GhostDNSbusters (Part 2)

team-cymru.com/blog/2020/10/07/ghostdnsbusters-part-2/

S2 Research Team View all posts by S2 Research Team October 7, 2020

This research was undertaken in collaboration with Manabu Niseki (@ninoseki on Twitter) and CERT.br (https://cert.br).

Manabu is a Tokyo-based researcher who has been tracking GhostDNS for a number of years. His leads and insight into GhostDNS assisted in confirming the findings documented in this blog post.

We will continue to collaborate with CERT.br on a shared goal of identifying the threat actors operating the infrastructure detailed in this blog.

This post picks up where we left off in our September 8, 2020 blog post titled "GhostDNSbusters". In that post, we identified:

- IP addresses being used by miscreants to compromise home routers
- IP addresses of rogue DNS servers
- Domain names affected by those DNS servers, directing users to phishing pages

This post will provide details on newly identified GhostDNS infrastructure, provide information about the phishing servers in use, and enumerate additional domain names targeted by miscreants.

Infrastructure Groups

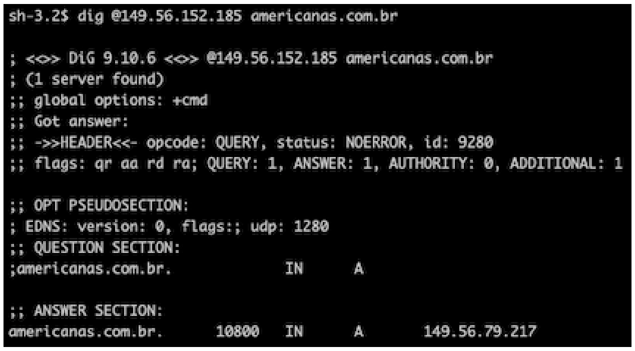
During the process of identifying active GhostDNS-related infrastructure, we observed several distinct "groups" of servers. Most involve a single DNS resolver and a single HTTP server used to host the phishing pages. However, one group uses six different DNS resolvers and two HTTP servers, and changes the HTTP servers on a weekly basis.

Internal Name	Timeframe Observed	DNS Server(s)	HTTP Server(s)	TTL	Wildcard DNS?
CDD	14-MAY – current	45.62.198.73 45.62.198.74 45.62.198.89 45.62.198.242 45.62.198.243 162.248.164.36	Two, which rotate each Monday. For the week of Oct 5: 45.62.198.165 45.62.198.166	60	YES
EDA	18-AUG – current	149.56.152.185	149.56.79.217	10800	NO
TOS	12-SEP – current	144.217.42.134	192.99.208.102	10800	NO
DDS	10-SEP – 23-SEP	107.155.152.20	107.155.152.26	10800	NO
ODA	08-AUG – current	107.155.152.13	70.37.165.155	10800	NO

Table 1: List of recently active GhostDNS infrastructure

The bottom four groups shown in Table 1 are configured in a similar way. Each has a single DNS server, which acts as authoritative for a distinct list of targeted domain names. When the domain name, or select hostnames within them are queried, the servers respond with the IP address of their associated phishing HTTP server. That response has a "time-to-live" of 10800 (measured in seconds, which is three hours).

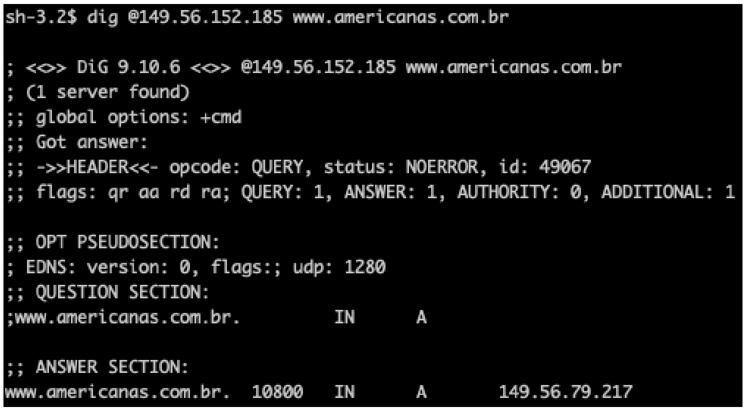
For example, here are some example queries and results from the "EDA" group, starting with one of the targeted domain names:



```
sh-3.2$ dig @149.56.152.185 americanas.com.br

; <<>> DiG 9.10.6 <<>> @149.56.152.185 americanas.com.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9280
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;americanas.com.br.             IN      A

;; ANSWER SECTION:
americanas.com.br.      10800   IN      A       149.56.79.217
```

Figure 1: Example query for a domain poisoned by the “EDA” DNS server

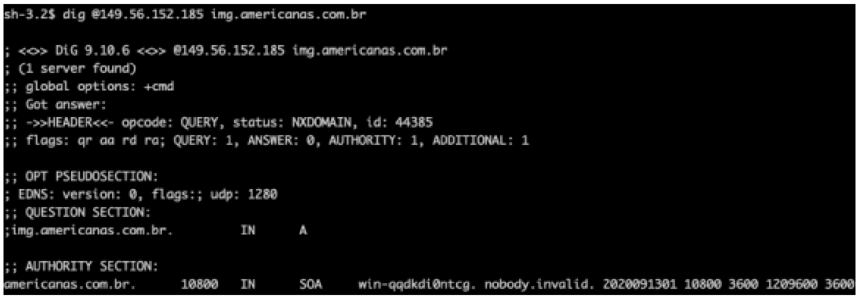
A query for the “www” hostname within that domain will also point to the phishing IP address:



```
sh-3.2$ dig @149.56.152.185 www.americanas.com.br

; <<>> DiG 9.10.6 <<>> @149.56.152.185 www.americanas.com.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49067
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.americanas.com.br.         IN      A

;; ANSWER SECTION:
www.americanas.com.br.  10800   IN      A       149.56.79.217
```

Figure 2: Example hostname query for a domain poisoned by the “EDA” DNS server

However, DNS wildcards are not used by this group, as seen here:

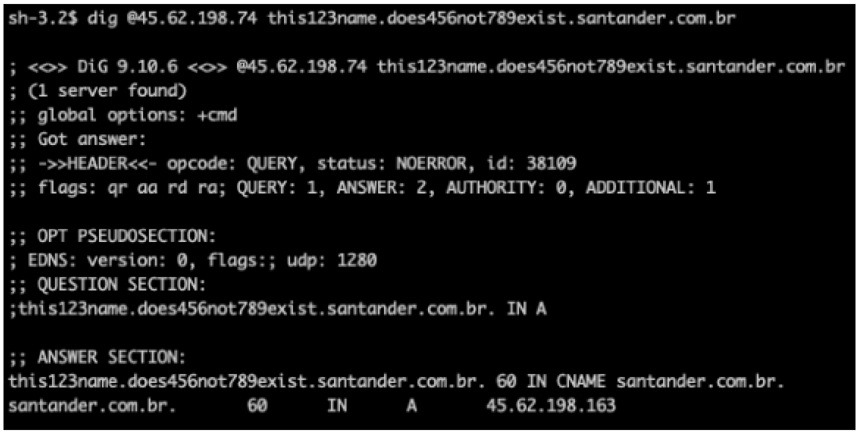


```
sh-3.2$ dig @149.56.152.185 img.americanas.com.br

; <<>> DiG 9.10.6 <<>> @149.56.152.185 img.americanas.com.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 44385
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;img.americanas.com.br.         IN      A

;; AUTHORITY SECTION:
americanas.com.br.      10800   IN      SOA     win-qqdkdi0ntcg. nobody.invalid. 2020091301 10800 3600 1209600 3600
```

Figure 3: Example NXDOMAIN query for a domain poisoned by the “EDA” DNS server

In the figure above (Figure 3), we see that the “img.americanas.com.br” query isn’t directed to the phishing server. Instead, a NXDOMAIN response is returned, which indicates that the hostname does not exist. (In reality, that hostname does exist, but since this DNS server is (maliciously) configured to be authoritative for the americanas.com.br. zone (domain), but doesn’t contain a record for the “img” hostname, and isn’t configured to perform DNS wildcarding, it returns an NXDOMAIN response.)

In contrast to the behavior observed by the other infrastructure groups, the CDD group takes a different approach. For all DNS zones that the DNS server is configured to answer authoritatively for, any hostname query will return a response with the IP address of a phishing HTTP server. Here’s an example:



```
sh-3.2$ dig @45.62.198.74 this123name.does456not789exist.santander.com.br

; <<>> DiG 9.10.6 <<>> @45.62.198.74 this123name.does456not789exist.santander.com.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38109
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;this123name.does456not789exist.santander.com.br. IN A

;; ANSWER SECTION:
this123name.does456not789exist.santander.com.br. 60 IN CNAME santander.com.br.
santander.com.br.       60      IN      A       45.62.198.163
```

Figure 4: Example wildcard response for a domain poisoned by a "CDD" DNS server

Also unique to the CDD group (compared to the four others mentioned in this blog post) are the weekly rotation of phishing servers, and the availability of SSL/TLS on them. CDD's phishing servers have a self-signed x.509 certificate that is reused when they rotate in new phishing servers. The x.509 certificate in use recently changed, presumably because it was due to expire soon.

Certificate observed prior to 2020-09-24:

```
subject= /C=BR/ST=SAO PAULO/L=OSASCO/O=Google. Inc./OU=Principal/CN=SAY MY NAME/emailAddress=localserver@google.com

issuer= /C=BR/ST=SAO PAULO/L=OSASCO/O=Google. Inc./OU=Principal/CN=SAY MY NAME/emailAddress=localserver@google.com

serial=D7AF0B2CBAD8370B

localserver@google.com

notBefore=Oct  8 23:28:42 2019 GMT

notAfter=Oct  7 23:28:42 2020 GMT

MD5: FCB3ECAA96C6A9026CD933281A30551F

SHA1: 4E04C2D45F37D7D4E757C27A0A0735B503F319E4
```

Certificate observed after 2020-09-24:

```
subject= /C=BR/ST=CATARINA/L=SUL/O=SULAMERICA/OU=SULAMERICA APPS/CN=MANITO MIGUELITO/emailAddress=manito@miguelito.com

issuer= /C=BR/ST=CATARINA/L=SUL/O=SULAMERICA/OU=SULAMERICA APPS/CN=MANITO MIGUELITO/emailAddress=manito@miguelito.com

serial=B7BDA9E48E5D2B43

manito@miguelito.com

notBefore=Sep 24 19:44:55 2020 GMT

notAfter=Sep 24 19:44:55 2021 GMT

MD5: EE8CF31BE39C5BC046BF5EB25FDACC80

SHA1: 8D9B394BA67D1913566115094C1AD0257FEFF26E
```

This reuse of x.509 certificates allows us to identify new and historical phishing servers used by this group, as we can use Augury to show us where/when this x.509 certificate has been observed.

Targeted Domains

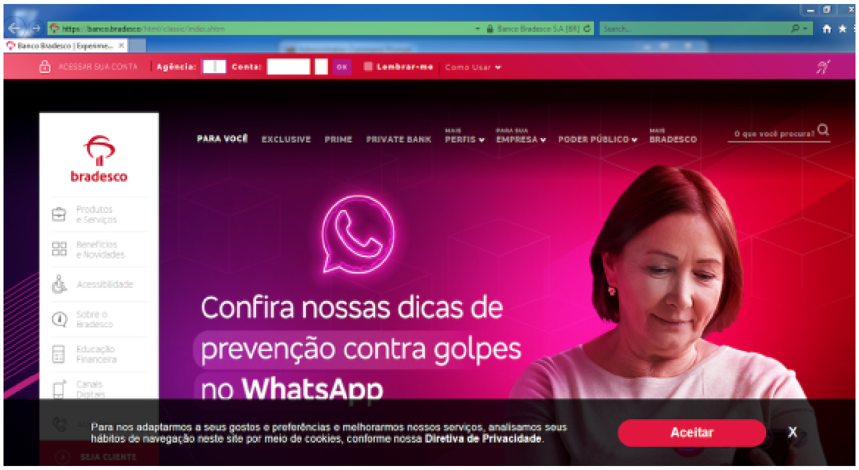
Similar to the earlier blog post in this series, Passive DNS (PDNS) and DNS Query datasets from Augury were utilized in order to provide further context around the nature of the requests being targeted by the attackers – for which their rogue DNS servers provide redirects to phishing pages. Each group has a unique list of domains that are hijacked. The following is a list of targeted domain names in use by recently-active GhostDNS servers, broken down by the "Internal Name" indicated earlier in this article:

CDD	EDA	TOS	DDS	ODA
banco.bradesco bancobrasil.com.br	americanas.com.br banco.bradesco	americanas.com.br banco.bradesco	americanas.com.br banco.bradesco	banco.bradesco bradescocelular.com.br
bb.com.br	bb.com.br	bancobrasil.com.br	bb.com.br	bradesco.b.br
bradesco.com.br	bradescocelular.com.br	bb.com.br	bradescocelular.com.br	bradesco.com.br
bradesconetempresa.b.br	bradesco.b.br	bradescocelular.com.br	bradesco.b.br	bradescopj.com.br
caixa.gov.br	bradesco.com.br	bradesco.b.br	bradesco.com.br	bradescoprime.com.br
itau.b.br	bradescopj.com.br	bradesco.com.br	bradescopj.com.br	caixa.gov.br
itau.com.br	bradescoprime.com.br	bradescopj.com.br	bradescoprime.com.br	cef.com.br
itaupersonnalite.com.br	caixa.gov.br	bradescoprime.com.br	caixa.gov.br	
santander.com.br	cef.com.br	caixa.gov.br	cef.com.br	
santandernet.com.br	citibank.com	cef.com.br	citibank.com	
santandernetibe.com.br	citibank.com.br	citibank.com	citibank.com.br	
sicredi.com.br	hotmail.com	citibank.com.br	itau.com.br	
	hotmail.com.br	itau.com.br	itaupersonnalite.com.br	
	itau.com.br	itaupersonnalite.com.br	santander.com.br	
	itaupersonnalite.com.br	netflix.com	santandernet.com.br	
	live.com	paypal.com	santandernetibe.com.br	
	lojasamericanas.com.br	santander.com.br	shoptime.com.br	
	msn.com	santandernet.com.br		
	msn.com.br	santandernetibe.com.br		
	netflix.com	shoptime.com.br		
	outlook.com	submarino.com.br		
	paypal.com			
	santander.com.br			
	santandernet.com.br			
	santandernetibe.com.br			
	shoptime.com.br			
	terra.com.br			

Table 2: List of domains targeted by each active GhostDNS infrastructure

Examples of Real Site vs. Phishing Sites

Here, we show a snapshot of the real Web site for banco.bradesco, as it appears in Internet Explorer 11:



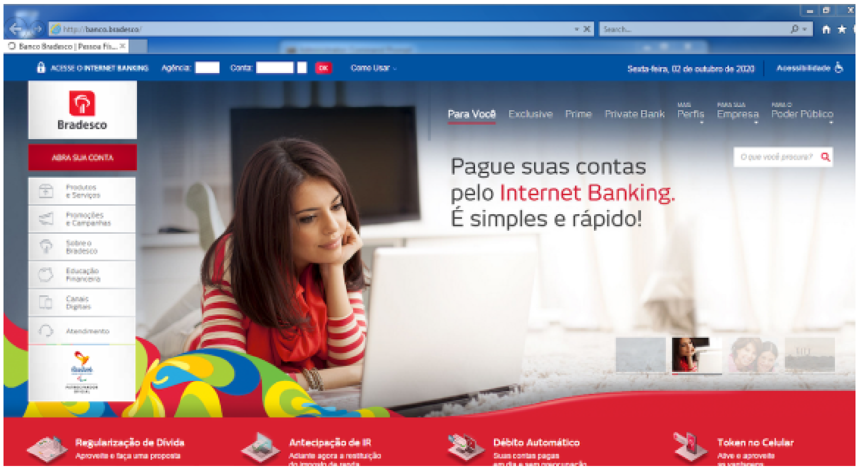
Confira nossas dicas de prevenção contra golpes no WhatsApp

Para nos adaptarmos a seus gostos e preferências e melhorarmos nossos serviços, analisamos seus hábitos de navegação neste site por meio de cookies, conforme nossa **Diretiva de Privacidade**.

Figure 5: Snapshot of the resulting page when typing "banco.bradesco" into IE11 and pressing Enter

We did not specify HTTPS when accessing the page – we simply typed banco.bradesco into the address bar and pressed Enter. As seen in the above screenshot (Figure 7), the address bar shows that we were taken to an SSL-encrypted URL. Also, because the address bar is highlighted in green, we know that the SSL (x.509) certificate presented for this session is a valid, EV certificate, issued by a trusted certificate authority.

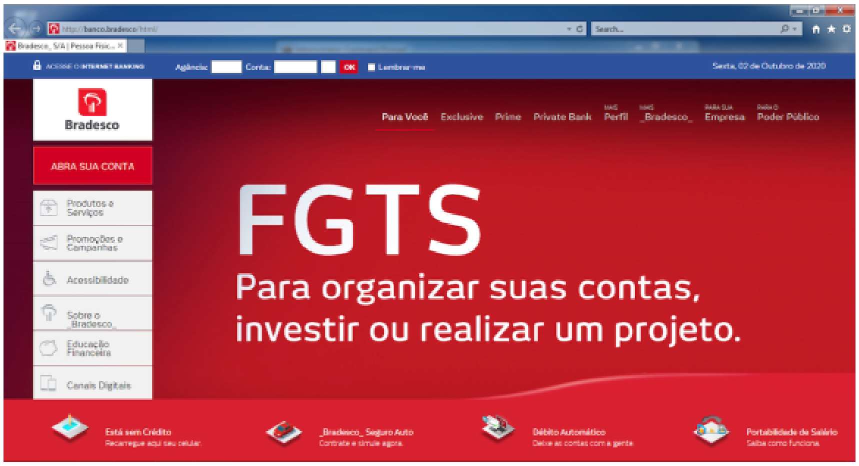
When the same action (typing banco.bradesco into the address bar and pressing Enter) is taken, but using the phishing server in use by the "EDA" group, the result is a non-encrypted page, using an outdated background, copied from the banco.bradesco site:



Pague suas contas pelo Internet Banking. É simples e rápido!

Figure 6: Snapshot of the banco.bradesco page, as served by the "EDA" group phishing server

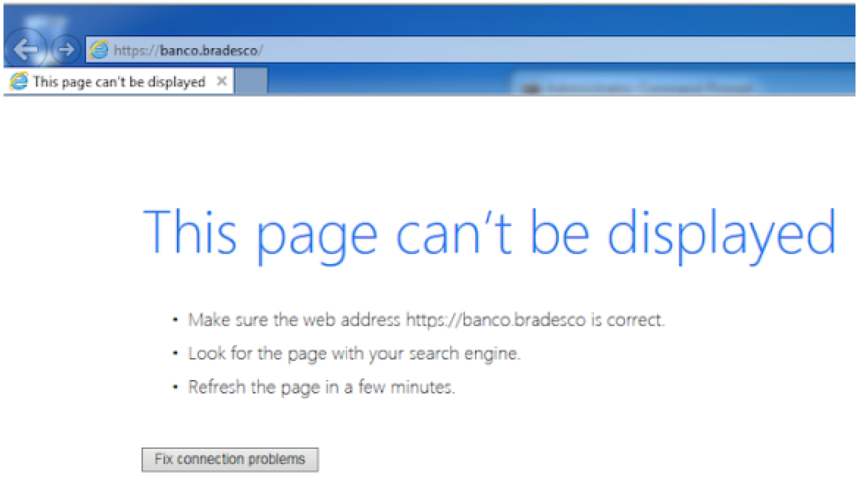
As seen in Figure 8, the page served by the "EDA" phishing server does not show an SSL-enabled connection in the address bar. A similar experience is observed when performing the same action, but using the "CDD" group phishing server:



FGTS
Para organizar suas contas, investir ou realizar um projeto.

Figure 7: Snapshot of the "banco.bradesco" page, as served by the "CDD" group phishing server

When using a URL that specifies SSL (HTTPS), the "EDA" phishing server doesn't respond, as the server is not listening on the port used by HTTPS (443/tcp).

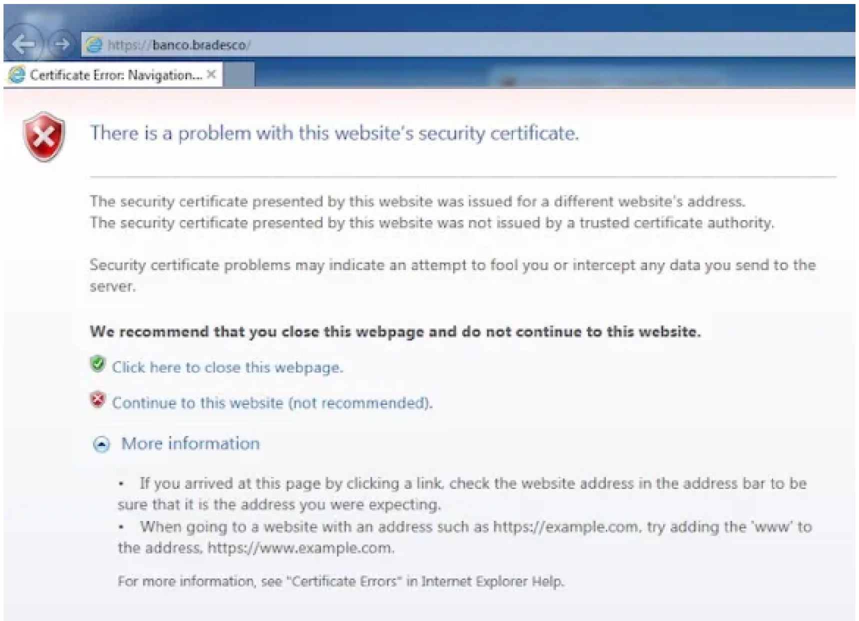


This page can't be displayed

- Make sure the web address https://banco.bradesco is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Figure 8: Snapshot of attempting to access https://banco.bradesco/, via the "EDA" group phishing server

Attempting to access the same (HTTPS) URL when using the "CDD" phishing server will cause an SSL certificate mismatch error to be displayed in the browser, as seen here:



There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.
The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.

For more information, see "Certificate Errors" in Internet Explorer Help.

Figure 9: Snapshot of attempting to access https://banco.bradesco/, via the "CDD" group phishing server

Indicators of Compromise

NOTE: This list contains GhostDNS-related DNS server and HTTP server IP addresses, as identified as active at some point between our previous GhostDNS blog post (September 8, 2020) and this one. Earlier indicators of compromise are available at the end of that blog post.

Rogue DNS servers [10]

45.62.198.73

45.62.198.74

45.62.198.89

45.62.198.242

45.62.198.243

107.155.152.13

107.155.152.20

144.217.42.134

149.56.152.185

162.248.164.36

HTTP Phishing servers [13]

45.62.198.154

45.62.198.155

45.62.198.156

45.62.198.157

45.62.198.160

45.62.198.161

45.62.198.162

45.62.198.163

45.62.198.165

45.62.198.166

70.37.165.155

107.155.152.26

149.56.79.215

149.56.79.217

192.99.208.102