Rhysida, Not Novel but Still Dangerous: DNS Revelations

Table of Contents

Executive Report

Rhysida, a new ransomware currently plaguing users may not be novel but it's proving to be just as effective. Fortra published an in-depth analysis of the malware currently holding the data of healthcare organizations primarily based in the U.S. hostage. Other countries and their government agencies shouldn't rest easy, though, as its operators have also gone after the Chilean army.

Since Rhysida's emergence, the cybersecurity community has been amassing indicators of compromise (IoCs) related to the threat. AlienVault OTX, for one, has collated 50 domains and three email addresses so far.

The WhoisXML API research team dove deeper into the ransomware operators' infrastructure via an IoC list expansion analysis in an effort to identify other potential attack vectors that may not yet be on organizations' radar. We found:

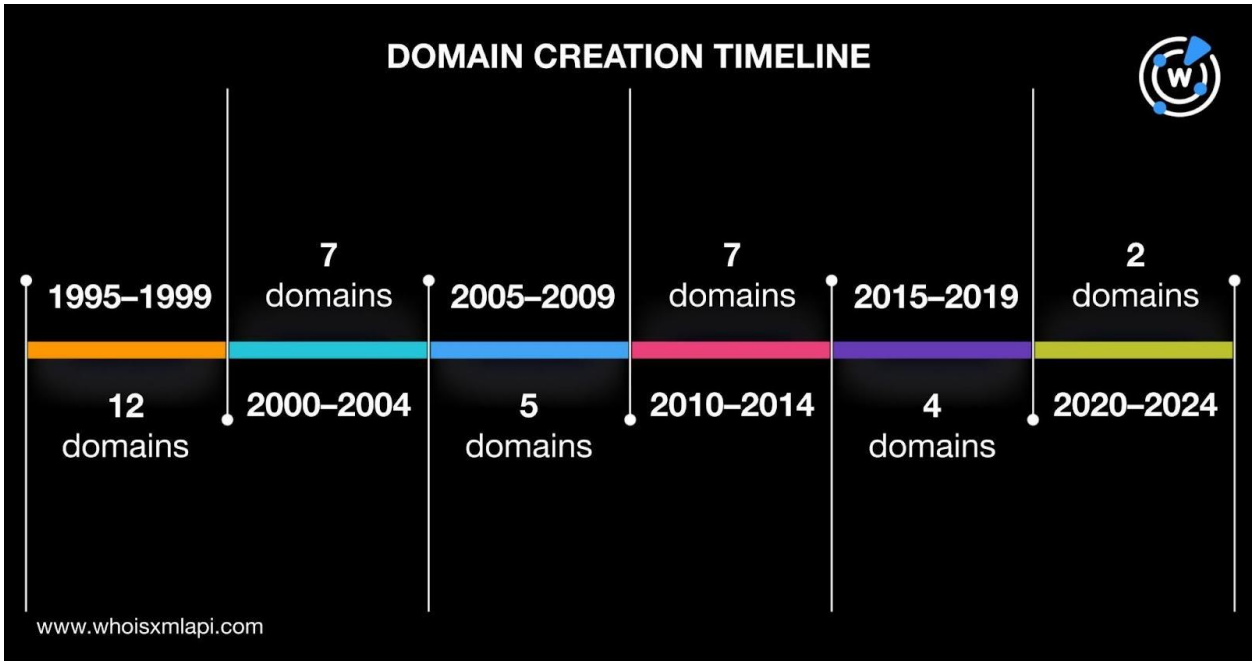
- 60 IP addresses to which 47 of the domains identified as IoCs resolved, eight of which are already being detected as malicious based on malware checks
- 1,461 domains hosted on 44 dedicated IP addresses that could be part of Rhysida's connected infrastructure, three of which turned out to be malicious based on a bulk malware check
- 11,774 domains that contained strings found among some of the IoCs, 19 of which are already classified as malicious based on a bulk malware check

Unreported IoC Facts

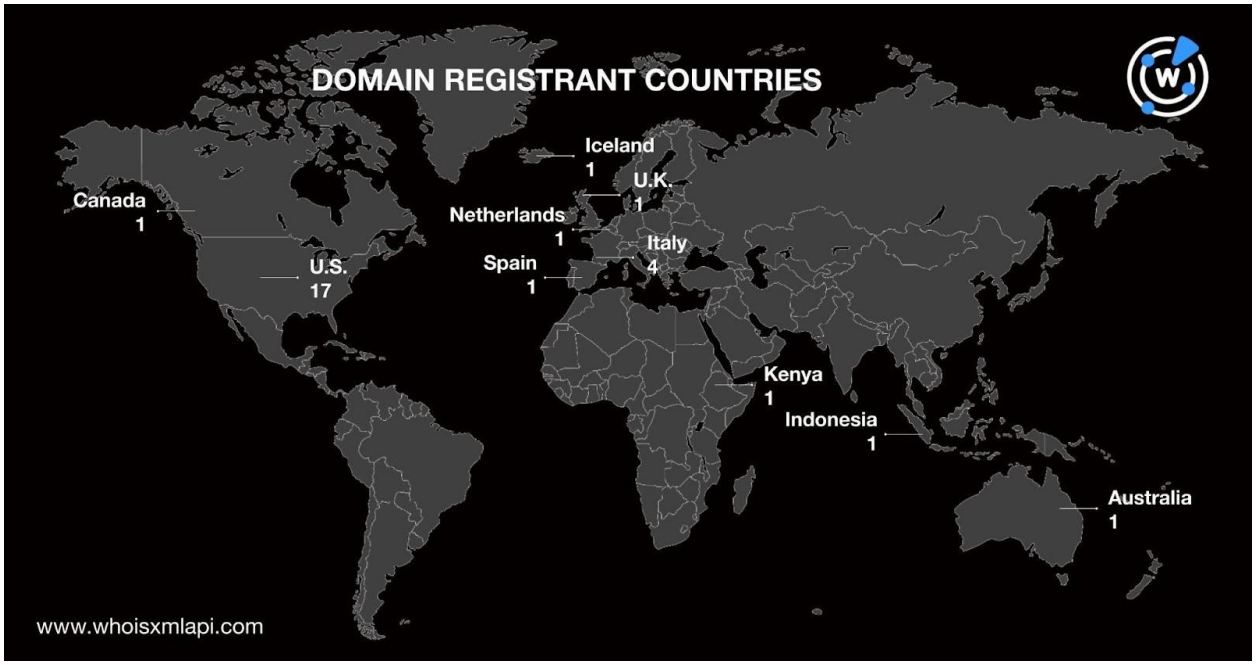
We began our in-depth analysis of Rhysida by looking for more information aided by our IP, DNS, and WHOIS tools.

A bulk WHOIS lookup for the 50 domains identified as Rhysida IoCs revealed that:

- Thirty-eight domains had publicly viewable registrars topped by GoDaddy.com (nine IoCs), followed by Network Solutions (six IoCs), and Hosting Concepts and Key-Systems (two IoCs each). The remaining 19 domains were spread across different registrars.
- Thirty-seven domains had creation dates spanning 1995 to 2021, which could mean the ransomware operators favored using aged over newly registered domains (NRDs). The highest number, in fact, were first created 24–28 years ago.



- One domain had an unredacted personal email address, which was historically used to register seven other domains based on reverse WHOIS searches, none of which are currently classified as malicious.
- Ten domains had registrant organizations.
- Twenty-nine domains had visible registrant countries led by the U.S. (17 IoCs) and Italy (four IoCs). The remaining eight IP addresses each originated from a different country.



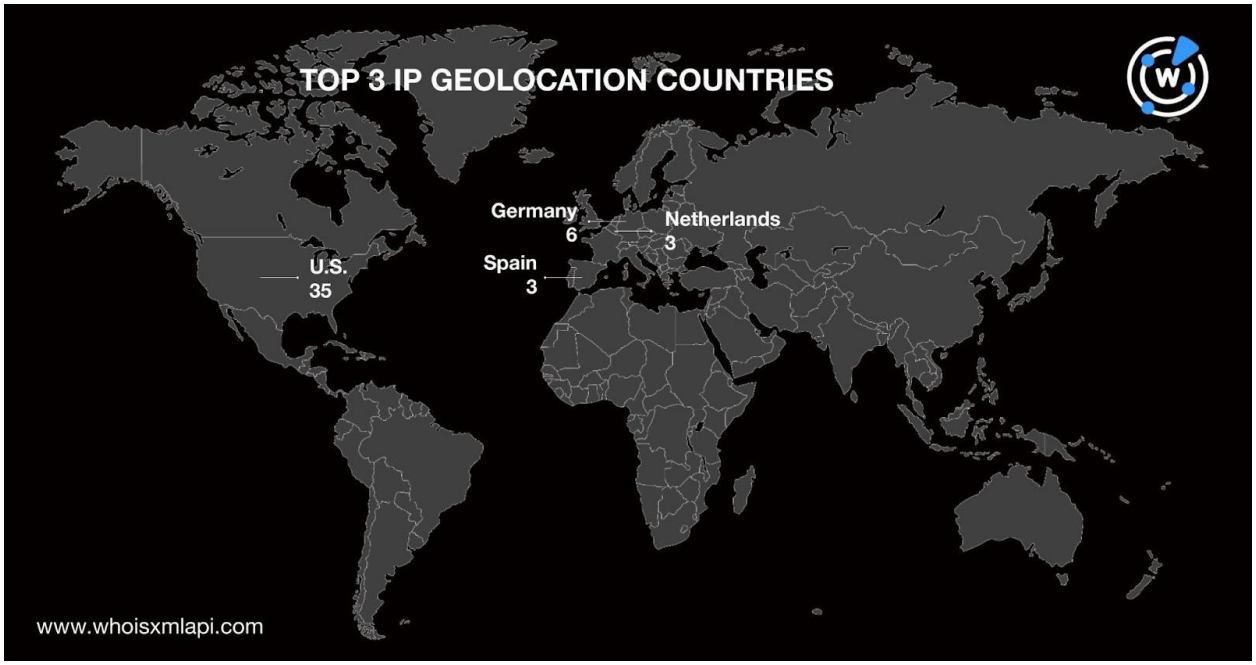
We also performed reverse WHOIS searches for the email addresses identified as IoCs but none were used to register domains.

IoC Expansion DNS Findings

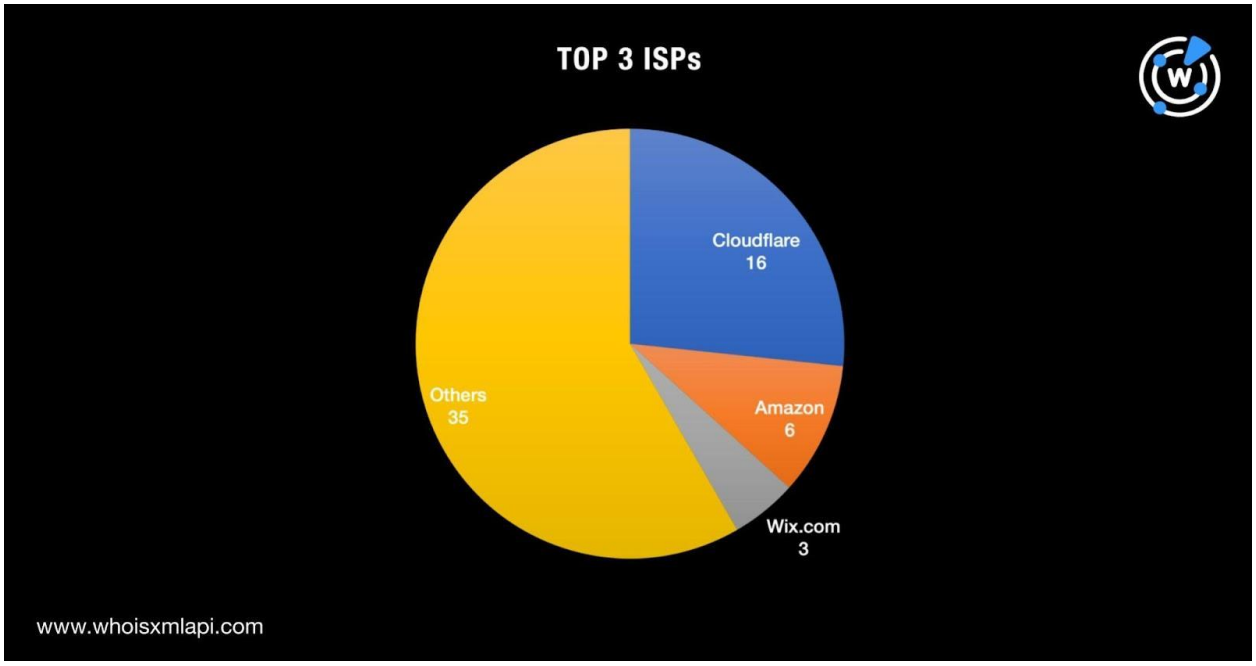
To determine other web properties that could be part of the Rhysida infrastructure, we expanded the current list of IoCs starting with DNS lookups that revealed that 47 of the domains resolved to 60 unique IP addresses, eight of which turned out to be malicious based on a bulk malware check.

A bulk IP geolocation lookup for the domain IoCs' hosts revealed that:

- The 60 IP addresses were spread across 15 countries led by the U.S. (35 IoCs), Germany (six IoCs), and Spain and the Netherlands (three IoCs each). The remaining 13 were spread across 11 other countries.

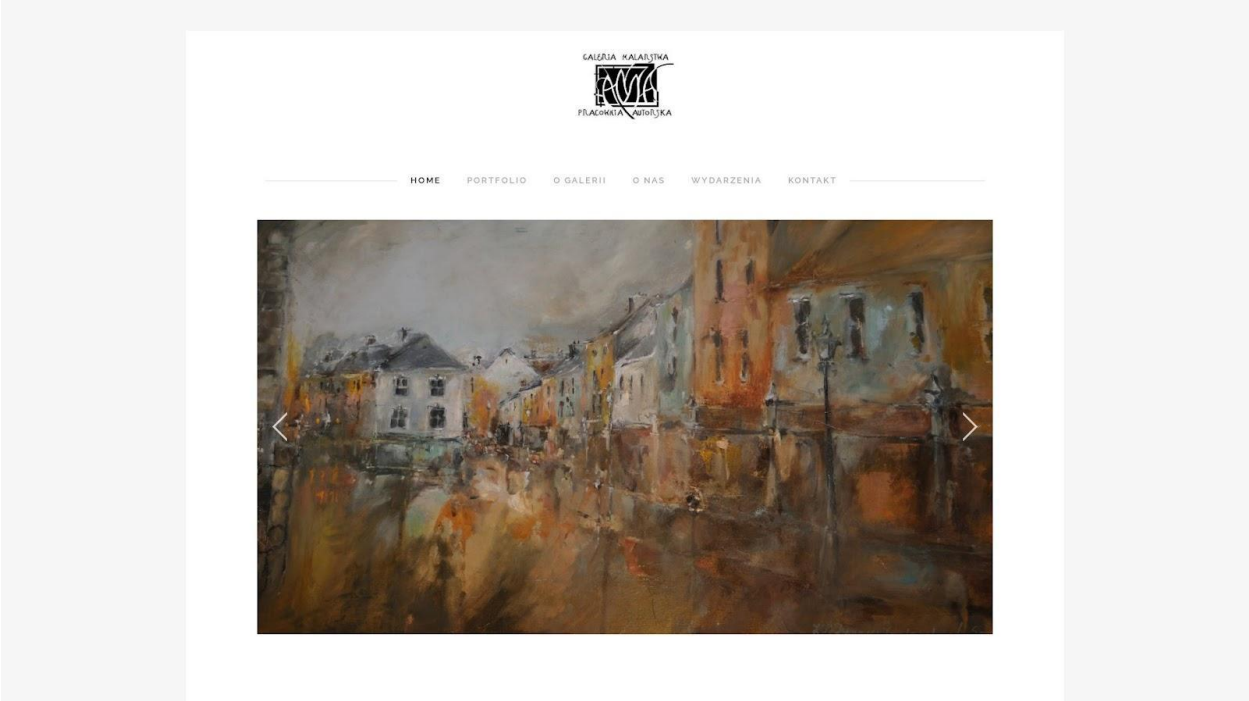


- They were distributed among 33 ISPs led by Cloudflare (16 IoCs), Amazon (six IoCs), and Wix.com (three IoCs).



Reverse IP lookups for the 60 IP resolutions showed that 44 were seemingly dedicated and played host to 1,461 domains not yet on the published list of IoCs. Three of the IP-connected

domains are already being detected as malicious and one continues to host a live page to date based on a screenshot lookup.



Screenshot of the page hosted on the malicious IP-connected domain galeriaanna[.]pl

To widen our threat hunting coverage, we also used these strings found among 47 of the domains identified as IoCs as Domains & Subdomains Discovery search terms:

- **ziegel-eder.**
- **unitedtractors.**
- **tyconz.**
- **townsquaremedia.**
- **thebiglifegroup.**
- **snjb.**
- **scharco.**
- **sapros.**
- **rouzbeh.**
- **rlbayless.**
- **ramtha.**
- **polanglo.**
- **pami.**
- **onionmail.**
- **nebraskaland.**
- **koper-it.**
- **knpgroup.**
- **kebs.**
- **jeffersoncountyhealthcenter.**
- **iris-depannage-informatique.**
- **imatica.**
- **ict-college.**
- **hollywoodforever.**
- **haemokinesis.**
- **greenfiber.**
- **fassi.**
- **eska-fuses.**
- **ejercito.**
- **ecaterham.**
- **cvalley.**

- **comune.**
- **collectivitedemartinique.**
- **cittanuova.**
- **bmgroup.**
- **bionpharma.**
- **ayto-arganda.**
- **axity.**
- **avannubo.**
- **amstutz.**
- **albertanewsprint.**

That led to the discovery of 11,774 domains, 19 of which turned out to be malicious according to a bulk malware check. Only one continues to host live content as of this writing. Based on a WHOIS lookup, dworekpodlipami[.]katowice[.]pl was created on 17 August 2006 with Home.pl S.A. as its registrar.

Screenshot of the page hosted on the malicious string-connected domain dworekpodlipami[.]katowice[.]pl

The 18 remaining malicious domains were either unreachable, parked, or led to blank or error pages.

—

Our in-depth analysis of the published Rhysida IoCs allowed us to uncover more than 18,000 possibly connected artifacts. It also shed more light on the ransomware operators' modus operandi. For instance, we found that they seem to prefer using aged domains over NRDs, with

the newest ones created two years ago. They also chose to distribute parts of their infrastructure to several service providers (registrars and ISPs alike) and countries.

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: Sample Artifacts and IoCs

Published Rhysida IoCs

- polytec[.]bmgroup[.]com
- ziegel-eder[.]de
- unitedtractors[.]com
- tyconz[.]com
- townsquaremedia[.]com
- thomas-hardye[.]net
- thebiglifegroup[.]com
- snjb[.]net
- sinbadclub[.]com
- scharco[.]eu
- sapros[.]de
- rouzbeh[.]info
- rlbayless[.]com
- rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad[.]onion
- ramtha[.]com
- polanglo[.]pl
- parisathletics[.]com
- pami[.]org[.]ar
- onionpmail[.]org
- onionmail[.]org
- oneexchangecorp[.]com
- newcenturyadvisors[.]com
- nebraskaland[.]com
- koper-it[.]nl
- knpgroup[.]com
- kebs[.]org
- jeffersoncountyhealthcenter[.]org
- itwfoodequipment[.]com
- iris-depannage-informatique[.]com
- imatica[.]com
- ict-college[.]net
- hollywoodforever[.]com
- haemokinesis[.]com
- greenfiber[.]com
- fassi[.]com
- eska-fuses[.]de
- ejercito[.]cl
- ecaterham[.]net
- cvalley[.]net
- comune[.]fe[.]it
- compassinf[.]com
- collectivitedemartinique[.]mq
- cittanuova[.]it
- bmgroup[.]com
- bionpharma[.]com
- ayto-arganda[.]es
- axity[.]com

- avannubo[.]com
- amstutz[.]ch
- albertanewsprint[.]com
- rhysidaofficial@onionpmail[.]org
- rhysidaofficial@onionmail[.]org
- rhysidaeverywhere@onionmail[.]org

Sample IP Resolutions

- 104[.]21[.]21[.]63
- 104[.]21[.]72[.]168
- 104[.]22[.]64[.]103
- 104[.]22[.]65[.]103
- 104[.]26[.]0[.]144
- 104[.]26[.]1[.]144
- 104[.]26[.]10[.]72
- 104[.]26[.]11[.]72
- 104[.]26[.]14[.]238
- 104[.]26[.]15[.]238
- 137[.]117[.]245[.]118
- 156[.]67[.]71[.]131
- 166[.]62[.]108[.]178
- 172[.]105[.]121[.]115
- 172[.]67[.]187[.]33
- 172[.]67[.]196[.]203
- 172[.]67[.]69[.]151
- 172[.]67[.]69[.]67
- 172[.]67[.]7[.]194
- 172[.]67[.]70[.]75

Sample Malicious IP Resolutions

- 104[.]26[.]0[.]144
- 104[.]26[.]1[.]144
- 104[.]26[.]10[.]72
- 185[.]230[.]63[.]107

Sample IP-Connected Domains

- 1407[.]productions
- 189[.]241[.]214[.]35[.]bc[.]googleusercontent[.]com
- 3etravel[.]me
- 63autobody[.]com
- 7p-emm[.]com
- 7p-emm[.]de
- 7p-enterprisemobility[.]com
- 7p-enterprisemobility[.]de
- 7p-mdm[.]com
- 7p-mdm[.]de
- 7pemm[.]com
- 7pemm[.]de
- 88slotdewa[.]fit
- 99vg99[.]com
- abcnalabama[.]org
- accent-hub[.]com
- achibo[.]de
- admedica-marketing[.]de
- adsupply-dev[.]com
- aduesterhus[.]net
- advocadagirona[.]cat
- affairy[.]com
- affairy[.]de
- affinitysolutions[.]es
- agenda[.]net[.]pl
- ahoramallorca[.]com
- ahsathletics[.]org
- aiguescb[.]com
- akom[.]waw[.]pl
- akom24[.]eu
- aktifmatinik[.]mq
- alansean[.]com
- albedo-blog[.]com

- albedotelecom[.]com
- alcsystemscanada[.]de
- alex-muehlbauer[.]de
- allenathletics[.]org
- allencollege[.]edu
- allterracentral[.]com
- alpe-gesundheit[.]de
- alpe-vertrieb[.]de
- alpe-vertriebskoordination[.]de
- altoonaathletics[.]com
- amazingchicken[.]co[.]uk
- americanhouse[.]pl
- ameterreading[.]com
- amrconnect[.]com
- analizabik[.]pl
- andreasbuder[.]at
- andrzejewskimarcin[.]pl
- angielskidk[.]pl
- animallibre[.]org
- anka[.]co[.]at
- ankara[.]bel[.]tr
- ankurdana[.]com
- anyspices[.]com
- anyspices[.]tettixsa[.]com
- apomeds[.]dev
- appholtcypher[.]com
- appku[.]byproweb[.]co[.]id
- appku[.]id
- appliancecity[.]co[.]uk
- apsprojekt-ana[.]de
- aptelo[.]eu
- aptelo[.]net
- aptelo[.]pl
- apuleat[.]it
- arabskitlumaczenia[.]com
- arahoster[.]com
- artgeo-kepno[.]pl
- artgeo[.]kepno[.]pl
- artgeokepno[.]pl
- artisanat-shop[.]com
- aslimadu[.]com
- asset[.]prtvstatic[.]com
- athleticschedulesonly[.]org
- auservis[.]com
- auto-schweer[.]de
- auto-sonnenschutz[.]net
- autoserwis-kielce[.]pl
- autosoftecu[.]com
- autyzmbeztabu[.]pl
- avancemgrup[.]cat
- avancemgrup[.]com
- avancemgrup[.]net
- avannubo[.]cat
- avannubo[.]es
- avannubo[.]eu
- avannubo[.]net
- avanvault[.]com
- avanvoip[.]com
- avanvoip[.]es
- avanzia[.]com[.]mt
- aystitches[.]com[.]ng
- b2blessing[.]com
- bagimoto[.]com
- bahsbluedevils[.]com
- balance-wohlbefinden[.]de
- basdfalcons[.]org
- basoli[.]com

Sample Malicious IP-Connected Domains

- dovdov[.]co[.]il
- galeriaanna[.]pl

Sample String-Connected Domains

- albertanewsprint[.]net
- amstutz[.]cc
- amstutz[.]de
- amstutz[.]pl
- amstutz[.]us
- amstutz[.]at
- amstutz[.]li
- amstutz[.]ai
- amstutz[.]fr
- amstutz[.]ca
- amstutz[.]cz
- amstutz[.]eu
- amstutz[.]me
- amstutz[.]nu
- amstutz[.]io
- amstutz[.]co
- amstutz[.]ar
- camstutz[.]ch
- amstutz[.]biz
- amstutz[.]xyz
- amstutz[.]com
- famstutz[.]de
- amstutz[.]dev
- amstutz[.]pro
- amstutz[.]org
- amstutz[.]net
- aamstutz[.]ch
- famstutz[.]ch
- amstutz[.]name
- amstutz[.]link
- amstutz[.]wine
- damstutz[.]com
- camstutz[.]com
- jamstutz[.]com
- amstutz[.]live
- amstutz[.]gmbh
- amstutz[.]tech
- hdamstutz[.]ch
- amstutz[.]coach
- mbcamstutz[.]eu
- sf-amstutz[.]ch
- amstutz[.]legal
- kdamstutz[.]net
- mbcamstutz[.]ch
- teamstutz[.]com
- ursamstutz[.]ch
- afamstutz[.]com
- ronamstutz[.]us
- amstutz[.]co[.]uk
- adamstutz[.]com
- hofamstutz[.]ch
- kdamstutz[.]com
- amstutz[.]earth
- leoamstutz[.]ch
- amstutz[.]email
- amyamstutz[.]ch
- ejamstutz[.]net
- robamstutz[.]com
- kenamstutz[.]net
- amstutz[.]online
- danamstutz[.]com
- urs-amstutz[.]ch
- amstutz[.]boston
- hansamstutz[.]ch
- amstutz[.]com[.]ar
- hediamstutz[.]ch
- jeffamstutz[.]io
- ouramstutz[.]com
- amyamstutz[.]com
- joelamstutz[.]ch
- kenamstutz[.]com
- adiamstutz[.]com
- ronamstutz[.]com
- mbcamstutz[.]com
- amstutz[.]family
- hansamstutz[.]ws
- solamstutz[.]com
- ronamstutz[.]org
- amstutz[.]global
- gabiamstutz[.]ch

- ruediamstutz[.]ch
- joelamstutz[.]com
- anitaamstutz[.]ch
- fredamstutz[.]com
- ryanamstutz[.]com
- daveamstutz[.]org
- eugenamstutz[.]ch
- ericamstutz[.]com
- tonyamstutz[.]com
- ireneamstutz[.]ch
- andiamstutz[.]com
- aaronamstutz[.]me
- oli-amstutz[.]com
- yann-amstutz[.]ch
- amyjamstutz[.]com
- silasamstutz[.]ch
- garyamstutz[.]com
- heli-amstutz[.]de
- fabioamstutz[.]ch
- karaamstutz[.]com
- lisaamstutz[.]com
- drewamstutz[.]com
- karinamstutz[.]ch
- ehrl-amstutz[.]de
- deanamstutz[.]com
- ruth-amstutz[.]ch
- elke-amstutz[.]de
- livioamstutz[.]ch
- kurtamstutz[.]com
- mbcamstutz[.]swiss
- stefanamstutz[.]ch
- estheramstutz[.]ch
- davidamstutz[.]net
- nadjaamstutz[.]com
- jennyamstutz[.]com
- ireneamstutz[.]com
- aaronamstutz[.]com
- markusamstutz[.]ch
- nanciamstutz[.]com
- lukas-amstutz[.]ch
- fabio-amstutz[.]ch
- adrianamstutz[.]ch
- davidamstutz[.]org
- amstutz[.]partners
- rudolfamstutz[.]ch
- kevinamstutz[.]com
- pierreamstutz[.]ch
- marcelamstutz[.]ch
- lydiaamstutz[.]com
- gerryamstutz[.]com
- gamstutz[.]digital
- pascalamstutz[.]ch
- danielamstutz[.]ch
- davidamstutz[.]com
- karenamstutz[.]com
- sport-amstutz[.]ch
- fabianamstutz[.]ch
- averyamstutz[.]com
- mesasamstutz[.]com
- kiaraamstutz[.]com
- karieamstutz[.]com
- larryamstutz[.]com
- laura-amstutz[.]ch
- jamesamstutz[.]com
- anita-amstutz[.]ch
- bruceamstutz[.]com
- jorgeamstutz[.]com
- anitaamstutz[.]com
- regulaamstutz[.]ch
- nicoleamstutz[.]com
- barbaraamstutz[.]ch
- jeremyamstutz[.]com
- farrynamstutz[.]com
- aaronamstutz[.]info
- carlos-amstutz[.]ch
- donnaramstutz[.]biz
- josephamstutz[.]com
- michaelamstutz[.]de
- arthuramstutz[.]com
- yannickamstutz[.]ch

- sandraamstutz[.]com
- kelleyamstutz[.]com
- danielamstutz[.]net
- gisbertamstutz[.]de
- annikaamstutz[.]com
- aubrieamstutz[.]com
- joshuaamstutz[.]com
- vincentamstutz[.]ch
- parkeramstutz[.]com
- tamara-amstutz[.]ch
- micheleamstutz[.]ch
- emilieamstutz[.]com
- nathanamstutz[.]net
- danielamstutz[.]org
- danielamstutz[.]art
- andreasamstutz[.]ch
- maurusamstutz[.]com
- donnaramstutz[.]com
- carrieamstutz[.]com
- nathanamstutz[.]com
- fabianamstutz[.]com
- simeonamstutz[.]com
- danielamstutz[.]com
- garyamstutz[.]co[.]za
- adrian-amstutz[.]ch
- stefanamstutz[.]com
- triciaamstutz[.]com
- physio-amstutz[.]ch
- janoschamstutz[.]com
- malerei-amstutz[.]ch
- ebneter-amstutz[.]ch
- drjasonamstutz[.]com
- charlesamstutz[.]org
- michelleamstutz[.]ch
- patrick-amstutz[.]ch
- balance-amstutz[.]ch
- charlesamstutz[.]com
- zimmereiamstutz[.]ch
- dominik-amstutz[.]ch
- familie-amstutz[.]de
- janetteamstutz[.]com
- amstutzamstutz[.]win
- daniela-amstutz[.]ch
- charlesamstutz[.]net
- therese-amstutz[.]ch
- michaelamstutz[.]com
- anthony-amstutz[.]me
- stephenamstutz[.]com
- barbaraamstutz[.]com
- holzbau-amstutz[.]ch
- anaelleamstutz[.]com
- dominik-amstutz[.]ws
- composeramstutz[.]com
- nathalieamstutz[.]com
- molkerei-amstutz[.]ch
- jenniferamstutz[.]com
- philippeamstutz[.]com
- frederic-amstutz[.]ch
- coiffeur-amstutz[.]ch
- melissalamstutz[.]com
- joelrubenamstutz[.]com
- guillermoamstutz[.]com
- bangerter-amstutz[.]ch
- wendyamstutz[.]realtor
- gabrielleamstutz[.]com
- christina-amstutz[.]ch
- madeleine-amstutz[.]ch
- christineamstutz[.]com
- fromagerieamstutz[.]ch
- christianamstutz[.]com
- xn--pfndlermitamstutz-rqb[.]ch
- consulting-amstutz[.]ch
- fromagerie-amstutz[.]ch
- ann-kathrinamstutz[.]ch
- architektur-amstutz[.]ch
- happilyeveramstutz[.]com
- schreinerei-amstutz[.]ch
- pfaendlermitamstutz[.]ch
- matthewjamesamstutz[.]com
- miracrivelliamstutz[.]com

- malermeister-amstutz[.]de
- vehknowsdstramstutz[.]party
- alexandriapaigeamstutz[.]com
- unternehmensberatung-amstutz[.]ch
- avannubo[.]eu
- avannubo[.]org
- avannubo[.]net
- avannubo[.]cat
- axity[.]co
- axity[.]cn
- axity[.]cl
- axity[.]pe
- axity[.]tn
- axity[.]de
- axity[.]se
- axity[.]ca
- axity[.]fr
- axity[.]mx
- axity[.]es
- axity[.]us
- waxity[.]fr
- maxity[.]es
- maxity[.]lv
- paxity[.]eu
- maxity[.]me
- laxity[.]ru
- maxity[.]cz
- taxity[.]su
- maxity[.]be
- laxity[.]io
- taxity[.]it
- laxity[.]jp
- maxity[.]cn
- maxity[.]de
- maxity[.]ru
- axity[.]app
- paxity[.]tk
- maxity[.]fr
- laxity[.]pw
- maxity[.]tv
- maxity[.]us
- taxity[.]ir
- maxity[.]eu
- saxity[.]de
- laxity[.]us
- maxity[.]co
- laxity[.]in
- taxity[.]ru
- taxity[.]tk
- axity[.]lat
- maxity[.]io
- taxity[.]ch
- axity[.]net
- paxity[.]fr
- faxity[.]se
- taxity[.]in
- baxity[.]ru
- laxity[.]pl
- axity[.]pro
- axity[.]org
- maxity[.]se
- faxity[.]tk
- maxity[.]at
- axity[.]biz
- maxity[.]it
- taxity[.]de
- taxity[.]eu
- taxity[.]fr
- saxity[.]fr
- maxity[.]ai
- laxity[.]ph
- maxity[.]ca
- taxity[.]be
- taxity[.]pl
- laxity[.]ir
- naxity[.]fr
- taxity[.]me
- laxity[.]dk
- faxity[.]eu
- taxity[.]cl

- maxity[.]uk
- faxity[.]cf
- axity[.]xyz
- maxity[.]in
- taxity[.]nl
- taxity[.]co
- waxity[.]ca
- praxity[.]ca
- taxity[.]xyz
- adaxity[.]ru
- blaxity[.]co
- imaxity[.]jp
- laxity[.]top
- zaxity[.]com
- fraxity[.]de
- praxity[.]es
- maxity[.]xyz
- laxity[.]bid
- draxity[.]tk
- reaxity[.]de
- taxity[.]pro
- ataxity[.]us
- zaxity[.]top
- adaxity[.]ch
- laxity[.]xyz
- axity[.]immo
- axity[.]info
- laxity[.]net
- praxity[.]be
- praxity[.]in
- praxity[.]no
- adaxity[.]no
- daxity[.]com
- adaxity[.]mx
- adaxity[.]eu
- upaxity[.]co
- laxity[.]biz
- praxity[.]co
- traxity[.]nl
- upaxity[.]ru
- laxity[.]org
- paxity[.]net
- raxity[.]com
- maxity[.]biz
- vaxity[.]com
- axity[.]date
- baxity[.]pro
- adaxity[.]kr
- praxity[.]uk
- adaxity[.]is
- saxity[.]com
- maxity[.]org
- zaxity[.]xyz
- jaxity[.]com
- praxity[.]de
- upaxity[.]tw
- adaxity[.]cl
- praxity[.]mx
- maxity[.]com
- taxity[.]app
- axity[.]club
- praxity[.]jp
- praxity[.]ie
- paxity[.]org
- haxity[.]com
- laxity[.]com
- faxity[.]net
- upaxity[.]ch
- faxity[.]dev
- caxity[.]com
- upaxity[.]no
- paxity[.]com
- faxity[.]com
- praxity[.]fr
- praxity[.]nl
- saxity[.]net
- faxity[.]org
- praxity[.]eu
- axity[.]tech
- taxity[.]org

- praxity[.]us
- adaxity[.]co
- baxity[.]com
- waxity[.]com
- taxity[.]biz
- taxity[.]net
- naxity[.]com
- praxity[.]dk
- adaxity[.]uk
- taxity[.]com
- adaxity[.]tw
- praxity[.]cn
- praxity[.]ru
- upaxity[.]kr
- maxity[.]net
- upaxity[.]is
- upaxity[.]uk
- upaxity[.]mx
- panaxity[.]co
- adaxity[.]xyz
- dynaxity[.]us
- relaxity[.]ca
- taxity[.]club
- graxity[.]com
- relaxity[.]co
- lunaxity[.]cf
- traxity[.]com
- axity[.]cloud
- apaxity[.]com
- axity[.]click
- praxity[.]com
- praxity[.]xxx
- imaxity[.]com
- relaxity[.]ch
- maxity[.]mobi
- praxity[.]net
- galaxity[.]co
- jiaxity[.]com
- paxity[.]info
- galaxity[.]io
- smaxity[.]com
- blaxity[.]com
- traxity[.]xyz
- claxity[.]com
- upaxity[.]net
- galaxity[.]ma
- chaxity[.]com
- flaxity[.]com
- tenaxity[.]co
- taxity[.]info
- staxity[.]com
- axity[.]ninja
- lunaxity[.]tk
- metaxity[.]cn
- praxity[.]xyz
- laxity[.]club
- galaxity[.]pl
- pesaxity[.]tk
- smaxity[.]net
- dynaxity[.]ch
- adaxity[.]org
- reaxity[.]com
- relaxity[.]ru
- upaxity[.]org
- upaxity[.]com
- relaxity[.]hk
- omaxity[.]com
- snaxity[.]com
- dnaxity[.]com
- braxity[.]com
- duaxity[.]top
- staxity[.]net
- dynaxity[.]de
- fraxity[.]com
- zaxity[.]club
- draxity[.]com
- qpaxity[.]com
- dynaxity[.]eu
- praxity[.]biz
- adaxity[.]com

- molaxity[.]cn
- galaxity[.]se
- ataxity[.]fun
- relaxity[.]eu
- galaxity[.]tk
- qulaxity[.]de
- kamaxity[.]tk
- laxity[.]info
- galaxity[.]de
- uvaxity[.]com
- dynaxity[.]cl
- blaxity[.]app
- oyaxity[.]com
- audaxity[.]uk
- baxity[.]info
- dynaxity[.]at
- udaxity[.]com
- vafaxity[.]ml
- itaxity[.]com
- relaxity[.]fr

Sample Malicious String-Connected Domains

- albertanewsprint[.]net
- taxity[.]online
- makermaxity[.]club
- bmgroup[.]me
- notiziedalcomune[.]com
- innovazioneincomune[.]info
- edenicvalley[.]com
- fassi[.]one
- organicvalley[.]organic
- ostrykebs[.]pl