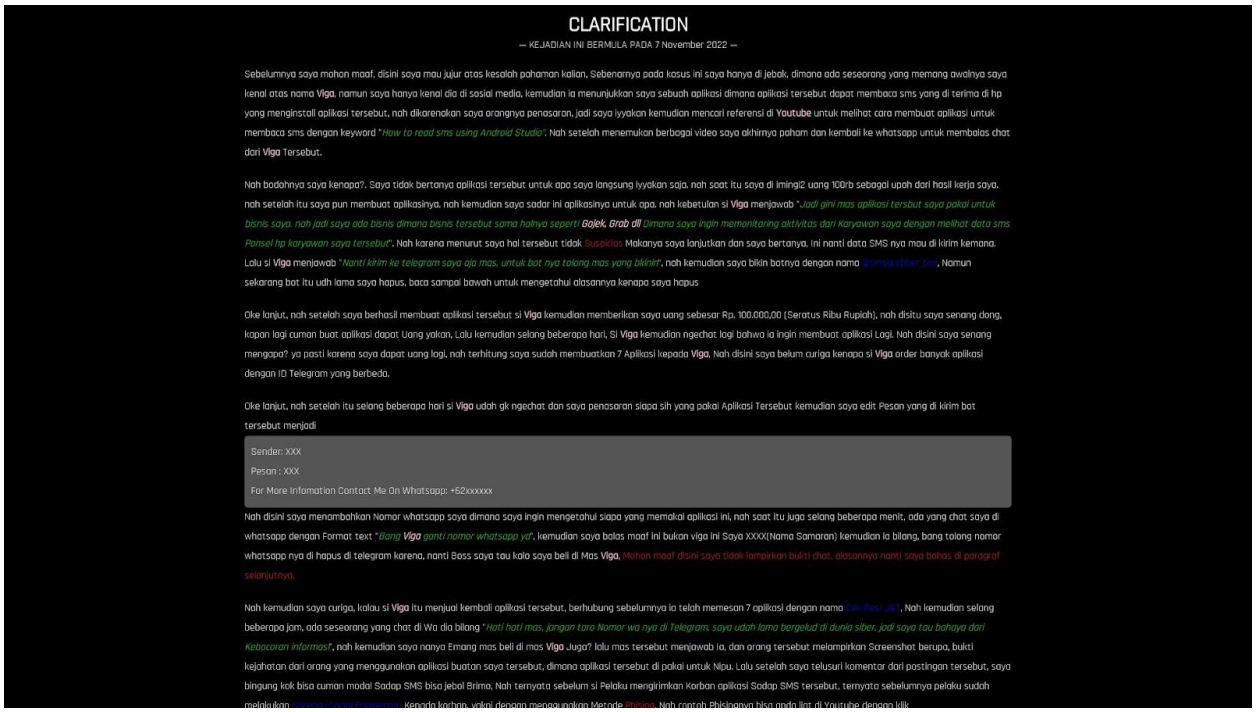
- graph-googleapis[.]com
- ionicio[.]com
- curls[.]safhosting[.]xyz
- arpanrizki[.]my[.]id
- dnster[.]my[.]id
- okep[.]renznesia[.]xyz
- ryucha[.]my[.]id
- panelllgege[.]001www[.]com
- nge[.]scrp[.]my[.]id
- apiii-xyz[.]yogax[.]my[.]id
- panel[.]archodex[.]xyz
- panel[.]curlz[.]online
- api[.]mlbb-x-02[.]ml

We began our investigation with a bulk WHOIS lookup for these domains, which revealed that only 11 had retrievable WHOIS records. A majority of these web properties (eight to be exact) were created just this year, two last year, and one as far back as 2010. They were spread across eight registrars—three were managed by Registrasi Neva Angkasa; two by CV Jogjacamp; and one each by ResellerCamp, WEBCC, Mat Bao Corporation, Web Commerce Communications Ltd., Hostinger, UAB, and Namecheap, Inc.



Of the seven that named their registrant countries, four were registered in Indonesia, two in Malaysia, and one in Iceland.

Only two of the IoCs—ionicio[.]com and arpanrizki[.]my[.]id—continue to host live content to this day based on our screenshot lookup results, which means they could still pose risks to unknowing users.



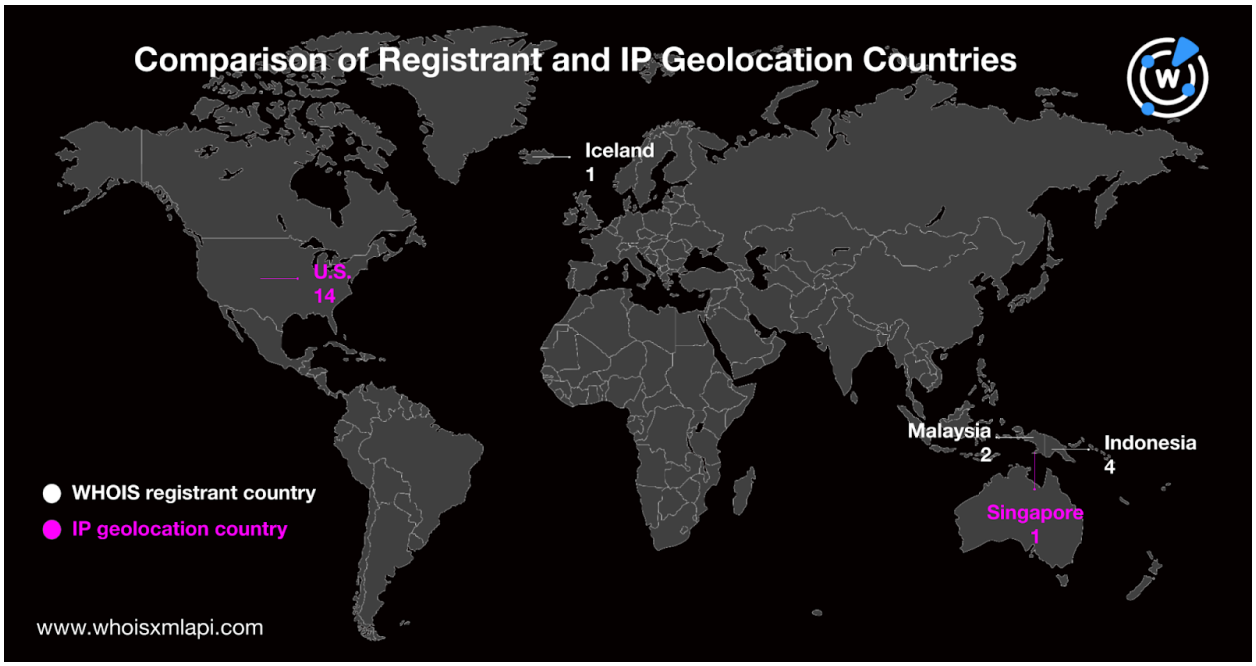
Screenshot of ionicio[.]com

Screenshot of arpanrizki[.]my[.]id

DNS lookups for the IoCs showed they resolved to 15 IP addresses, eight of which are:

- 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

Of these IP hosts, 14 originated from the U.S. and one from Singapore, notably different from their registrant countries.

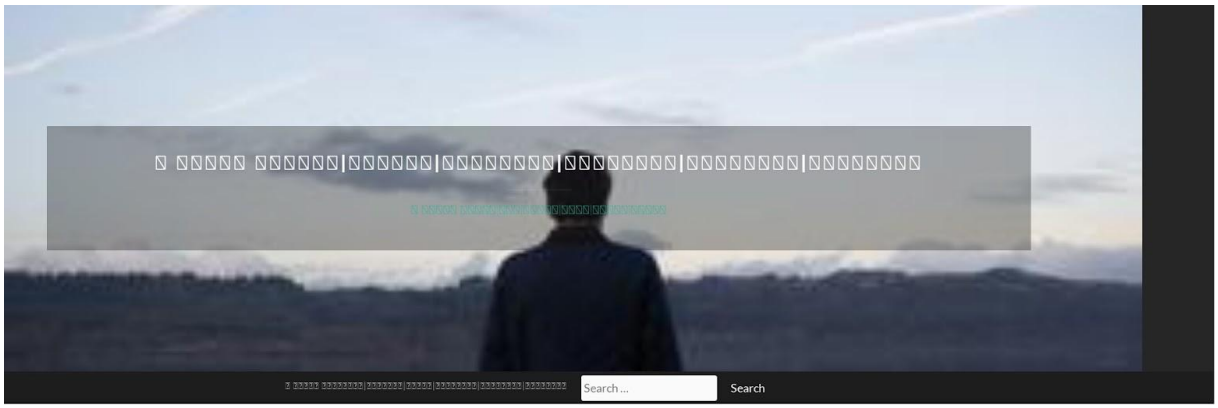


Next, reverse IP lookups for the IoCs' IP hosts allowed us to uncover nearly 2,400 possibly connected domains. Fourteen of the domains were classified as malicious by various malware engines. We named seven of these below.

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

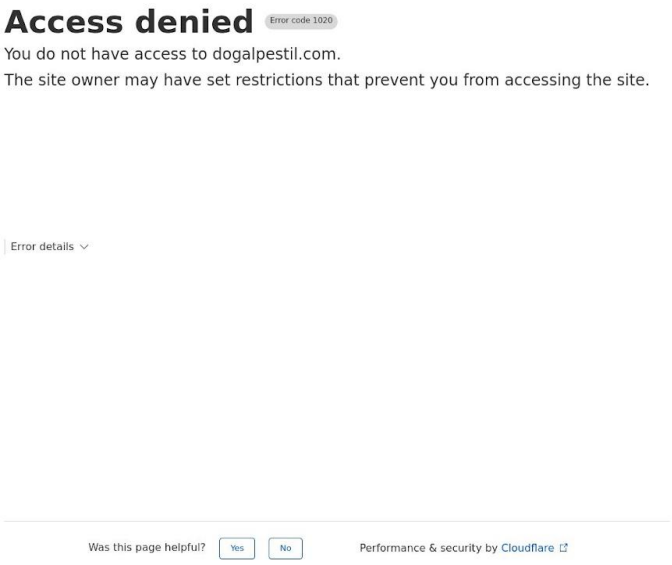
Three of the malicious digital properties seemingly remain live—beorganfamlayer[.]xyz, which appears to be an e-commerce site; biz-necessity[.]com, which looks like a personal blog; and dogalpestil[.]com, a restricted website.

Screenshot of beorganfamlayer[.]xyz



2022-12-13-06:35 / HTTP://BIZ-NECESSITY.COM

Screenshot of biz-necessity[.]com



Screenshot of dogalpestil[.]com

To identify more artifacts, we looked at the IoCs' historical WHOIS records and found two unredacted registrant email addresses. One of these was used to register two of the publicly reported IoCs—ionicio[.]com and graph-googleapis[.]com. It's also interesting to note that another domain connected to the said email address (i.e., api-xyz[.]com) bore a resemblance to yet another identified IoC (i.e., apiii-xyz[.]yogax[.]my[.]id).

Material Tailwind IoC List Expansion

The Material Tailwind report, meanwhile, enumerated three IP addresses—85[.]239[.]54[.]17, 135[.]125[.]137[.]220, and 46[.]249[.]58[.]140—as IoCs.

A bulk IP geolocation lookup for these IP addresses showed three distinct origin countries (i.e., Germany, the Netherlands, and the U.S.) and Internet service providers (ISPs) (i.e., BlueVPS OU, OVH SAS, and Serverius Holding B.V.).

Unlike IconBurst, however, we only found a single domain—parsee[.]xyz—hosted on one of the IoCs. Using the string "parsee" as a Domains & Subdomains Discovery search term led to the discovery of 14 possibly connected domains. These newly discovered digital properties only differed in that they had TLD extensions other than .xyz. We named seven of them below.

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

While none of them have been dubbed malicious by any malware engine, their striking resemblance to parsee[.]xyz could make them logical additions to the threat actors' arsenal.

—

Judging from the widespread nature of the IconBurst and Material Tailwind networks and the additional artifacts our IoC expansion exercises uncovered, we haven't seen the last of software supply chain attacks. That said, we second ReversingLabs's call to action for organizations to shore up their defenses against web properties that serve as hosts to open-source repositories of weaponized npm and PyPI packages.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Domains That Shared the IconBurst IoCs' IP Hosts

- 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[.]josindustrial[.]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[.]juanravavr[.]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