WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Gauging How Big a Threat Gigabud RAT Is through an IoC List Expansion Analysis

Table of Contents

Executive Report

Targeting governments the world over in cyber attacks is not a novel concept. Doing that using mobile apps, however, is quite new as a tactic. And that's what Cyble researchers reported as Gigabud RAT's modus operandi—trailing its sights on citizens of Thailand, the Philippines, and Peru who use government-owned institutions' mobile apps.

The Cyble analysis identified 10 indicators of compromise (IoCs) for this threat—six malware hashes and four URLs. We stripped down the URLs to three domains and one IP address in hopes of identifying more artifacts that could assuage potential targets' fears should the threat actors trail their sights on them. Our IoC list expansion exercise led to the discovery of:

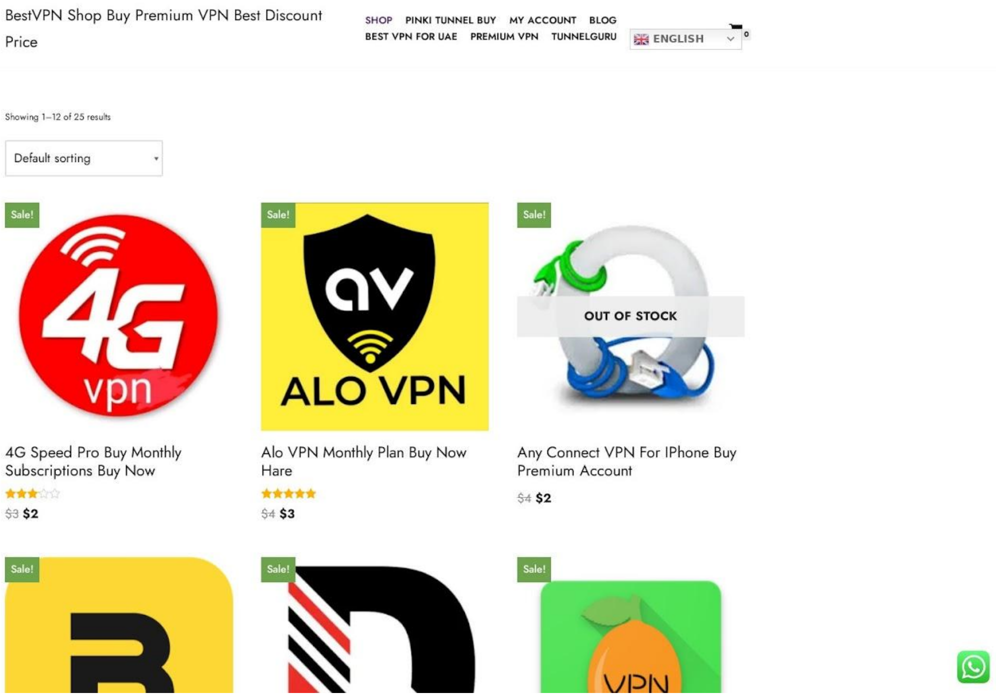
- Three IP addresses to which the domains resolved
- 301 IP-connected domains, seven of which turned out to be malicious
- 367 string-connected domains, eight of which have been dubbed malware hosts
- 519 brand-connected domains, 11 of which were tagged malicious

Uncovering Facts about Gigabud RAT Infrastructure

WHOIS lookups for the domains identified as IoCs revealed interesting similarities, including that they all pointed to the U.S. as their registrant country and were newly registered—between November and December 2022. Interestingly, though, while the IoC cmnb9[.]cc was registered in the U.S., its IP host 18[.]143[.]123[.]20 was geolocated in Singapore.

DNS lookups for the domains tagged as IoCs gave us three additional IP addresses—18[.]143[.]123[.]20, 104[.]21[.]41[.]159, and 172[.]67[.]148[.]55.

Using these IP addresses as reverse IP/DNS lookup search terms allowed us to uncover 301 more possibly connected domains, as they shared the IoCs' IP hosts. A bulk malware check for the artifacts showed that seven were malicious. Two of these dangerous properties should be avoided most since screenshot lookups revealed that they're live—bestvpnshop[.]com (looks to be a shop selling virtual private network [VPN] services) and brandmybooks[.]com (seems like an online betting site).



BestVPN Shop Buy Premium VPN Best Discount Price

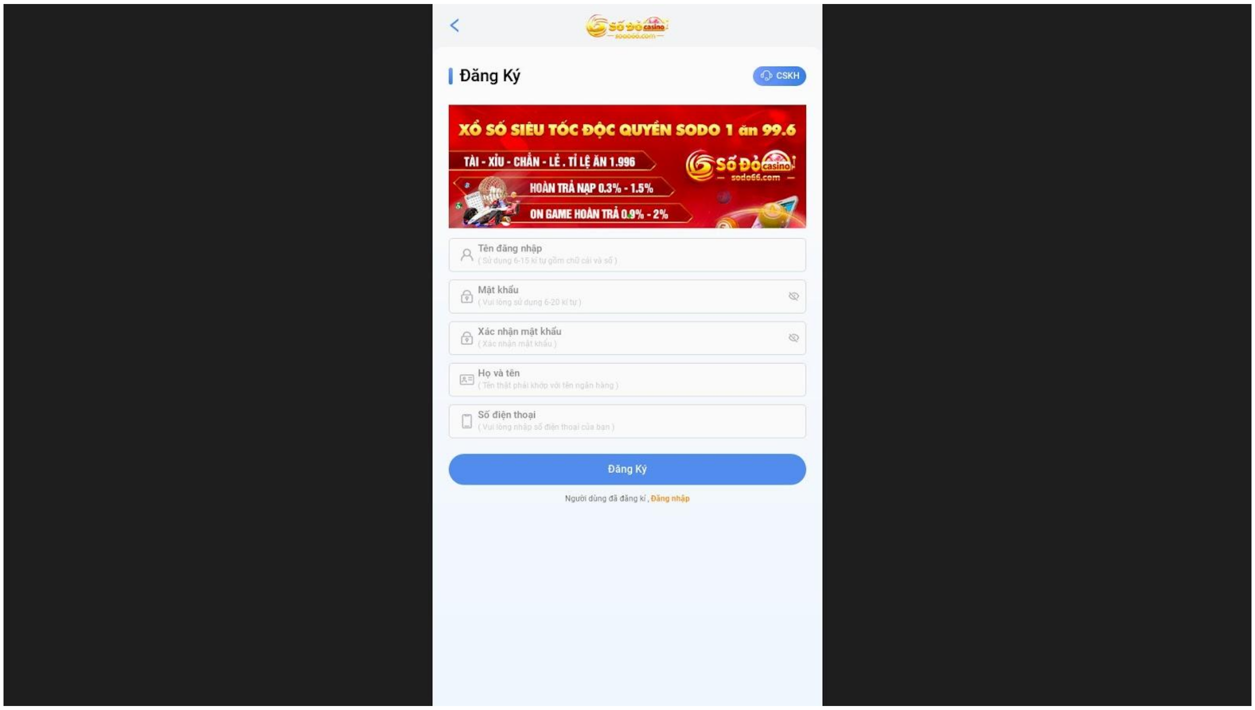
Showing 1–12 of 25 results

4G Speed Pro Buy Monthly Subscriptions Buy Now
~~$3~~ $2

Alo VPN Monthly Plan Buy Now Hare
~~$4~~ $3

Any Connect VPN For IPhone Buy Premium Account
~~$4~~ $2

Screenshot of bestvpnshop[.]com


Số Đỏ casino
sodo66.com
Đăng Ký
CSKH
XỔ SỐ SIÊU TỐC ĐỘC QUYỀN SODO 1 ăn 99.6
TÀI - XỈU - CHẴN - LẺ . TỈ LỆ ĂN 1.996
HOÀN TRẢ NẠP 0.3% - 1.5%
ON GAME HOÀN TRẢ 0.9% - 2%
Số Đỏ casino
sodo66.com
Tên đăng nhập
(Sử dụng 6-15 kí tự gồm chữ cái và số)
Mật khẩu
(Vui lòng sử dụng 6-20 kí tự)
Xác nhận mật khẩu
(Xác nhận mật khẩu)
Họ và tên
(Tên thật phải khớp với tên ngân hàng)
Số điện thoại
(Vui lòng nhập số điện thoại của bạn)
Đăng Ký
Người dùng đã đăng kí , Đăng nhập

Screenshot of brandmybooks[.]com

To further our search for more Gigabud RAT digital breadcrumbs, we used the unique strings found among the IoCs as Domains & Subdomains Discovery search terms (see the table below).

IoC	String Used as Search Term
● lionaiothai[.]com ● cmnb9[.]cc ● bweri6[.]cc	● ***lionaiothai.*** ● ***cmnb*.*** ● ***bweri*.***

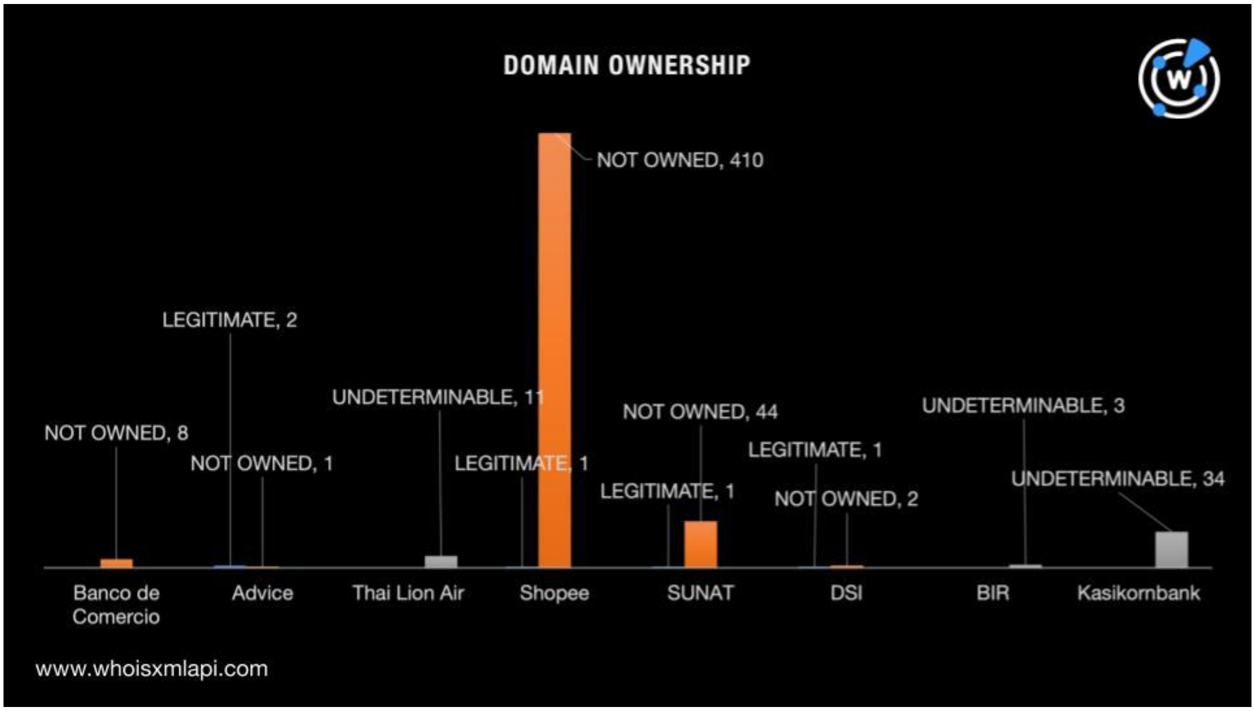
Our search led to the discovery of 367 domains, eight of which were confirmed to be malware hosts. Including these in blocklists is advisable.

The Gigabud RAT analysis also mentioned eight organization targets—Banco de Comercio, Advice, Thai Lion Air, Shopee, SUNAT, DSI, BIR, and Kasikornbank. Using their names as Domains & Subdomains Discovery search terms (see the table below for the exact strings used) enabled us to find 519 additional domains, 11 of which were dubbed malware hosts. Note that we limited our search to those that began with the single strings and string combinations that started with the first term and contained the second one.

Target Organization	String Used as Search Term

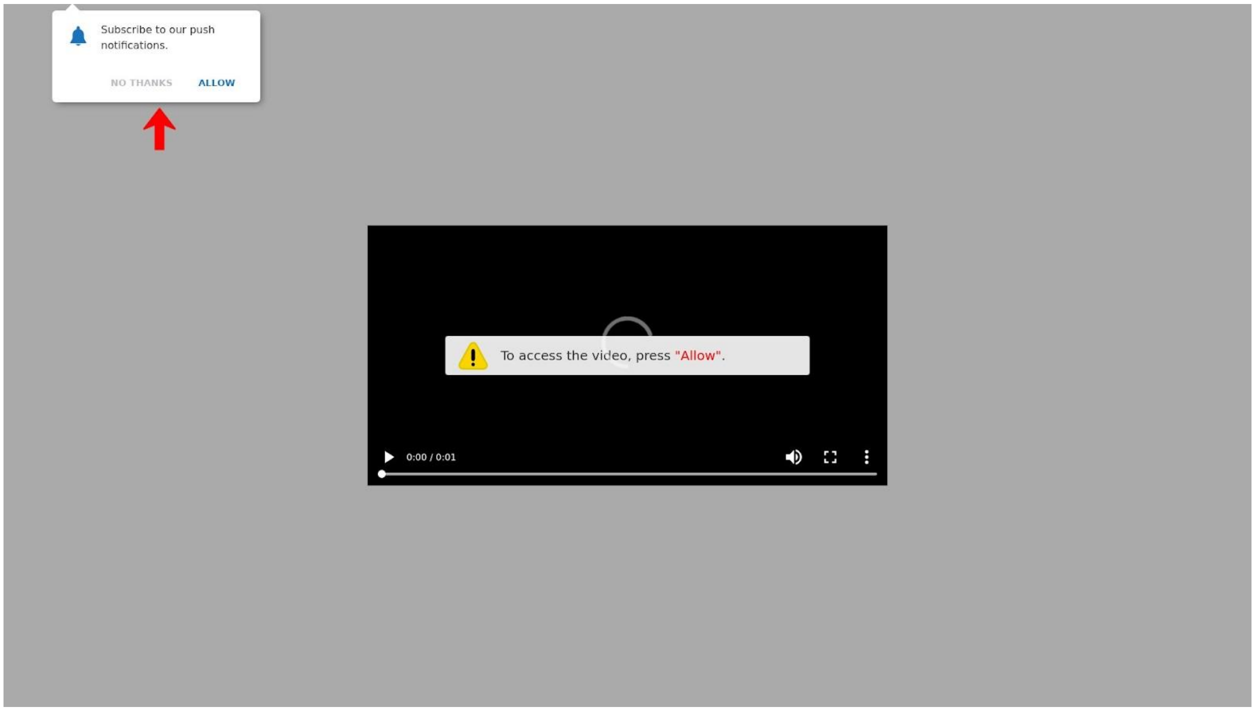
Banco de Comercio	***bancomercio.***
Advice	***advice.*** + ***th***
Thai Lion Air	***lionairthai.***
Shopee Thailand	***shopee.***
SUNAT	***sunat.***
DSI (Department of Special Investigation Thailand)	***dsi.*** + ***th***
BIR (Bureau of Internal Revenue Philippines)	***bir.*** + ***ph***
Kasikornbank	***kasikornbank.***

WHOIS record comparisons between the legitimate and potential typosquatting domains showed that only five of the 519 artifacts or less than 1% were owned by the organizations whose names appeared in them. Note, though, that we weren't able to confirm the legitimacy of the Thai Lion Air, BIR, and Kasikornbank domains because their WHOIS records were redacted.



Screenshot lookups for all the connected domains via IP host, string, and brand name showed that 217 continued to be accessible and host live content. Error, index, and blank pages, along with those whose domains are currently up for sale and under construction or repair, were excluded. Some looked to be game download, adult content, tutorial service provider, shopping, and business sites. Given their ties to the IoCs, they may at least be worth monitoring for signs of suspicious activity or compromise.

At least three websites may warrant inclusion in blocklists since they host a video that would only play if users download a codec—a tried-and-tested cybercriminal tactic to spread malware.

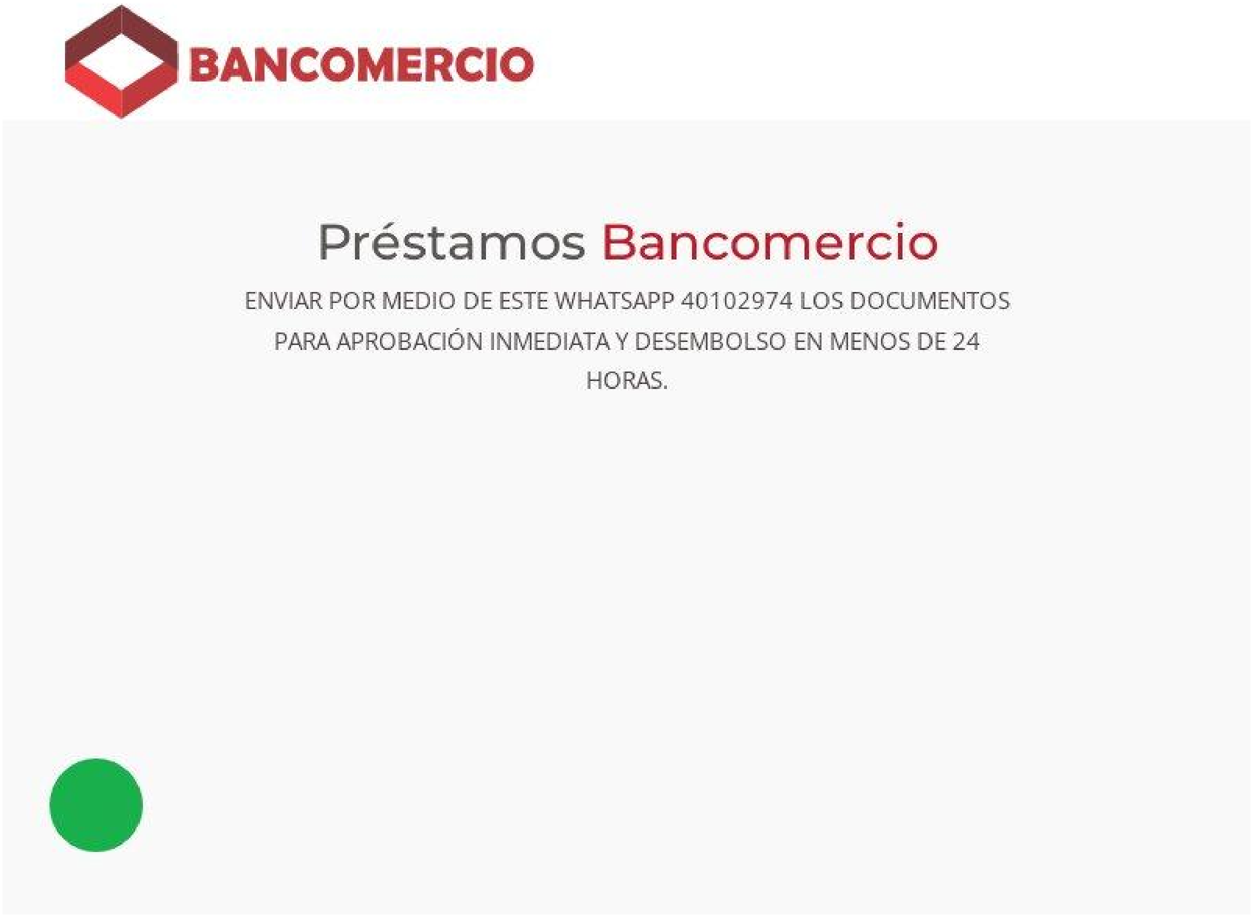


Subscribe to our push notifications.

To access the video, press "Allow".

Screenshot of aldbzuic[.]cf, aqyrobcs[.]gq, and bezrkure[.]ga

Sites that seem to be mimicking the target institutions, such as bancomercio[.]credit below should be blocked as well.



BANCOMERCIO

Préstamos Bancomercio

ENVIAR POR MEDIO DE ESTE WHATSAPP 40102974 LOS DOCUMENTOS PARA APROBACIÓN INMEDIATA Y DESEMBOLSO EN MENOS DE 24 HORAS.

Screenshot of bancomercio[.]credit

—

Our expansion of four Gigabud RAT IoCs—three domains and one IP address—uncovered 1,190 yet-unpublished artifacts that could be connected to the threat, including 26 that turned out to be confirmed malware hosts. Organizations and individuals alike, particularly the clients of the target institutions, should be wary of clicking the look-alike domains as well as the possibly connected web properties. All of them could be sources of Gigabud RAT that steals banking credentials and records their screen content.

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

IoCs Identified by Cyble

- lionaiothai[.]com
- cmnb9[.]cc
- bweri6[.]cc
- 8[.]219[.]85[.]91

Sample IP Address Resolutions of the Domains Identified as IoCs

- 18[.]143[.]123[.]20
- 104[.]21[.]41[.]159

Sample Domains That Shared the IoCs' IP Hosts

- 123mkv[.]top
- 1billclub88[.]com
- 1vx0lvodabe4bf[.]fun
- 2xsvb1a[.]shop
- 36sag6[.]com
- 3lancer[.]io
- 479fire[.]org
- 500dresses[.]org
- 5219q[.]com
- 5bbprofit[.]shop
- 6gmmdv[.]net
- 77663885[.]com
- 778charlie[.]com
- 91mw[.]net
- 9519265[.]com
- a-great-criminal-justice-yg[.]fyi
- a1freegames[.]com
- aackj6[.]cc
- aackj7[.]cc
- aarmi[.]org
- abatic[.]ca
- abokcakingau[.]tk
- acalrimrirar[.]ga
- acc311[.]com
- acgemidisanar[.]ml
- ackneecesrodce[.]tk
- acmc-corrosion[.]com
- actigarconog[.]tk
- adelabel[.]com
- admiredwattdistr[.]top
- adrilpart[.]cf
- adxhype[.]com
- africatime[.]com
- agenartersauflor[.]tk
- ahenectheacase[.]cf
- aidingtheenemy[.]com
- aips[.]gr
- ajogaron[.]dplus[.]org
- akbar-marble[.]com
- aknoo[.]com
- alapictos[.]ml
- albanygate[.]com
- aldbzuic[.]cf
- alentatgio[.]tk
- alkhabbazsa[.]com
- allefree[.]co
- alwide[.]ga
- amcomcatalscepma[.]ga
- americanfleetautoservice[.]com
- amisucisunnes[.]cf

Sample Malicious IP-Connected Domains

- 123mkv[.]top
- bagi2diamongratis[.]baruup2022[.]cf
- baruup2022[.]cf
- bestvpnshop[.]com

Sample Domains That Contained Strings Found among the IoCs

- lionaiothai[.]cc
- cmnbrazil[.]org
- cmnb[.]vip
- cmnba[.]com
- cmnbdrz[.]cn
- cmnby[.]loan
- cmnbe[.]com
- cmnbns[.]info
- cmnbmn[.]gq
- cmnb10pnq[.]nom[.]za
- cmnbui[.]ga
- cmnbp[.]com
- cmnb5stepprocess[.]net
- cmnbpro[.]com
- cmnb[.]xin
- cmnb07[.]cn
- cmnbt[.]link
- cmnbgg[.]com
- cmnbisystore[.]com
- cmnbr[.]com
- cmnbhrsf[.]cn
- cmnbvcbxvxcxbbmn[.]net
- cmnb[.]icu
- cmnbjt[.]wang
- cmnbilingualschool[.]com
- cmnbf[.]top
- cmnbs[.]loan
- cmnbainsight[.]com
- cmnbb[.]tk
- cmnbgh[.]top
- cmnbui[.]ml
- cmnb7ke[.]cyou
- cmnbdz[.]cn
- cmnb5stepprocess[.]biz
- cmnbewr[.]info
- cmnb92[.]ltd
- cmnbz6e92o[.]biz
- cmnbrands[.]network
- cmnbj[.]loan
- cmnbnvamaygmlfxsdisuozpvwot[.]biz
- cmnbgr[.]top
- cmnbgp[.]top
- cmnbahi[.]info
- cmnbid[.]com
- cmnbj[.]com
- cmnbg[.]loan
- cmnb5stepprocess[.]org
- cmnbfk[.]top
- cmnbrands[.]com[.]my
- cmnb[.]co[.]kr

Sample Malicious String-Connected Domains

- cmnbmo[.]cf
- cmnbmo[.]gq
- cmnbpp95[.]icu
- cmnbv[.]bid

Sample Domains That Contained the Brands of the Target Institutions

- bancomercio[.]es
- bancomercio[.]com[.]pe
- bancomercio[.]site
- bancomercio[.]info
- bancomercio[.]com
- bancomercio[.]pe
- bancomercio[.]com[.]br
- bancomercio[.]credit
- bancomercio[.]net
- advice[.]th
- advice[.]co[.]th
- advice[.]in[.]th
- lionairthai[.]in
- lionairthai[.]com[.]tw

- lionairthai[.]com
- lionairthai[.]co[.]uk
- lionairthai[.]net
- lionairthai[.]co[.]in
- lionairthai[.]com[.]vn
- lionairthai[.]cn
- lionairthai[.]co
- lionairthai[.]tw
- lionairthai[.]com[.]cn
- shopee[.]xn--6qq986b3xl
- shopee[.]com[.]bz
- shopee[.]wine
- shopee[.]ooo
- shopee[.]ac[.]cn
- shopee[.]family
- shopee[.]space
- shopee[.]co[.]za
- shopee[.]cheap
- shopee[.]tv
- shopee[.]house
- shopee[.]ind[.]in
- shopee[.]to
- shopee[.]world
- shopee[.]poker
- shopee[.]bio
- shopee[.]kz
- shopee[.]shopping
- shopee[.]ke
- shopee[.]mv
- shopee[.]gift
- shopee[.]tools
- shopee[.]org[.]pl
- shopee[.]mobi
- shopee[.]town
- shopee[.]nu
- xn--shop-jpa9v[.]ph
- shopee[.]golf
- shopee[.]me
- shopee[.]so
- shopee[.]party
- shopee[.]one
- shopee[.]delivery
- shopee[.]love
- shopee[.]nom[.]za
- shopee[.]app
- shopee[.]express
- shopee[.]gifts
- shopee[.]net[.]ph
- shopee[.]xn--3ds443g
- shopee[.]capital
- shopee[.]beauty
- shopee[.]ren
- shopee[.]com[.]pt
- shopee[.]wang
- shopee[.]ltd
- shopee[.]life
- xn--shope-7ra[.]com
- shopee[.]shop[.]pl
- shopee[.]kiwi
- xn--hop-uraa50b[.]ph
- shopee[.]cards
- shopee[.]gdn
- shopee[.]bz
- shopee[.]rip
- shopee[.]kim
- shopee[.]rs
- shopee[.]marketing
- shopee[.]discount
- shopee[.]re
- shopee[.]lol
- shopee[.]net
- shopee[.]ml
- shopee[.]chat
- shopee[.]monster
- shopee[.]city
- shopee[.]green
- shopee[.]supply
- shopee[.]info[.]vn
- shopee[.]immo
- shopee[.]mk

- shopee[.]luxury
- shopee[.]engineer
- shopee[.]eu
- shopee[.]audio
- shopee[.]jewelry
- shopee[.]events

Sample Malicious Brand-Connected Domains

- shopee[.]party
- shopee[.]gq
- shopee[.]ga
- shopee[.]ee
- xn--shpee-1ta[.]vn
- shopee[.]moda