From Counterfeiting to Phishing: Cybersquatting Properties Target Network Device Makers

Table of Contents

Executive Report

Early last July 2022, news broke out about the arrest of a CEO who allegedly sold fake Cisco networking devices. While he used e-commerce sites as sales channels, the idea that counterfeit products are also peddled through cybersquatting domains is not too far-fetched. In fact, we demonstrated this at Europol's 13th Operation In Our Sites (IOS), along with other organizations in the cybersecurity community.

Aside from counterfeiting, cybersquatting domains can also serve as vehicles for other types of cybercrime, such as spear phishing, scams, and spamming. In line with that, WhoisXML API researchers monitored the Domain Name System (DNS) for cybersquatting domains targeting Cisco and its major competitors—Avaya, Broadcom, Juniper Networks, and Netgear. Our findings include:

- 2,700+ cybersquatting domains and subdomains targeting the five network hardware providers were added from 1 June to 8 August 2022
- More than 99% of the properties couldn't be publicly attributed to the legitimate companies
- About 86% of the properties actively resolved to IP addresses
- Despite being relatively new, more than a dozen properties have already been flagged as malicious

Dissecting the Cybersquatting Properties Targeting Network Hardware Providers

We used the company names as search strings to retrieve relevant properties using Domains & Subdomains Discovery. To lessen the number of false positives, we added restrictions, such as excluding domains that contained the string "francisco" for Cisco cyber resources.

We found 2,797 cybersquatting properties added from 1 June to 8 August 2022. We then analyzed these resources using IP, WHOIS, and other DNS intelligence tools.

Who Owns the Properties?

Before proceeding with any other analyses, we thought it'd be interesting to establish attribution for the properties. Does the targeted company own them? Based on the Bulk WHOIS Lookup results, the cybersquatting properties could hardly be attributed to the network hardware providers.

In particular, only eight domains shared the same publicly available registrant details as the official domains of the companies, and they were all owned by Cisco. About 85% of the non-publicly attributable domains actively resolved to 1,400+ unique IP addresses.

Where Are the Cybersquatting Resources Located?

More than 60% of the properties resolved to IP addresses geolocated in the U.S., while the rest were distributed across 49 other countries. The locations didn't differ much from the registrant countries of most of the domains. About 46% of them were registered in the U.S. as well, and the remaining domains were registered across 47 other countries.

The table below shows the top 10 countries in terms of IP geolocation and WHOIS registration, along with the percentage of properties attributed to them.

Top 10 IP Geolocations	Top 10 Registrant Countries
1. U.S. (60.34%) 2. Germany (6.54%) 3. Canada (4.85%) 4. U.K. (4.85%) 5. France (3.16%) 6. Ireland (2.39%) 7. Switzerland (2.21%) 8. Russia (1.94%) 9. Netherlands (1.67%) 10. China (1.32%)	1. U.S. (45.59%) 2. Iceland (5.74%) 3. Canada (5.50%) 4. Austria (4.28%) 5. U.K. (2.75%) 6. France (1.78%) 7. Germany (0.89%) 8. China (0.89%) 9. Japan (0.65%) 10. Finland (0.49%)

Table 1: *Top 10 locations of the cybersquatting properties*

What Organizations Oversee the Properties?

Part of our study was to find out who had authority over the properties. For the domains, that would be GoDaddy, since it is the top registrar of the cybersquatting resources, accounting for

16% of the registrations. It was followed by MarkMonitor, Namecheap, Network Solutions, Info.at Google, Amazon, PDR Ltd., 123-Reg Limited, and Wix. The rest were distributed across 154 other registrars.

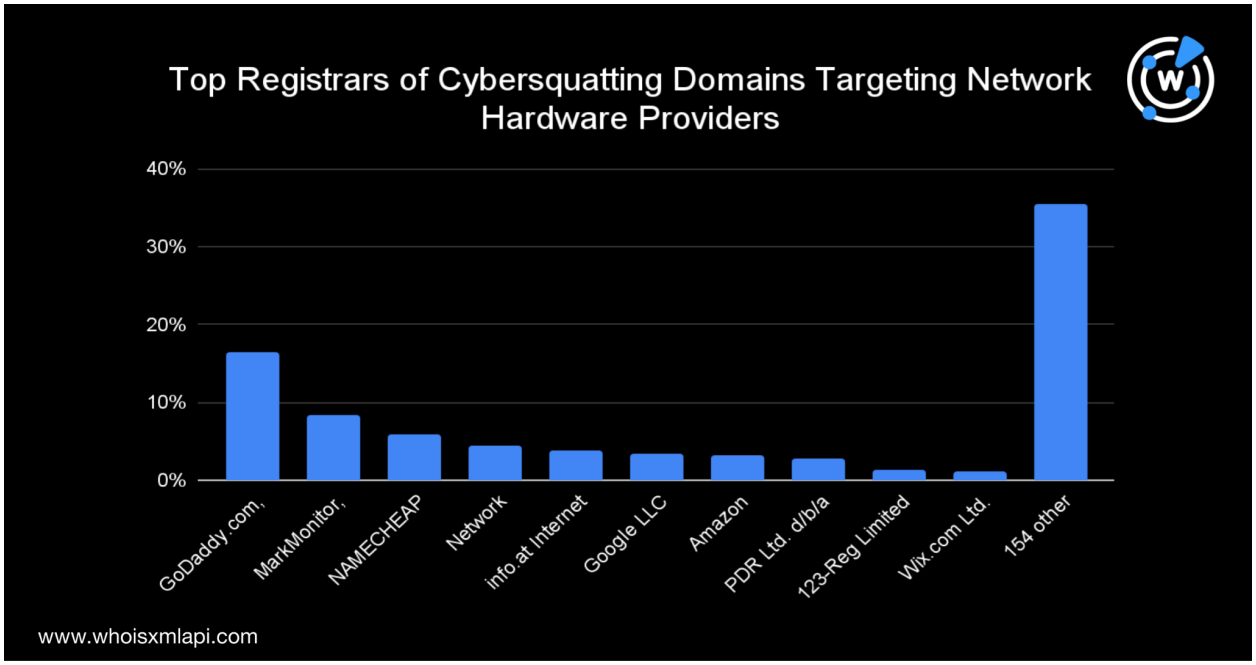

Chart 1: *Top 10 registrars of the cybersquatting domains*

Most of the cybersquatting domains in the study (19%) resolved to IP addresses belonging to Amazon. Google accounted for 10%, followed by Cloudflare, Microsoft, Fastly, OVH, Linode, Hetzner, Digital Ocean, and Wix.

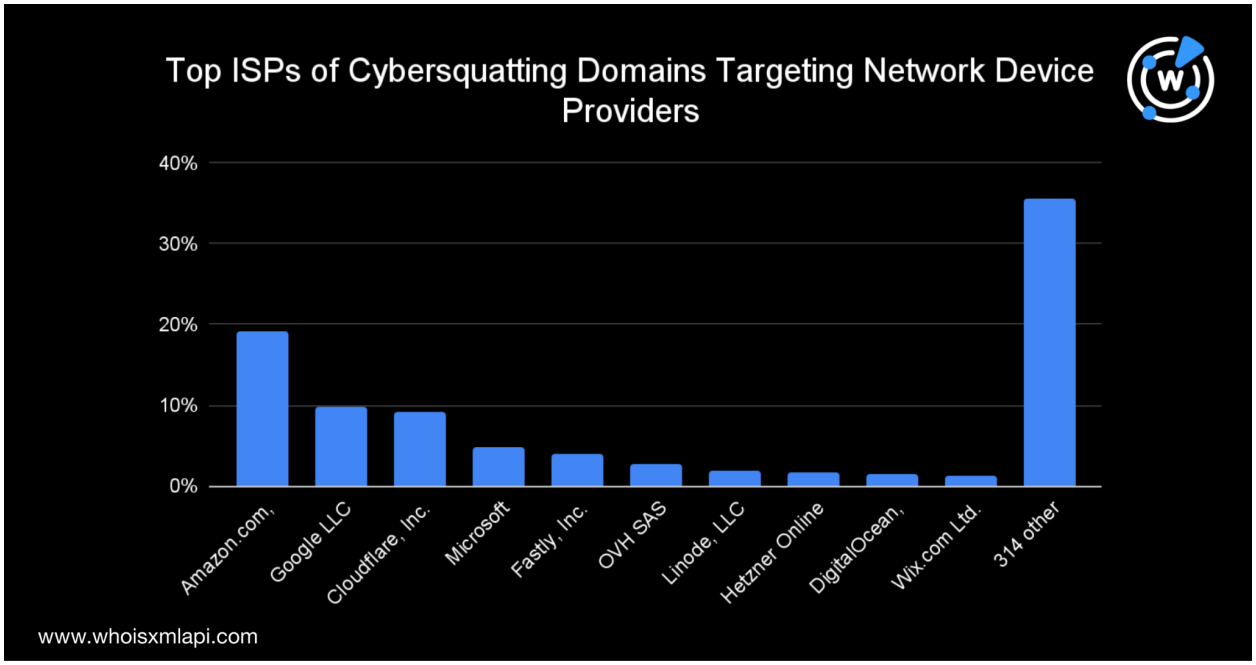

Chart 2: *Top 10 Internet service providers (ISPs) of the resolving cybersquatting domains*

Malicious Properties Alert

More than a dozen cybersquatting resources have been reported as malicious since 8 August 2022. Among them is netgearextendersetups[.]com, which resolved to 190[.]115[.]26[.]62. Five other similar-looking cybersquatting domains also resolved to the same IP address but haven't been flagged yet. These are:

- netgearwifiextendersetupen[.]com
- netgearextendersetupwifi[.]com
- netgearextender-setup[.]com
- netgearwifiextendersetup[.]us
- netgearwifiextendersetupgo[.]com

Aside from resolving to the same IP address, these domains also shared the same registrar and nameserver. The rest of their WHOIS details were redacted, except for netgearwifiextendersetup[.]us. We retrieved a public email address that was historically tied to 17 suspicious-looking domains, according to Reverse WHOIS Search. Some seemed to mimic the login pages of router and entertainment sites. These are shown in the screenshot below.

Only time can tell if they will also be weaponized, but keeping an eye on them and other cybersquatting properties could be a good cybersecurity practice.

—

We began with cybersquatting properties, some of which could be benign. Still, a deep dive into the malicious ones led us to more suspicious properties that could harm users and their networks.

The suspicious properties we uncovered in this post can be used to sell fake network devices. They can also be weaponized to serve as phishing, scam, and malware distribution vectors.

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 Domains

Sample Cybersquatting Domains

- academiacisco[.]vg
- alibazziciscollegeghobayri[.]info
- armornetgear[.]com
- authorjuniperjillianjoy[.]biz
- avaya-9611g-10[.]com[.]de
- avaya9611g-hr-int-5683[.]vg
- avaya-9641g-int-8016[.]net[.]ph
- avayacare[.]ru

- bloodofjuniper[.]com
- cec-cisco[.]ru
- cisco-034[.]nom[.]za
- cisco119[.]ws
- cisco12-2[.]com[.]de
- cisco3[.]ml
- ciscobisco[.]com
- cisco-campusnet-1[.]nom[.]za
- cisco-core[.]com[.]de
- ciscocyberresiliencebootcamp[.]com
- ciscodesigned[.]cn
- ciscofc4[.]ws
- cisco-fw[.]msk[.]ru
- cisco-helpdesk[.]cf
- ciscokw[.]xn--kpry57d
- ciscolassiterphotography[.]com
- ciscolegacyparts[.]com
- ciscomblet[.]tk
- ciscomind[.]com
- cisconetprotects[.]com
- cisconetworks[.]co
- ciscongtifaper[.]ga
- ciscononother[.]com
- ciscoseaport[.]com
- ciscosecureclient[.]vip
- ciscosecurecloud[.]com
- ciscosseptic[.]com
- ciscosurport[.]life
- ciscotechnologyevents[.]co[.]uk
- ciscotechnologyevents[.]com
- ciscotoolbag[.]com
- ciscowebshop[.]xn--kpry57d
- davinciscorner[.]in
- delavaya-business[.]services
- havayahyogaschool[.]com
- havayarn[.]com
- ivr-havaya[.]net
- jahancisco[.]com
- juniper[.]plus
- juniperadvisorygroup[.]com
- juniperandpinedesigns[.]com
- juniperappworks[.]com
- juniperathletics[.]com
- juniperbasil[.]net
- juniperbasilproductions[.]com
- juniperbloomorganizingllc[.]com
- juniperbuildcon[.]com
- juniperbyjenna[.]com
- juniperclinics[.]com[.]cn
- junipercocomello[.]com
- juniperdl[.]com[.]cn
- juniperfax[.]com
- juniperfinancialconsulting[.]com
- junipergrovedesigns[.]com
- juniperhouseproductions[.]com
- juniperk9training[.]com
- juniperlooker[.]com
- juniperluna[.]rocks
- junipermoonholistic[.]com
- junipermoonmagicalwares[.]com[.]au
- juniperpersonalfitness[.]com
- juniperplantco[.]com
- juniperpond[.]ws
- juniperpreserve[.]org
- juniperpreserves[.]org
- juniperreserve[.]com
- junipersage[.]co[.]uk
- junipersales[.]info
- juniperschild[.]co[.]uk
- juniperskies[.]xn--kpry57d
- juniperslt[.]com
- juniper-studio[.]co
- junipertechco[.]com
- junipertreecare[.]co[.]uk
- junipertreelearning[.]com
- juniperuspub[.]hu
- junipervacollective[.]com
- junipervalleycapital[.]com
- juniperwenatchee[.]com

- lifejuniperfinancial[.]com
- marciscorner[.]biz
- mirkocisco[.]com
- mustbroadcompany[.]buzz
- navayahotelsandresorts[.]net[.]in
- ravayatirim[.]com
- rinnovatocisco[.]it
- sageandjuniperjewelry[.]com
- sahayakdravayafoundation[.]com
- steveciscoblog[.]com
- t4avaya[.]com
- zavayalee[.]com
- zifcisco[.]ws

Sample Cybersquatting Subdomains

- cisco[.]360s[.]mx
- cisco[.]4lima[.]ch
- cisco[.]8ipz[.]info
- cisco[.]bbswaimao[.]com
- cisco[.]chzim[.]com
- cisco[.]debug[.]com[.]ua
- cisco[.]dekstop[.]my[.]id
- cisco[.]drud[.]us
- cisco[.]fin[.]ci
- cisco[.]gleeze[.]com
- cisco[.]indosoft[.]tech
- cisco[.]jeffghanbari[.]ir
- cisco[.]kienle[.]at
- cisco[.]kinghost[.]net
- cisco[.]mackay[.]tech
- cisco[.]marsmice[.]com
- cisco[.]meyer-gruhl[.]de
- cisco[.]mywire[.]org
- cisco[.]nsupdate[.]info
- cisco[.]otdev[.]org
- cisco[.]pages[.]dev
- cisco[.]rimstorm[.]xyz
- cisco[.]utcenter[.]ru
- cisco[.]wavekarthosting[.]com
- cisco[.]ydn[.]id[.]au
- cisco[.]acdc[.]dev
- cisco[.]a-ket[.]net
- cisco[.]aquila[.]it
- cisco[.]bankofcyprus[.]com
- cisco[.]bukhara[.]su
- cisco[.]digitalinfolive[.]online
- cisco[.]dynu[.]net
- cisco[.]egtvedt[.]no
- cisco[.]home-webserver[.]de
- cisco[.]ibrahim-akbar[.]me
- cisco[.]itdesk[.]tech
- cisco[.]jkrealtyaz[.]com
- cisco[.]juliahub[.]app
- cisco[.]mananraj[.]co[.]in
- cisco[.]mchm[.]site
- cisco[.]mexiaisd[.]net
- cisco[.]nid[.]io
- cisco[.]official[.]academy
- cisco[.]onrender[.]com
- cisco[.]pathwise[.]ca
- cisco[.]pooyandegan[.]net
- cisco[.]shafqatahmed[.]net
- cisco[.]signifi[.]club
- cisco[.]siteweb[.]cn
- cisco[.]skin[.]market
- cisco[.]sleepfit[.]com[.]au
- cisco[.]sunguanqi[.]com
- cisco[.]tbtmarketing[.]com
- cisco[.]tnlvl[.]com
- cisco[.]twill[.]tech
- cisco[.]underground[.]top
- cisco0[.]filegear-de[.]me
- cisco0[.]gr[.]com
- cisco0[.]ngrok[.]io
- cisco0[.]on-web[.]fr

- cisco0[.]pagespeedmobilizer[.]com
- cisco1[.]nid[.]io
- cisco1[.]opencraft[.]hosting
- cisco2[.]8ipz[.]info
- cisco2[.]cloudns[.]in
- cisco2[.]githubpreview[.]dev
- cisco2[.]homesecuritymac[.]com
- cisco2[.]tnlvl[.]com
- cisco2[.]apple-ervin[.]com
- cisco2[.]avalon[.]company
- cisco2[.]utwente[.]io
- cisco3[.]siteleaf[.]net
- cisco3[.]hamrah-gsm[.]com
- cisco3[.]mycloud[.]by
- cisco4[.]mo-siemens[.]io
- cisco4[.]tuxfamily[.]org
- cisco4[.]wedeploy[.]io
- cisco6[.]qualifioapp[.]com
- cisco7[.]crd[.]co
- cisco7[.]ed[.]pw
- cisco8[.]withyoutube[.]com
- cisco8[.]operaunite[.]com
- ciscob[.]platter-app[.]com
- ciscob[.]siteleaf[.]net
- ciscob[.]herokuapp[.]com
- ciscoj[.]townnews-staging[.]com
- ciscoj[.]nid[.]io
- ciscol[.]repl[.]co
- ciscon[.]definima[.]net
- ciscon[.]gwiddle[.]co[.]uk
- ciscos[.]homesecuritymac[.]com
- ciscos[.]0e[.]vc
- ciscos[.]browsersafetymark[.]io
- ciscos[.]jp[.]net
- ciscos[.]localroofingpros[.]com
- ciscot[.]vipsinaapp[.]com
- ciscow[.]1kapp[.]com
- ciscox[.]acdc[.]dev
- fcisco[.]gwiddle[.]co[.]uk
- tcisco[.]cloudcontrolapp[.]com

Sample Malicious Properties Flagged during the Malware Check Dated 9 August 2022

- broadcomparehere[.]buzz
- cisco-help[.]cf
- ciscokn[.]info
- ciscovpn2[.]com
- experiencebroadcommon[.]xyz
- mustbroadcompany[.]buzz
- myciscologin[.]cf
- netgear[.]my[.]id
- netgearextendersetups[.]com
- ranbroadcompare[.]buzz