New RomCom Variant Spotted: A Comparative and Expansion Analysis of IoCs

Table of Contents

Executive Report

The threat actors behind the RomCom malware, known for extorting government agencies, recently resurfaced with a new RomCom variant called “Snipbot” or “RomCom 5.0” by Palo Alto Networks Unit 42.

RomCom was first detected in 2022 when threat actors used fake online tools mimicking SolarWinds, Advanced IP Scanner, PDF Reader Pro, and other popular software to trick users into downloading and installing the malware. Back then, WhoisXML API researchers analyzed related threat IoCs and found several potential artifacts.

The malware has much evolved since then. Snipbot is stealthier than earlier versions, although it is based on RomCom 3.0 and uses techniques utilized by RomCom 4.0. It leverages initial downloaders with valid code signing certificates, making target systems think the downloaders are from trusted sources and effectively bypassing security controls. The threat actors can then execute commands and download more modules that aim to steal data.

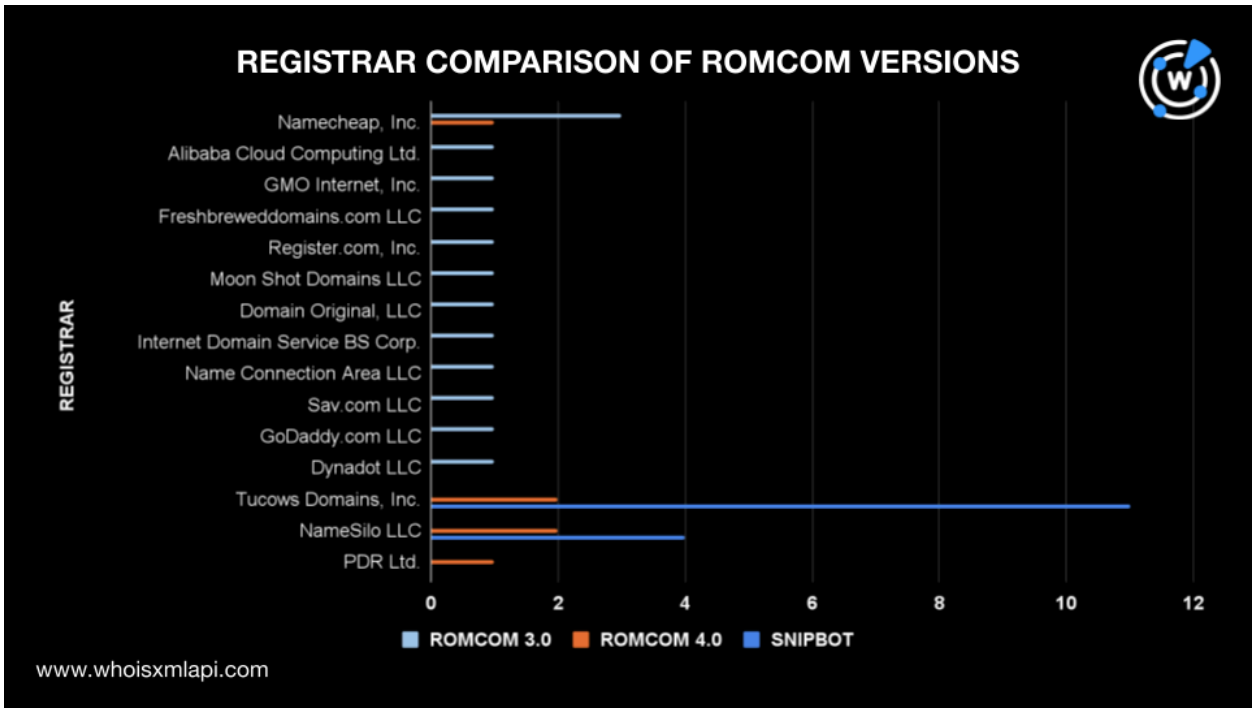
Our researchers sought to compare the IoCs of the three most recent RomCom versions and pivot off these indicators to uncover relevant threat artifacts. Snipbot IoCs comprising 17 domains and one IP address were derived from Unit 42, while the IoCs of versions 3.0 (56 domains and two IP addresses) and 4.0 (nine domains) were published by Trend Micro in 2023. The analysis led to the discovery of:

- 20 email-connected domains, some were found to be malicious
- 27 additional IP addresses, all of which were found to be malicious
- 122 IP-connected domains, some were found to be malicious

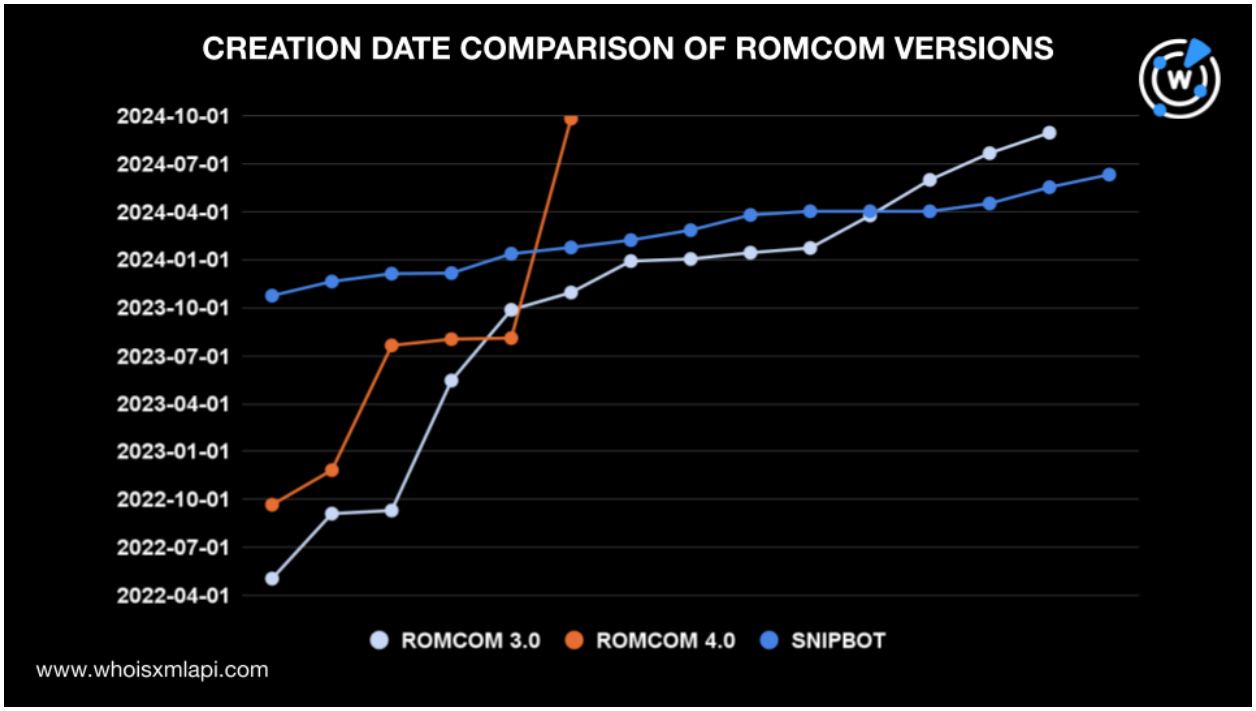
Comparative IoC Analysis of the Different RomCom Versions

We performed separate bulk WHOIS lookups for each list to compare the IoCs of the three RomCom versions. We excluded domain IoCs that did not have current WHOIS data from our analysis. We were left with 42 of the 56 RomCom 3.0 IoCs, three of the nine RomCom 4.0 IoCs, and two of the 17 Snipbot IoCs. Below are our findings for the remaining indicators.

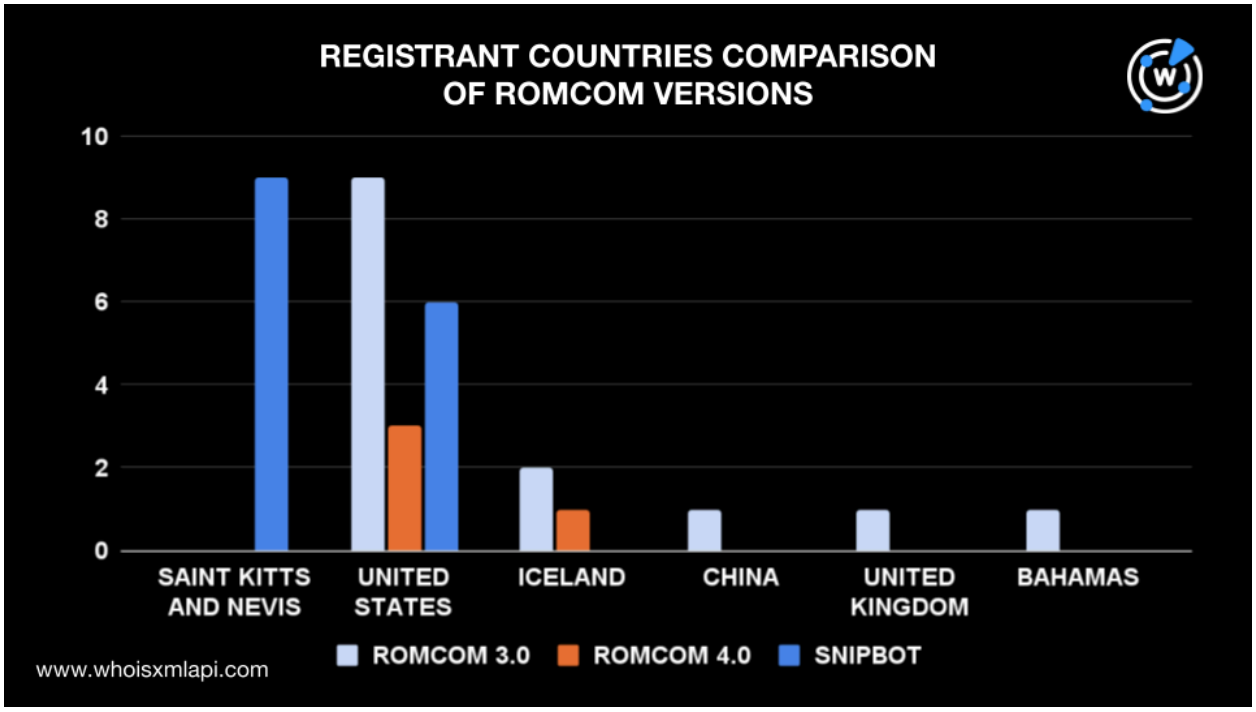
- The RomCom 3.0 domain IoCs were spread across 12 registrars, as seen in the chart below. However, the 4.0 and Snipbot IoCs were administered by only a few registrars, some of which overlapped. For instance, Tucows Domains, Inc. accounted for two RomCom 4.0 and 11 Snipbot IoCs, while NameSilo LLC was the registrar of two RomCom 4.0 and four Snipbot IoCs.



- Four Snipbot domain IoCs were registered in the last quarter of 2023, but they were not detected in any incident until February 2024. A similar pattern can be seen for the 3.0 and 4.0 domain IoCs. Some were registered in 2022 but weren't detected until 2023.

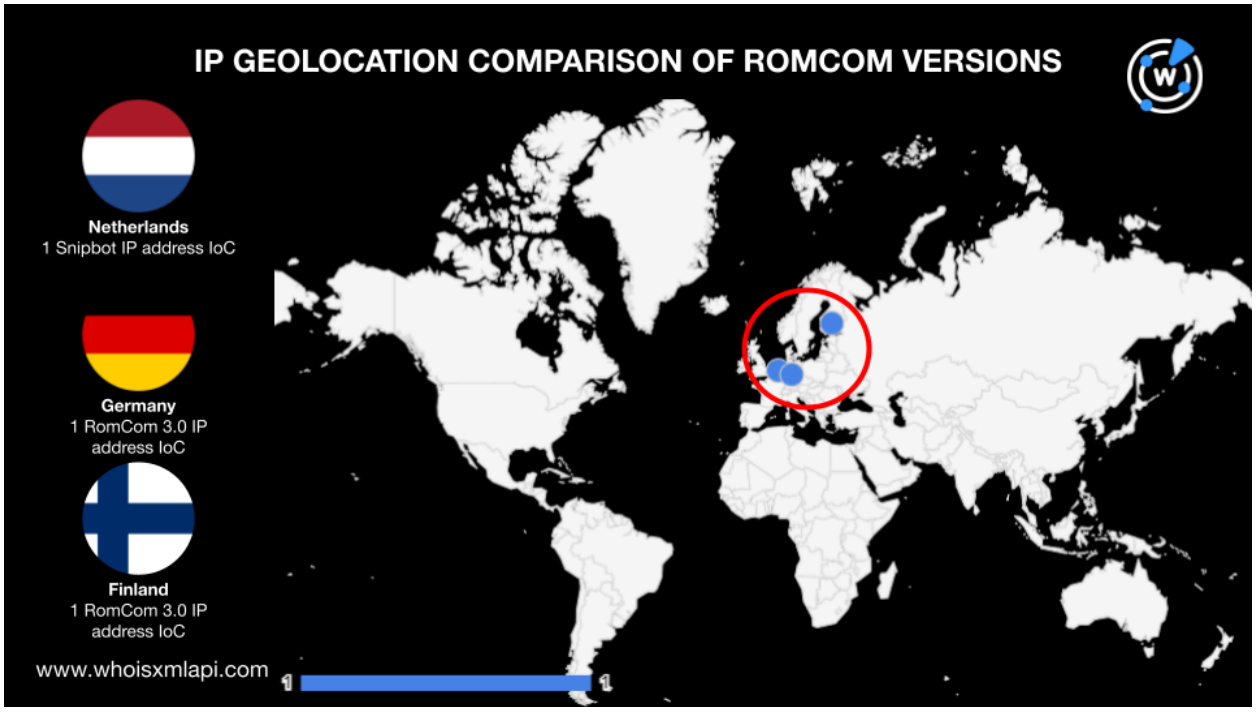


- Only two registrant countries were consistent across the domain IoCs in the different RomCom versions. Nine from version 3.0, three from version 4.0, and six from Snipbot were registered in the U.S. Two domain IoCs from RomCom 3.0 and one from 4.0 were registered in Iceland. The IoCs of the newest version were primarily registered in Saint Kitts and Nevis.



Next, we ran a bulk IP geolocation lookup for the three IP addresses identified as IoCs (one for Snipbot and two for RomCom 3.0) and found that:

- The Snipbot IoC originated from the Netherlands, while the RomCom 3.0 IoCs were geolocated in Germany and Finland. A closer look at these three geolocations revealed that they were concentrated in somewhat nearby countries.



- The three IP IoCs had different ISPs. The two RomCom 3.0 IoCs were administered by Aeza and OVHcloud, while the Snipbot IoC did not have an ISP on record though its Autonomous System (AS) name was LIMENET.

Uncovering Potential RomCom Threat Artifacts

The IoC list expansion for all three RomCom versions was performed on 82 domain IoCs, which we queried on WHOIS History API. The results showed they had 155 email addresses in their historical WHOIS records, 31 of which were public.

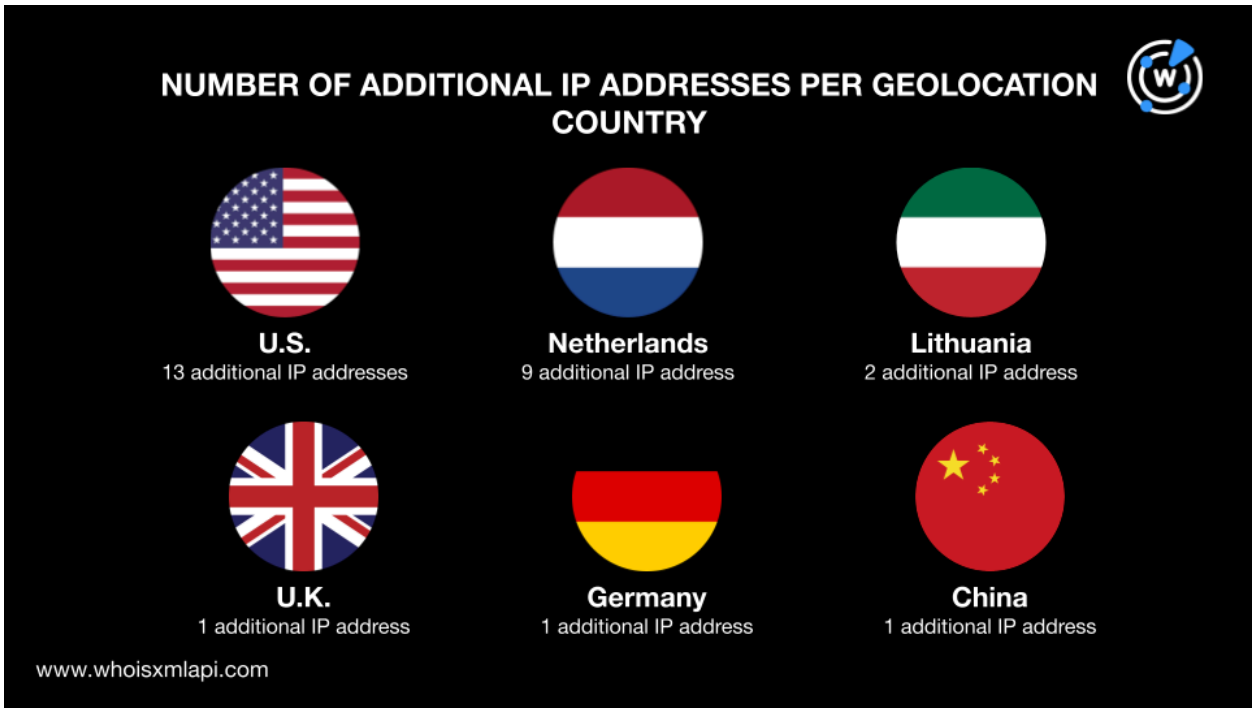
We queried the 31 public email addresses on Reverse WHOIS API and found 20 email-connected domains after removing duplicates and the IoCs. According to Threat Intelligence Lookup, one of these artifacts was involved in a malware attack.

The next step in our threat-hunting efforts was to run the 82 domain IoCs on DNS Lookup to find their IP resolutions. We found that 57 did not have active resolutions, while the remaining 25 resolved to 27 unique IP addresses, which were not on the original IoC list. Threat Intelligence Lookup revealed that all of them were associated with various threats. Some examples are shown below.

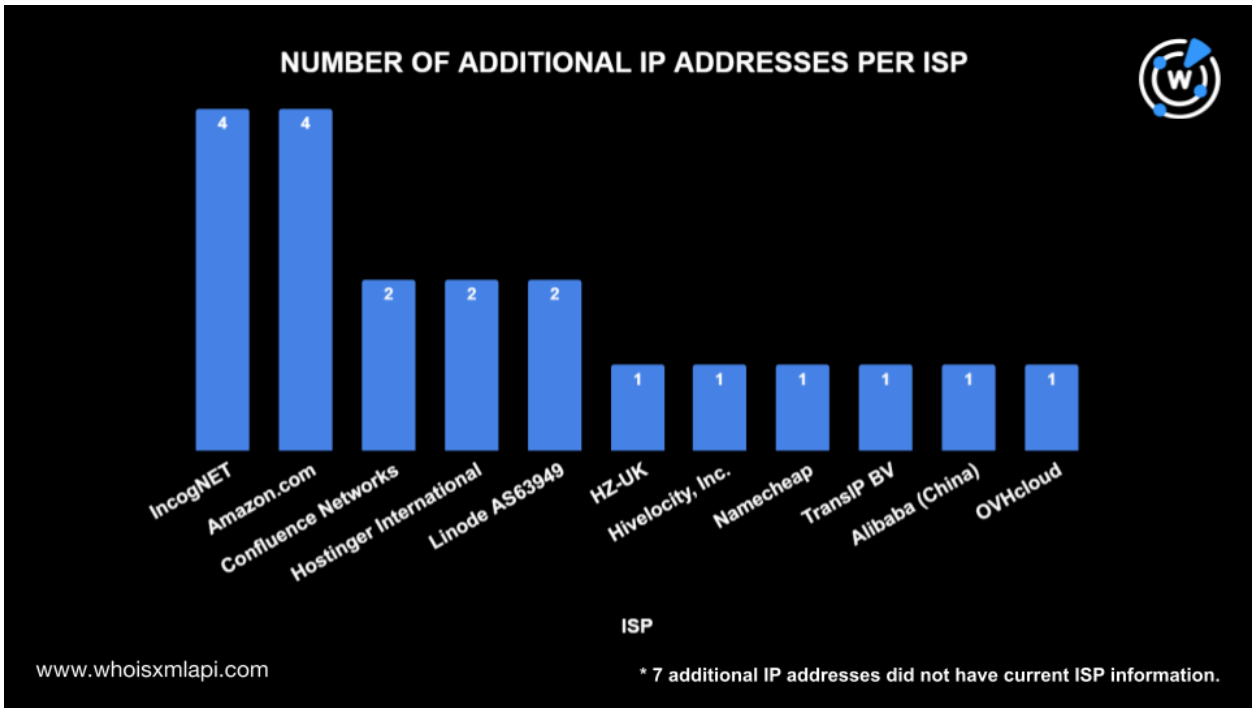
ADDITIONAL IP ADDRESS	ASSOCIATED THREAT TYPES
91[.]92[.]250[.]240	Attack Generic Malware Spam
23[.]184[.]48[.]90	Command-and-control (C&C) Malware
103[.]224[.]182[.]253	Attack C&C Generic Malware Phishing Spam

A bulk IP geolocation lookup for the 27 additional IP addresses revealed that:

- They were spread across six geolocation countries, with the U.S. accounting for a majority of the IP addresses—13 to be exact. The Netherlands accounted for nine IP addresses; Lithuania, two; and the U.K., Germany, and China each accounted for one IP address.



- IncogNET and Amazon.com administered four additional IP addresses each, while Confluence Networks, Hostinger International, and Linode AS63949 accounted for two additional IP addresses each. HZ-UK, Hivelocity, Inc., Namecheap TransIP BV, Alibaba (China), and OVHcloud administered one additional IP address each. Seven additional IP addresses did not have current ISP information.



Next, we queried the three IP addresses identified as IoCs and the 27 additional IP addresses on Reverse IP Lookup. We found that while two had no resolving domains, 15 could be dedicated. They led to 122 IP-connected domains and subdomains after filtering out duplicates, the IoCs, and the email-connected domains. Some of them were involved in phishing and malware attacks.

—

Our WHOIS and DNS comparative analysis of the IoCs of three different RomCom versions unveiled some overlaps, notably regarding registrar distribution and date of creation. A deeper analysis of the 82 domains and three IP addresses tagged as IoCs led to the discovery of 169 threat artifacts comprising 20 email-connected domains, 27 additional IP addresses, and 122 IP-connected domains. Several of these artifacts 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

- newhuaren[.]us
- neighborhoodpostcards[.]us
- 0a0[.]us
- solpolas[.]com
- autoinsurancecompany[.]us
- egetcha[.]com
- neumatico[.]info
- emailawebpage[.]com
- middle-class[.]club
- taxpayers[.]club

Sample Additional IP Addresses

- 91[.]92[.]250[.]240
- 91[.]92[.]254[.]54
- 91[.]92[.]254[.]234
- 23[.]184[.]48[.]90
- 91[.]92[.]242[.]87
- 23[.]137[.]248[.]220
- 79[.]141[.]170[.]34
- 91[.]92[.]250[.]106
- 38[.]180[.]5[.]251
- 192[.]64[.]119[.]157
- 91[.]195[.]240[.]12
- 103[.]224[.]182[.]253
- 204[.]11[.]56[.]48
- 99[.]83[.]138[.]213
- 86[.]105[.]245[.]69
- 208[.]91[.]197[.]46
- 114[.]55[.]25[.]226
- 135[.]148[.]90[.]231
- 45[.]84[.]204[.]53
- 13[.]248[.]213[.]45

Sample IP-Connected Domains

- 1drivemss[.]click
- advancecuttinq[.]com
- baskayaziraataletleri[.]com
- beeflowhive[.]com[.]ua
- benefad[.]com
- bigvuti[.]top
- biller[.]ae
- campingtatarak[.]pl
- cancellation-directdebit-westpac[.]com
- cashindash[.]com
- climateua[.]com

- cloudcreative[.]digital
- clsminer[.]com
- cmbhvac[.]com
- cognosco[.]ltd
- cryptonator[.]cloud
- ctt-post[.]cc
- dfly[.]lt
- digitalmart[.]icu
- divan[.]af
- electronice-carti[.]com
- eobot[.]net
- erbilbranda[.]net
- evridf[.]cfd
- extchker[.]click
- fas3mine[.]com
- fastbitchange[.]online
- fileshare[.]direct
- filjan[.]de
- filjannowastrona1511[.]pl
- fokk[.]in
- futrzanyogrod[.]pl
- ghazwanhasan[.]com
- globalvacationoffers[.]com
- glow-eg[.]com
- growthprofitsolutions[.]site
- guidelines[.]icu
- health-association[.]org
- help-banking-westpac[.]com
- hogwarts[.]team
- incodey[.]com
- insightgenix[.]org
- internet-banking-westpac[.]com
- ip215[.]ip-51-195-49[.]eu
- jakobscatering[.]com
- jufy[.]eu
- kampstor[.]com
- karizmacatering[.]com
- kitab-evi[.]com
- knigi-online[.]com[.]ua