On a DNS Threat Hunt for DISGOMOJI

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

Cyber espionage is not uncommon and often occurs between rivals. And though the cyber attackers' tactics and techniques remain the same, their tools do not. The latest UTA0137 attack, for example, has taken to using DISGOMOJI, a malware written in Golang and disguised as various emojis to infiltrate target Indian organizations. UTA0137 is a threat group believed to be affiliated with Pakistani hackers. The malware, meanwhile, also has ties to an attack instigated by Transparent Tribe, a Pakistan-nexus hacking crew.

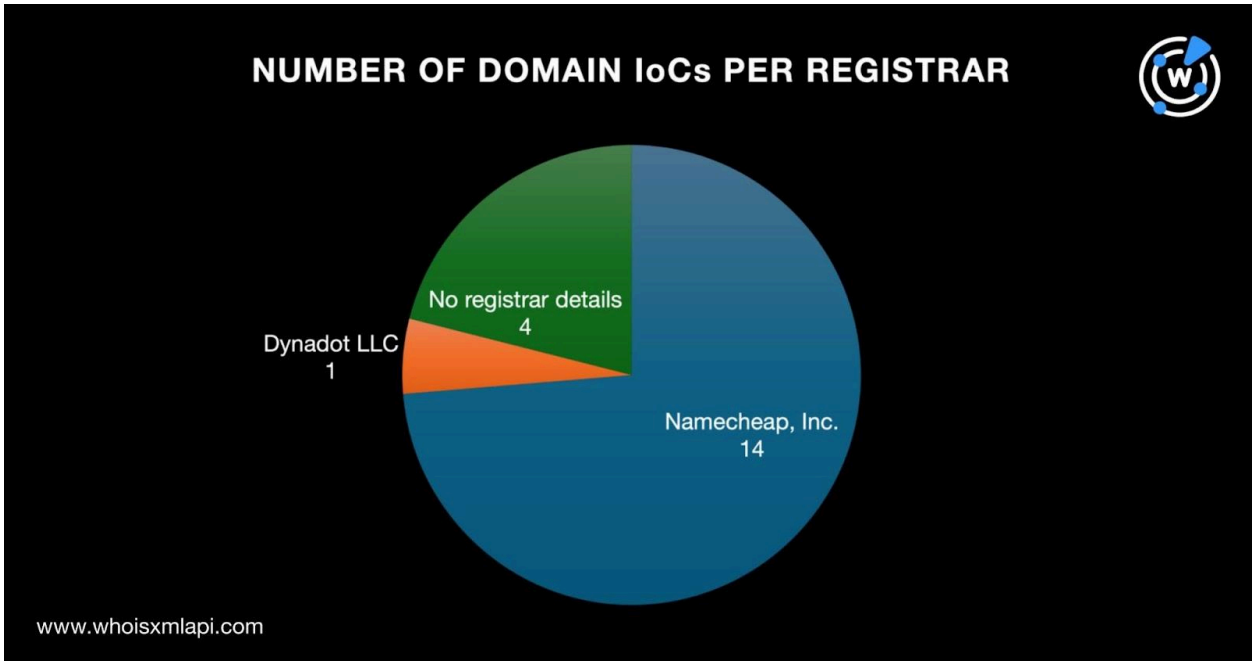
Volexity analyzed the cyber attack and disclosed 24 indicators of compromise (IoCs) comprising 19 domains and five IP addresses on 13 June 2024. The WhoisXML API research team expanded the current list of IoCs and found other potentially connected threat artifacts, including:

- Five email-connected domains
- Eight additional IP addresses, all of which turned out to be malicious
- 320 IP-connected domains
- 31 string-connected domains

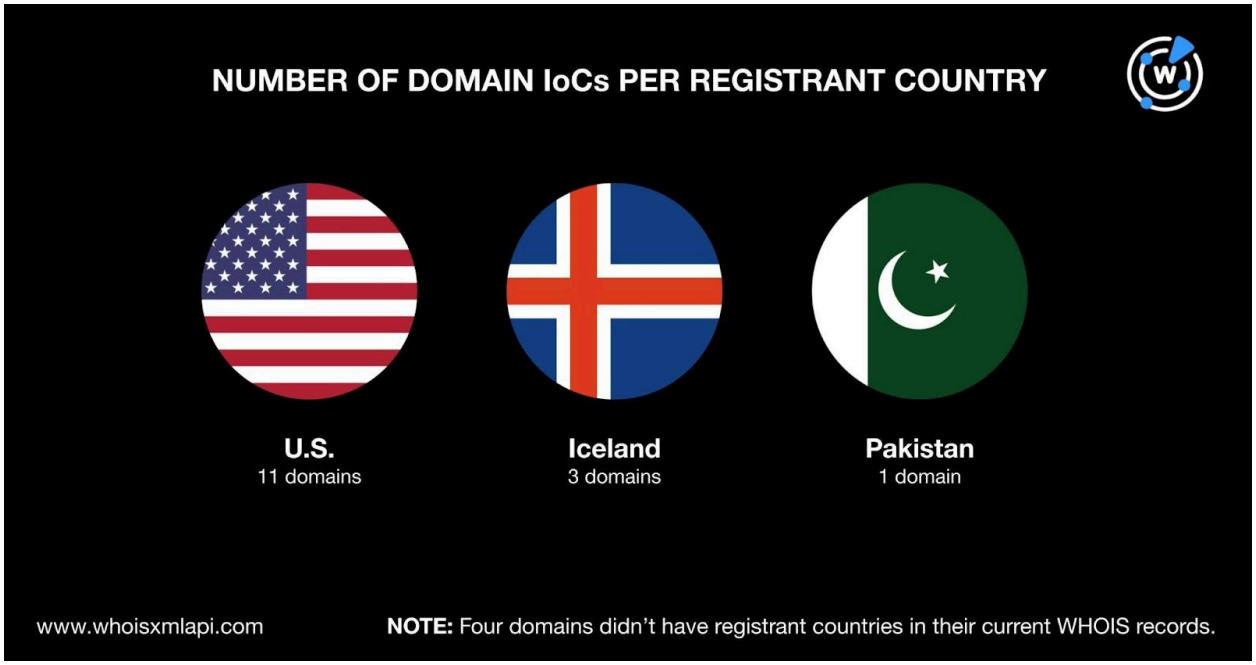
More about the DISGOMOJI IoCs

The DNS can always give more information about IoCs based on their WHOIS and DNS records. We began our DNS investigation with a bulk WHOIS lookup for the 19 domains tagged as IoCs. Our query allowed us to determine that:

- A huge majority of the domain IoCs, 14 to be exact, were administered by Namecheap, Inc. One fell under the purview of Dynadot LLC. Four, however, did not have registrars in their current WHOIS records.

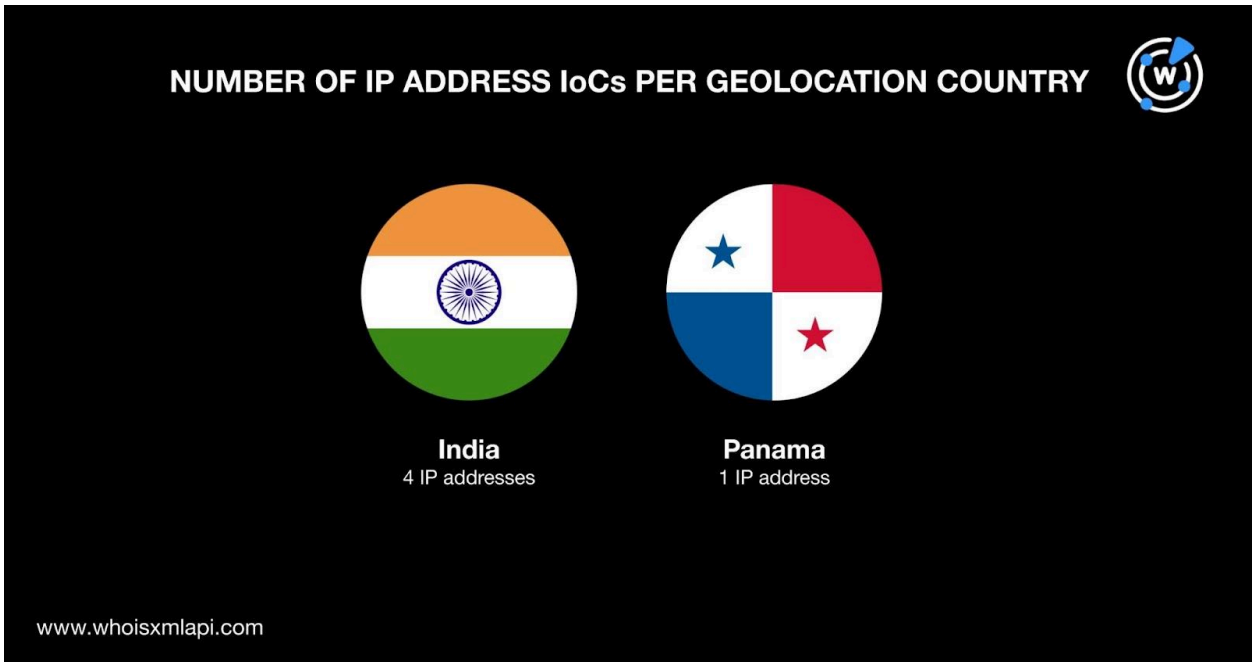


- The UTA0137 threat actors seemed to favor using newly registered domains (NRDs) for this particular attack, given that the domain IoCs were only created between 2023 and 2024. Note, though, that four of the IoCs did not have creation dates in their current WHOIS records and so might be inactive.
- The U.S. topped the list of registrant countries, accounting for 11 of the domain IoCs. Iceland followed with three IoCs. Pakistan completed the list of registrant countries with one IoC. Note that four domain IoCs did not have registrant countries in their current WHOIS records.

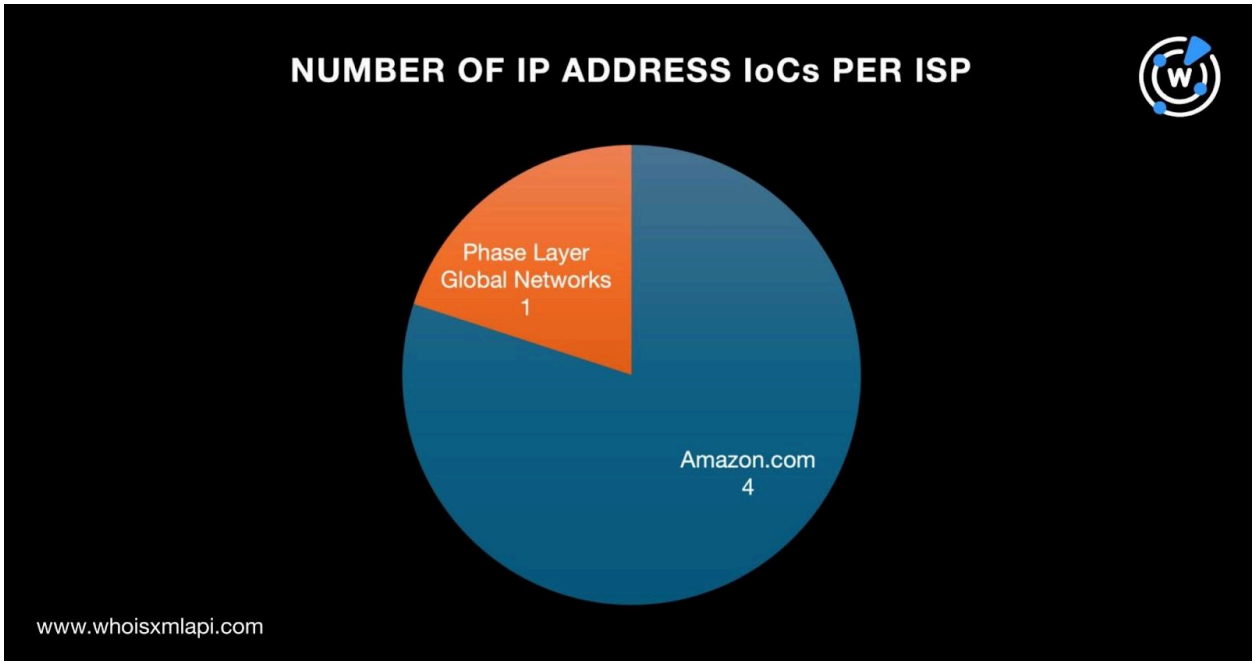


Next, we performed a [bulk IP geolocation lookup] for the five IP addresses tagged as IoCs. We found out that:

- The IP address IoCs were spread across two geolocation countries. Four originated from India and one from Panama.



- The IP address IoCs were administered by two ISPs—four by Amazon.com and one by Phase Layer Global Networks.



Other DISGOMOJI DNS Facts

After obtaining more information about the IoCs, we proceeded with looking for potentially connected DISGOMOJI artifacts.

We began by searching for email-connected domains. We ran WHOIS History API queries for the 19 domains tagged as IoCs, which allowed us to gather two email addresses from their historical WHOIS records. One of them was public.

A Reverse WHOIS API query for the public email address uncovered five email-connected domains after duplicates and the IoCs were filtered out.

Next, we sought out IP-connected domains. We began by running DNS lookups for the 19 domains tagged as IoCs. We found out that they resolved to eight unique IP addresses, which all turned out to be malicious according to Threat Intelligence Lookup. Take a look at five examples with their associated threat types below.

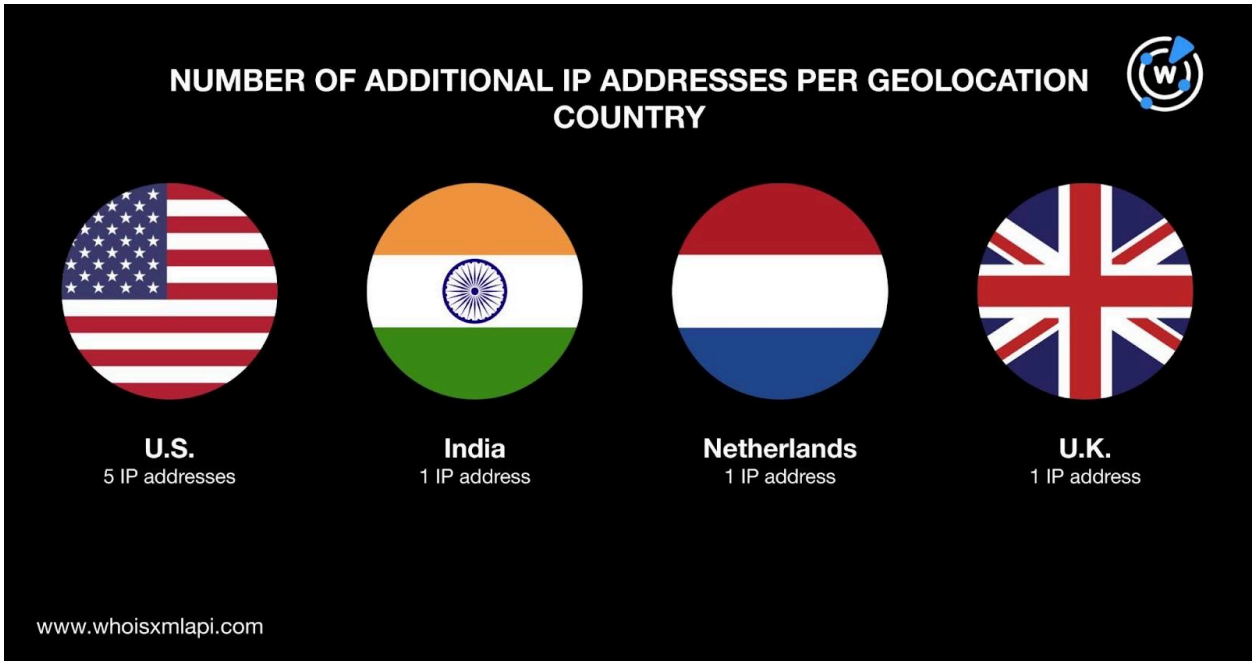
SAMPLE MALICIOUS IP ADDRESSES	
IP ADDRESS	**ASSOCIATED THREAT TYPE**

104[.]155[.]138[.]21	Attack Command and control (C&C) Generic Malware Phishing
104[.]21[.]89[.]254	Attack Malware Phishing
107[.]178[.]223[.]183	Attack C&C Generic Malware Phishing
153[.]92[.]7[.]29	Malware
172[.]67[.]150[.]126	Attack Malware Phishing

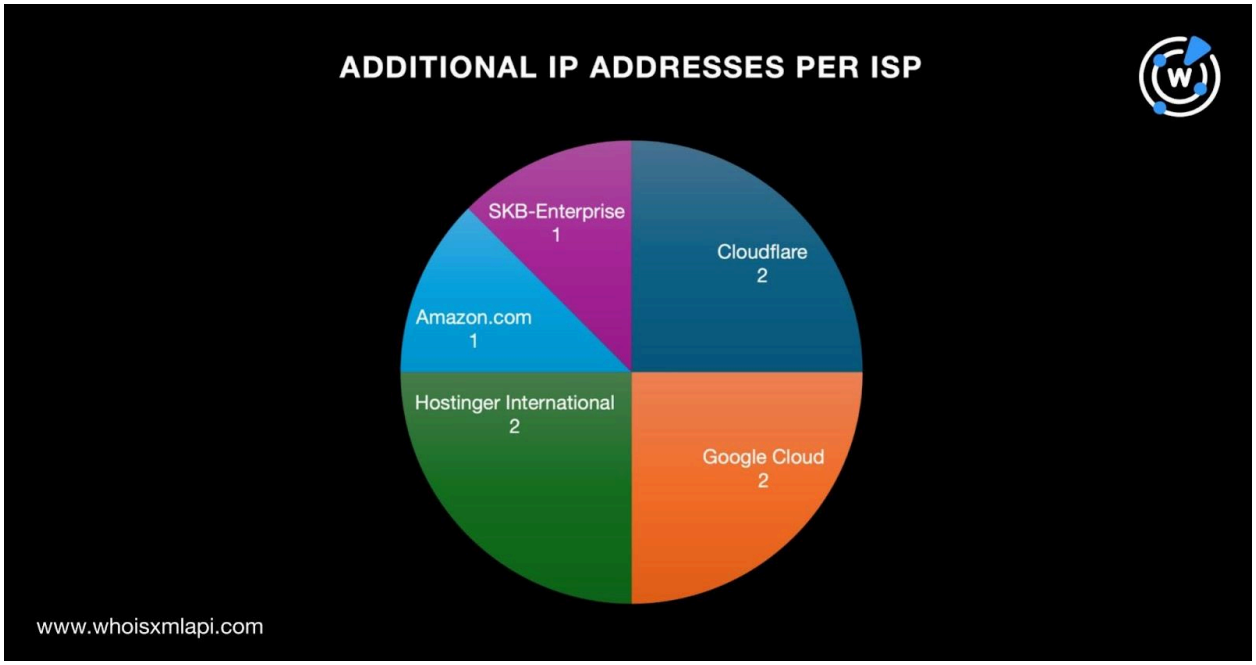
Consistent with the DISGOMOJI attack, all of the possibly connected IP addresses were associated with malware infection, among other threats, of course.

A bulk IP geolocation lookup for the eight additional IP addresses showed that:

- They originated from four countries led by the U.S., which accounted for five IP addresses. One IP address each pointed to India (consistent with one of the IoCs' geolocation countries), the Netherlands, and the U.K.



- They were spread across five ISPs. Cloudflare, Google Cloud, and Hostinger International administered two IP addresses each. Amazon.com (consistent with one of the IoCs' ISPs) and SKB-Enterprise, meanwhile, handled one each.



We now had 13 IP addresses (five IoCs and eight additional) to work with. Reverse IP Lookup revealed that three of them did not have active domain resolutions. Of the 10 that are in use,

five were shared while the remaining five could be dedicated hosts. Altogether, the five possibly dedicated IP addresses hosted 320 IP-connected domains after duplicates, the IoCs, and the email-connected domains were filtered out.

Based on the results of our Screenshot API queries, 289 of the IP-connected domains remained accessible to date.

To cover all the bases, we scoured the DNS next for string-connected domains using Domains & Subdomains Discovery. Since the oldest domain IoCs were created in 2023, we limited our search to domains added since 1 January 2023 that started with the exact text strings found in the 19 domains tagged as IoCs. Only seven of the domain IoC text strings, however, appeared in other domains given our strict parameters. They were:

- **awesindia.**
- **clawsindia.**
- **emailnic.**
- **infosec2.**
- **ordai.**
- **parichay.**
- **publicinfo.**

We found 31 string-connected domains after duplicates, the IoCs, and the email- and IP-connected domains were filtered out. Screenshot API showed that 22 of them remained accessible to date.

—

Our DNS hunt for DISGOMOJI artifacts led to the discovery of 364 web properties comprising five email-connected domains, eight additional IP addresses, 320 IP-connected domains, and 31 string-connected domains. We also found that all of the connected IP addresses were associated with various threats, which could be valuable information for organizations that fit the bill for usual UTA0137 targets.

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

- e-dscards[.]com
- gamingign[.]com
- lastdayfreecoins[.]com

Sample Additional IP Addresses

- 104[.]155[.]138[.]21
- 104[.]21[.]89[.]254
- 107[.]178[.]223[.]183
- 153[.]92[.]7[.]29

Sample IP-Connected Domains

- 6ixslots[.]com
- 6ixslots[.]net
- abo-rashed[.]online
- advokatristicdusan[.]com
- akshaypatra[.]online
- aksiomcode[.]com
- aliunlockers[.]com
- alkataba-zawajmsyar[.]online
- alkataba[.]online
- alkhtaba[.]online
- almw3alj[.]online
- almw3allj[.]online
- almw3lyj[.]online
- almwalj[.]online
- alrawhany[.]online
- alrwhane[.]online
- alrwhany-mw3alyg[.]space
- alshka[.]online
- alshkaa[.]online
- alshykh[.]online
- alzawaj-almsyar[.]com
- alzawaj-almsyar[.]online
- am-amer[.]online
- am-fahd[.]online
- am-mahyr[.]online
- am-musab[.]online
- am-remal[.]online
- am-salm[.]online
- am-satam[.]com
- ankama-gift[.]boutique
- ankama-gift[.]store
- ankama-mystery[.]info
- ankama-premuim[.]info
- ankama-wakfu[.]buzz
- antalyahills[.]site
- antalyahills79[.]online
- antarangdesigns[.]in
- arthaatmedia[.]com
- audiodackfederalcu[.]com
- beaconlightckm[.]com
- bgvsindia[.]org
- binarymagic[.]in
- bit-globalworldfinance[.]org
- bodywisenutrition[.]in
- boomdigital[.]in
- brix-forex[.]com
- bulkcart[.]co[.]in
- busrentalinnepal[.]com
- campershive[.]com
- caomod[.]site

Sample String-Connected Domains

- awesindia[.]net
- awesindia[.]org
- clawsindia[.]ph
- emailnic[.]com
- emailnic[.]net
- emailnic[.]org
- infosec2[.]com
- infosec2[.]ws
- ordai[.]xyz
- parichay[.]buzz
- parichay[.]co
- parichay[.]co[.]uk
- parichay[.]com
- parichay[.]com[.]np
- parichay[.]info
- parichay[.]link