Probing the DNS for Signs of XLoader Abuse

Table of Contents

Executive Report

XLoader has been plaguing macOS users since it was first discovered in 2021. Back then, though, it only posed a threat to those who opted to install Java on their systems. That's no longer the case, however, as its latest variant, encased in compromised OfficeNote installation packages (currently in beta mode), can cause damage to any macOS devices.

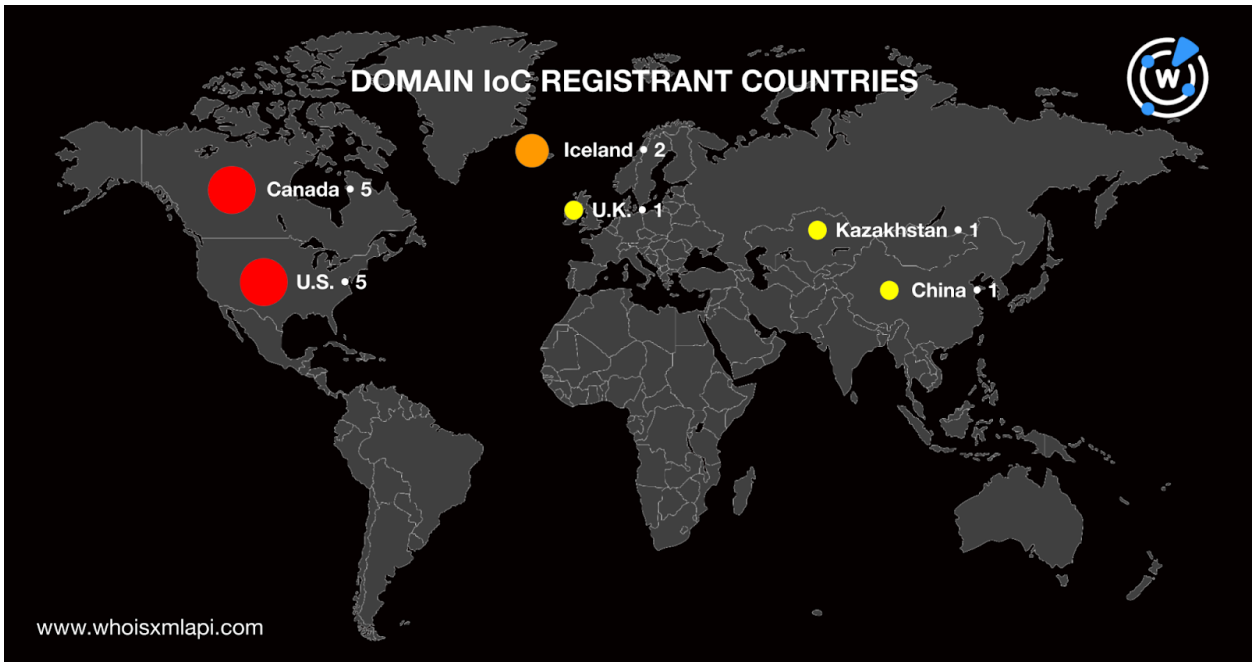
SentinelOne published 19 indicators of compromise (IoCs)—15 domains (extracted from the reported host names) and four IP addresses—for the latest XLoader variant, which we at WhoisXML API subjected to a DNS deep dive. Our probe led to the discovery of:

- 24 unreported IP resolutions, 19 of which turned out to be malicious based on a bulk malware check
- 53 domains that shared some of the IoCs' dedicated IP hosts, three of which have been tagged as malicious
- 446 domains that contained text strings found among some of the IoCs

XLoader Infrastructure Revelations

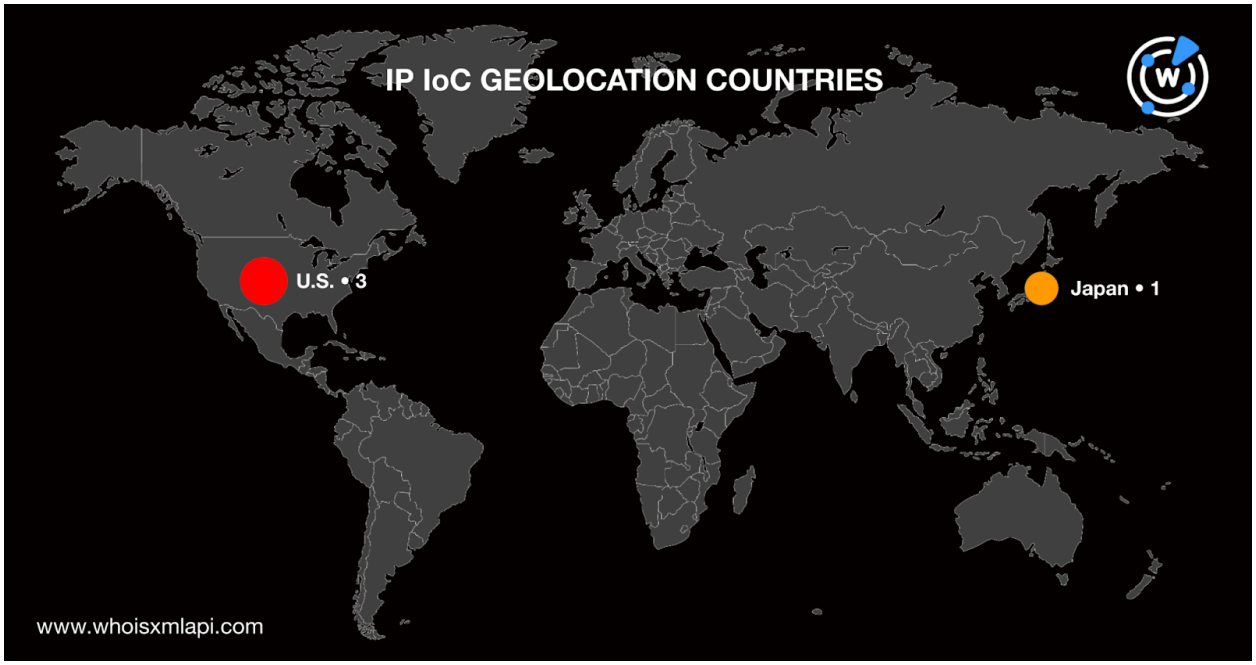
We began our DNS probe with a bulk WHOIS lookup for the 15 domains identified as XLoader IoCs and found that:

- The domains were distributed among eight registrars topped by GoDaddy.com, Google, and Namecheap, each accounting for three IoCs.
- All of the domains were newly created, between May and August 2023.
- All of the IoCs' registrant email addresses have been either redacted or privacy protected.
- Only one of the 15 domains—qhsbobfv[.]top—had a publicly viewable registrant name written in Chinese.
- The IoCs were spread across six registrant countries topped by Canada and the U.S. (five domains each) and Iceland (two domains).



A bulk IP geolocation lookup for the four IP addresses tagged as IoCs followed, which led to these discoveries:

- The IP addresses originated in two countries—three in the U.S. and one in Japan.
- Each IoC was administered by a different Internet service provider (ISP), namely, Namecheap, Inc.; Hostinger International Limited; Google LLC; and Rackip Consultancy Pte. Ltd.



Note that a comparison of the domains and IP addresses classified as XLoader IoCs revealed these similarities:

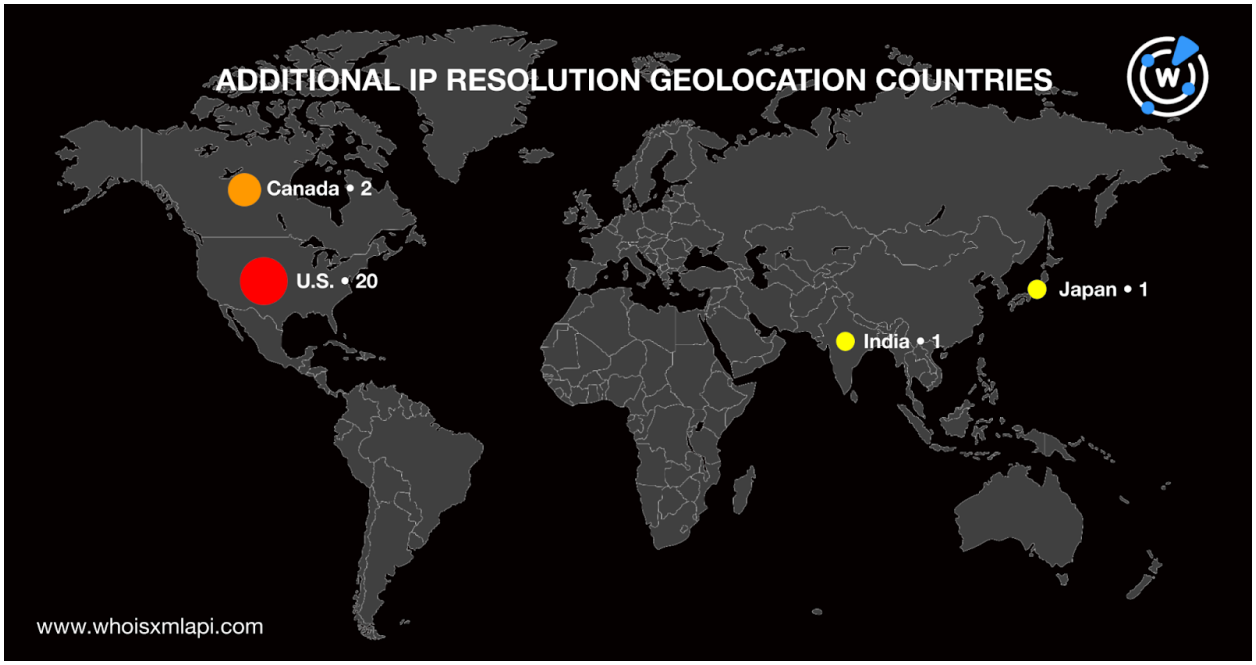
- Only the U.S. was named both domain registrant and IP geolocation country.
- Namecheap, Hostinger, and Google appeared as both registrars and ISPs.

XLoader IoC DNS Probe Findings

Next, we began our list expansion with DNS lookups for the domains identified as IoCs. That led to the discovery of 27 IP resolutions for 11 domains, three of which were already part of SentinelOne's list. None of the domains with active IP resolutions shared any of the identified hosts.

A bulk IP geolocation lookup for the 24 additional IP addresses revealed that:

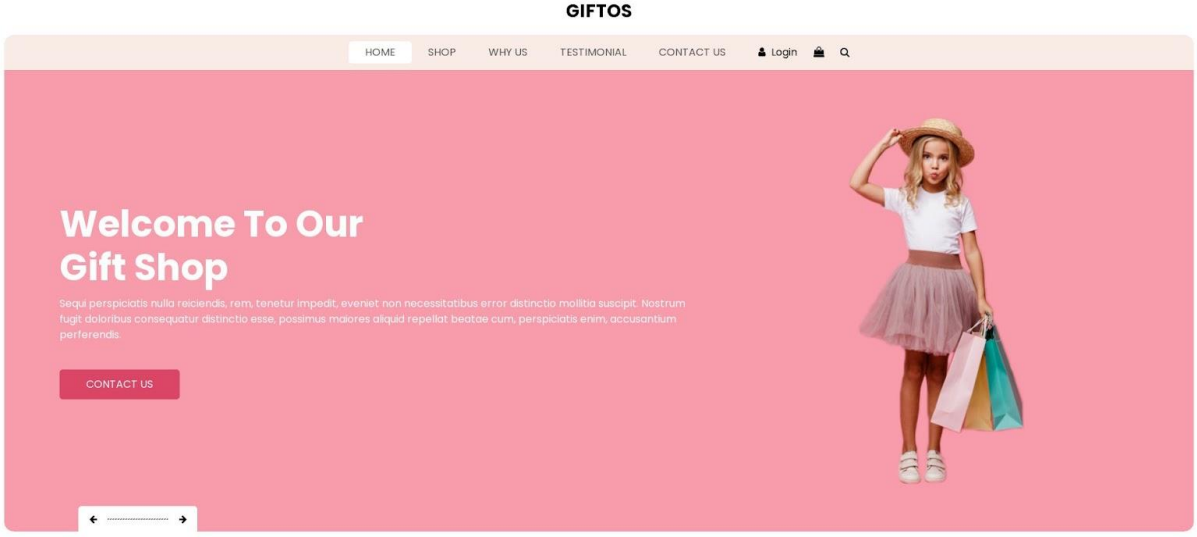
- Twenty-one of the unreported IP resolutions shared the IoCs' geolocation countries—20 from the U.S. and one from Japan.
- The remaining three unpublished IP resolutions were spread across two countries—two from Canada and one from India.
- Six of the additional IP resolutions shared the three of the IoCs' ISPs—Google, Hostinger, and Rackip Consultancy.



A bulk malware check for the unreported IP resolutions showed that 19 were malicious.

Our DNS lookups also revealed that six of the now 27 IP addresses in total—the three identified as IoCs and 24 additional resolutions—were seemingly dedicated. They hosted a total of 53 unique domains, three of which turned out to be malicious according to a bulk malware check.

Screenshot lookups for the three malicious IP-connected domains showed they continued to host or lead to live pages. Artkit[.]top led to an e-commerce shop while both e6796[.]com and e9579[.]com led to an app store.



Screenshot of artkit[.]top

Screenshot of e6796[.]com and e9579[.]com

Next, we used text strings found among the 15 domains identified as IoCs to look for similar-looking XLoader artifacts via Domains & Subdomains Discovery. Specifically, we looked for domains containing, or in certain cases starting, with the strings:

- **spv88.**
- **raveready.**
- **qq9122.**
- **qhsbobfv.**
- **pinksugarpopmontana.**
- **nationalrecoveryllc.**
- **mommachic.**
- **lushespets.**
- **kiavisa.**
- **hatch.**
- **growind.**
- **corkagenexus.**
- **brioche-amsterdam.**
- **akrsnamchi.**
- **activ-ketodietakjsy620.**

Our DNS foray uncovered 446 string-connected domains.

Finally, we know from the SentinelOne post that XLoader targets macOS and soon-to-launch app OfficeNote. We thus used the brands as Domains & Subdomains Discovery search terms (exactly matched **macos** and contained **officenote**) to look for subdomains that could figure in future campaigns, possibly phishing attacks against the brands or their users. We found 492 brand-containing subdomains in total.

Bulk WHOIS lookups for the **macos** and **officenote** subdomains revealed that:

- The 469 **macos** subdomains all fell under different domains, only one of which—macOS's official domain macos[.]apple[.]com, was publicly attributable to Apple, Inc.
- The 23 **officenote** subdomains fell under 10 domains, none of which could be publicly attributed to the app's developer—Jiransoft Co. Ltd.

—

Our XLoader DNS deep dive led to the discovery of more than 500 possibly connected artifacts. It also allowed us to uncover close to 500 subdomains containing the two brands the threat actors trailed their sights on—macOS and OfficeNote.

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

XLoader IoCs SentinelOne Identified

- spv88[.]online
- raveready[.]shop
- qq9122[.]com
- qhsbobfv[.]top
- pinksugarpopmontana[.]com
- nationalrecoveryllc[.]com
- mommachic[.]com
- lushespets[.]com
- kiavisa[.]com
- hatch[.]computer
- growind[.]info
- corkagenexus[.]com
- brioche-amsterdam[.]com
- akrsnamchi[.]com
- activ-ketodietakjsy620[.]cloud
- 66[.]29[.]151[.]121
- 62[.]72[.]14[.]220
- 142[.]251[.]163[.]121
- 137[.]220[.]225[.]17

Sample Additional IP Resolutions

- 172[.]67[.]188[.]73
- 23[.]227[.]38[.]67
- 137[.]220[.]225[.]54
- 216[.]239[.]38[.]21
- 23[.]227[.]38[.]68
- 45[.]79[.]19[.]196
- 104[.]21[.]26[.]182
- 154[.]41[.]232[.]126
- 104[.]21[.]32[.]235
- 216[.]239[.]34[.]21
- 173[.]255[.]194[.]134
- 172[.]67[.]138[.]86

Sample Malicious Additional IP Resolutions

- 216[.]239[.]38[.]21
- 23[.]227[.]38[.]68
- 45[.]79[.]19[.]196
- 104[.]21[.]26[.]182
- 104[.]21[.]32[.]235
- 216[.]239[.]34[.]21
- 173[.]255[.]194[.]134
- 216[.]239[.]36[.]21
- 72[.]14[.]185[.]43
- 216[.]239[.]32[.]21

Sample IP-Connected Domains

- 5575ky[.]com
- 6691ky[.]com
- 74858af1f[.]n[.]fnvip100[.]com
- abctech[.]life
- aozoraclothing[.]com
- artkit[.]top

- bacfashion[.]xyz
- beautwin[.]info
- blackswancomex[.]org
- bondbind[.]life
- droudfurs[.]life
- e6796[.]com
- e6893[.]com
- e6916[.]com
- e7371[.]com
- e7613[.]com
- e7653[.]com
- e9381[.]com
- e9579[.]com
- e9737[.]com

Sample String-Connected Domains

- brioche-amsterdam[.]nl
- labrioche-amsterdam[.]nl
- labrioche-amsterdam[.]com
- growind[.]tk
- growind[.]in
- growind[.]io
- growind[.]ru
- growind[.]es
- growind[.]nl
- growind[.]net
- egrowind[.]ws
- agrowind[.]pl
- agrowind[.]nl
- agrowind[.]es
- growind[.]com
- agrowind[.]ro
- agrowind[.]ru
- agrowind[.]dk
- vgrowind[.]com
- egrowind[.]com
- agrowind[.]com
- magrowind[.]com
- wegrowind[.]com
- growind[.]com[.]br
- webgrowind[.]com
- growind[.]com[.]de
- growind[.]com[.]ar
- nopagrowind[.]nl
- coenogrowind[.]ml
- evergrowind[.]com
- stargrowind[.]com
- agrowind[.]com[.]tr
- ackgrowind[.]party
- almenilogrowind[.]tk
- vingsumagrowind[.]gq
- montenegrowind[.]com
- axworogrowind[.]co[.]id
- hatch[.]lighting
- hatch[.]tools
- hatch[.]xin
- hatch[.]tokyo
- hatch[.]limited
- hatch[.]ee
- hatch[.]financial
- hatch[.]ga
- hatch[.]xn--kprw13d
- xn--htch-5q5a[.]com
- hatch[.]rsvp
- hatch[.]page
- hatch[.]com[.]ru

Sample Brand-Containing Domains

- officenote[.]jugem[.]jp
- officenote[.]proposal-voicenote[.]clu b
- officenote[.]nadiyoram[.]com
- officenotescs[.]dns-dns[.]com
- officenotedoc[.]nadiyoram[.]com

- officenotepiao[.]simple[.]com
- officenotes-be[.]onrender[.]com
- officenotevoic[.]serveftp[.]com
- officenotes-api[.]onrender[.]com
- miamiofficenotes[.]wordpress[.]com
- www[.]officenotescs[.]dns-dns[.]com
- brunsonofficenotes[.]blogspot[.]com
- funnyofficenotebooks[.]odkelneradomilionera[.]pl
- scarofficenotes[.]demo[.]volusion[.]com
- miamiofficenotes[.]files[.]wordpress[.]com
- officenote-shop[.]yts[.]wpn[.]mybluehostin[.]me
- www[.]funnyofficenotebooks[.]odkelneradomilionera[.]pl
- www[.]officenote-shop[.]yts[.]wpn[.]mybluehostin[.]me
- officenotetoile-albertville[.]notaires[.]fr
- officenote-com[.]mail[.]protection[.]outlook[.]com
- officenotes-be[.]onrender[.]com[.]cdn[.]cloudflare[.]net
- officenote365-com[.]mail[.]protection[.]outlook[.]com
- servcorpofficenote-com02b[.]mail[.]protection[.]outlook[.]com
- macos[.]kinderproduktychlodzone[.]pl
- macos[.]sillysock[.]codes
- macos[.]crabb[.]ca
- macos[.]computertraining[.]cf
- macos[.]nyquistmaster[.]com
- macos[.]remi-bouille[.]fr
- macos[.]onquip[.]com
- macos[.]id[.]xyz
- macos[.]free-aa[.]com
- macos[.]kinderpanchlodek[.]com[.]pl
- macos[.]zalon[.]com
- macos[.]liefert-es[.]com
- macos[.]graduacionessoleil[.]com[.]mx
- macos[.]hoit[.]asia
- macos[.]ca2[.]cc
- macos[.]wangk[.]win
- macos[.]filch[.]online
- macos[.]spot7[.]org
- macos[.]pravdomil[.]cz
- macos[.]winsec[.]support
- macos[.]pagespeedmobilizer[.]com
- macos[.]smaugstrove[.]live
- macos[.]fallguys-shop[.]com
- macos[.]kinderbueno[.]ch
- macos[.]tictacsmyle[.]com[.]pl
- macos[.]freeboxos[.]fr
- macos[.]law[.]blog