Documento conjunto LACNOG-M³AAWG

Melhores Práticas Operacionais Atuais (BCOP)

Requisitos Mínimos de Segurança para Aquisição de CPE

Lucimara Desiderá, M.Sc. CISSP

Analista de Segurança no CERT.br/NIC.br
Coordenadora LAC-AAWG

Recomendações Mínimas de Segurança em Roteador Doméstico Definidas nas Novas Práticas Conjuntas LACNOG e M3AAWG

3 JUN 2019 09h05

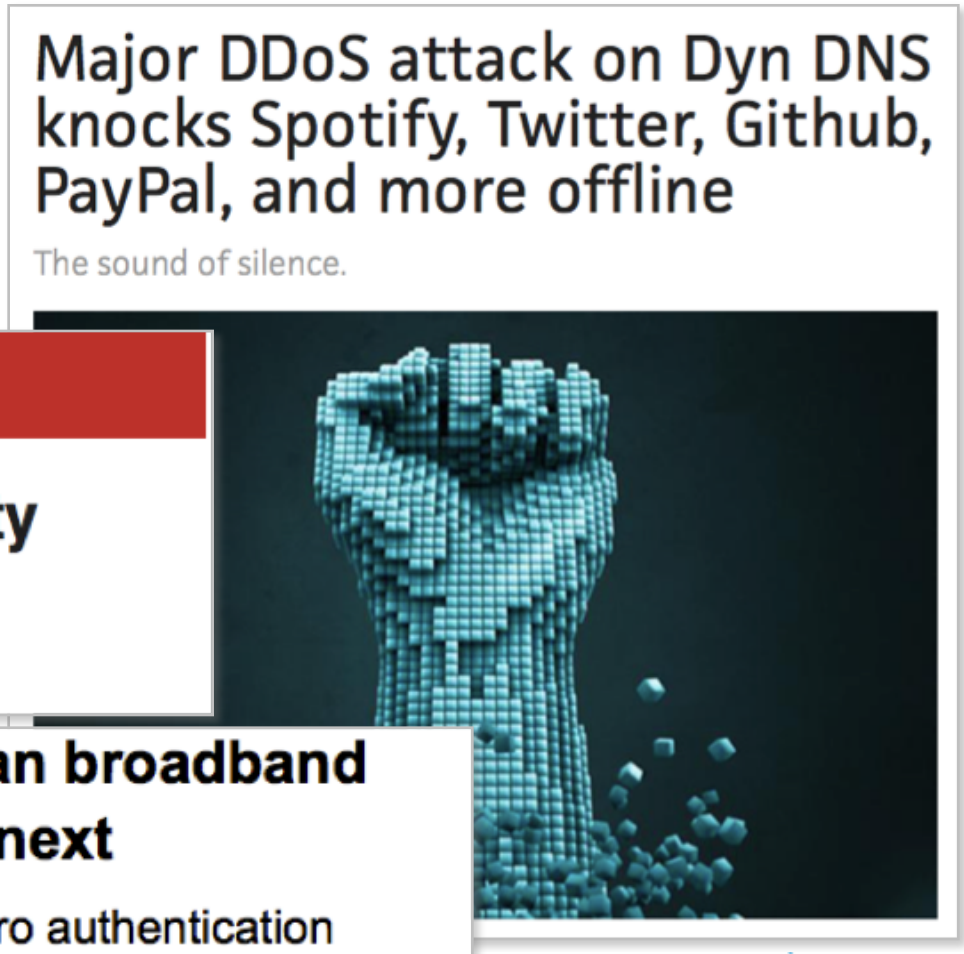
COMENTÁRIOS

As novas recomendações de melhores práticas para os provedores de serviços de Internet (ISPs, na sigla em inglês) publicadas pelo LACNOG (Grupo de Operadores de Rede da América Latina e o Caribe) e M^{3}AAWG (*Messaging, Malware and Mobile Anti-Abuse Working Group*) este mês definem os critérios básicos de segurança para os roteadores domésticos e outros equipamentos para conexão de usuário (*customer premise equipment*, CPE) e espera-se que ajudem a proteger a Internet contra ataques comuns, especialmente ataques de negação de serviço (DoS, na sigla em inglês) resultantes do abuso desses dispositivos. As recomendações fortalecerão os esforços de segurança dos provedores de serviço de Internet ao identificar requisitos para os dispositivos de *hardware* conectados às suas redes, que são suscetíveisàexploração quando proteções básicas são ignoradas.

https://www.terra.com.br/noticias/dino/recomendacoes-minimas-de-seguranca-em-roteador-domestico-definidas-nas-novas-praticas-conjuntas-lacnog-e-m3aawg,a4a7c7f5e8ca681f8cd17bd7336e3e4dm7wjf8lt.html

Setembro/2016, Mirai é identificado

- 22 e 23/09 – 620Gbps contra o Blog do Brian Krebs
- 21/10 – DDoS contra a Dyn
- 27/11 – Surgimento da variante para CPEs



BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

'Mirai bots' cyber-blitz 1m German broadband routers – and your ISP could be next

Malware waltzes up to admin panels with zero authentication

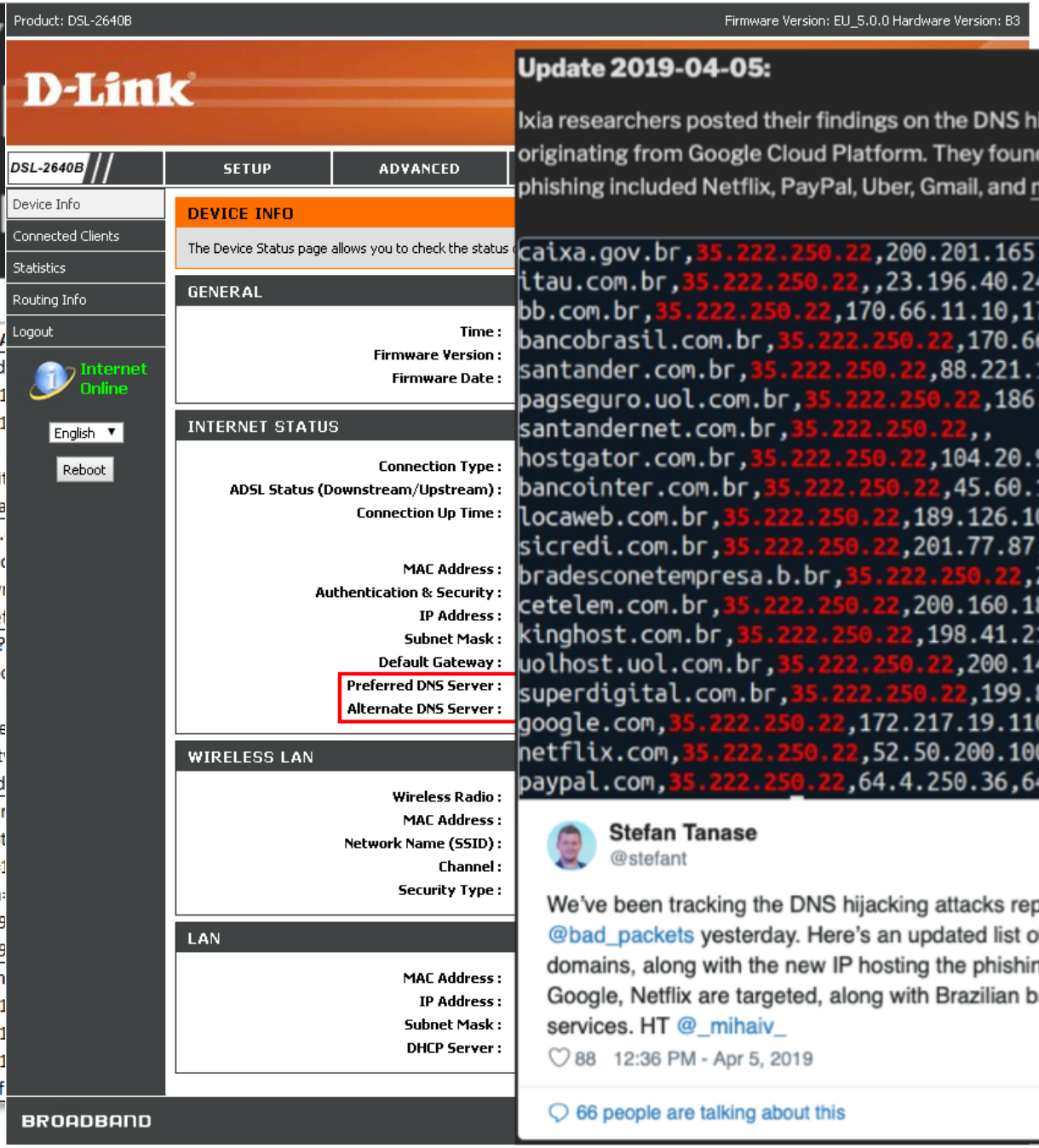
Brad Chacos | *@BradChacos* Oct 21, 2016 3:34 PM
Senior Editor, PCWorld

http://www.bbc.co.uk/news/amp/37439513
http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html
http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/

APRIL 4, 2019 BY

Ongoing D
consumer

Target Device	Exploit A
ARG-W4 ADSL Routers	/form2d &dns1=1 &dns2=1 &dns3= &submit &save=a
D-Link Routers (Multiple)	/dnscfg. &dnsSec &dnsDy &dnsRef
DSLink 260E Routers	/action? &dns_pc &id=57 &dns_se &priorit &cmdad
Secutech Routers	/wan_dr &reboot &dsen=1 &dnsen= &ds1=19 &ds2=19
TOTOLINK Routers	/boafrm &dns1=1 &dns2=1 &dns3=1 &dnsref



Update 2019-04-05:

Ixia researchers posted their findings on the DNS hijacking attacks originating from Google Cloud Platform. They found sites targeted for phishing included Netflix, PayPal, Uber, Gmail, and more.

```
caixa.gov.br,35.222.250.22,200.201.165.253,200.201.16
itau.com.br,35.222.250.22,,23.196.40.246
bb.com.br,35.222.250.22,170.66.11.10,170.66.11.10
bancobrasil.com.br,35.222.250.22,170.66.11.10,170.66.
santander.com.br,35.222.250.22,88.221.16.112,92.122.2
pagseguro.uol.com.br,35.222.250.22,186.234.145.200,18
santandernet.com.br,35.222.250.22,,
hostgator.com.br,35.222.250.22,104.20.91.5,104.20.90.
bancointer.com.br,35.222.250.22,45.60.101.27,45.60.11
locaweb.com.br,35.222.250.22,189.126.100.6,189.126.10
sicredi.com.br,35.222.250.22,201.77.87.14,
bradesconetempresa.b.br,35.222.250.22,200.155.86.35,2
cetelem.com.br,35.222.250.22,200.160.185.92,200.160.1
kinghost.com.br,35.222.250.22,198.41.215.162,198.41.2
uolhost.uol.com.br,35.222.250.22,200.147.4.76,200.147
superdigital.com.br,35.222.250.22,199.83.135.173,192.
google.com,35.222.250.22,172.217.19.110,172.217.20.14
netflix.com,35.222.250.22,52.50.200.100,52.208.135.54
paypal.com,35.222.250.22,64.4.250.36,64.4.250.37
```

Stefan Tanase
@stefant

We've been tracking the DNS hijacking attacks reported by @bad_packets yesterday. Here's an updated list of targeted domains, along with the new IP hosting the phishing sites. Paypal, Google, Netflix are targeted, along with Brazilian banks and hosting services. HT @_mihaiv_

♡ 88 12:36 PM - Apr 5, 2019

66 people are talking about this

https://badpackets.net/ongoing-dns-hijacking-campaign-targeting-consumer-routers/

Por que se preocupar com segurança de CPE?

Impactos operacionais e de negócios:

- Comprometimento da rede do provedor
  - Alguém está usando seus recursos
- Degradação ou indisponibilidade de serviços
  - Você pode perder clientes
- Suporte técnico e trabalho de reparo
  - Você está perdendo dinheiro
- Proteja a reputação do seu ISP
  - Clientes, parceiros e listas negras

Problemas que a BCOP trata:

- Credenciais padrão para um grande número de dispositivos
- Credenciais que não podem ser alteradas (*hard-coded*)
- Uso de protocolos e algoritmos obsoletos e inseguros
- Acessos não documentados (*backdoors*)
- Falta de mecanismo de atualização automatizado e seguro para corrigir problemas de segurança
- Serviços desnecessários e/ou inseguros ativados por padrão
- Serviços que não podem ser desativados
- Gerenciamento remoto inseguro
- Suporte à correções de segurança

Documento conjunto LACNOG-M³AAWG

"Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition"

Lançamento oficial em 08/05/2019 no LACNIC 31

https://www.lacnog.net/docs/lac-bcop-1
https://www.m3aawg.org/CPESecurityBP

Traduções:

https://www.m3aawg.org/published-documents

- Japonês (JP-AAWG)
- Espanhol, Português e Koreano (revisão final)
- Alemão e Francês (por vir)

lacnog

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

O que tem na BCOP?

Um checklist de referência para decisões de hardware

→ Pedir aos fornecedores produtos melhores

→ segurança por padrão

Índice