# Uncloaking the Underbelly of JinxLoader

## Table of Contents



## Executive Report

Cybercriminals are known for using so-called “loaders” like Xloader to initiate computer infections. Worse, even newbies can now get their hands on these malware distributors via hacker forums. Case in point? JinxLoader, one of the latest malicious offerings up for grabs on the likes of hackforums[.]net.

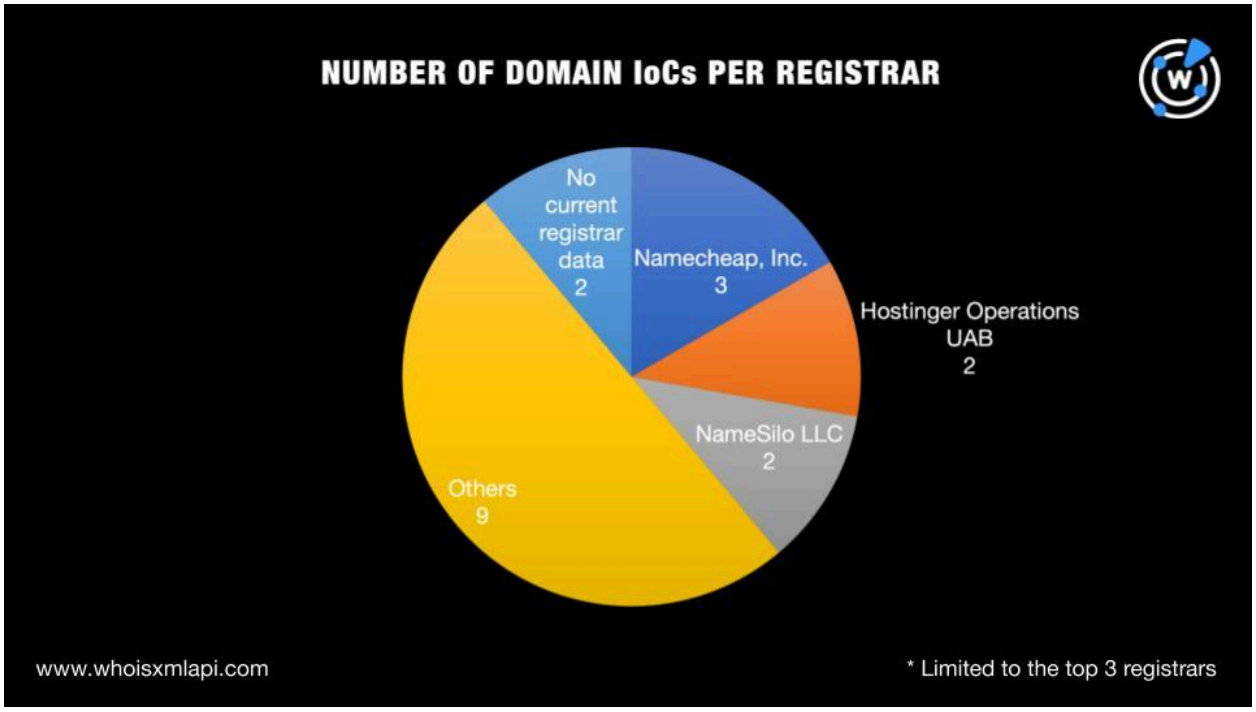
Palo Alto’s Unit 42 published 19 JinxLoader indicators of compromise (IoCs) comprising 18 domains and one IP address in late November 2023. The WhoisXML API research team sought to determine if the JinxLoader operators left more digital traces through a DNS deep dive that brought to light:

- 314 email-connected domains
- 158 IP-connected domains, one of which turned out to be malicious
- 1,116 string-connected domains, one of which turned out to be malicious

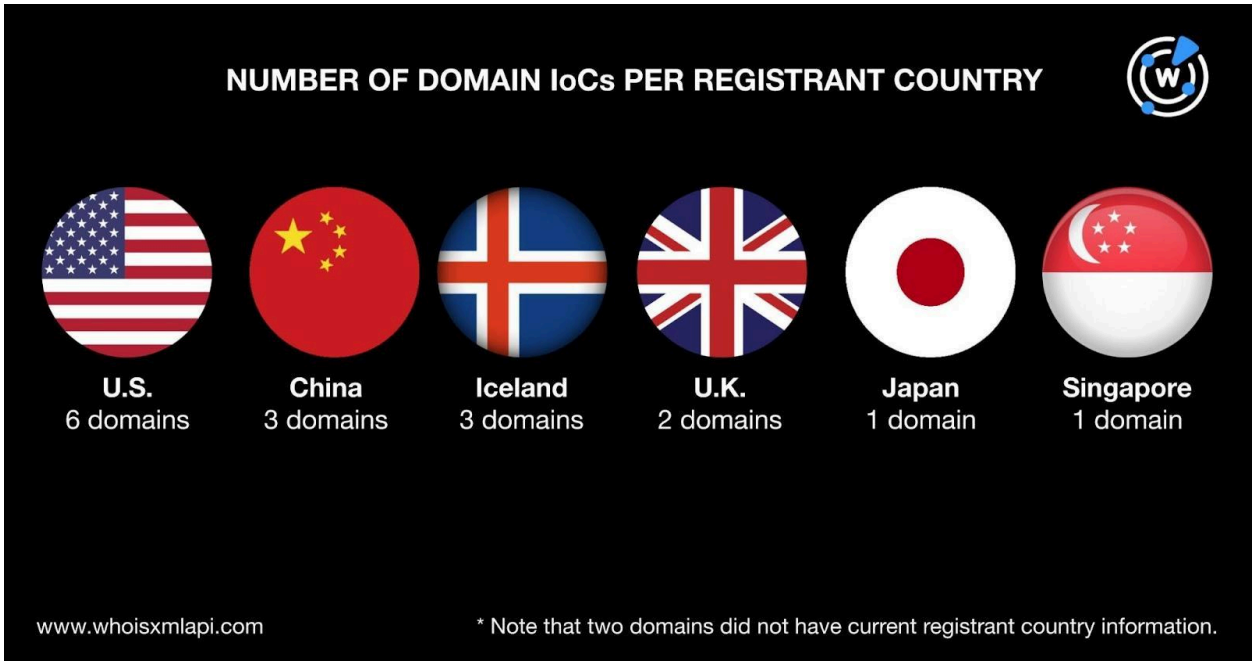
### Behind the JinxLoader IoCs

As with every investigation, we sought to discover more about the 21 JinxLoader IoCs starting with a bulk WHOIS lookup for the 18 domains that led to these findings:

- The 18 domains identified as IoCs were distributed among 12 registrars led by Namecheap, Inc., which accounted for three domains. Hostinger Operations UAB and NameSilo LLC tied in second place with two domains each. One domain each was administered by Chengdu West Dimension Digital Technology Co. Ltd.; Domain International Services Limited; Dynadot LLC; Eranet International Limited; GMO Internet, Inc.; Gname.com Pte. Ltd.; IONOS SE; Name.com, Inc.; and Network Solutions LLC. The remaining two did not have current registrar data.




- Although a majority of the domain IoCs were relatively new—created in 2023, one was aged, created way back in 2005. Two, however, did not have creation dates in their current WHOIS records.
- The 18 domains were spread across six registrant countries topped by the U.S., which accounted for six of them. China and Iceland took the second spot with three domains each while the U.K. with two domains placed third. Japan and Singapore accounted for one domain each. Finally, two did not have current registrant country information.




- It is also worth noting that two of the domain IoCs—e3iaibr[.]icu and ldhqi4[.]fun—had registrant organizations in their current WHOIS records although they looked more like individual names.

An IP geolocation lookup, meanwhile, for the IP address classified as an IoC showed it was geolocated in Japan with Alibaba (U.S.) Technology Co. Ltd. as its ISP.

## In Search of JinxLoader DNS Connections

We began our search for JinxLoader traces in the DNS with WHOIS History API searches for email addresses. We found 41 results after duplicates and the IoCs were removed. Seven of the email addresses were public.

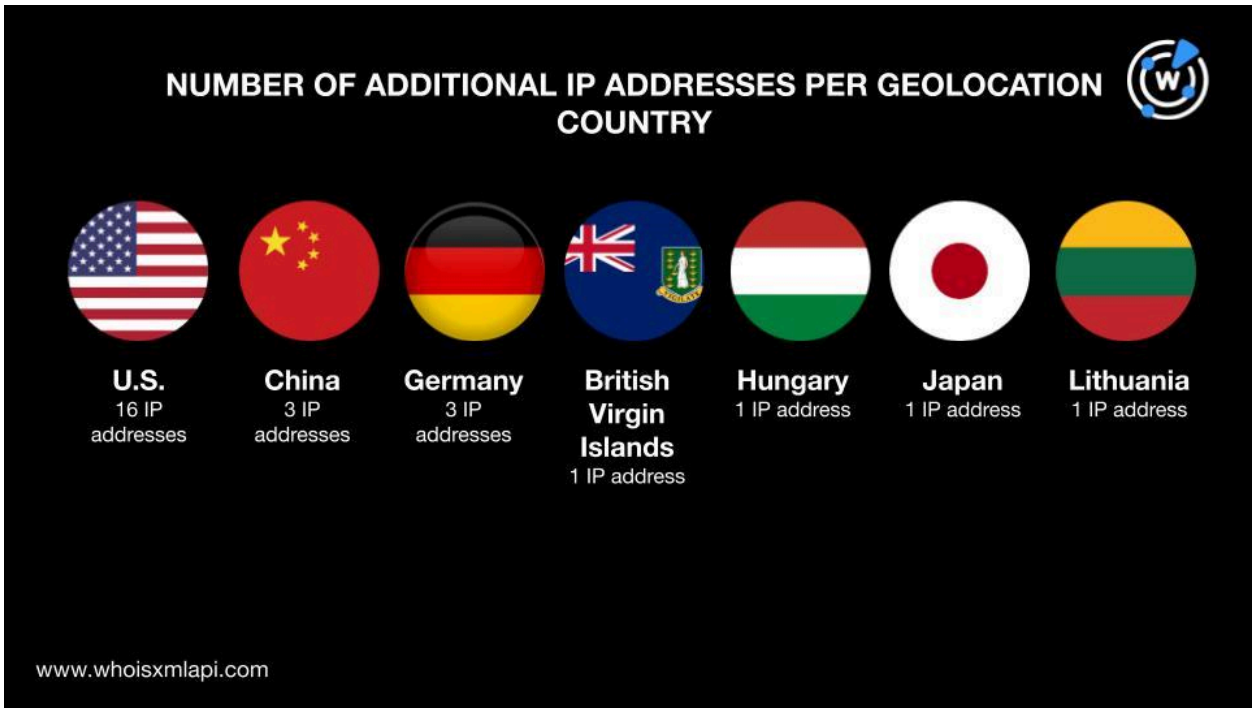
Reverse WHOIS API searches showed that three of the public email addresses appeared in the current WHOIS records of 314 other domains after duplicates and the IoCs were filtered out.

Screenshot API searches for the 314 email-connected domains revealed that 115 remained accessible to date.

Next, we subjected the 18 domain IoCs to DNS lookups, which showed that 17 actively resolved to 26 IP addresses after duplicates and the IoC were removed.

IP geolocation lookups for the 26 additional IP addresses led to these findings:

- The U.S. topped the list of geolocation countries, accounting for 16 IP addresses. China and Germany took the second spot with three IP addresses each. The remaining four were scattered across the same number of nations—the British Virgin Islands, Hungary, Japan, and Lithuania.




Note that Japan, an IP address IoC geolocation country, also appeared as an origin of one additional IP address.

- Half of the additional IP addresses, 13 to be exact, were administered by Amazon. Namecheap, Inc. accounted for four IP addresses. One each fell under the dominion of Confluence Networks, Inc.; DingFeng XinHui (Hong Kong) Technology Limited; Gigabit Solution Limited; GMO Internet, Inc.; Hetzner Online GmbH; Hostinger International Limited; Juraj Pusic; Peg Tech, Inc., and SEDO GmbH.

Threat intelligence lookups for the 26 additional IP addresses revealed that 14 were associated with various threats. Take a look at the detailed results for five of them below.

| IP ADDRESSES | ASSOCIATED THREAT TYPES |
|---|---|
| 103[.]107[.]239[.]13 | Malware |

| | |
|---|---|
| 118[.]27[.]125[.]154 | Malware |
| 154[.]215[.]150[.]218 | Malware |
| 162[.]0[.]235[.]58 | Generic<br>Malware<br>Phishing |
| 162[.]255[.]119[.]78 | Malware |

Reverse IP lookups for the 26 additional IP addresses showed that five of them could be dedicated. They hosted 158 unique domains that were not part of the list of IoCs or email-connected domains.

Threat Intelligence API, meanwhile, revealed that one—echolinkevolve[.]xyz—was seemingly associated with malware distribution.


**Screenshot of malicious IP-connected domain echolinkevolve[.]xyz**

Screenshot API showed that 72 of the 158 IP-connected domains remained accessible. It is also worth noting that 12 of them looked quite suspicious—brightpathtechgroups[.]top, frontiersunrisepro[.]life, greensagesstrategies[.]top, ivisas-affaires[.]com, mailerpay[.]com, matrixleapsystems[.]xyz, nexusglobalfusions[.]top, oceanicpulsetek[.]xyz, pbc-finance[.]com, solarflaredisruptors[.]life, trebletech[.]xyz, and visionquestengage[.]life—in that they shared the same content as malicious IP-connected domain echolinkevolve[.]xyz.

To cover all our bases, we used Domains & Subdomains Discovery with the **Starts with** parameter to look for other possibly connected domains, specifically those containing text strings found among the IoCs. We uncovered 1,116 such properties for eight strings, namely:

- **219855.**
- **austintrafficlawyer**
- **infinite-7**
- **overthemoonphoto**
- **terranovaservices**
- **vietdot**
- **wgs.**
- **worldlife**

Threat Intelligence API showed that one string-connected domain—worldlifefree[.]info—was associated with malicious command-and-control (C&C) and malware distribution.

Screenshot API, meanwhile, showed that 472 of the 1,116 string-connected domains remained accessible as of this writing.

—

Our foray into the DNS for more signs of JinxLoader led to the discovery of 1,588 potentially connected artifacts. We also uncovered 26 additional IP addresses that played host to the domain IoCs, several of which turned out to be malicious. A couple of the connected domains were also associated with various threats.

***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

## Sample Email-Connected Domains

- 0reader[.]com
- 2makingchanges[.]com
- 3hmechanical[.]com
- acapulcocondo[.]com
- accloanpro[.]com
- addlikebrasil[.]com
- airforcefanatics[.]com
- alafarpe[.]com
- alansells[.]com
- alternatesmoking[.]com
- annarborsunless[.]com
- apartmentsinmemphis[.]com
- apocalyst[.]com
- arcvoyager[.]com
- ardhie[.]com
- arjwedding[.]com
- aromamusicals[.]com
- asdlionheart[.]com
- ashlandskateboards[.]com
- atlantaapartments[.]online
- atlantabraces[.]com
- autoreview[.]com
- autosubastascr[.]com
- azapair[.]com
- baltimoredivorcelawyers[.]com
- baltimorehomes[.]online
- bankruptcychoice[.]com
- bankruptcydallas[.]com
- bankruptcylawyerflorida[.]com
- bankruptcylist[.]com
- barabeesh[.]com
- blogmakeover[.]net
- bluecastdenim[.]com
- bohoandrock[.]com
- boisepersonalinjuryattorney[.]com
- bonitaspringshomesforsale[.]com
- bostonbankruptcyattorneys[.]com
- buydestin[.]com
- buyjacksonville[.]com
- bybproductions[.]com
- caldwellassociates[.]net
- californiapatentlawyer[.]com
- carrentalagencies[.]com
- carrentalslasvegas[.]com
- casenumber900300[.]com
- casenumber900301[.]com
- casenumber900302[.]com
- casenumber900303[.]com
- casenumber900304[.]com
- casenumber900305[.]com

## Sample Additional IP Addresses

- 103[.]107[.]239[.]13
- 118[.]27[.]125[.]154
- 13[.]33[.]21[.]102
- 13[.]33[.]21[.]123
- 13[.]33[.]21[.]27
- 13[.]33[.]21[.]76
- 154[.]215[.]150[.]218
- 162[.]0[.]235[.]58
- 162[.]255[.]119[.]78
- 168[.]119[.]136[.]101
- 192[.]64[.]119[.]27
- 198[.]177[.]123[.]106
- 208[.]91[.]197[.]132
- 2600:9000:2363:1000:e:5d8c:1280:93a1

- 2600:9000:2363:200:e:5d8c:1280:93a1
- 2600:9000:2363:4600:e:5d8c:1280:93a1
- 2600:9000:2363:6200:e:5d8c:1280:93a1
- 2600:9000:2363:ae00:e:5d8c:1280:93a1
- 2600:9000:2363:b600:e:5d8c:1280:93a1
- 2600:9000:2363:c600:e:5d8c:1280:93a1

## Sample IP-Connected Domains

- 0a3kf3o[.]icu
- 0btpoh2[.]cfd
- 0hyxcdq1aiqwgwhymbqj[.]cfd
- 0nqj3ve[.]icu
- 121490[.]cn
- 16yk5knq[.]icu
- 20jpfxm[.]icu
- 23l24r9[.]icu
- 264325[.]wang
- 2pjwwxbkbwcl4j9ekpul[.]cfd
- 308qc97[.]icu
- 32462[.]in
- 3bj3bix[.]icu
- 3cjvzjrr4j[.]top
- 3i2im5[.]cfd
- 3m3derbsl0t1qqe[.]top
- 3n5oeqt[.]icu
- 3nt2gy3[.]icu
- 3u1wxs5[.]icu
- 3x3d1xp[.]icu
- 3xrs2zkqwqwnrhkszhxa[.]cfd
- 40rs1sz5[.]icu
- 41unj9h[.]icu
- 462245[.]cn
- 46ck6m5[.]icu
- 4bcotvnywtadaax[.]cfd
- 515106[.]nl
- 54zj2xe[.]icu
- 55jd5ms3[.]icu
- 5azyb4qe90[.]top
- 5es7g3p[.]icu
- 5mafzoi[.]icu
- 5s8odv4[.]icu
- 5soc75[.]fun
- 652325[.]wang
- 66498[.]in
- 6g8plzex6amfdj0numws[.]cfd
- 74cskewr[.]icu
- 7vlz0ff[.]icu
- 86dh3c[.]cfd
- 8f0aeoh[.]icu
- 90sjrpd[.]icu
- 921388[.]nl
- 94v26uu[.]icu
- 963695[.]cc
- 9tu5bvi[.]icu
- aio4bpg[.]icu
- b6lry[.]top
- b9sr33of[.]icu
- bhhvspg[.]cfd

## Sample String-Connected Domains

- 219855[.]biz
- 219855[.]cc
- 219855[.]cn
- 219855[.]com
- 219855[.]net
- 219855[.]top
- 219855[.]vip
- 219855[.]wang

- 219855[.]xyz
- austintrafficlawyers[.]com
- infinite-777[.]com
- overthemoonphotoboothrental[.]com
- overthemoonphotographer[.]com
- overthemoonphotography[.]ca
- overthemoonphotography[.]com
- overthemoonphotography[.]com[.]au
- overthemoonphotography[.]design
- overthemoonphotography[.]info
- overthemoonphotography[.]life
- overthemoonphotography[.]net
- overthemoonphotography[.]net[.]au
- overthemoonphotography[.]nl
- overthemoonphotography[.]org
- overthemoonphotographyblog[.]com
- overthemoonphotographybytiffany[.]com
- overthemoonphotographyla[.]com
- overthemoonphotogrpahy[.]life
- overthemoonphotos[.]ca
- overthemoonphotos[.]com
- terranovaservices[.]ca
- terranovaservices[.]com
- terranovaservices[.]net
- terranovaservices[.]org
- terranovaservicesllc[.]com
- vietdot[.]tk
- vietdot[.]vn
- vietdota[.]com
- vietdota2[.]com
- vietdota2open[.]com
- vietdota3[.]tk
- vietdotcomrightclothes[.]com
- vietdotdot[.]com
- vietdothai[.]com
- vietdotnet[.]com
- vietdotravel[.]com
- vietdots[.]com
- wgs[.]ac
- wgs[.]adv[.]br
- wgs[.]ae
- wgs[.]ai
- wgs[.]airline[.]aero
- wgs[.]app
- wgs[.]asia
- wgs[.]at
- wgs[.]au
- wgs[.]autos
- wgs[.]be
- wgs[.]best
- wgs[.]bet
- wgs[.]biz
- wgs[.]biz[.]id
- wgs[.]bj[.]cn
- wgs[.]black
- wgs[.]blue
- wgs[.]buzz
- wgs[.]bz
- wgs[.]ca
- wgs[.]cambs[.]sch[.]uk
- wgs[.]casino
- wgs[.]cc
- wgs[.]center
- wgs[.]church
- wgs[.]cl
- wgs[.]cloud
- wgs[.]club
- wgs[.]cm
- wgs[.]cn
- wgs[.]co
- wgs[.]co[.]at
- wgs[.]co[.]id
- wgs[.]co[.]im
- wgs[.]co[.]in
- wgs[.]co[.]jp
- wgs[.]co[.]kr
- wgs[.]co[.]nz
- wgs[.]co[.]uk
- wgs[.]co[.]za

- wgs[.]com
- wgs[.]com[.]au
- wgs[.]com[.]br
- wgs[.]com[.]cn
- wgs[.]com[.]do
- wgs[.]com[.]mx
- wgs[.]com[.]ng
- wgs[.]com[.]pl
- wgs[.]com[.]sg
- wgs[.]com[.]tr
- wgs[.]com[.]tw
- wgs[.]com[.]ua
- wgs[.]company