WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

From URSNIF IoCs to Software Spoofing: Using DNS Intel to Connect the Dots

Table of Contents

Executive Report

Financially motivated threat actors called “TA544” were first detected in 2017. TA544 is known for high-volume campaigns, sending hundreds of thousands of malicious messages daily.

While the threat actors used several malware payloads, they are widely known for distributing the URSNIF banking trojan. Proofpoint researchers[1] also found TA544 using a new malware dubbed “WikiLoader,” which subsequently led to the installation of URSNIF into target systems.

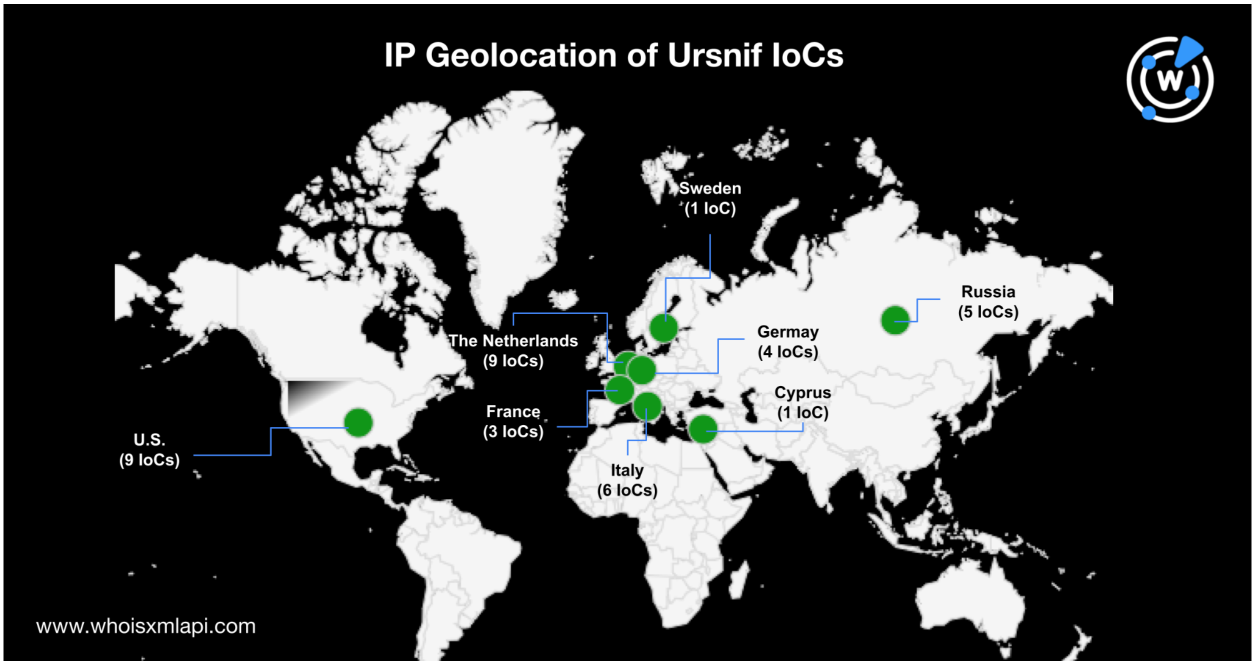
WhoisXML API researchers gathered 21 domain names and 24 IP addresses publicly listed as indicators of compromise (IoCs)[2,3,4,5] as part of recent URSNIF campaigns targeting companies in Italy. Our analysis and expansion of the IoCs led to these key findings.

- 18 artifacts comprising 10 IP-connected domains and eight email-connected domains
- Eight malicious IP- and email-connected artifacts
- 1,067 string-connected artifacts comprising 476 domains starting with the string **avast** and 591 domains containing the string **debian** registered from 1 January–28 August 2023
- 653 unique IP addresses hosting 805 string-connected artifacts, some of which were malicious based on a bulk malware check

URSNIF IoC Profile and Analysis

We sought to identify the registrars and Internet service providers (ISPs) administering the IoCs. To do that, we ran a bulk WHOIS lookup and found that most of the domains were managed by the American Registry for Internet Numbers (ARIN) and Réseaux IP Européens (RIPE). The top registrars, meanwhile, included Web Commerce Communications (WEBCC) and several Europe-based entities, such as OVH, Scaleway, and Aruba.

We also conducted a bulk IP geolocation lookup on the IoCs and found that about 37% of them were administered by Nice IT Services Group, Inc. and DigitalOcean LLC. The resolving IoCs were primarily geolocated in Europe (74%), with the rest in the U.S. (24%) and the Middle East (2%). The map below shows the breakdown per country.



URSNIF IoC List Expansion

Threat actors use several web resources in their campaigns, and TA544 is no exception. As such, we analyzed the IoCs using DNS intelligence to retrieve domain connections.

First, we obtained their registrant email addresses by looking up the IoCs' historical WHOIS records. We found 26 email addresses, but very few were unredacted. More than half had the email domain whoisprotection[.]cc. Still, reverse WHOIS searches for the remaining non-redacted email addresses yielded eight artifacts linked to the IoCs.

Reverse IP lookups for the IP addresses tagged as IoCs further revealed that only eight had resolving domains, which led us to 10 additional artifacts. In total, we found 18 IP- and email-connected domains, eight of which were already flagged as malicious.

Some of the artifacts continued to host or redirect to live pages, including what appeared to be an e-commerce website and an Apache test page.

A Deeper Probe Led to More Potential Threats

From the list of IoCs and artifacts, we noticed domain names that seemed to spoof Avast and Debian (i.e., avas1t[.]de and debian-package[.]center). Both domains have been reported as malicious on several security databases, prompting us to find out what other similar-looking domains are currently out in the wild.

To do that, we used Domains & Subdomains Discovery and retrieved all domains starting with **avast** and containing **debian** that were added from the beginning of this year to 28 August 2023. We found 476 and 591 cybersquatting domains, respectively.

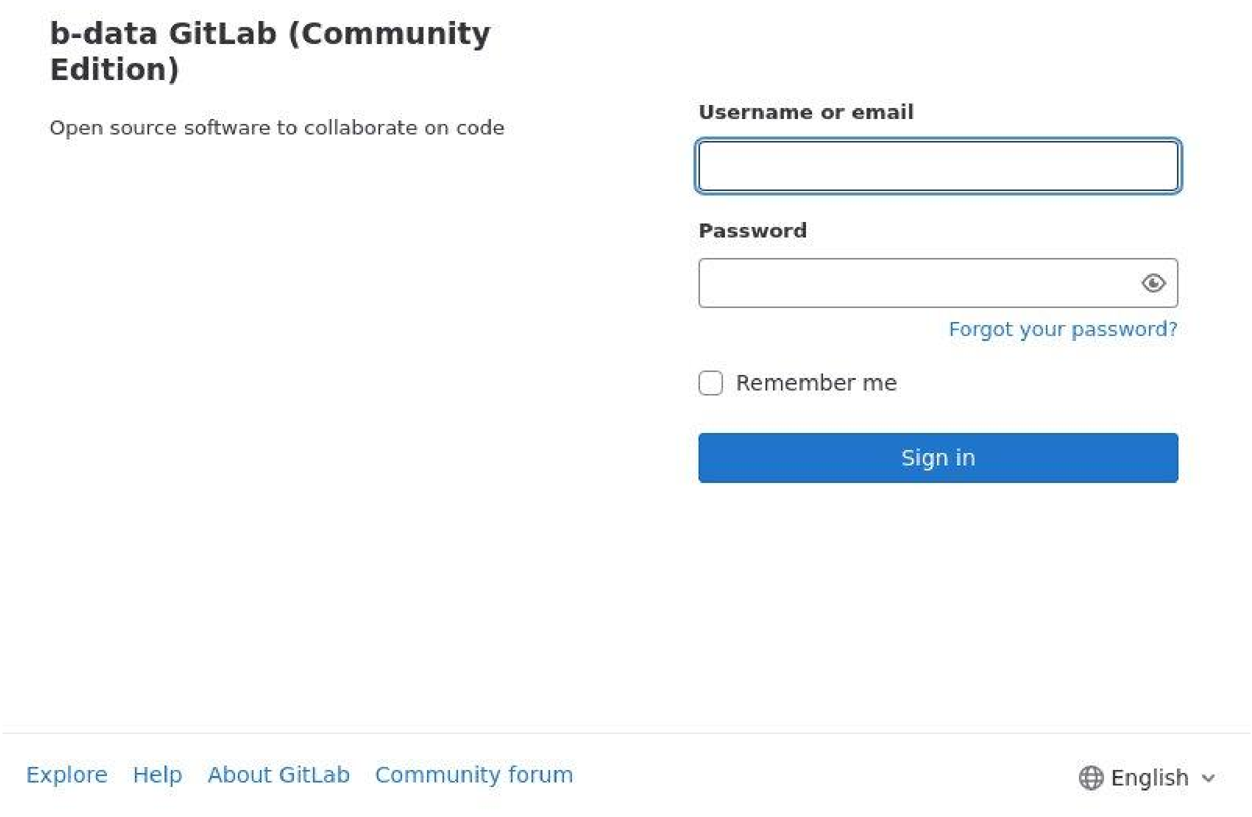
We ran a bulk IP geolocation lookup to see which ones resolved to IP addresses. We found 1,462 resolutions attributed to 805 string-connected artifacts. Ranking the IP addresses based on their number of resolutions, 13 stood out since they each had more than a dozen resolutions.

While that may not be suspicious under normal circumstances, the fact that they were cybersquatting domains may hint at possible malicious or suspicious IP networks. An even more alarming finding is that various security engines flagged a few of the IP addresses as malicious.

Malicious IP Address	Number of Resolutions	Sample Resolving Domains and Subdomains
54[.]153[.]56[.]183	31	avastone[.]com[.]de avast2014win81[.]com[.]de duchangzuidebianhucijisilu[.]se[.]net
34[.]102[.]136[.]180	24	avasthome[.]site avastargallery[.]com debianns[.]com
91[.]216[.]248[.]22	21	avastwin81[.]clan[.]rip avastwin81[.]webspace[.]rocks agenda-debian-test[.]2ix[.]de
91[.]216[.]248[.]21	20	avast-free-antivirus[.]2ix[.]de debian4[.]clan[.]rip debian6[.]4lima[.]ch
91[.]216[.]248[.]20	18	avast2014pojie[.]4lima[.]de debianpcjjos[.]lima-city[.]de httpd-debian[.]lima-city[.]de

45[.]79[.]222[.]138	9	avastwin81[.]com[.]ph debian6[.]org[.]ph debianvm[.]mil[.]ph
162[.]55[.]0[.]137	9	avast-free-antivirus[.]square7[.]de debian3[.]bplaced[.]net debianhelp[.]square7[.]de
15[.]197[.]142[.]173	8	avastgalaxy[.]com avastlog[.]com avastore2023[.]com

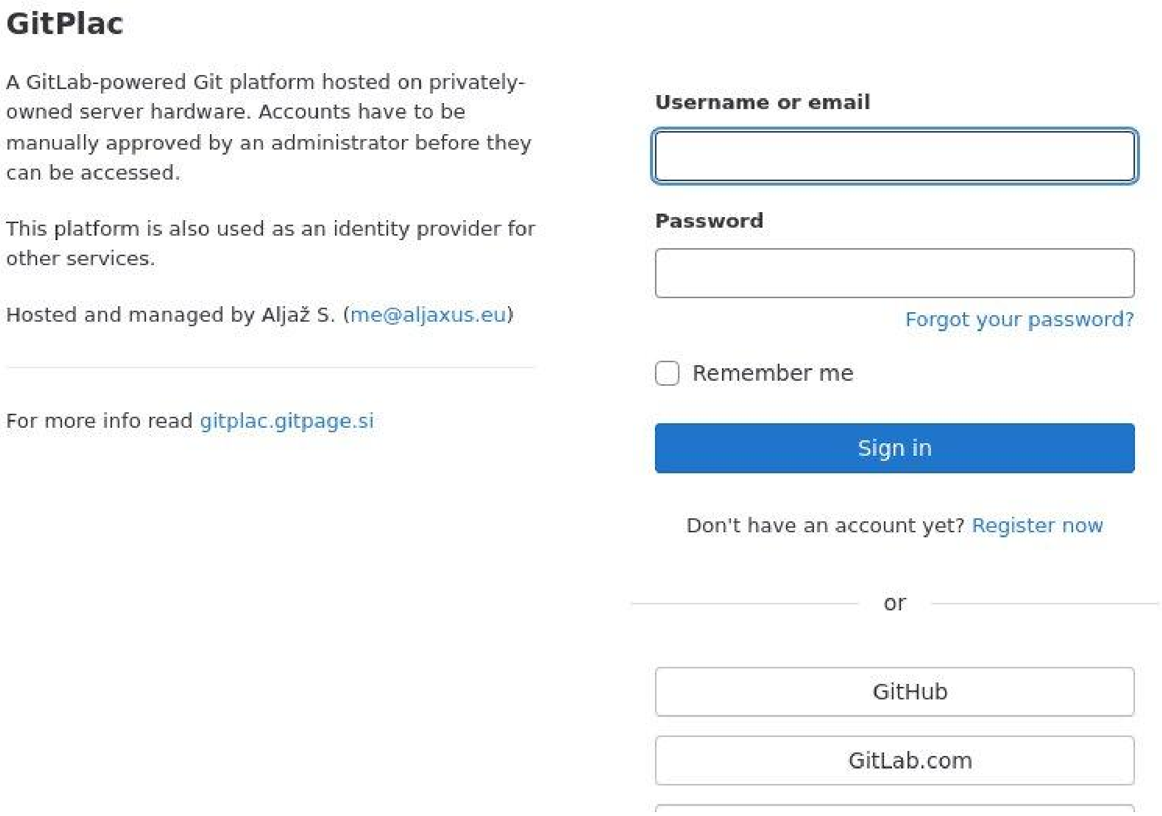
Some of the cybersquatting domains and subdomains also hosted or redirected to questionable live pages. For example, these showed very similar login pages.



b-data GitLab (Community Edition)

Open source software to collaborate on code

Screenshot of avast2014fanghuoqiang[.]b-data[.]io



GitPlac

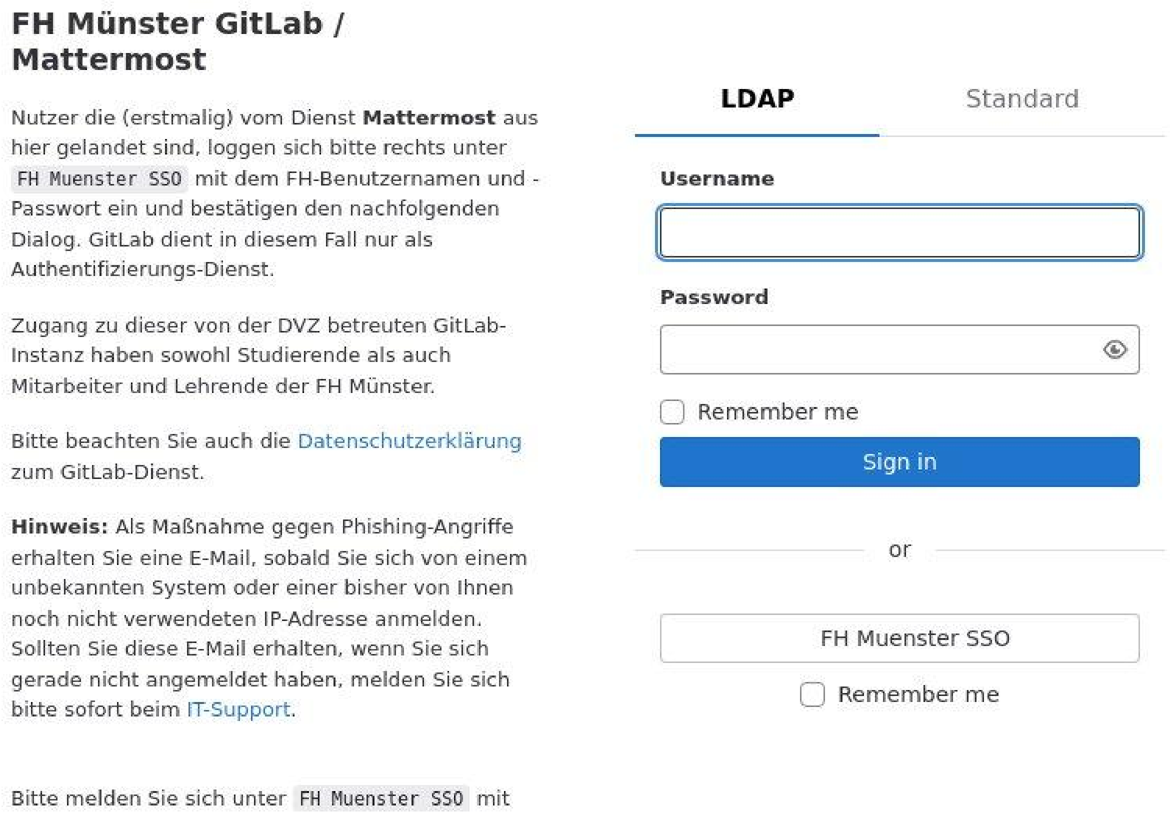
A GitLab-powered Git platform hosted on privately-owned server hardware. Accounts have to be manually approved by an administrator before they can be accessed.

This platform is also used as an identity provider for other services.

Hosted and managed by Aljaž S. (me@aljaxus.eu)

For more info read gitplac.gitpage.si

Screenshot of avast2014pojie[.]gitpage[.]si



FH Münster GitLab / Mattermost

Nutzer die (erstmalig) vom Dienst **Mattermost** aus hier gelandet sind, loggen sich bitte rechts unter `FH Muenster SSO` mit dem FH-Benutzernamen und -Passwort ein und bestätigen den nachfolgenden Dialog. GitLab dient in diesem Fall nur als Authentifizierungs-Dienst.

Zugang zu dieser von der DVZ betreuten GitLab-Instanz haben sowohl Studierende als auch Mitarbeiter und Lehrende der FH Münster.

Bitte beachten Sie auch die Datenschutzerklärung zum GitLab-Dienst.

Hinweis: Als Maßnahme gegen Phishing-Angriffe erhalten Sie eine E-Mail, sobald Sie sich von einem unbekannten System oder einer bisher von Ihnen noch nicht verwendeten IP-Adresse anmelden. Sollten Sie diese E-Mail erhalten, wenn Sie sich gerade nicht angemeldet haben, melden Sie sich bitte sofort beim IT-Support.

Bitte melden Sie sich unter `FH Muenster SSO` mit

Screenshot of mydebianblog[.]fh-muenster[.]io

Whether or not these cybersquatting domains were directly related to URSNIF and TA544, they still raised suspicion because of their connection to malicious IP addresses and their impersonation of widely used systems.

—

URSNIF has consistently evolved and remained persistent over the years, with threat actors using the Trojan to target hundreds of banks and steal thousands of sensitive credentials. The cybersecurity community can benefit from any insight that can help prevent the threat it poses. As such, the artifacts we discovered in this research may aid security investigators in tackling URSNIF and the threat actors behind it.

If you wish to perform a similar investigation or 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: Source, Sample Artifacts, and IoCs

Sources

[1]
https://www.proofpoint.com/us/blog/threat-insight/out-sandbox-wikiloader-digs-sophisticated-evasion
[2] https://otx.alienvault.com/pulse/64ca52f8517d45663b05655d
[3] https://otx.alienvault.com/pulse/64c3b9dc8c9f288d10c98fe9
[4] https://otx.alienvault.com/pulse/64b7cdb9fe627a02501b2be1
[5] https://otx.alienvault.com/pulse/64d3b6cc6616bf4a9ef77b54

All Domains and IP Addresses Publicly Listed as IoCs

- 9ygw2[.]com
- astrolabecommunication[.]fr
- avas1t[.]de
- bbpline[.]com
- centrograndate[.]it
- delideta[.]com
- e9bja[.]com
- hq3ll[.]com
- ilfungodilacco[.]it
- inspiration-canopee[.]fr
- ioyyf[.]com
- itwicenice[.]com
- n2f79[.]com
- nikotta[.]com
- osteopathe-claudia-grimand[.]fr
- p-e-c[.]nl
- studiolegalecarduccimacuzzi[.]it
- sunniznuhqan[.]com
- tobmojiol2adf[.]com
- vivalisme[.]fr
- yourbed[.]it
- 45[.]92[.]229[.]195
- 45[.]9[.]148[.]99
- 45[.]9[.]148[.]236
- 45[.]9[.]148[.]234
- 161[.]35[.]236[.]24
- 138[.]68[.]115[.]96
- 67[.]205[.]134[.]224
- 159[.]223[.]235[.]198
- 159[.]203[.]85[.]196
- 138[.]197[.]212[.]204
- 159[.]203[.]102[.]122
- 45[.]9[.]148[.]59
- 45[.]9[.]148[.]129
- 45[.]9[.]148[.]125
- 45[.]9[.]148[.]117
- 185[.]82[.]127[.]183
- 109[.]105[.]198[.]129

- 91[.]212[.]166[.]44
- 31[.]172[.]83[.]49
- 173[.]44[.]141[.]237
- 91[.]201[.]65[.]64
- 152[.]89[.]198[.]29
- 173[.]44[.]141[.]199
- 170[.]130[.]165[.]159

Sample IP-Connected Artifacts

- debian-package[.]center
- edizionestraordinaria[.]net
- 31[.]172[.]83[.]49[.]sslip[.]io
- epidine[.]com
- freduska[.]com
- mimemoa[.]com
- njamma[.]com
- streetfee[.]com
- twinean[.]com
- weseens[.]com

Sample Email-Connected Domains

- tagpris[.]com
- intelligence-cooperative[.]fr
- tilbudgratis[.]com
- novacteur[.]fr
- tilbudgratis[.]net
- asymethique[.]fr
- sporactif[.]fr
- sens-inverse[.]fr

Sample Sample String-Connected Artifacts

- avastfficevcestluticevtces[.]fun
- avasthelp[.]ga
- avastudios23[.]com
- avast[.]gq
- avasteyr[.]com
- avastlowin[.]com
- avastwin81[.]nid[.]io
- avast[.]partners
- avastudios[.]software
- avastudios[.]domains
- avastudios[.]fun
- avastudios[.]group
- avastbuilders[.]ca
- avastcleanscan[.]click
- avastfrance[.]store
- avastguide[.]store
- avast2014fanghuoqiang[.]blogspot[.]bg
- avastif[.]ga
- avast2014win81[.]arab
- avastdystributor[.]pl
- avast[.]fnwk[.]site
- avasthome[.]site
- avastoes[.]com
- avast-free-antivirus[.]info[.]at
- avastacia[.]com
- avastlysafe[.]com
- avastone[.]com[.]de
- avastbrasil[.]click
- avasted-fix[.]fun
- avastusruum[.]ee
- avastorebrasil[.]com
- avastudios[.]website
- avastudios[.]email
- avastudios[.]team
- avastudios[.]university

- avast-frlivraison[.]skin
- avast[.]gotpantheon[.]com
- avast-ye-marketing[.]com
- avast2014gaojiban[.]us[.]org
- avastmobilenotary[.]com
- avast[.]karacol[.]su
- avastea[.]com
- avastme[.]pro
- avastai[.]ee
- avast[.]co[.]de
- avastpulkit[.]workers[.]dev
- avasthelion[.]com
- avastartrade[.]com
- avast[.]com[.]eg
- avastal[.]ee
- avastplumbingandheating[.]co[.]de
- avastinfo[.]store
- avastameyheskoos[.]com
- avastgalaxy[.]com
- avast-antispam-02772[.]online
- avast2014jihuoma[.]cyon[.]link
- avastdetectedsecuresecured[.]top
- avasthet[.]com
- avastudiobali[.]com
- avastudios[.]rip
- avastudios[.]enterprises
- avast[.]resindevice[.]io
- avasta[.]us
- avast-check-27892[.]online
- avastt-fr[.]xyz
- avastar[.]cn
- avast[.]szczecin[.]pl
- avast-austria[.]at
- avastantivirus[.]co[.]de
- avast-4-whs-edition-1-year-company[.]xn--fiqs8s
- avast2014win81[.]myshopblocks[.]com
- avastwin81[.]crd[.]co
- avasted[.]club
- avast-detected-safe-secured[.]top
- avastudios[.]support
- avastudios[.]app
- avastudios[.]company
- avast-nas[.]direct[.]quickconnect[.]to
- avastnotary[.]com
- avastargallery[.]com
- avastoneunlockedapk[.]net
- avastabikes-jp[.]com
- avast-antispam-625[.]online
- avast-ye-marketing[.]co[.]uk
- avastylus[.]co[.]de
- avasthasyoga[.]com
- avastwinkletoes[.]com
- avast2014gaojiban[.]yali[.]mythic-beasts[.]com
- avast2014pojie[.]blogspot[.]com[.]au
- avastwin81[.]siteleaf[.]net
- avastin[.]com[.]de
- avastrealty[.]llc
- avastte[.]cn
- avastoreonline[.]com
- avastfrance[.]co
- avastano[.]be
- avastfreeantivirus2014[.]blogspot[.]fi
- avastwin81[.]clan[.]rip
- avast[.]cloudapps[.]digital
- avast2014pojie[.]msk[.]ru
- debian[.]vg
- debian[.]pt
- debian[.]ma
- debian[.]la
- debian[.]im
- debian[.]zip
- xdebian[.]cn
- mdebian[.]pl
- debian[.]fyi
- debian6[.]ws
- debian[.]cfd
- debian[.]arab

- debian-sd[.]me
- debian15[.]com
- debianns[.]com
- debianday[.]cz
- debian14[.]com
- debiant[.]link
- debian6[.]site
- debian[.]co[.]de
- debian11[.]com
- debiane8[.]com
- debianiran[.]tk
- debian[.]family
- debian[.]giving
- nextdebian[.]vg
- debiandns[.]org
- xcdebianhg[.]ws
- debian[.]org[.]mx
- debiantat[.]com
- debian2[.]co[.]pw
- debian023[.]xyz
- debian[.]studio
- eyedebian1[.]ws
- debianbsb[.]org
- 123debian[.]xyz
- debianlive[.]ru
- bdebianca[.]com
- debiantop[.]xyz
- debian[.]int[.]la
- debian[.]net[.]br
- debian[.]net[.]tr
- debianer[.]wiki
- debian6[.]0e[.]vc
- debianios[.]com
- debianget[.]com
- debian[.]com[.]uy
- debian[.]org[.]ng
- debian7[.]uk[.]net
- debianlink[.]top
- debian6[.]org[.]ph
- debian-cave[.]me
- debian8[.]oya[.]to
- debiangate[.]xyz
- lildebian[.]shop
- debian11[.]store
- debian3[.]uwu[.]ai
- debian6[.]uwu[.]ai
- debian-2[.]or[.]pw
- debian1[.]eu[.]com
- debian5[.]oya[.]to
- debian1[.]fin[.]ci
- debian4[.]nid[.]io
- debian8[.]hu[.]net
- debian[.]mex[.]com
- debianku[.]my[.]id
- go-debian[.]asia
- debian-node[.]me
- debian2[.]hu[.]net
- videbianya[.]com
- sp2[.]debian[.]net
- tix[.]debian[.]net
- debian2[.]eu[.]com
- debiancc[.]se[.]net
- clamd-debian[.]ws
- debiancc[.]nid[.]io
- debianlinux[.]sbs
- debianka[.]com[.]de
- activedebian[.]ru
- rocm[.]debian[.]net
- debian[.]software
- debianpc[.]online
- elte[.]debian[.]net
- debian01[.]com[.]ph
- rodsdebian11[.]ga
- debianpixel[.]com
- linuxdebian[.]net
- debian8[.]mex[.]com
- debianhacker[.]xn--fiqs8s
- debianvm[.]mil[.]ph
- debian-home[.]com
- stijl4debian[.]nl

- debian5[.]carrd[.]co
- debian5[.]lenug[.]su
- debian7[.]ddnss[.]de
- salsa[.]debian[.]net
- tanda[.]debian[.]net
- karinedebian[.]ovh
- debian4[.]clan[.]rip
- debian[.]iopsys[.]se