Insights into an Active Spam Domain Portfolio

Table of Contents

Executive Report

Malicious spam, possibly the oldest kind of cyber threat, likely remains one of enterprises' biggest security concerns.

Regardless of form and affected device, clicking a malicious link embedded in a spam email or downloading a malware-laden attachment can lead to financial, data, or identity theft. To this end, knowing and consequently blocking access to where these harmful messages come from is of utmost importance to companies.

As part of our ongoing effort to make the Internet safer, we sought to expand an initial list of 53 verified malicious spam domains aided by WHOIS, DNS, and IP intelligence. Our findings include:

- 71 IP addresses to which the domains identified as indicators of compromise (IoCs) resolved, a majority of which are geolocated in the U.S.
- 18 unredacted email addresses used to register the IoCs obtained from historical WHOIS records
- 354 additional domains that shared the IoCs' registrant email addresses or IP hosts

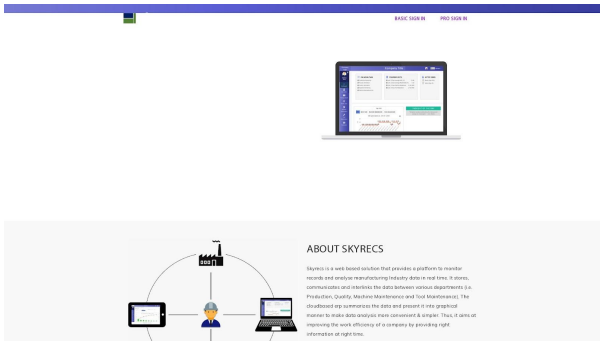
Insights Gleaned from the Initial List of IoCs

We began our investigation by looking for identifiable characteristics among the IoCs. To do so, we ran them through a bulk WHOIS lookup that revealed:

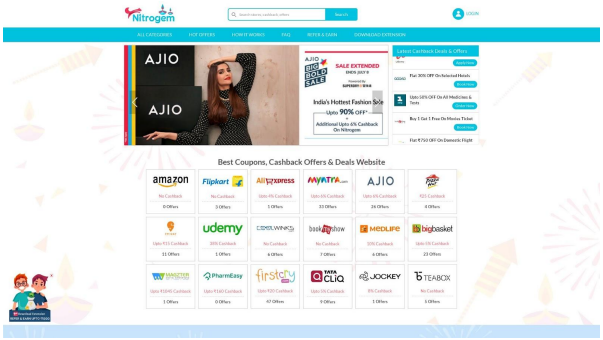
- Four domains with retrievable current WHOIS records—chbit[.]com, ghqd[.]net, mvgu[.]net, and nitrogem[.]com.
- All four IoCs were newly registered domains (NRDs) whose registrant details have been withheld for privacy.

- Four of the IoCs—corvusrex[.]com, skyrecs[.]com, nitrogem[.]com, and cinelon[.]com—continue to host live content that look to belong to legitimate businesses based on the results of screenshot lookups. If they were primarily created for malicious spam campaigns, then their owners exerted effort to mask their criminal intent by building believable business websites.

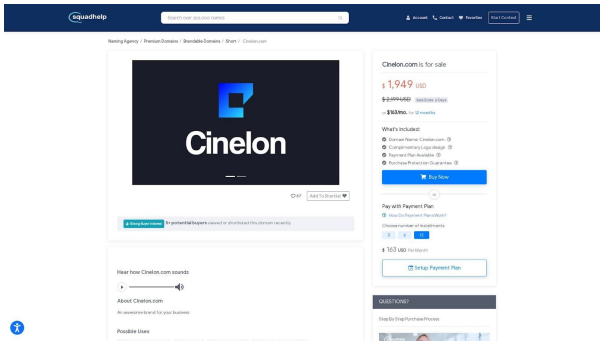
Screenshot of corvusrex[.]com



Screenshot of skyrecs[.]com



Screenshot of nitrogem[.]com



Screenshot of cinelon[.]com

WHOIS, DNS, and IP Intelligence-Enhanced Insights

We subjected the IoCs to DNS lookups, which led to the discovery of 71 IP addresses to which they resolved. While none of them are currently detected as malicious, their connection to confirmed malicious spam domains warrant that they at least be monitored for signs of criminal activity.

A bulk IP geolocation lookup for the IP addresses showed that most of them were geolocated in the U.S., China, Germany, and Japan. Apart from Japan, the U.S., China, and Germany were part of Spamhaus's list of top spam-sending countries as of 29 September 2022.

The 10 Worst Spam Countries

As of 29 September 2022 the world's worst Spam Haven countries for enabling spamming are:

1	**China**	Number of Current Live Spam Issues: 13727
2	**United States of America**	Number of Current Live Spam Issues: 8118
3	**France**	Number of Current Live Spam Issues: 920
4	**Turkey**	Number of Current Live Spam Issues: 783
5	**Saudi Arabia**	Number of Current Live Spam Issues: 761
6	**Mexico**	Number of Current Live Spam Issues: 740
7	**Dominican Republic**	Number of Current Live Spam Issues: 678
8	**Russian Federation**	Number of Current Live Spam Issues: 668
9	**India**	Number of Current Live Spam Issues: 627
10	**Germany**	Number of Current Live Spam Issues: 593

Next, we performed historical WHOIS searches for the IoCs, which uncovered 18 registrant email addresses. The majority of them (79%) were QQMail (i.e., qq.com) accounts although their owners would be hard to identify given the use of random characters (i.e., letters and numbers) instead of proper names.

To further expand the list of potentially related threat artifacts, the IP addresses were used as reverse IP search terms. That led to the discovery of 354 domains. Fortunately, none of them are currently deemed malicious. Several, however, shared similarities with the IoCs, and so warrant closer attention from security teams. These domains include 87 NRDs whose registrant details have been redacted.

—

Even if no organization can escape spam, protecting against outright malicious emails that can lead to financial and reputational damages can still be made more effective by identifying and blocking threats from the source with the aid of WHOIS, DNS, and IP intelligence.

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 Artifacts and IoCs

Domains Identified as IoCs

- couliormag[.]com
- dgep[.]net
- actrarlo[.]com
- bassdor[.]com
- njbookbar[.]com
- ppmbiz[.]com
- coldland[.]info
- corvusrex[.]com
- genetocs[.]com
- dxemco[.]com
- eaddus[.]com
- batamam[.]com
- chbit[.]com
- fpxu[.]net
- frmuz[.]com
- shapphic[.]com
- skyrecs[.]com
- niklaselin[.]com
- nitrogem[.]com
- shangagri[.]com
- kawarh[.]net
- levb[.]net
- ghqd[.]net
- healthworldwideinc[.]com
- cproshq[.]com
- ebiotrae[.]com
- kasbh[.]net
- kavri[.]net

- mutw[.]net
- mvgu[.]net
- mazagi[.]net
- mcdat[.]net
- hgqk[.]net
- mnetbank[.]com
- mnmcurl[.]com
- snaoontool[.]com
- cinelon[.]com
- myxd[.]net
- nhgra[.]com
- eatmebay[.]com
- ettyproductionslimited[.]com
- pritebay[.]com
- rxmegastore[.]net
- mxrjeans[.]com
- nicademiks[.]com
- correbags[.]com
- coycerca[.]com
- nickjotel[.]com
- okadake[.]net
- echanblad[.]com
- goingles[.]com
- mcoot[.]net
- metsgee[.]com

Sample IP Addresses to Which the Domains Identified as IoCs Resolved

- 34[.]102[.]136[.]180
- 195[.]201[.]124[.]255
- 107[.]151[.]97[.]149
- 168[.]119[.]245[.]137
- 198[.]105[.]254[.]11
- 66[.]96[.]160[.]153
- 68[.]233[.]44[.]100
- 66[.]212[.]148[.]115
- 173[.]248[.]130[.]76
- 159[.]69[.]186[.]9
- 74[.]81[.]170[.]110
- 170[.]178[.]178[.]49
- 210[.]188[.]195[.]7
- 210[.]68[.]95[.]96
- 8[.]5[.]1[.]51
- 127[.]0[.]0[.]1
- 170[.]178[.]178[.]60
- 54[.]64[.]203[.]206
- 52[.]69[.]166[.]231
- 162[.]215[.]2[.]16

Email Addresses Used to Register the Domains Identified as IoCs

- 695225826@qq[.]com
- 1904823@qq[.]com
- 1260214595@qq[.]com
- zyj860503@163[.]com
- 441664720@qq[.]com
- b86313887@126[.]com
- szjkdc168@163[.]com
- 3191557@qq[.]com
- 626968750@qq[.]com
- 76364@qq[.]com
- 406220911@qq[.]com
- 1111209@qq[.]com
- 1916682185@qq[.]com
- 80697020@qq[.]com
- 1276200633@qq[.]com
- 320115888@qq[.]com
- 50136851@qq[.]com
- 31311604@qq[.]com

Sample Possibly Connected Domains Since They Shared the IoCs' Registrant Email Addresses or IP Hosts

- www[.]quhuishou[.]cn
- imap[.]tw123[.]net
- vshidai[.]com
- imap[.]lanalo[.]com
- chevrontexaco[.]com[.]cn
- mail[.]jukeslotselfservice[.]com
- vqtu[.]com
- mgfcw[.]com
- imap[.]s18s[.]com
- imap[.]rmeadvisors[.]com
- omzzwnq[.]lwqdaaljeocg[.]hath[.]network
- www[.]vantkonkelgoed[.]eu
- bemdbjr[.]onzsyzeekmpa[.]hath[.]network
- groentensoep[.]xyz
- tyqyikp[.]lwqdaaljeocg[.]hath[.]network
- canmarti[.]info
- ejizfds[.]lwqdaaljeocg[.]hath[.]network
- www[.]mu2020[.]net
- sryreie[.]tk
- gaihaicretatho[.]tk
- forum[.]cheatsvalley[.]com
- gzwtmrmjotut[.]www[.]51[.]la
- 3467fb0rpu[.]iloveyouvk[.]com
- stgz[.]www[.]51yes[.]com
- shoptik[.]parsianec[.]com
- ezezmbansfqrir[.]www[.]51yes[.]com
- 7hsf[.]0n1[.]net
- 1122nb[.]cn[.]k7mm[.]com
- qjgtyhqd[.]51yes[.]com
- gbcn[.]51yes[.]com
- parkerny[.]cn
- webmail[.]crystallighttherapy[.]com
- www[.]cqen[.]com
- email[.]anibina[.]com
- st[.]jindun[.]com[.]cn
- webmail[.]winwaycharts[.]com
- cressman[.]com[.]cn
- dhjh[.]wang
- email[.]highlineboatsales[.]com
- email[.]northcountry-auctions[.]com
- xn--15qy9kozbc58b[.]xn--vuso9br23e[.]com
- yobctools[.]com
- kdyj[.]toycandy[.]cn
- endemikbitki[.]com
- un3a1[.]jistar[.]cn
- federalfleet-ca[.]gdn
- ccnjo[.]102986595[.]cn
- 553713[.]xjycr[.]com