DNS Abuse in Phishing Cases Handled by CERT.br

Cristine Hoepers
cristine@cert.br

Computer Emergency Response Team Brasil
Brazilian Network Information Center
Brazilian Internet Steering Committee

General Statistics of Reported Phishing Cases

Jan–Nov/2010

Total cases	7065
Unique Targets	204
Targetting Brazilian Brands	5121
Targetting Other Brands	1944
Unique URLs	6952
Unique Hashes	3232
Country Codes IPs' were allocated to	68
ASes	711
Unique IPs	3204
Domains	4310
ccTLDs	92
gTLDs	10
Links to IPs only	527

Statistics – IP allocation

#	Country Code	Cases	(%)
1	BR	2537	35.91
2	US	2406	34.06
3	DE	284	4.02
4	FR	238	3.37
5	NL	164	2.32
6	RU	155	2.19
7	GB	118	1.67
8	IT	118	1.67
9	CN	113	1.60
10	CA	104	1.47

- Most content hosted in Brazil was regarding international Brands
- Most content affecting Brazilian brands were hosted at US IPs

#	ASN	Cases	(%)
1	28299 (Cyberweb)	504	7.08
2	15201 (UOL)	494	6.94
3	27715 (LocaWeb)	335	4.70
4	21844 (ThePlanet)	282	3.96
5	2914 (NTT America)	241	3.38
6	7738 (Oi)	185	2.60
7	16276 (OVH)	175	2.46
8	26496 (GoDaddy)	174	2.44
9	46475 (Limestone)	163	2.29
10	18479 (Plug-In)	162	2.27

- Top ASNs were Hosting Services

Statistics – gTLDs

#	gTLD	Cases	(%)
1	.com	1883	72.62
2	.net	374	14.42
3	.org	235	9.06
4	.info	53	2.04
5	.biz	25	0.96
6	.asia	9	0.35
7	.mobi	6	0.23
8	.cat	3	0.12
9	.edu	3	0.12
10	.name	2	0.08

Domains specially created, with mention to brands or advertisement campaigns of these brands

- **.com – 80**
- **.net – 25**
- **.org – 4**
- **.info – 5**
- **.biz – 2**

None of them involving a hosting service domain or short URL service.

Statistics – ccTLDs

#	ccTLD	Cases	(%)
1	.br	2090	56.55
2	.de	151	4.09
3	.ru	142	3.84
4	.fr	80	2.16
5	.pl	80	2.16
6	.cn	79	2.14
7	.nl	79	2.14
8	.au	77	2.08
9	.tk	77	2.08
10	.ly	76	2.06
11	.it	74	2.00
12	.to	62	1.68
13	.cc	32	0.87

Short URL	Cases	(%)
bit.ly	76	1.08
path.to	62	0.88
migre.me	28	0.40
tiny.cc	12	0.17

Domains specially created, with mention to brands or advertisement campaigns of these brands:

- .br – 53, various
- .tk – 49, all in the form of famous-brand.tk
- .it – 27, all subdomains of free hosting service domains
- .ru – 18, all subdomains of free hosting service domains
- .fr – 9, all subdomains of free hosting service domains

Short URLs were abused to create URLs of the type:

- bank.com.br.bit.ly/ldkaflkja

Other Issues

- Cache poisoning – no official reports, not easy to detect if you are not at the affected network
- Other attacks:
  - Recursive DNS Servers' compromises
    - authoritative responses
    - the attackers control at what times the malicious zones are up
  - Malware changing the client "hosts" file
    - have hundreds of entries, including AV's, Vendors' update sites, and the brands being targetted
    - majority of attacks that subvert DNS use this technique

Links

- CERT.br
  http://www.cert.br/
- NIC.br
  http://www.nic.br/
- CGI.br
  http://www.cgi.br/