



Divulging the DNS Secrets of DarkSpectre

Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Artifacts](#)

Executive Report

Koi Security has been monitoring a threat group they have dubbed “DarkSpectre” for more than a year now. The group was behind at least three major malware campaigns leveraging Zoom Stealer, [ShadyPanda](#), and GhostPoster that have affected more than 8.8 million users over the course of their seven-year-long operation.

The researchers uncovered another DarkSpectre campaign that affected 2.2 million users so far. The group reportedly used a new GhostPoster-linked Opera browser extension that has been installed nearly 1 million times as of December 2025.

Koi Security identified 20 IoCs in their [report](#) comprising three subdomains, 12 domains, one IP address, and four email addresses.

We extracted unique domains from the subdomains, bringing the total number of domains to 15. We then excluded legitimate domains from our IoC list with the help of [Jake AI](#). The results showed that eight were legitimate domains, leaving us with seven for further analysis. That said, we further investigated 15 IoCs in all comprising three subdomains, seven domains, one IP address, and four email addresses. Our analysis led to these discoveries:

- 57 unique client IP addresses communicated with one domain identified as an IoC
- 8,579 email-connected domains, three of which turned out to be malicious
- Three additional IP addresses, two of which turned out to be malicious
- Five IP-connected domains, one of which turned out to be malicious
- 15 string-connected domains
- 250 string-connected subdomains

A Further Scrutiny of the Subdomain IoCs

We took a closer look at the three subdomains identified as IoCs aided by Jake AI. We discovered that while two of them were part of legitimate web infrastructures but could have



been compromised for attacks, one—policies[.]extfans[.]com—was illegitimate and currently inactive.

What can you tell me about policies.extfans.com?

Of course! I can certainly look into that for you. To give you a complete picture of `policies.extfans.com`, I'll check the WHOIS information for the parent domain, perform a DNS lookup on the subdomain, check for any security threats, and look at its SSL certificate details.

Let's get started.

- Used `whois` tool from WhoisXML API (13.33s)
- Used `dns_lookup` tool from WhoisXML API (391ms)
- Used `threat_intelligence` tool from WhoisXML API (767ms)
- Used `ssl_certificates` tool from WhoisXML API (591ms)

Based on my investigation of `policies.extfans.com`, here is a summary of my findings:

policies.extfans.com

- WHOIS Information:** The parent domain, `extfans.com`, was registered in 2018 through GoDaddy, and the registrant's information is protected by a privacy service.
- DNS Records:** The subdomain `policies.extfans.com` does not have any "A" records, which means it does not point to an IP address.
- Threat Intelligence:** I found no malicious activity associated with this subdomain.
- SSL Certificate:** I was unable to retrieve an SSL certificate because the domain is unreachable.

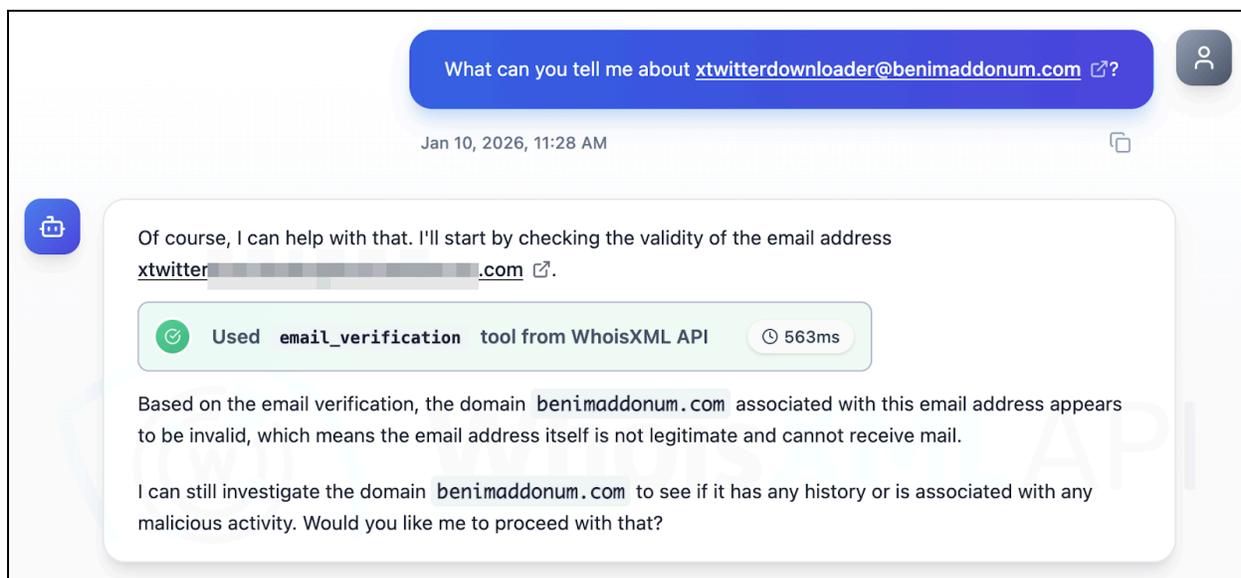
Conclusion: `policies.extfans.com` is not a legitimate or active website. The absence of DNS records indicates that this subdomain is not configured to be accessible on the internet. While the parent domain `extfans.com` is registered, this specific subdomain is not in use.

I hope this information helps! Let me know if you have any other questions.

Jake AI result for the policies[.]extfans[.]com query

An Examination of the Email IoCs

Next, we investigated the four email addresses identified as IoCs using Jake AI. While three of them were deemed legitimate, one was tagged as invalid.



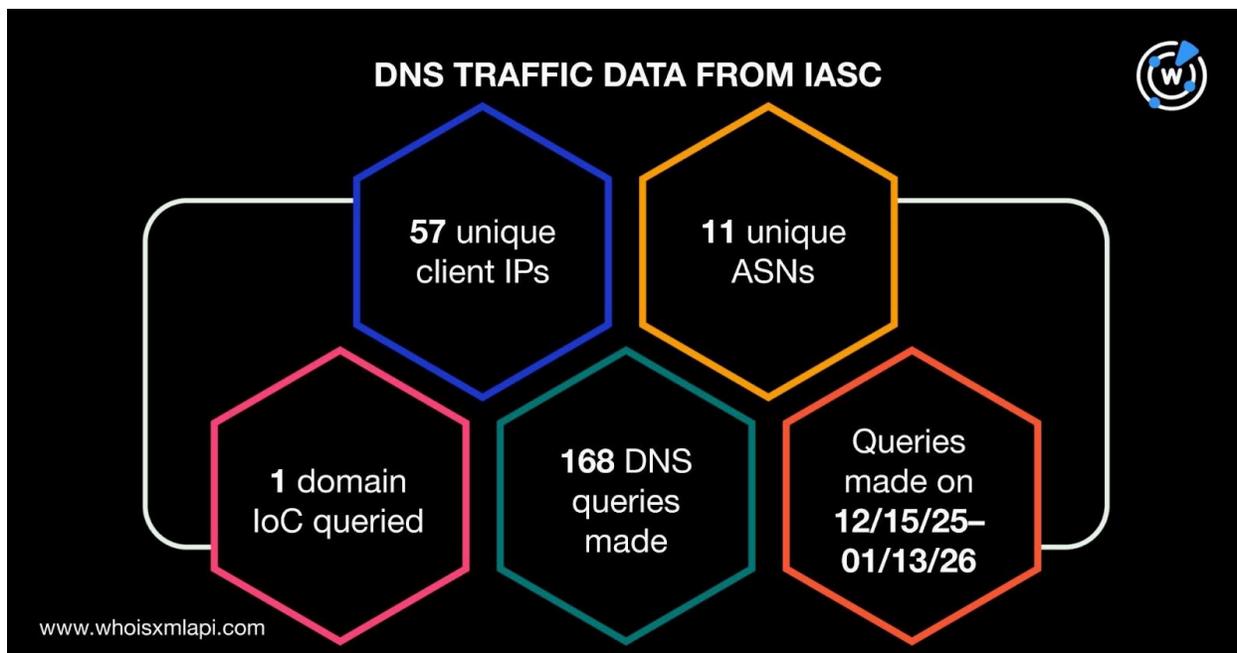
Jake AI query result for one of the email addresses identified as loCs

It is also worth noting that one other email address from the four identified as loCs was used to register domains. We will thus include it in our search for new artifacts later.

A Dissection of the Domain loCs

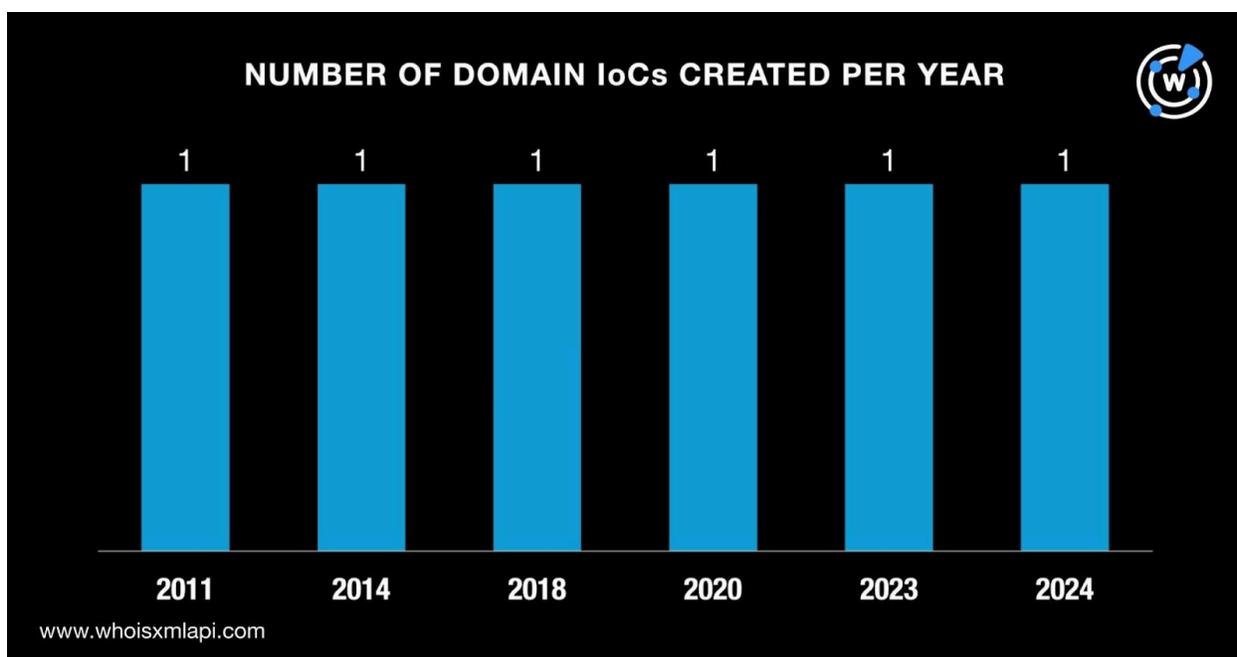
We looked more closely at the seven domains identified as loCs next.

Sample network traffic data from the [IASC](#) revealed that 57 unique client IP addresses under 11 distinct ASNs communicated with one domain identified as an loC via 168 DNS queries made between 15 December 2025 and 13 January 2026.



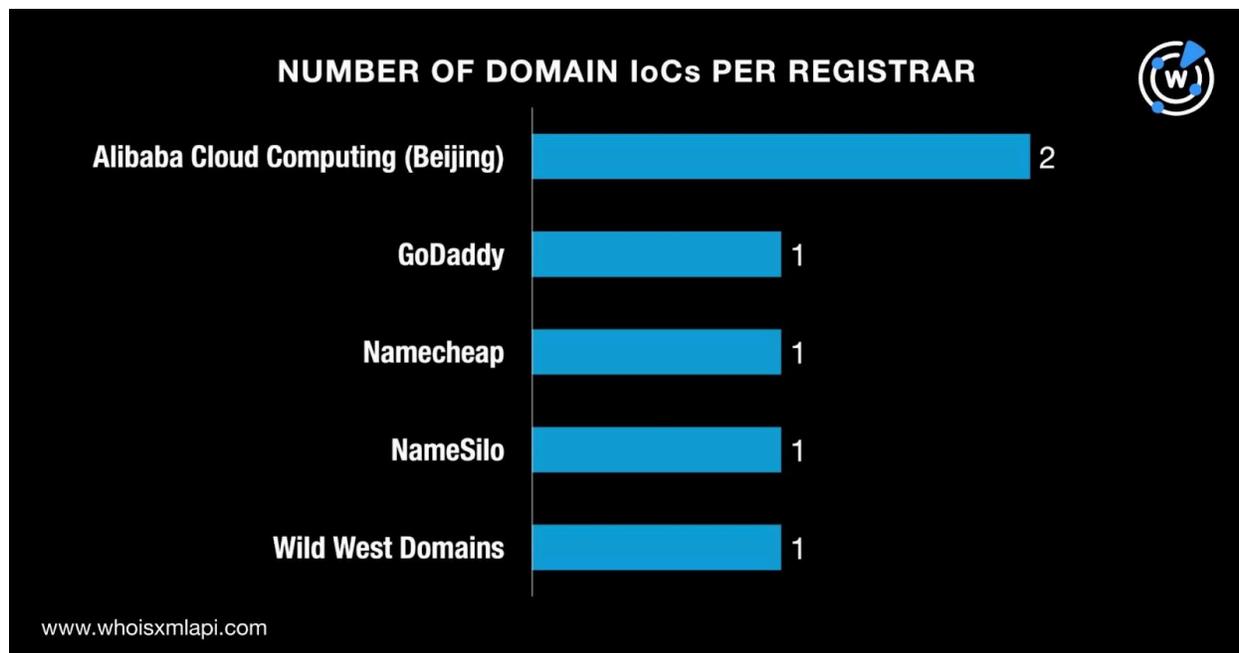
We also queried the seven domains identified as loCs on [WHOIS API](#) and found out that only six had current WHOIS records.

- They were created between 28 July 2011 and 24 September 2024, hinting at DarkSpectre’s preference for aged domains in their attacks. One domain each was registered in 2011, 2014, 2018, 2020, 2023, and 2024.

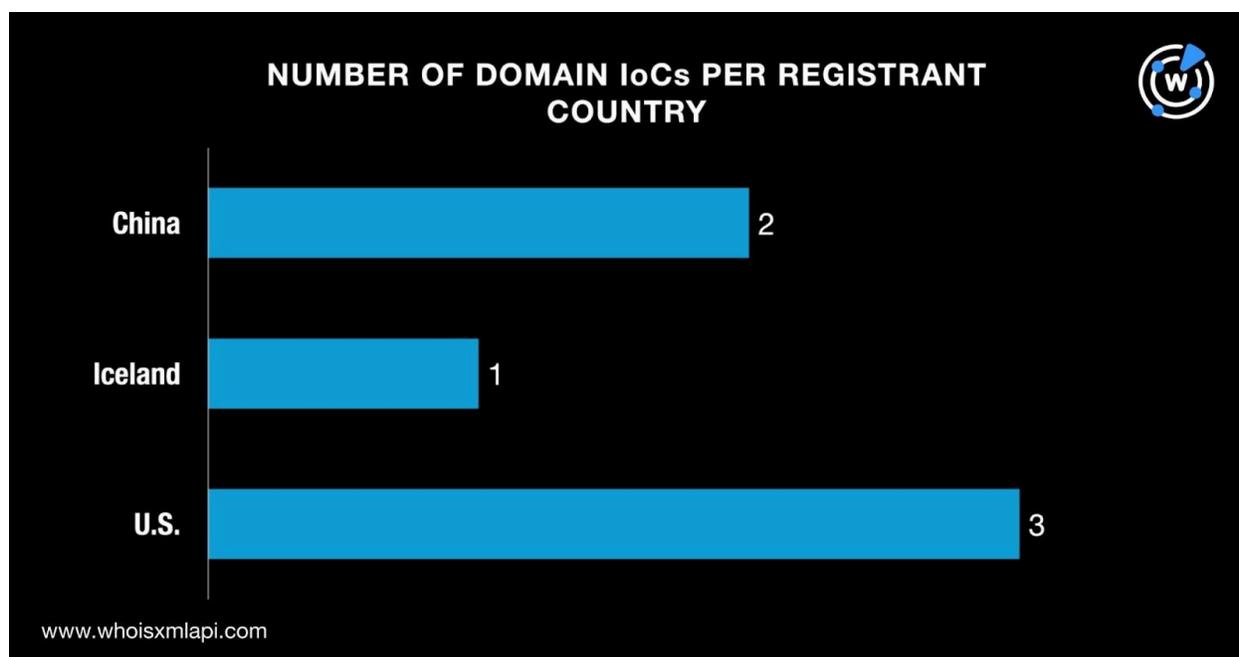




- They were administered by five different registrars—two by Alibaba Cloud Computing (Beijing) and one each by GoDaddy, Namecheap, NameSilo, and Wild West Domains.



- They were registered in three different countries—three in the U.S., two in China, and one in Iceland.





[DNS Chronicle API](#) queries for the seven domains identified as IoCs showed that only six had historical domain-to-IP resolutions. Altogether, they recorded 1,283 resolutions over time. The domain gmzdaily[.]com posted the oldest resolution on 5 February 2017.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
gmzdaily[.]com	393	02/05/17	12/17/25
infinitynewtab[.]com	261	02/06/17	11/16/22
extfans[.]com	205	06/11/18	4/28/23

An Investigation into the IP IoC

An [IP Geolocation API](#) query for the sole IP address identified as an IoC revealed that it was geolocated in China under the administration of China Unicom.

Interestingly, though, the IP address is currently not in use nor has not recorded historical IP-to-domain resolutions over time.

The Hunt for New Artifacts

After obtaining more information about the IoCs, we went on to search for new DarkSpectre-connected artifacts.

First, we queried the seven domains identified as IoCs on [WHOIS History API](#) and discovered that five of them had email addresses in their historical WHOIS records. We amassed nine email addresses in all and found out that seven were public email addresses. We now had eight public email addresses—seven from our searches and one tagged as an IoC (i.e., from the “An Examination of the Email IoCs” section)—for further analysis.

[Reverse WHOIS API](#) queries for the eight email addresses showed that one could belong to a domainer so we excluded the domains connected to it for the next step. The results for the remaining seven email addresses led to the discovery of 8,579 unique email-connected domains after those already identified as IoCs were filtered out.

The results of our [Threat Intelligence API](#) queries for the 8,579 email-connected domains revealed that three have already been weaponized for various attacks. An example is the domain rayganesh[.]com, which has been associated with malware distribution between 9 March 2023 and 1 January 2026.

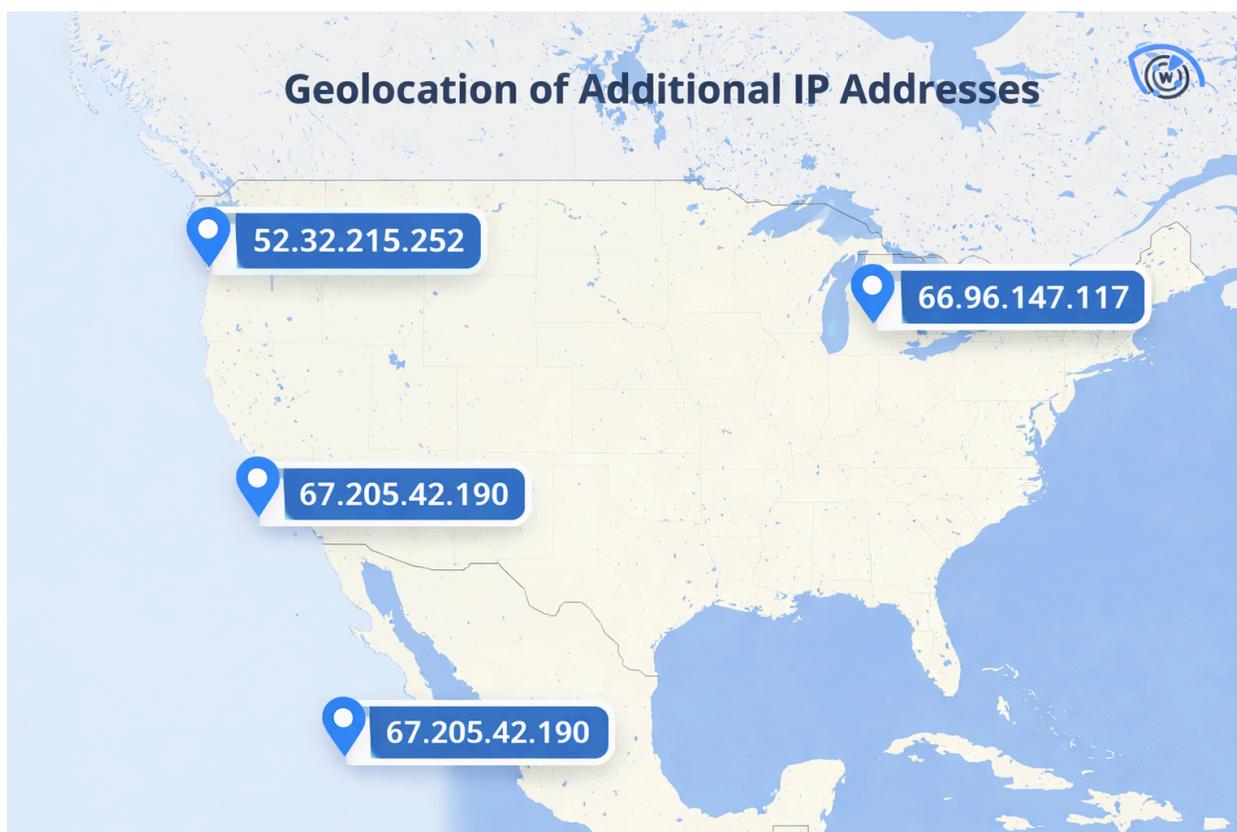


Next, we queried the seven domains identified as IoCs on [DNS Lookup API](#) and found out that three actively resolved to three unique additional IP addresses.

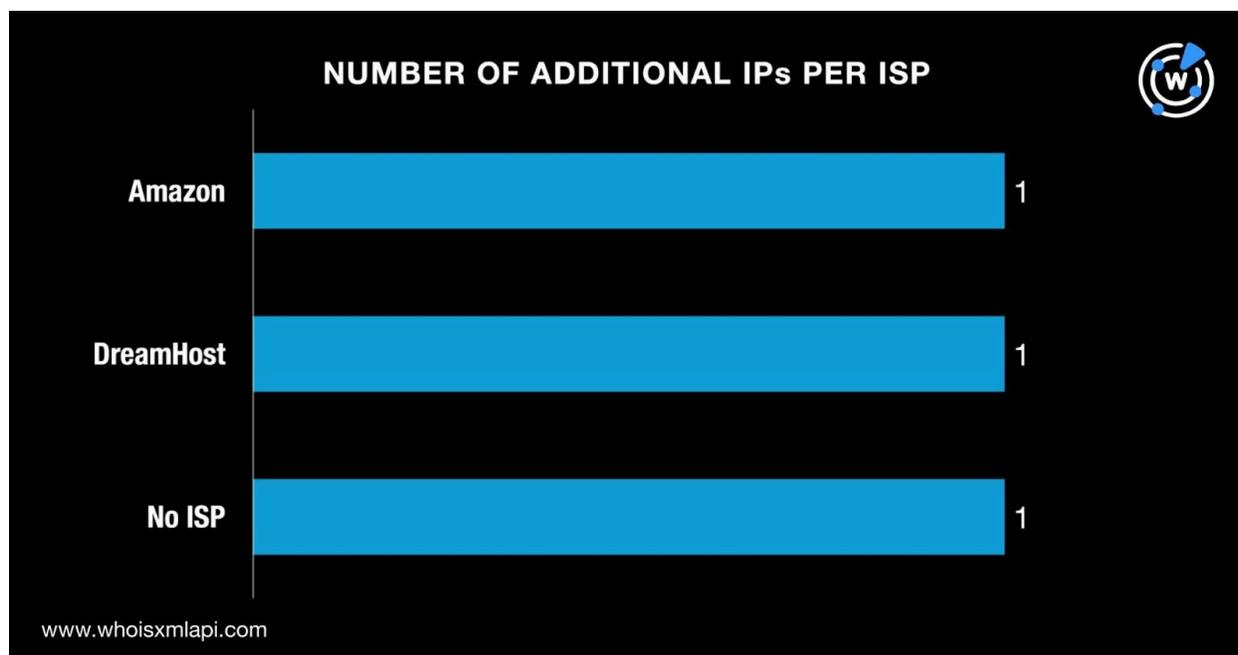
Threat Intelligence API queries for the three additional IP addresses revealed that two have already been weaponized for various attacks. An example is 66[.]96[.]147[.]117, which has been associated with malware distribution between 29 March 2023 and 29 December 2025 and a generic threat between 9 April 2023 and 12 October 2025.

A [Bulk IP Geolocation Lookup](#) query for the three additional IP addresses, meanwhile, showed that:

- They were all geolocated in the U.S.



- While one of them did not have an ISP on record, the other two were administered by Amazon and DreamHost.



We were now armed with four IP addresses—one identified as an IoC and three additional—for the next step. We queried them on [Reverse IP API](#) and discovered that two could be dedicated hosts. We uncovered five unique IP-connected domains after those already tagged as IoCs and the email-connected domains were filtered out.

Threat Intelligence API queries for the five IP-connected domains showed that one has already been weaponized for various attacks.

Next, we extracted seven unique text strings from the seven domains identified as IoCs. Our [Domains & Subdomains Discovery](#) searches for the strings revealed that four appeared at the start of domains other than those already tagged as IoCs. They were:

- **extfans.**
- **infinitynewtab.**
- **jt2x.**
- **userscss.**

We collated 17 unique string-connected domains after those already identified as IoCs and the email- and IP-connected domains were filtered out.

We also extracted these three unique text strings from the three subdomains identified as IoCs:

- **.extfans**
- **.cloudfunctions**
- **zoocorder.**



Our Domains & Subdomains Discovery searches for subdomains other than those already tagged as IoCs that contained the text strings above turned up 250 unique string-connected subdomains.

—

Our in-depth analysis of the DarkSpectre IoCs revealed that 57 unique client IP addresses communicated with one domain identified as an IoC.

In addition, we uncovered 8,852 new artifacts comprising 8,579 email-connected domains, three additional IP addresses, five IP-connected domains, 15 string-connected domains, and 250 string-connected subdomains. It is also worth noting that at least six of the new artifacts we unearthed have already figured in various malicious campaigns.

If you wish to 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

- 000105[.]com
- 000216[.]com
- 000230[.]com
- a1-satellitstv[.]com
- a1atek[.]com
- a2zembr[.]com
- b2b999[.]com
- b2wn[.]com
- b4ah[.]com
- c5icorp[.]com
- cabalic[.]com
- cabbagecards[.]com
- d-rigs[.]com
- d1king[.]com
- d2comp[.]com
- e-adam[.]com
- e-amsoil[.]com
- e-frugal[.]com
- fabricbid[.]com
- facemds[.]com
- facintel[.]com
- g-mobi[.]com
- g3vision[.]com
- g701[.]com
- h2otow[.]com
- h5jia[.]com
- h5plus[.]com
- i144[.]com
- i936[.]com
- i9inspect[.]com
- jackbkatz[.]com
- jackbunny[.]com
- jackskeytoliving[.]com
- k7g[.]net
- k953[.]com
- k9logo[.]com
- laalaw[.]com
- labellableu[.]com
- labrush[.]com
- m18-m18[.]info
- m2gl[.]com
- macamendment[.]com
- n-doc[.]com
- n40p[.]com
- n8skow[.]com
- o2et[.]com
- o3zq[.]com
- obpcorp[.]com
- p3ym[.]com
- pack175[.]com
- paclky[.]com
- qamlaakm[.]com
- qarrn[.]com
- qatargallery[.]net
- r0mp[.]com
- raajmedia[.]com
- rabideaucalc[.]com
- s573[.]com
- saabyes[.]com
- saadens[.]com
- t1soft[.]com
- t26fonts[.]com
- t2para3[.]com
- u2mansion[.]com
- u4ld[.]com
- uapbsga[.]com
- vailx[.]com
- valentinoyoga[.]com
- valiantspirits[.]com
- w2di[.]com
- wabusi[.]com
- wabymoon[.]com



- xahccw[.]com
- xasain[.]com
- xbajie[.]com
- y2ktravels[.]com
- y4bs[.]com
- yaghobian[.]com
- z7k[.]net
- z856[.]com
- zahks[.]com

Sample Additional IP Addresses

- 52[.]32[.]215[.]252
- 66[.]96[.]147[.]117

Sample IP-Connected Domains

- dealaced[.]com
- liveupdt[.]com
- trendupdeal[.]com

Sample String-Connected Domains

- extfans[.]cn
- infinitynewtab[.]cn
- jt2x[.]aquila[.]it
- userscss[.]com

Sample String-Connected Subdomains

- ww25[.]extfans-com[.]connext[.]com
[.]co
- medias3[.]cloudfunctionsupportmedi
as2[.]parissportifs[.]com
- us-central1[.]cloudfunctions-1261[.]
paypal-vending[.]com
- hosts[.]cloudfunctionsv40[.]azurewe
bsites[.]net
- studio-test--zoocorder[.]us-central1[
.]hosted[.]app
- meettimerserver-dot-zoocorder[.]uc[
.]r[.]appspot[.]com
- studio--zoocorder[.]us-central1[.]hos
ted[.]app