Is There More to the New Transparent Tribe TTPs?

Table of Contents

Executive Report

The Pakistan-India rivalry has been going on for some time now, not just in sports events but also online in the form of cyber attacks. Zscaler ThreatLabz has been monitoring a result of this ongoing friction—Transparent Tribe, also known as "APT-36"—since the start of this year.

In the past, the threat group relied on malvertising and phishing to steal confidential information from their target Indian governmental organizations. They've seemingly upped the ante just this month with new tools, tactics, and procedures (TTPs), including abusing the legitimate Kavach app and Google Ads and using a new exfiltration tool dubbed "Limepad." Given all that, the researchers published 15 domains as indicators of compromise (IoCs), namely:

- xlapp[.]workbooks[.]open
- kavach[.]mail[.]nic-updates[.]in
- kavach[.]mail[.]gov[.]in
- wzxdao[.]com
- nic-updates[.]in
- ncloudup[.]com
- kavachsupport[.]com
- kavachguide[.]com
- kavachdownload[.]in
- kavach-app[.]in
- kavach-app[.]com
- getkavach[.]com
- get-kavach[.]in
- gcloudsvc[.]com
- acmarketsapp[.]com

In an effort to make the Internet transparent and safer, we used the domains above as jump-off points to conduct an in-depth IoC expansion analysis aided by our WHOIS, IP, and DNS intelligence sources. Our investigation revealed:

- 13 IP addresses to which the IoCs resolved
- 1,511 domains that shared the IoCs' IP hosts

- 687 more domains that shared the IoCs' strings—"kavach," "wzxdao," "nic-updates," "ncloudup," "gcloudsvc," and "acmarketsapp"
- 62 unredacted registrant email addresses from the additional domains' current WHOIS records
- 11,592 more domains that shared the newly found artifacts' registrant email addresses
- 31 malicious artifacts

What Our Closer Look Revealed

We began our foray into the public IoCs by subjecting them to DNS lookups that showed they resolved to 13 unique IP addresses, seven of which are:

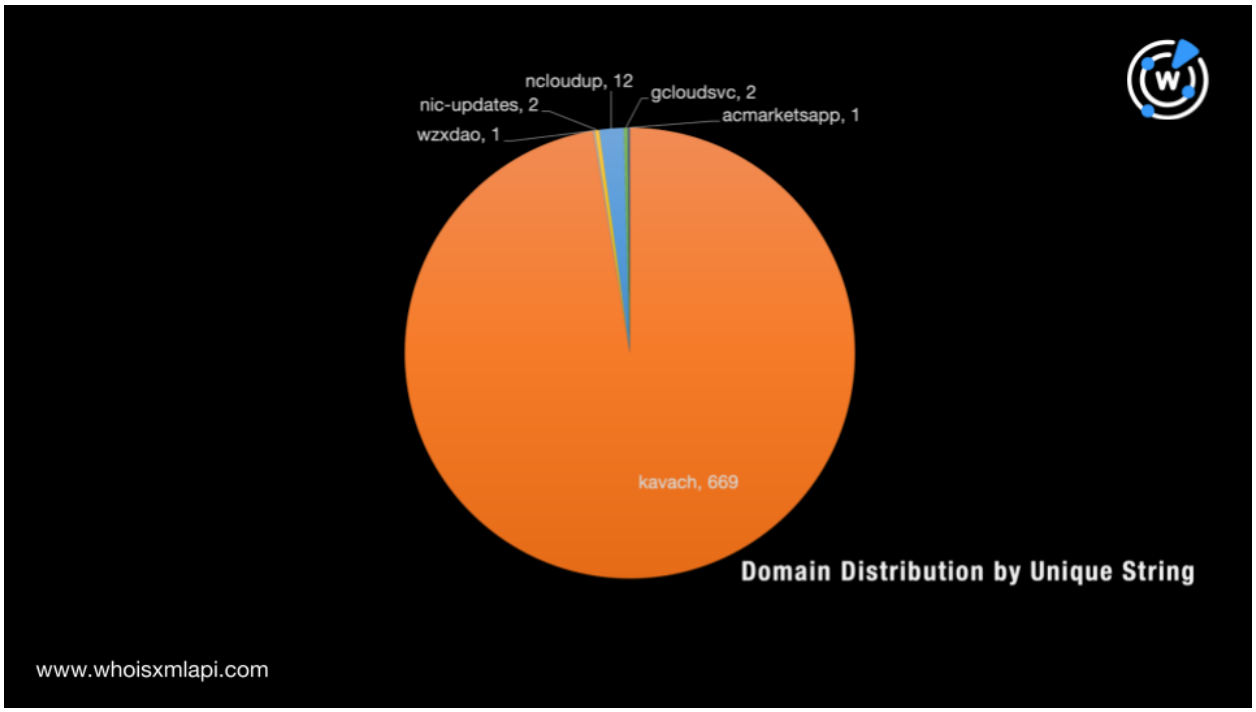
- 172[.]67[.]130[.]228
- 104[.]21[.]3[.]152
- 176[.]57[.]188[.]221
- 65[.]108[.]136[.]118
- 172[.]67[.]195[.]216
- 104[.]21[.]52[.]54
- 164[.]100[.]15[.]168

These IP addresses were mostly concentrated in the U.S. though one host each traced their origins to four other countries—Germany, Finland, India, and the Netherlands. Given the attack's target—Indian governmental organizations—the use of these locations could be a ploy to mislead investigators regarding the attackers' actual origins.

Using the IP addresses above as reverse IP lookup search terms allowed us to collate 1,512 possibly connected domains.

We noticed unique strings from among the IoCs, including "kavach," "wzxdao," "nic-updates," "ncloudup," "gcloudsvc," and "acmarketsapp" and used these as Domains & Subdomains Discovery search terms to gather more potentially related artifacts. That led to the discovery of 687 more domains, some of which also contained interesting strings like "insurance" (e.g., insurancekavach[.]com) and "corona" (e.g., coronakavachapp[.]com). These could figure in attacks targeting insurance companies and their employees and customers or people in search of COVID-19 related information.

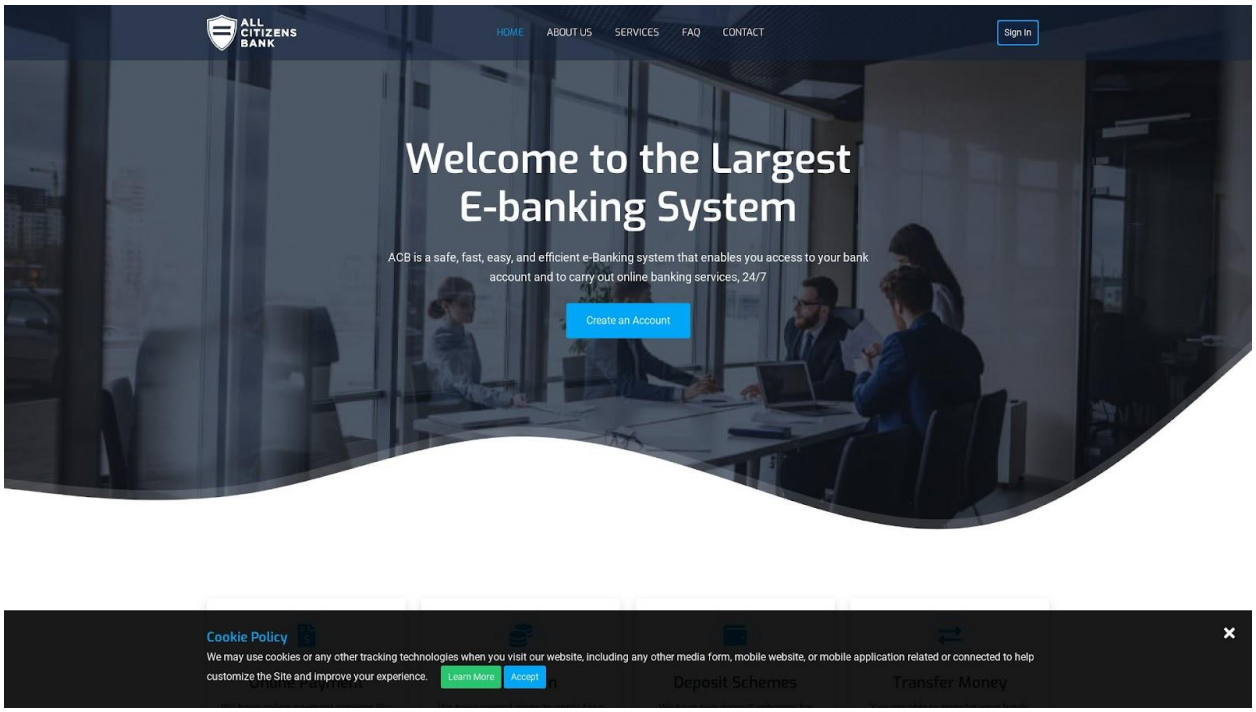
Here is an overview of the additional artifacts that contained the same unique strings seen among the domains identified as IoCs below.



A bulk WHOIS lookup for the 600+ domains allowed us to uncover 62 unredacted registrant email addresses, seven of which appear to belong to legitimate businesses so they were excluded from our next step. As the remaining 55 email addresses could belong to potential attackers given their ties to the IoCs, we subjected them to reverse WHOIS searches, which gave us 11,592 more domains.

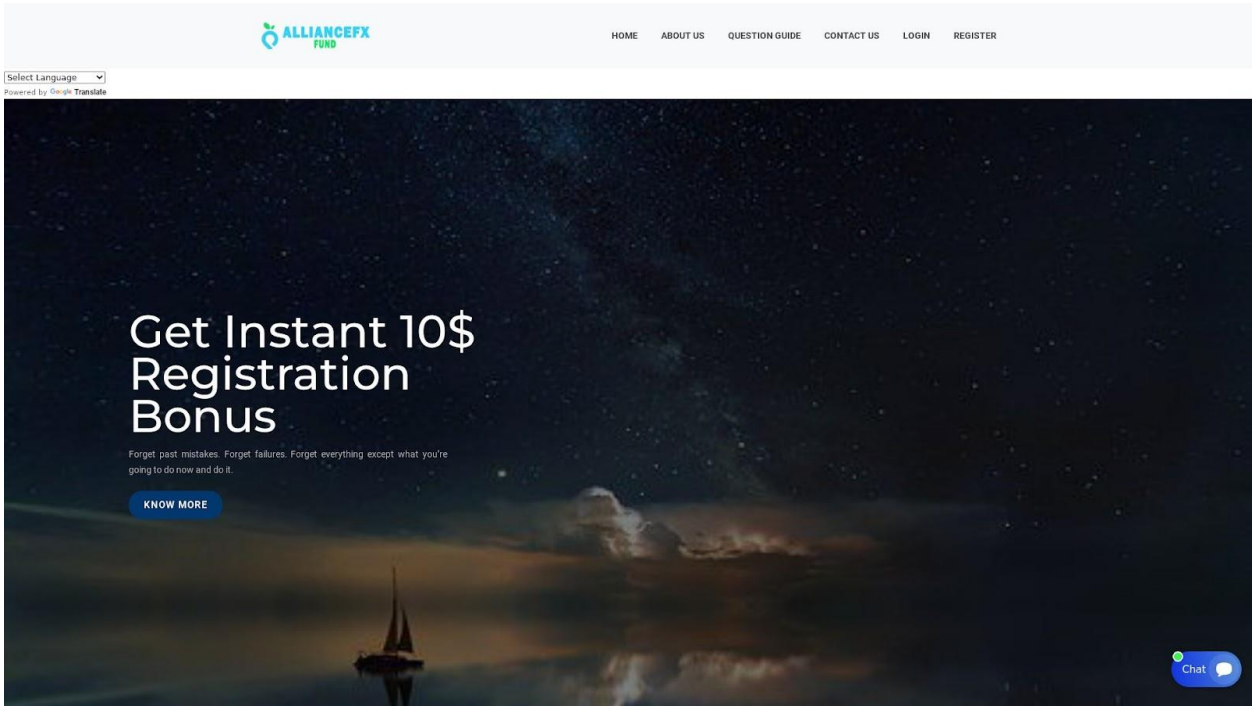
Further scrutiny of the 11,000+ domains showed that 1,086 of them had retrievable WHOIS records. In addition, a majority of them (399 domains) identified Iceland as their registrant country, followed by the U.S. (291 domains), Canada (23 domains), India (16 domains), and China (11 domains). These locations, apart from the U.S. and the Netherlands, didn't match the top 5 IP geolocation countries.

Screenshot lookups for the 11,000 artifacts also showed interesting results, possibly worthy of monitoring for security reasons. Some of them could be mimicking legitimate business websites like those shown below.



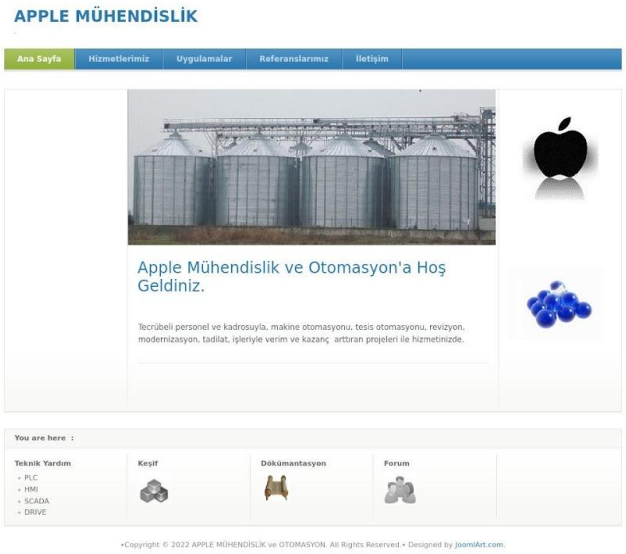
Screenshot of allcitibank[.]com

Note that Citizens Bank exists but the site above isn't its homepage.



Screenshot of alliancefxfund[.]com

Moneysmart.gov.au's website [warns users of transacting with "Alliance FX Capital Ltd."](#) as it could be involved in scams. It is, in fact, one of the companies users shouldn't deal with.



Screenshot of applemuhendislik[.]com

Despite the presence of "Apple" in the domain and the company's logo on the webpage, it has no apparent connection to Apple, Inc. Even though the site's owner may not have created it to lure potential attack victims in, they could be considered guilty of copyright infringement.

More than expanding the publicized list of IoCs with possibly connected artifacts, we were also able to identify 31 additional domains that should probably be included in blocklists, as our bulk malware check showed they were confirmed as either malware hosts or known spam sources.

—

Our deep dive into the digital breadcrumbs that the Transparent Tribe actors could have left allowed us to determine that potential targets should probably include 13 IP addresses and 13,758 domains to their monitoring lists and 31 domains in their blocklists to ensure utmost

protection against the threat. Also, apart from Kavach and Google Ads, the group could also abuse Citibank (allcitibank[.]com), Amazon (amazoncloudupdater[.]net), and Digital Ocean (digitaloceancloudupdator[.]online) and their customers.

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

Sample Domains That Shared the IoCs' IP Hosts

- 87shuwu8[.]cc
- 908e6v[.]com
- 9486335[.]com
- 95bounderrv[.]com
- 999lucky676[.]com
- a-great-ca-cruise[.]fyi
- a-great-indiamba[.]fyi
- a-great-intl-singapore-real-estate[.]fyi
- a[.]networkbridge[.]cloud
- a1[.]qolkrex[.]foundation
- aahhandymanandmore[.]com
- aansslagdccle[.]com
- ab-baby[.]com
- abacuscorpfinance[.]com
- abanking-mellat[.]ga
- abankng-mellat[.]tk
- abavcha[.]tk
- abcshopfitter[.]com
- abdulrehman[.]naufilsakran[.]com
- abjarholding[.]com
- ablapatli[.]cf
- abqpartypix[.]com
- abretamez[.]tk
- absirhabebig[.]ml
- absolutelypamperedspoodles[.]com
- abviconcayvan[.]ml
- academy[.]georgezafiris[.]com
- acaudelletra[.]cat
- acbauslapeawti[.]tk
- accentsofculture[.]com
- accessdigitaltrade[.]com
- account[.]creditfinancialunion[.]net
- accountingpoint[.]com[.]pk
- accounts[.]beverlytrades[.]com
- accountweb[.]site
- accpols[.]com
- acepunsuroco[.]tk
- acexilix[.]tk
- achato[.]fr
- acmarketsapp[.]com
- acott-sculptor[.]com
- actionemploifrance[.]com
- actioneo[.]ga
- actisoowiggdicheck[.]tk
- activeatnight[.]com
- ad[.]furtcoincapital[.]com
- adaptogenselixirlove[.]com
- adazzledentistry[.]com
- admin[.]firstvpn[.]io
- admin[.]oumechtaqcar[.]ma
- admin[.]p500trades[.]co
- adnnjxbi[.]gq
- adorablefrenchieforhomes[.]com

- adovcanmaty[.]gq
- ads-datascience-india-ok[.]live
- ads[.]alfaprima[.]id
- adsociety[.]ophirium[.]io
- adventureandintrigue[.]com
- adwumam[.]com
- aerofincash[.]ltd
- aesthetictouchservices[.]com
- afara[.]obosit[.]com
- aff[.]rich4444[.]com
- affordableconcreteco[.]com[.]au
- afriattire[.]com
- africacapitaldigest[.]co
- afrish[.]povertymustdie[.]africa
- afritels[.]povertymustdie[.]africa
- agaloredar[.]tk
- agcivilconstructioncompany[.]com
- agointernational[.]business
- agribusinessonline[.]com
- ahkolnbj[.]gq
- ahmadrosyihuddin[.]cf
- ahurtunhelane[.]tk
- aideemploifrance[.]com
- aimaspace[.]net
- airconditioningrepairhuntley[.]com
- airdrop[.]ethchain[.]me
- airline-flight-tickets[.]online
- airpod[.]fun
- airtensor[.]com
- airtightpriorityмail[.]com
- aiudga32[.]com
- aiven8[.]me
- aj[.]ajgospel[.]org
- ajess[.]org[.]in
- ajgospel[.]org
- ajswildlifesolutions[.]com
- akgearleo[.]cf
- akrampromo[.]com
- akramuldev[.]com
- akukwesiri[.]com
- al-etihad-cbbk[.]com
- al-etihad-holdings[.]com
- al-safarlaw[.]com
- alalamalarabyalyom[.]com
- alaperadcio[.]tk
- alarmaselite[.]com
- albertconstructionltd[.]com

Sample Domains That Contained the Same Strings as the IoCs

- acmarketsapp[.]com
- gcloudsvc[.]com
- gcloudsvcs[.]com
- kavachikavachi[.]com
- kavach[.]tv
- kavach[.]cn
- kavach[.]io
- kavach[.]ml
- kavach[.]in
- kavach[.]co
- kavach[.]tk
- kavach[.]ca
- kavach[.]jp
- kavach[.]ga
- kavacha[.]in
- kavach[.]net
- kavachi[.]de
- ekavach[.]in
- kavachi[.]ca
- kavachh[.]in
- vajrakavachainfra[.]com
- parmeshwarkavachan[.]in

- kavachocolateinfo[.]com
- kavachiconsulting[.]com
- kavachinvestments[.]com
- rashtriya-kavach[.]tech
- veronikavachulova[.]com
- kavacharestaurant[.]com
- upstart-wt-kavach[.]com
- kavachengineering[.]com
- kavachselfdefense[.]com
- kavachconstruction[.]com
- bhubaneswarikavach[.]com
- atimaharudrakavach[.]com
- zelenakavachudnutie[.]sk
- kavachchildprotect[.]com
- chhinnamastakavach[.]com
- kavachocholateshop[.]com
- ayushmaankavachngo[.]com
- kavachmalhotra[.]website
- kavachcombatsystem[.]com
- yodha-rakshakavach[.]com
- kavachdesignstudio[.]com
- coronakavachpolicy[.]com
- adunikavachanagalu[.]com
- nazarsurakshakavach[.]com
- adhunikavachanagalu[.]com
- kavachahairbraiding[.]com
- bharatdefencekavach[.]com
- maabaglamukhikavach[.]com
- shriamoghshivkavach[.]com
- manavkavachsansthan[.]org
- neelsaraswatikavach[.]com
- kavachasportsacademy[.]com
- kavachafashiondesign[.]com
- agnisurakshakavacham[.]com
- kavachasportsacademy[.]org
- surakshakavachonline[.]com
- kavachaconstructions[.]com
- ramrakshakkavachbook[.]ooo
- kavachelectricgloves[.]com
- mahamrityunjoykavach[.]com
- kavachkalishaktiyonse[.]xyz
- nazarsurakshakavach[.]co[.]in
- chandisaptasatikavach[.]com
- kavachkalishaktiyonse[.]com
- kavachsafetysolutions[.]com
- coronakavachinsurance[.]com
- kavachinoaustralia[.]com[.]au
- kavachafashion-design[.]com
- surakshakavachlimited[.]com
- kavachsecurityservice[.]com
- skandhashashtikavacham[.]com
- kavachmanpowerfacility[.]com
- indiankavachindustries[.]com
- kavachaconstructions[.]co[.]in
- panchmukhihanumankavach[.]com
- visnusahashranaamkavach[.]com
- kavachipropertysolutions[.]com
- kavachhealthcareproducts[.]com
- kavachfinancialservice[.]co[.]uk
- nazarsurakshakavach[.]download
- kavachmonitoringsoftware[.]com
- kavachtradersanddevelopers[.]in
- universalsurkshakavachyantra[.]in
- ncloudup[.]com
- owncloudup[.]ml
- wincloudup[.]tk
- oncloudup[.]com
- raincloudup[.]xyz
- incloudupdte[.]com
- madeincloudup[.]com
- suncloudupdates[.]com
- incloudupdtetld[.]com
- zeoncloudupload[.]com
- amazoncloudupdater[.]net
- digitaloceancloudupdator[.]online
- nic-updates[.]in

- hallwang-clinic-updates[.]com
- wzxdao[.]com

Sample Unredacted Registrant Email Addresses Found in the Artifacts' Current WHOIS Records

- seoc[REDACTED]@gmail[.]com
- for[REDACTED]@gmail[.]com
- agnisurakshaka[REDACTED]@gmail[.]com
- ALALAMALARAB[REDACTED]@GMAIL[.]COM
- benjami[REDACTED]@gmail[.]com
- technologi[REDACTED]@gmail[.]com
- [REDACTED]@anacopia[.]com
- NexotronicM[REDACTED]@gmail[.]com
- websoftit[REDACTED]@gmail[.]com
- lokeshr[REDACTED]@gmail[.]com
- obimo[.][REDACTED]@gmail[.]com
- [REDACTED]@yahoo[.]com
- migu[REDACTED]@hotmail[.]com
- book[REDACTED]@cape[.]com
- alg[REDACTED]@gmail[.]com
- f[REDACTED]@stolz[.]com[.]ua
- webm[REDACTED]@infiniteconnectionsinc[.]com
- DO[REDACTED]@SHIMATECH[.]COM[.]AU
- citigol[REDACTED]@gmail[.]com
- qpalz[REDACTED]@gmail[.]com

Note that we redacted some characters from the email addresses for privacy reasons.

Sample Domains That Shared the Artifacts' Registrant Email Addresses

- healthkavach[.]com
- giftarticle[.]com
- healthkavach[.]in
- agnisurakshakavacham[.]com
- alalamalarabyalyom[.]com
- ibiit[.]ly
- allcitibank[.]com
- peakcryptostack[.]com
- liteforexeu[.]com
- andrewdan[.]com
- bridgetrustfx[.]com
- bookstorerestaurant[.]com
- wellfleetoyster[.]com
- wellfleetoyster[.]net
- pkavach[.]com
- pathakcorporation[.]com
- pathakindia[.]com
- maxkirana[.]com
- benchmarkinfra[.]com
- aecprocure[.]com
- kavachcapital[.]com
- shrikart[.]com
- pathakinc[.]com
- kavachcapital[.]net
- psalunkemarathasoyrik[.]com
- shreeindustriesbutibori[.]com
- bharatcit[.]com
- shricart[.]com

- pathakcorp[.]com
- kavachpay[.]com
- shrikart[.]net
- kavachpay[.]net
- bharatcit[.]net
- maxkirana[.]net
- aecprocure[.]net
- hindkids[.]com
- hindjournal[.]com
- etestport[.]com
- bharathousing[.]net
- bharathousing[.]com
- hostrons[.]com
- archetivestudio[.]com
- pathakgroup[.]in
- citigoldltd[.]com
- vedicastroclinic[.]com
- divineindiatours[.]com
- cottageyesplease[.]com
- ashmincargo[.]com
- alacartetour[.]com
- aliveworldtours[.]com
- allindia-tours[.]com
- aliveindiatours[.]com
- sikhtourism[.]com
- indiaalacarte[.]com
- vedicastrologerindia[.]com
- jyotisharemedies[.]com
- vedickavach[.]com
- hotelmarblepalace[.]com
- yespleasehotels[.]com
- wrapparels[.]com
- vikassuri[.]com
- kitchenrama[.]com
- shantiyagya[.]com
- shigetatravels[.]com
- shigetatravel[.]com
- parvindersingh[.]com
- natrajyesplease[.]com
- melantea[.]com
- kitchnrama[.]com
- homeayur[.]com
- avishkarindia[.]net
- bhasintea[.]com
- avishkarindia[.]com
- skmishralegalassociates[.]com
- jagmeetkohli[.]com
- cafefesta[.]com
- kainalli[.]com
- malhotrarestaurant[.]com
- viaggideindia[.]com
- jkdoverseas[.]com
- kainallievents[.]com
- alacarteindia[.]com
- rajourigardenonline[.]com
- rajourionline[.]com
- kainallifresh[.]com
- mekados[.]com
- sikhpoloclub[.]com
- steelcoroofing[.]com
- kainallionline[.]com
- gangafujihomevaranasi[.]com
- taxiinindia[.]com
- indiaaircharters[.]com
- steelcogh[.]com
- kainallikids[.]com
- hnhairexports[.]com
- exoticexpeditions[.]net
- mithilamakhana[.]com
- skmishraandassociates[.]com
- manaliyesplease[.]com
- holidaygetawayz[.]com
- viajes-mundo[.]com
- exoticexpeditions[.]co[.]in
- rajourigardenonline[.]in
- mmeducationaltrust[.]org

- giantearthmovers[.]in
- grandpresident[.]in
- professional-catering[.]com
- hapiday[.]in
- tantravani[.]com
- cottagecrownplaza[.]com
- yespleasetravels[.]com
- incredibletoursofindia[.]com
- luxurytrain[.]net
- rajasthanculturetours[.]com
- cumminsindian[.]com
- ustechhelpinc[.]com
- sukhgroup[.]com
- manaliexpress[.]com
- manalixpress[.]com
- unitedindiaholidays[.]com
- kanishholidays[.]com
- harveeindia[.]com
- anandexports[.]net
- destinationhospitality[.]com
- tourbonanza[.]com
- travellerstrip[.]com
- myindiatoursntravels[.]com
- exotiqueworld[.]com
- exotiqueexpeditions[.]com
- bharatiyamtours[.]com
- sikhtourismindia[.]com
- tours2india[.]net
- shreeniwasjaipur[.]com
- indiatoursanddiscovery[.]com
- amritsar-tourism[.]com
- viacomtourstravels[.]com
- viacomtours[.]com
- exoticindiatour[.]com
- kuksamachar[.]com
- kukpunjabisamachar[.]com
- akalimpex[.]com
- chalindia[.]com
- indiantravelpackage[.]com
- guidesinindia[.]com
- webcom-etrade[.]com
- xpertstrade[.]com
- xcellencetechnologies[.]com
- tripindiatours[.]com
- indushenna[.]com
- newlifeorthopaedic[.]com
- xcellencevisa[.]com
- webcom-technologies[.]com
- ayurvedadelhi[.]com
- hygynlife[.]com
- indiahairstyleexports[.]com
- bhartiyamtours[.]com
- cottagegroupofhotels[.]com
- charmsofkenya[.]com
- charmsofsrilanka[.]com
- charmsofindia[.]com
- aaishindia[.]com
- visit-indya[.]com
- indiangoldentriangle[.]com
- machincrafts[.]com
- iiglta[.]com
- tegoverseas[.]com
- vdra[.]com
- sino-vediccancerclinic[.]com
- jayindia[.]com
- kukhindisamachar[.]com
- lamode[.]biz
- concokorea[.]com
- concokoreamall[.]com
- poolandbit[.]com
- concopleasure[.]com
- poolandbtc[.]com
- crevatrading[.]com
- geschenktur[.]com
- applemuhendislik[.]com
- bahcevanlar[.]com

- invistsc[.]com
- krnwebdev[.]com
- renovationuk[.]com
- sivenaz[.]com
- gtbd[.]org[.]tr
- lightschool[.]net
- akikmetal[.]com[.]tr
- turkishdayinlondon[.]com
- innovaart[.]com[.]tr
- mustafatemin[.]com
- invistfc[.]com
- kapsam[.]org[.]tr
- uesistem[.]com
- yekfeninsaat[.]com
- jssal[.]com
- salihcomert[.]com
- omktech[.]com
- yekfen[.]com
- yavuzgurdal[.]com
- recepyapici[.]com
- desustroy[.]com
- ozmendev[.]com
- pure-n[.]com
- webdevscope[.]com
- rumiingolstadt-ev[.]com
- sanalkonferans[.]net
- sanaltoplanti[.]net
- erkantaskin[.]net
- 1stimme1schritt[.]com
- 1stimme1schritt[.]net
- cinarlidogalgaz[.]com
- invistgc[.]com
- fix-bau-immobilien[.]com
- cinarlidogalgaz[.]com[.]tr
- globalsigortadanismanlik[.]com
- e-ohstrainingschool[.]com
- dogruaciyapidenetim[.]com[.]tr
- 1stimme1schritt[.]org
- mostsuccessfulturks[.]org
- ceptensigorta[.]com
- bulutsigorta[.]com
- kiyed[.]org
- gidatarimpolitikalari[.]net
- esaendustri[.]com
- carelinktrust[.]com
- gidatarimpolitikalari[.]com
- ufuktercume[.]com
- meetforedu[.]net
- containerboot[.]com
- yalcinlar-insaat[.]com
- foodoms[.]com
- taksiduraksistemi[.]com
- newbridgegc[.]com
- meetforedu[.]com
- lafontene[.]com
- freelancesms[.]com
- elbisenibul[.]com
- containerayakkabi[.]com
- containershoe[.]com
- alberaconsulting[.]com
- agromachuk[.]com
- mentorasgrup[.]com
- pptegitim[.]com
- efecizme[.]com
- balkanedu[.]com
- mavieng[.]com
- e-egitimyazilimi[.]com
- vodnoconsultancy[.]com
- aegrup[.]com
- debkon[.]org
- beyazoklava[.]com
- metsangrup[.]com
- sahincik[.]com
- hasanakbayrak[.]com
- dictumworld[.]com
- pasiad[.]net

- etrasu[.]com
- voicesinbritain[.]com
- voicesinbritain[.]org
- hizmetsources[.]org
- etrasu[.]net
- voicesinbritain[.]net
- etrakimya[.]com
- etramuhendislik[.]com
- etrasuaritma[.]com
- etrasucevre[.]com
- etrasulab[.]com
- etrasu[.]org
- kentsel-donusum-merkezi[.]com
- sanli-yapi[.]com
- hizmetresearch[.]org
- hizmetsources[.]com
- hizmetresearch[.]com
- bronzmakine[.]com
- hatmiserif[.]com
- mealiserif[.]com
- zuzu27[.]com
- vladislavardzinba[.]com
- cevsenikebir[.]com
- elkulubuddaria[.]com
- kulubuddaria[.]com
- turkishdayinlondon[.]org
- aytekgucuyener[.]com
- mentorasgroup[.]com
- is-guvenligi-merkezi[.]com
- farkliyansimalar[.]com
- hucumatisitte[.]com
- deryadankatreler[.]com
- ozlenengunler[.]com
- adanmisruhlar[.]com
- evraduezkar[.]com
- hizmetlibrary[.]info
- agrofarmerltd[.]com
- kocadanhocaolmaz[.]com
- dusuncehelezonu[.]com
- hutuvatisitte[.]com
- hizmeterleri[.]com
- birdemetdua[.]com
- ibretlikhatiralar[.]com
- institutefordialoguestudies[.]org
- hizmetresources[.]org
- kaligrafistanbul[.]com
- dialogue-society[.]com
- umraniyedeyuva[.]com
- umraniyedekres[.]com
- tazarru[.]com
- esenbahce[.]com
- hazalesenbahce[.]com
- hizmetresearch[.]info
- etrasu[.]info
- hizmetsources[.]info
- kadinlarkulturdernegi[.]org
- farkliseslerinahengi[.]com
- dengekariyer[.]net
- sanatixtanbul[.]com
- ozlemguzelyazici[.]com
- etileraksigorta[.]com
- aksigortaetiler[.]com
- olcmedegerlendirme[.]net
- manageyourworks[.]com
- uskudardaonaokulu[.]com
- mirascilaryurdu[.]com
- uygunsigorta[.]com
- etfal[.]net
- mujdekocamanakbayrak[.]com
- ucuzsigortacim[.]com
- ozkansengil[.]com
- tekelim[.]com
- 3ssystemsolutions[.]com
- botekdenizcilik[.]com
- latifkoru[.]com
- gecebekcisi[.]net

- genelmotor[.]net
- aricimetal[.]com
- nefismuhasebesi[.]com
- sevgiyolununyolculari[.]com
- zeitechnik[.]com
- zeitechnic[.]com
- monomobilya[.]com
- recogrup[.]com
- maviotomasyon[.]com
- 5acompany[.]com
- haseya[.]com
- ozsevindikelektrik[.]com
- bilkaotomasyon[.]com
- haremobilya[.]com
- enucuzsigortacim[.]com
- sontekklima[.]com
- curakshadistribution[.]com
- dagafoundation[.]com
- businessintelligenceindia[.]com
- buildyourowndevice[.]com
- archanadaga[.]com
- curakshasystems[.]com
- curakshaenterprises[.]net
- cybersuraksha[.]com
- csecure[.]net
- dagadigital[.]com
- threatfocus[.]net
- securityfusion[.]net
- dsecure[.]net
- securityengineering[.]net
- forensicfocus[.]net
- techtq[.]com
- shukra[.]net
- curakshatechnologies[.]net
- curakshatechnologies[.]com
- vediclore[.]com
- threatcontainment[.]net
- parishram[.]net
- vishwanath[.]net
- vulnerabilityanalysis[.]net
- wealthstack[.]net
- vedicvoice[.]net
- vedicessence[.]net
- vediclore[.]net
- vedicsoul[.]net
- vaidyanath[.]net
- threatresearch[.]net
- threatremediation[.]net
- trendsight[.]net
- swarmskill[.]com
- traderesearch[.]net
- twinsecurity[.]net
- techtq[.]net
- systemsinnovation[.]net
- swarmskill[.]net
- techforensics[.]net
- techresponse[.]net
- swarmsystems[.]net
- swaraksha[.]net
- surakshit[.]net
- suvidha[.]net
- strategydynamics[.]net
- strategybuzz[.]net
- shivashakti[.]net
- securetrend[.]net
- securitygadgets[.]net
- securevolution[.]net
- sentientswarm[.]net
- securitydynamics[.]net
- safemumbai[.]com
- safemumbai[.]net
- safelifestyle[.]net
- securemydevice[.]net
- securemumbai[.]net
- securemydevices[.]net
- securehumanity[.]net

- secureindia[.]net
- secureinvesting[.]net
- securecognition[.]net
- securityoperationscenter[.]net
- scientificstudy[.]net
- researchanalysis[.]net
- restorefaith[.]net
- reactivesecurity[.]net
- networktheory[.]net
- navgraha[.]net
- muhurta[.]net
- malwareresearch[.]net
- manvantara[.]net
- maheshwara[.]net
- fundsecure[.]net
- businessforums[.]net
- kavacha[.]net
- kedarnath[.]net
- knowledgecenter[.]net
- intelligencefocus[.]net
- indiaview[.]net
- indiaunleashed[.]net
- innovationinsight[.]net
- infosecguru[.]net
- infosecjobs[.]net
- infosecindia[.]net
- infosecmumbai[.]net
- curakshatech[.]net
- curakshaservices[.]net
- curakshatech[.]com
- curakshastore[.]net
- curakshastore[.]com
- curakshaservices[.]com
- fullrecovery[.]net
- curakshainterns[.]com
- fraudinvestigations[.]net
- fortunesecure[.]net
- extremeinnovation[.]net
- extremeintelligence[.]net
- exploitanalysis[.]net
- exploitlabs[.]net
- exploitdevelopment[.]net
- exploitchain[.]net
- esuraksha[.]net
- economicinsight[.]net
- deviceintegrator[.]net
- dhanush[.]net
- infosecmumbai[.]com
- indianunleashed[.]com
- dagafoundation[.]net
- dagadigital[.]net
- cybersuraksha[.]net
- curakshainterns[.]net
- complexitydynamics[.]net
- businessintelligenceindia[.]net
- bhrigu[.]net
- biginitiative[.]net
- fortunesecure[.]com
- exploitchain[.]com
- kindhands[.]net
- chummerz[.]com
- saturdaysoccerstars[.]com
- eventwhereis[.]com
- mavadd[.]at
- dospini[.]com
- somethingoriental[.]com
- playamatch[.]net
- layacar[.]com
- bloomboxsydney[.]com
- zenowith[.]com
- coolairwa[.]com
- qacity[.]net
- t10co[.]com
- pricechaser[.]net
- pricetracer[.]net
- shima[.]tech

- plusfitness[.]mobi
- pricecatch[.]me
- pricewatch[.]me
- endsforbeginnings[.]com
- feed[.]run
- bemyvalet[.]com
- youdirectinternational[.]com
- spotmypark[.]com
- emergencyss[.]net
- leighmilne[.]com
- threeheavenlysisters[.]com
- orders-now[.]com
- watechdiving[.]com
- jodiecallum[.]com
- orderstaken[.]com
- staticdocs[.]com

Sample Malicious Possibly Connected Domains

- a[.]networkbridge[.]cloud
- app[.]bonnuit[.]site
- assaass[.]website
- authenticprosperity[.]top
- bc05156e99738e1c0d5feb8529138 8ce[.]com
- bdsodecia[.]com
- bonnuit[.]site
- bptransactbank[.]com
- charteredcitybk[.]com
- coinbase[.]newsession0[.]com
- cpcalendars[.]visaprepaidprocessing [.]newsession0[.]com
- customcreationsstore[.]com
- felizpago[.]com
- found[.]newsession0[.]com
- getkavach[.]com
- mykavach[.]com
- kavachapp[.]com
- kavachguide[.]com
- kavach-apps[.]com
- kavachsupport[.]com