ERT Threat Alert
DNS Hijacking Targets Brazilian Banks
August 10, 2018

Abstract

The Radware Threat Research Center has identified a hijacking campaign aimed at Brazilian bank customers via their IoT devices and is attempting to gain their bank credentials.

The research center has been tracking malicious activity targeting DLink DSL modem routers in Brazil since June 8th. Via old exploits dating from 2015, a malicious agent is attempting to modify the DNS server settings in the routers of Brazilian residents, redirecting all their DNS requests through a malicious DNS server. The malicious DNS server is hijacking requests for the hostname of Banco de Brasil (www.bb.com.br) and redirecting to a fake, cloned website hosted on the same malicious DNS server which has no connection whatsoever to the legitimate Banco de Brasil website.

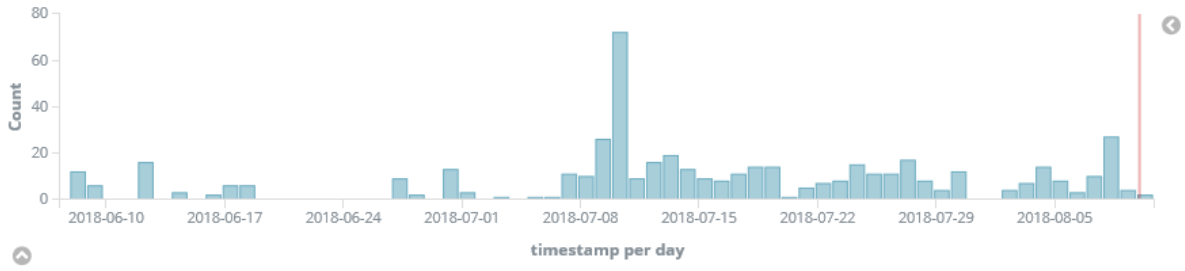
Itau Unibanco, another Brazilian financial institution (hostname www.itau.com.br), is also being redirected, although not backed by a cloned website (for now). For all other DNS requests, the malicious server works as a forwarder and resolves just as an ISP DNS server would. The malicious DNS server set up by the hackers effectively becomes a middleman that provides the malicious actor with the flexibility to bring up fake portals and web fronts to collect sensitive information from users whose routers were infected.

Unique about this approach is that the hijacking is performed without any interaction from the user. Phishing campaigns with crafted URLs and malvertising campaigns attempting to change the DNS configuration from within the user's browser have been reported as early as 2014 and throughout 2015 and 2016. In 2016, an exploit tool known as RouterHunterBr 2.0 was published on the internet and used the same malicious URLs, but there are no reports that Radware is aware of currently of abuse originating from this tool.

The attack is insidious in the sense that a user is completely unaware of the change. The hijacking works without crafting or changing URLs in the user's browser. A user can use any browser and his/her regular shortcuts, the user can type in the URL manually or even use it from mobile devices, such as a smart phone or tablet. The user will still be sent to the malicious website instead of to their requested website and the hijacking effectively works at the gateway level.

Attack Methods

Since June 12, Radware's deception network has been recording multiple infection attempts for an old D-Link DSL router exploit.



The exploit allows unauthenticated remote configuration of DNS server settings on the modem router. The malicious URL takes the following form.

```
/dnscfg.cgi?dnsPrimary=<malicious_DNS_IP>&dnsSecondary=<malicious_DNS_IP >&dnsDynamic=0&dnsRefresh=1
```

Exploits were published as early as February, 2015 for multiple DSL routers, mostly D-Link.

- Shuttle Tech ADSL Modem-Router 915 WM / Unauthenticated Remote DNS Change. Exploit http://www.exploit-db.com/exploits/35995/
- D-Link DSL-2740R / Unauthenticated Remote DNS Change Exploit http://www.exploit-db.com/exploits/35917/
- D-Link DSL-2640B Unauthenticated Remote DNS Change Exploit https://www.exploit-db.com/exploits/37237/
- D-Link DSL-2780B DLink_1.01.14 – Unauthenticated Remote DNS Change https://www.exploit-db.com/exploits/37237/
- D-Link DSL-2730B AU_2.01 – Authentication Bypass DNS Change https://www.exploit-db.com/exploits/37240/
- D-Link DSL-526B ADSL2+ AU_2.01 – Unauthenticated Remote DNS Change https://www.exploit-db.com/exploits/37241/

Radware's deception network recorded almost 500 attempts between June 8 and August 10. Radware's Sao-Paulo based honeypots captured these attempts, without exception. The rest of our global deception network did not capture any of these attempts, meaning the malicious agent was focusing attacks at Brazilian targets only. This was likely intended to increase efficiency while staying undetected.

Exploit attempts were performed from a handful of servers. Most of the servers were located in the United States, but the only active server is located in Brazil. Below are the five IPs accounting for the 500 attempts.

```
IP                  CC    Country         ASNum      Name
23.99.225.247       US    United States   AS8075     Microsoft Corporation
13.66.164.227       US    United States   AS8075     Microsoft Corporation
40.122.39.130       US    United States   AS8075     Microsoft Corporation
104.215.81.130      US    United States   AS8075     Microsoft Corporation
13.66.249.87        US    United States   AS8075     Microsoft Corporation
200.196.240.136     BR    Brazil          AS11419    Telefonica Data S.A.
```

Originally the malicious DNS server IP used in the exploit was 69.162.89.185. The IP changed to 198.50.222.136 on August 2, 2018. Resolving the hostname for Banco de Brazil (www.bb.com.br) through the malicious DNS server.

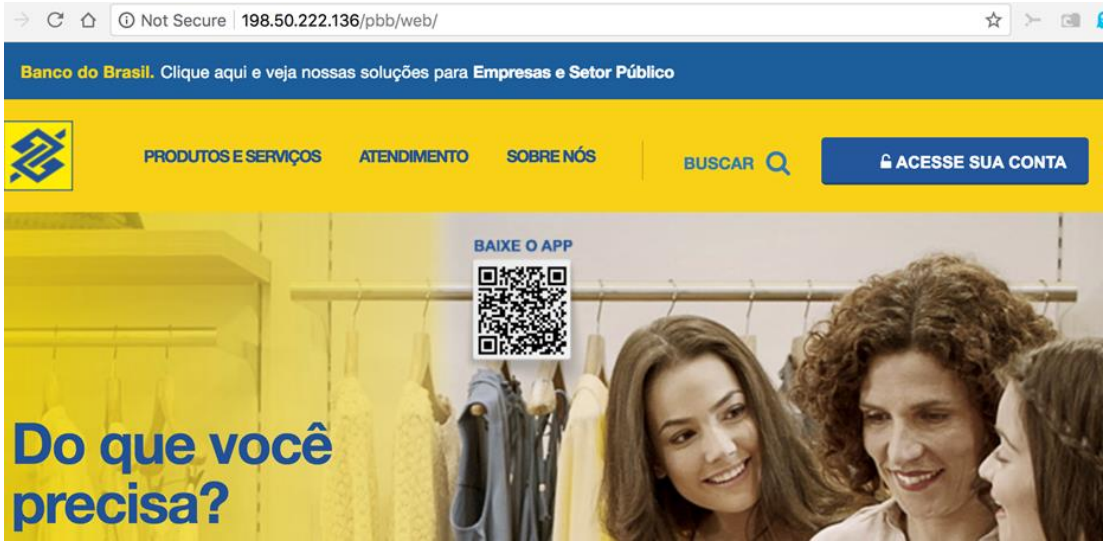
```
$ dig www.bb.com.br @198.50.222.136
; <<>> DiG 9.10.3 <<>> www.bb.com.br @198.50.222.136
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49313
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.bb.com.br.                 IN      A

;; ANSWER SECTION:
www.bb.com.br.          10800   IN      A       198.50.222.136

;; AUTHORITY SECTION:
www.bb.com.br.          10800   IN      NS      win-eknrp3tthaf.

;; Query time: 94 msec
;; SERVER: 198.50.222.136#53(198.50.222.136)
;; WHEN: Fri Aug 10 02:20:53 CEST 2018
```

```
;; MSG SIZE  rcvd: 87
```

Equally so for Itau Unibanco.

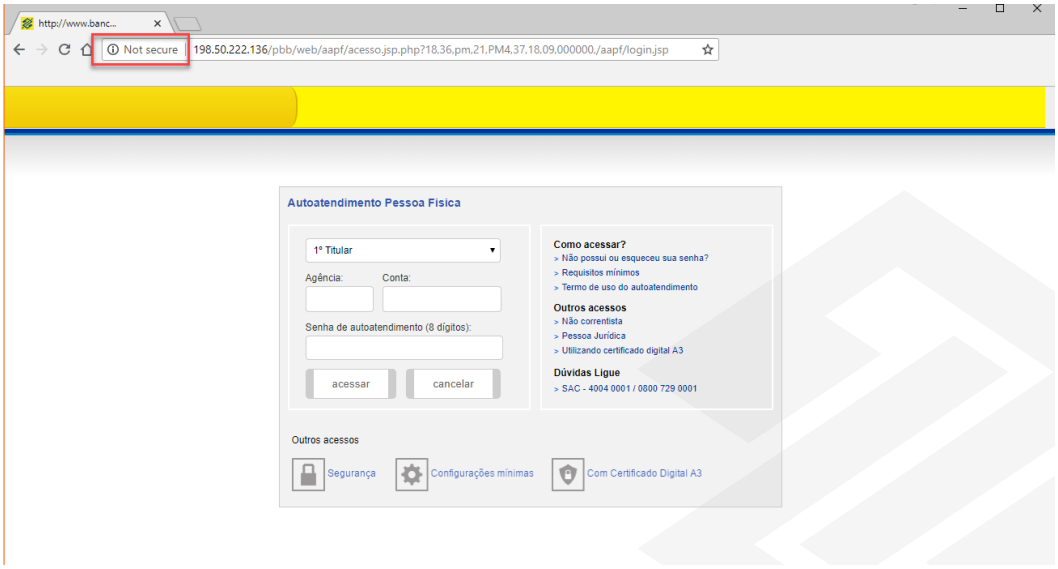
```
$ dig www.itau.com.br @198.50.222.136
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.itau.com.br @198.50.222.136
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49427
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.itau.com.br.            IN      A

;; ANSWER SECTION:
www.itau.com.br.      10800   IN      A       198.50.222.136

;; AUTHORITY SECTION:
www.itau.com.br.      10800   IN      NS      win-eknrp3tthaf.

;; Query time: 93 msec
;; SERVER: 198.50.222.136#53(198.50.222.136)
;; WHEN: Fri Aug 10 02:22:28 CEST 2018
;; MSG SIZE  rcvd: 89
```

The fake cloned website for Banco de Brasil is located at https://198.50.222.136/pbb/web and uses a self-signed certificate with a validity starting date of August 1, 2018, matching the change of malicious DNS server IP in the exploit attempts. Radware underscores that the fake cloned website for Banco de Brasil is hosted on a malicious server that has no connection whatsoever to the legitimate Banco de Brasil website.

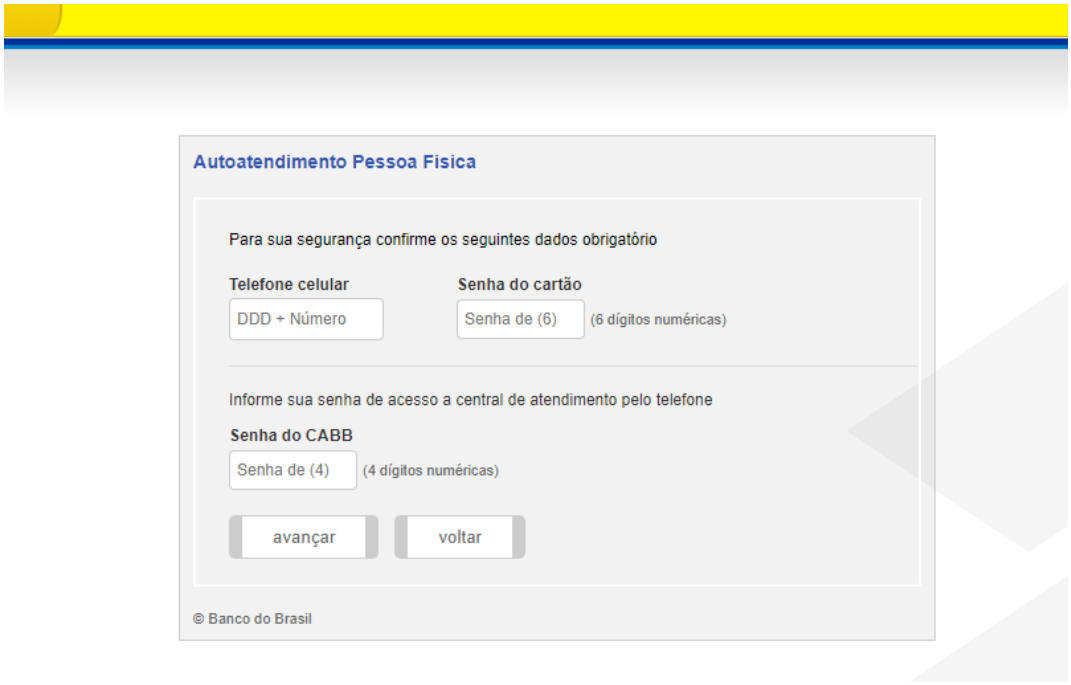



```
$ curl -vk https://198.50.222.136/pbb/web/
* Server certificate:
*  subject: CN=WIN-EKNRP3TTHAF
*  start date: Aug  1 19:36:40 2018 GMT
Content-Type: text/html
Last-Modified: Fri, 04 May 2018 00:36:26 GMT
```

When trying to access the account through the fake cloned website, the user is presented with a form asking for the bank agency number, account number and an eight-digit pin.

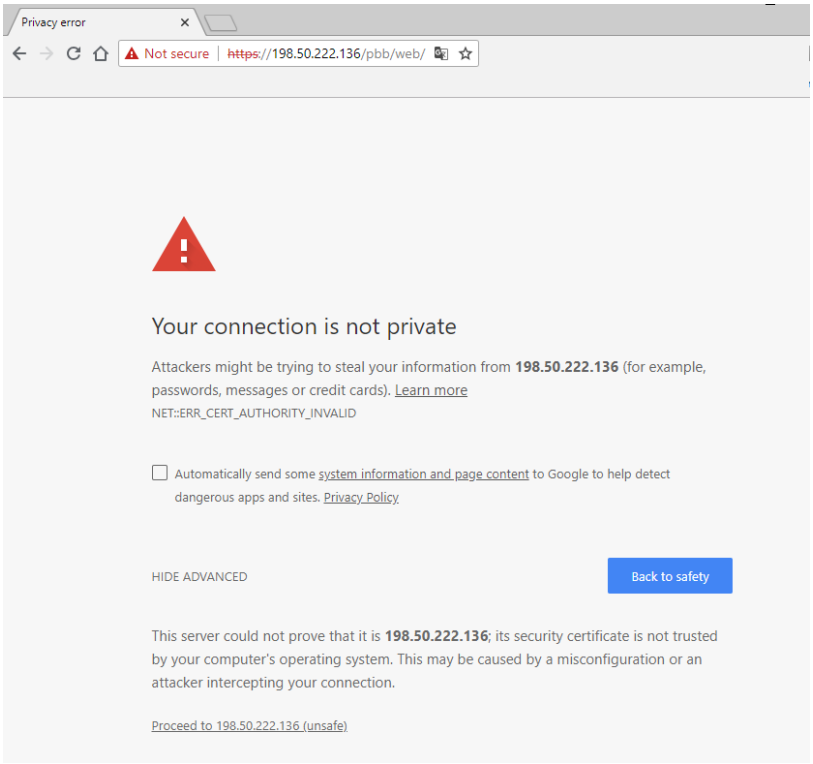


Next, the fake site requires confirmation of identity by asking users to provide mobile phone, card pin, and a CABB number.



Impact On Users

The banks referenced above were not directly attacked nor breached, however their users can suffer financial and private data losses through this malicious hijacking attack. The ‘only’ indicator for the user is the invalid SSL certificate which all modern browsers clearly indicate when using secure connections. It is not even possible to access the website without explicitly confirming the “Not Secure” exception. However, the malicious website, unlike the original website, does allow unsecure connections. If the user, for some reason, bookmarked or typed a unsecured URL (http:// instead of https://), the malicious website stays in unsecure connection and there will be no visible warning for the user.



Another impact on the victims will occur when the malicious DNS server goes offline or is taken down. The attacker is attempting to modify both primary and secondary name servers with the same malicious server IP, meaning that when the malicious server is offline, all infected homes will fail to further resolve any hostnames and their internet will be virtually inaccessible until the users manually update their router settings or the ISP overrides the settings.

Mitigation Recommendations

The targeted banks have been notified as soon as Radware discovered the hijacking. Radware worked closely with the cloud provider hosting the malicious DNS and websites and all of them have been taken offline since 1pm CEST.

Check mobile devices', computers' or routers' primary and secondary DNS server settings in the IP configuration. Start with the router. It is most likely using DHCP on the router for devices inside the home. If so, all devices will expose the malicious server IP as primary and secondary DNS server. A convenient way for checking DNS servers used by your devices and router is through websites like http://www.whatsmydnsserver.com/.

Only modems and routers that were not updated in the last two years can be exploited. Updates will protect the owner of the device and also prevent devices being enslaved for use in DDoS attacks or used to conceal targeted attacks.

All modern browsers clearly indicate an issue with the certificate of the fake website when using secure connections. These warnings should never be ignored and exception popups should not be approved without further consideration or investigation. When facing such a situation, users should be urged to contact the helpdesk of the organization they were trying to access.

Reasons for Concern

Radware has witnessed consumer IoT devices being enslaved in botnets devised to perform DDoS attacks, mine cryptocurrency, provide anonymizing proxy services to conceal attacks, and collect confidential information. Most of the activities related to IoT malware victimizing consumers' IoT devices are not directed at the device owners. Owners are mostly unaware or they don't care as long as the primary function of the device is not compromised. BrickerBot was the first exception. It forced users to take action because BrickerBot essentially "bricked" their devices.

This new attack targets the IoT device owner, attempting to obtain their sensitive data. It is yet another reason for consumers to care about the state of their devices and ensure best practices are met while buying from vendors that meet and demonstrate secure standards in the development of their devices.

While this particular attack was using a two year-old exploit, most exploits on IoT devices witnessed in the past year have been abusing remote command executions in the context of a user with administrative rights. If is not farfetched to image a malicious agent crafting a similar hijacking attack using command-line scripts imbedded in the RCE exploit URLs.

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.