Rounding Up the DNS Traces of RA World Ransomware

Table of Contents

Executive Report

Symantec recently reported that a China-based threat actor who has been involved in installing backdoors in the systems of target government institutions (i.e., cyber espionage) has turned toward spreading RA World ransomware (i.e., a cybercriminal act) this time. Going from one act to the other is not usual for attackers. Why did the researchers think that was the case? Because the tools involved in China-linked espionage campaigns were used in a recent ransomware attack.

The report identified five indicators of compromise (IoCs) comprising three domains and two IP addresses. WhoisXML API expanded the current list of IoCs and uncovered other connected artifacts, namely:

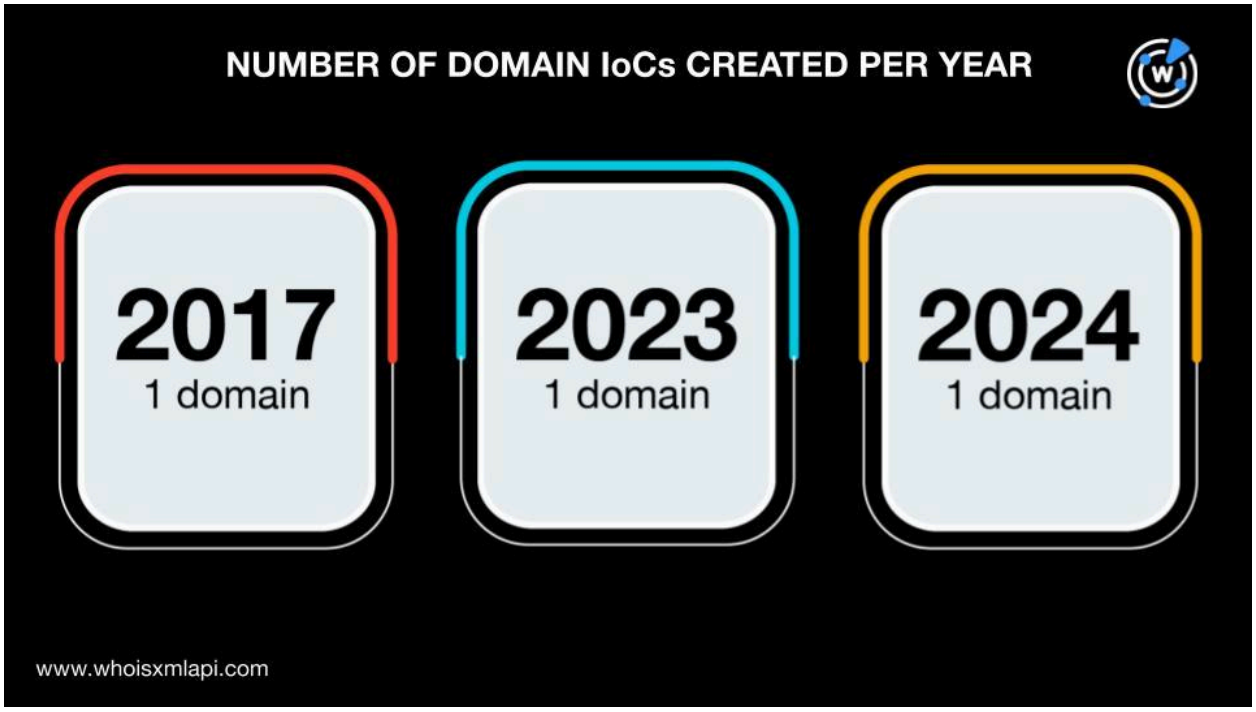
- 11 email-connected domains
- Two additional IP addresses
- Four IP-connected domains, one of which turned out to be malicious
- 12 string-connected domains
- 194 string-connected subdomains

Behind the RA World IoCs

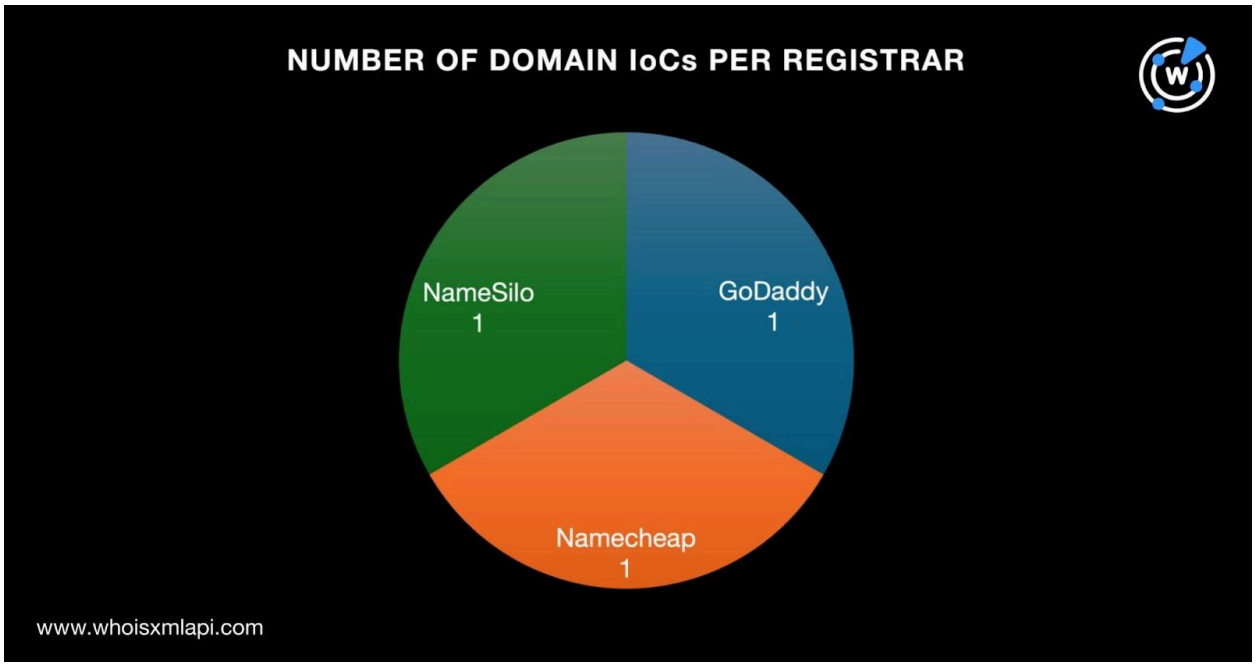
Before going into expanding the current list of IoCs, we took a closer look at its contents first.

We started by querying the three domains identified as IoCs on Bulk WHOIS API and found that:

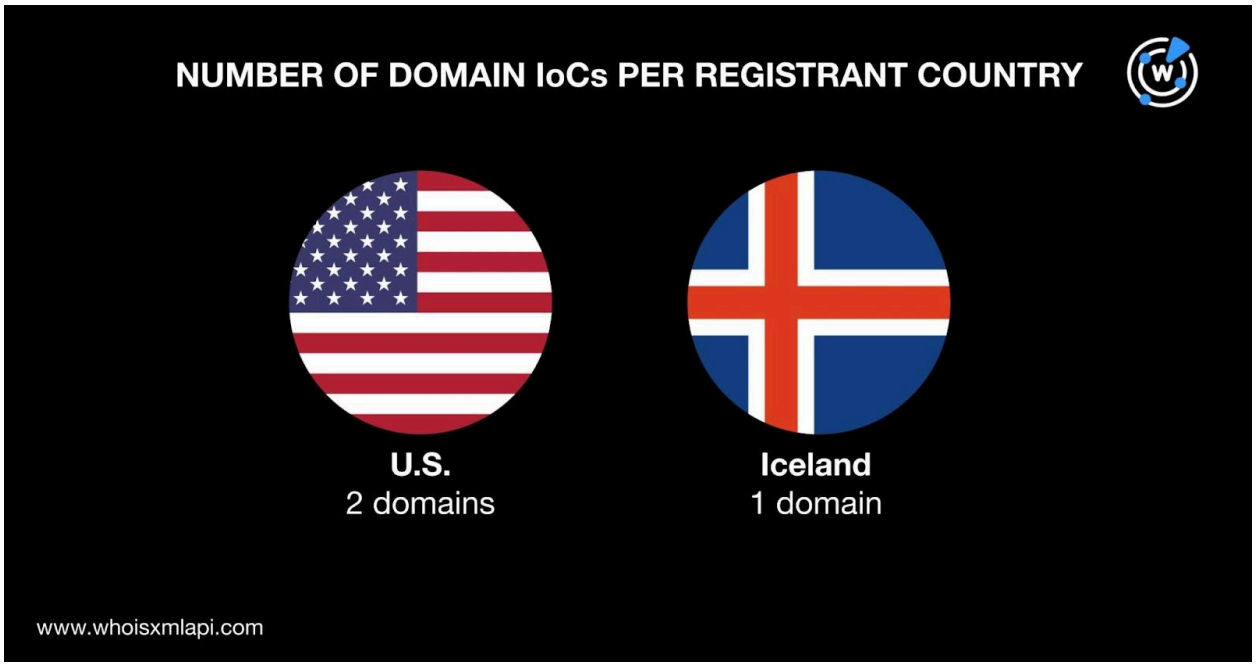
- One domain each was created in 2017, 2023, and 2024.



- The three domains were split across three registrars—GoDaddy, Namecheap, and NameSilo.



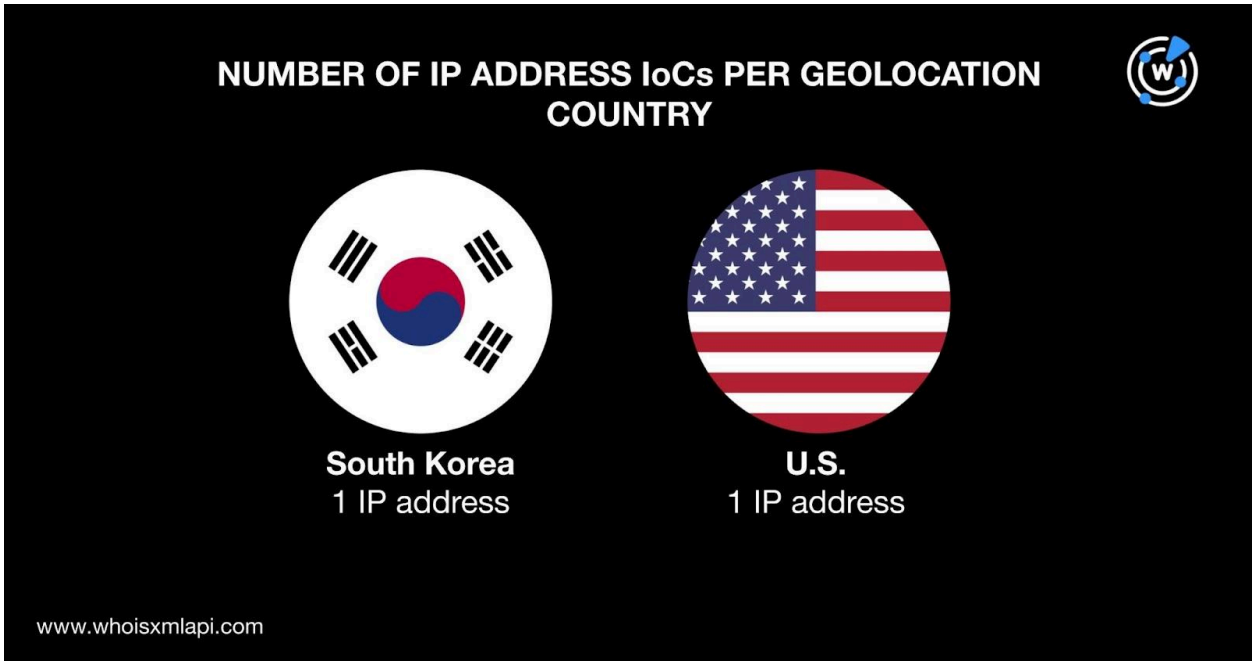
- The three domains were registered in two countries led by the U.S., which accounted for two of them. The last domain was registered in Iceland.



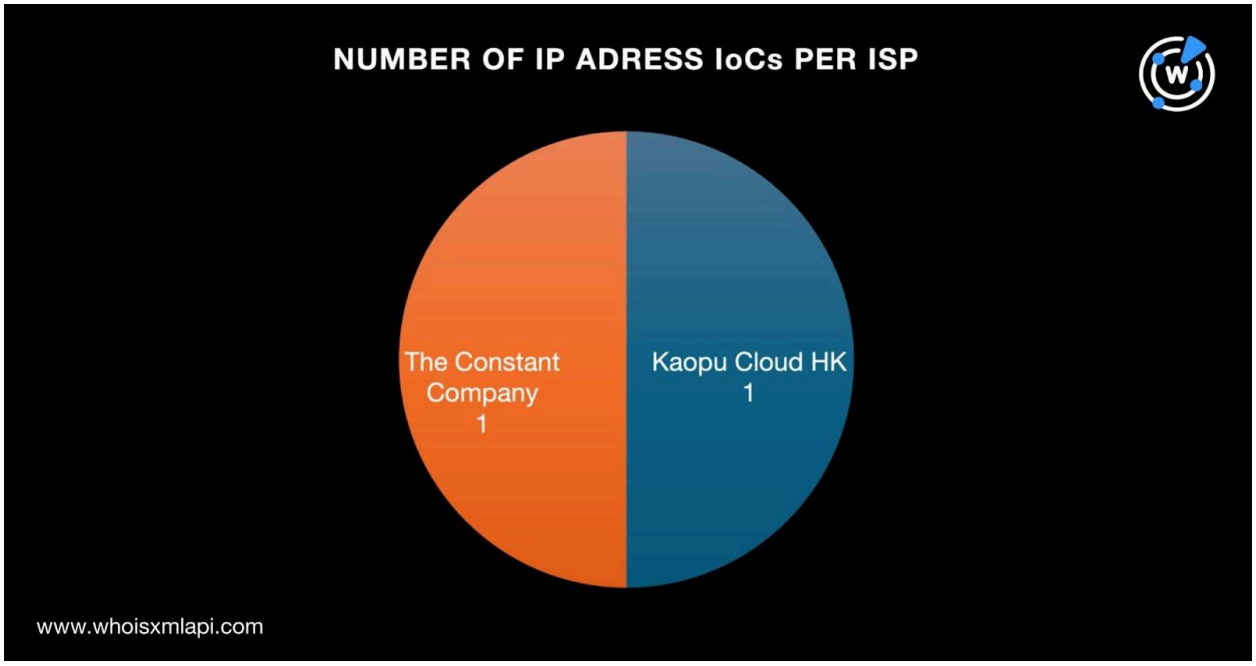
A DNS Chronicle API query for the three domains tagged as IoCs showed that only two had historical IP resolutions. In particular, they recorded 69 IP resolutions over time. The domain blueskyanalytics[.]net posted the older first IP resolution—2 December 2019.

We then took a closer look at the two IP addresses identified as IoCs by querying them on Bulk IP Geolocation Lookup. Our findings revealed that:

- One IP address each was geolocated in South Korea and the U.S.



- The IP addresses were administered by two registrars—Kaopu Cloud HK and The Constant Company.



We queried the two IP addresses tagged as IoCs on DNS Chronicle API as well. They recorded 26 domain resolutions over time. The IP address 158[.]247[.]213[.]167 posted the older IP resolution date—5 October 2019.

RA World IoC List Expansion Analysis Findings

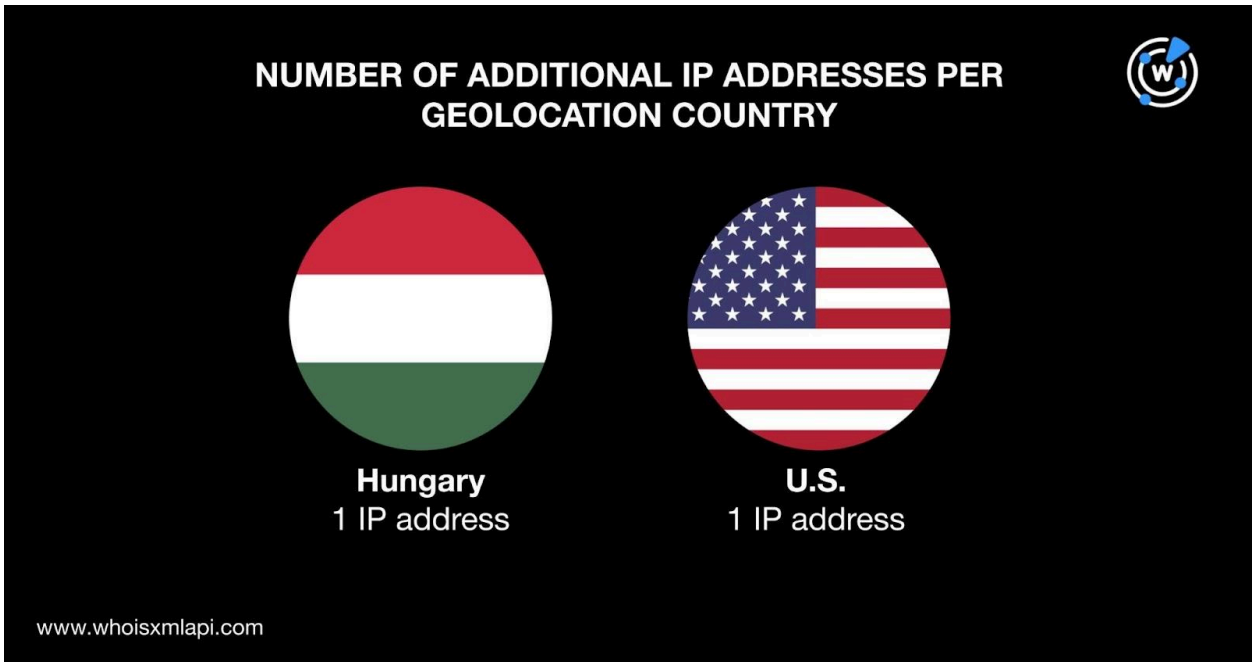
We began our search for potentially connected artifacts by querying the three domains identified as IoCs on WHOIS History API. Our findings showed that altogether, they had 11 email addresses in their historical WHOIS records. Closer scrutiny of these addresses revealed that three were public email addresses.

We then queried the three public email addresses on Reverse WHOIS API. While no domains had any of them in their current WHOIS record, all three did appear in the historical WHOIS records of 11 email-connected domains after duplicates and those already identified as IoCs were filtered out.

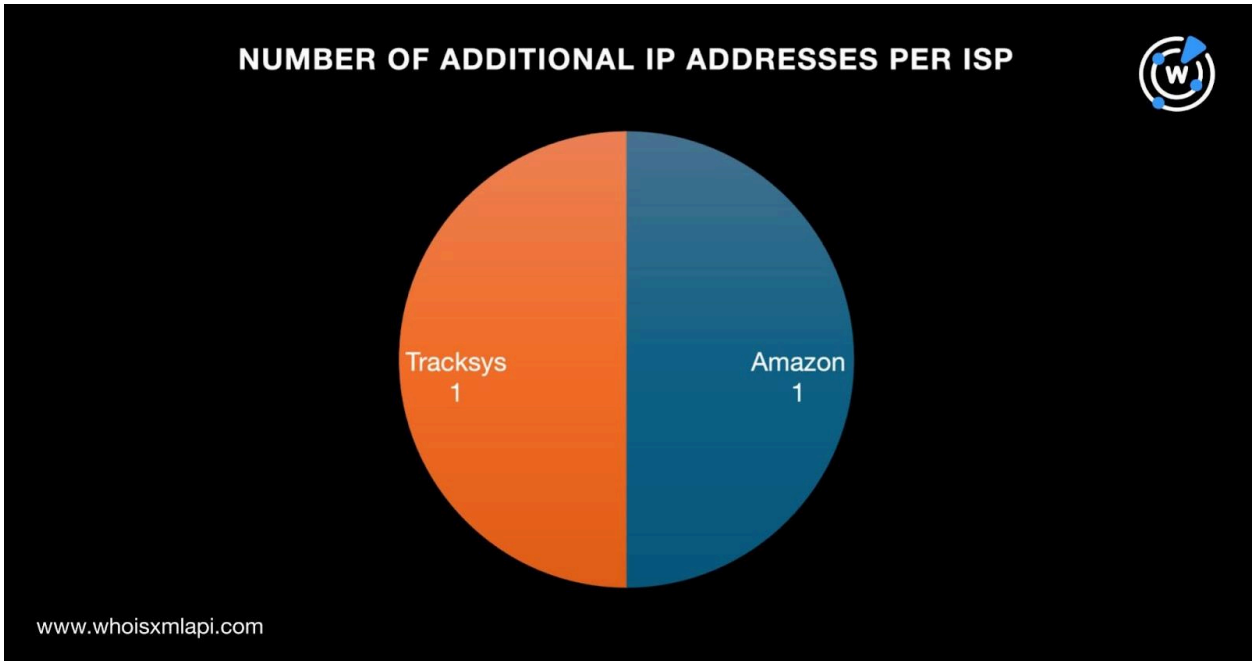
Next, a DNS Lookup API query for the three domains tagged as IoCs showed that two actively resolved to two additional IP addresses after those already identified as IoCs were filtered out.

A Bulk IP Geolocation Lookup for the two additional IP addresses showed that:

- They were geolocated in different countries—one in Hungary and the other in the U.S.



- One IP address was administered by Amazon while the other was under Tracksys.



After that, we now had four IP addresses (i.e., the IoCs and additional ones) to use for the next part of our investigation. We queried them on Reverse IP API and found that only three hosted other domains. Specifically, they hosted four other domains after duplicates, the IoCs, and the email-connected domains were filtered out.

A Threat Intelligence API query for the four IP-connected domains revealed that one—plugins[.]jetbrians[.]net—was associated with malware distribution.

As the final step in our quest to uncover more connected artifacts, we looked for other domains and subdomains that contained the same text strings as those found in the domains identified as IoCs.

Our Domains & Subdomains Discovery searches unearthed 12 domains after duplicates, those already tagged as IoCs, and the email- and IP-connected domains were filtered out. The 12 string-connected domains started with these three strings:

- blueskyanalytics.
- jetbrians.
- tracksyscloud.

A Bulk WHOIS API query for the 12 string-connected domains showed that only one—blueskyanalytics[.]org—shared a commonality with the IoC blueskyanalytics[.]net, its registrar.

Our search for string-connected subdomains, meanwhile, showed results containing these three strings:

- blueskyanalytics
- jetbrians
- tracksyscloud

We collated 194 string-connected subdomains in all. While none of them have seemingly been weaponized for attacks to date, given their similarities with the strings found in the domains identified as IoCs, they could be part of the threat actor's infrastructure.

All in all, we uncovered 223 connected web properties, 27 of which were domains. Screenshot API showed that 16 of the 27 connected domains remained accessible to date.

Note, too, that the attacker may have also opted to use domain names that could be confused for belonging to legitimate companies. Why? Blue Sky Analytics is the name of a geospatial data intelligence company, jetbrians could be typosquatting on the JetBrains brand known for software development tools.

Apart from the legitimate organizations above, several other companies shared the text strings found in the domains tagged as IoCs. They, too, could end up being spoofed in future malicious campaigns.

The results of our Bulk WHOIS API query for the 12 string-connected domains that contained the brand names possibly being mimicked earlier also revealed that none of them shared a single data point with the legitimate company domains.

—

Our DNS deep dive into the recent RA World ransomware attack, likely spearheaded by a long-time China-linked espionage actor, led to the discovery of 223 potentially connected web properties. All in all, we found 11 email-connected domains, two additional IP addresses, four IP-connected domains, 12 string-connected domains, and 194 string-connected subdomains. In addition, one of the domains has already figured in a malicious campaign.

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

- blueskyanalytic[.]com
- blueskyanalytic[.]net
- blueskystat[.]com
- tracksyscloud[.]com
- tracksysinformationsystem[.]com
- whiteferns[.]com

Sample IP-Connected Domains

- blueskyanalytics[.]ai
- plugins.jetbrians[.]net

Sample String-Connected Domains

- blueskyanalytics[.]ca
- blueskyanalytics[.]co
- blueskyanalytics[.]co[.]uk
- jetbrians[.]com
- jetbrians[.]ga
- jetbrians[.]org
- tracksyscloud[.]cfd

Sample String-Connected Subdomains

- acessonet[.]blueskyanalytics[.]netlify[.]app
- adserver[.]blueskyanalytics[.]netlify[.]app
- alfa[.]blueskyanalytics[.]netlify[.]app
- bcvloh[.]blueskyanalytics[.]netlify[.]app
- blueskyanalytics-ca[.]mail[.]protection[.]outlook[.]com
- blueskyanalytics-cd-0w1zsby7gybdux5d[.]edge[.]tenants[.]eu[.]auth0[.]com
- c[.]blueskyanalytics[.]netlify[.]app
- calendar[.]blueskyanalytics[.]netlify[.]app
- cat[.]blueskyanalytics[.]netlify[.]app
- db[.]blueskyanalytics[.]netlify[.]app
- db2[.]blueskyanalytics[.]netlify[.]app
- delta[.]blueskyanalytics[.]netlify[.]app
- est[.]blueskyanalytics[.]netlify[.]app
- exchange[.]blueskyanalytics[.]netlify[.]app
- facebook[.]blueskyanalytics[.]netlify[.]app
- field[.]blueskyanalytics[.]netlify[.]app

- forums[.]blueskyanalytics[.]netlify[.]app
- games[.]blueskyanalytics[.]netlify[.]app
- gold[.]blueskyanalytics[.]netlify[.]app
- gordon[.]blueskyanalytics[.]netlify[.]app
- hr[.]blueskyanalytics[.]netlify[.]app
- jetbrians-toolbox-online[.]michaelpaces[.]com
- jetbrians-toolbox-online[.]spapashon[.]com
- jetbrians-toolbox-secure[.]kollabity[.]com
- law[.]blueskyanalytics[.]netlify[.]app
- library[.]blueskyanalytics[.]netlify[.]app
- ll[.]blueskyanalytics[.]netlify[.]app
- magento[.]blueskyanalytics[.]netlify[.]app
- mailers[.]blueskyanalytics[.]netlify[.]app
- mantis[.]blueskyanalytics[.]netlify[.]app
- nc[.]blueskyanalytics[.]netlify[.]app
- neptune[.]blueskyanalytics[.]netlify[.]app
- newsletter[.]blueskyanalytics[.]netlify[.]app
- oc[.]blueskyanalytics[.]netlify[.]app
- office[.]blueskyanalytics[.]netlify[.]app
- om[.]blueskyanalytics[.]netlify[.]app
- panelstats[.]blueskyanalytics[.]netlify[.]app
- panelstatsmail[.]blueskyanalytics[.]netlify[.]app
- pgadmin[.]blueskyanalytics[.]netlify[.]app
- r[.]blueskyanalytics[.]netlify[.]app
- radio[.]blueskyanalytics[.]netlify[.]app
- res[.]blueskyanalytics[.]netlify[.]app
- savecom[.]blueskyanalytics[.]netlify[.]app
- scrm01[.]blueskyanalytics[.]netlify[.]app
- server[.]blueskyanalytics[.]netlify[.]app
- tdatabrasil[.]blueskyanalytics[.]netlify[.]app
- telecom[.]blueskyanalytics[.]netlify[.]app
- telefonia[.]blueskyanalytics[.]netlify[.]app
- undefined[.]blueskyanalytics[.]netlify[.]app
- uninet[.]blueskyanalytics[.]netlify[.]app
- upc-h[.]blueskyanalytics[.]netlify[.]app
- v[.]blueskyanalytics[.]netlify[.]app
- vc[.]blueskyanalytics[.]netlify[.]app
- vcenter[.]blueskyanalytics[.]netlify[.]app
- wap[.]blueskyanalytics[.]netlify[.]app
- web[.]blueskyanalytics[.]netlify[.]app
- web5[.]blueskyanalytics[.]netlify[.]app
- x[.]blueskyanalytics[.]netlify[.]app