باسمه تعالی

بررسی بات‌نت GhostDNS

مهر ۹۷

فهرست مطالب

1 چکیده

حمله DNSchanger موضوع جدیدی نیست و از سال‌ها پیش فعال بوده و گاه و بیگاه یک حمله از آن نوع صورت می‌گرفته است. بدافزار DNSChanger می‌تواند درخواست‌های اینترنتی کاربر آلوده را از طریق سوءاستفاده از سرویس DNS به سایت‌های جعلی و مخرب هدایت کند. به این ترتیب با تغییر آدرس سرور DNS مورد استفاده دستگاه، درخواست‌های ارسالی از آن به جای هدایت به سرورهای DNS واقعی و معتبر در اینترنت، به یکی از سرویس‌دهنده‌های تحت کنترل مهاجم فرستاده می‌شود.

اخیراً شرکتRadware در مورد بدافزارای تحت عنوان GhostDNS گزارشی منتشر کرده است. از 20 سپتامبر 2018، کمپین این بدافزار با مجموعه‌ای از اسکنرهای جدید، شروع به افزایش قابل توجه تلاش خود کرده است. همانند سایر حملات Dnschanger، این کمپین تلاش می‌کند تا رمز عبور صفحه مدیریت تحت وب مسیریاب‌های خانگی را حدس بزند یا از طریق سوء استفاده از فایل dnscfg.cgi اقدام به دور زدن احراز هویت نماید. سپس آدرس DNS پیش فرض مسیریاب را از طریق پیکربندی DNS مربوطه، به DNS سرور جعلی تغییر دهد.

اما این کمپین فراتر از DNSChangerهای رایج عمل می‌کند. در مجموعه این بدافزار، سه برنامه مرتبط DNSChanger شناسایی شده است، که با توجه به زبان برنامه نویسی با نام Shell DNSChanger، Js DNSChanger و PyPhp DNSChanger نامگذاری شده‌اند. کل کمپین شامل ماژول تغییردهنده DNS، فیشینگ سیستم‌های وب، سیستم مدیریت وب و سیستم‌های DNS مخرب است. این چهار بخش با هم کار می‌کنند تا عمل ربودن DNS را انجام دهند.

در حال حاضر این کمپین عمدتاً بر روی کشور برزیل تمرکز دارد، تاکنون آدرس بیش از 100 هزار مسیریاب آلوده (که 87.8٪ در برزیل واقع شده‌اند) و بیش از 70 مسیریاب/firmware که در این حمله درگیر بوده‌اند و بیش از 50 نام دامنه -از جمله برخی از بانک‌های بزرگ در برزیل که برای دزدیدن رمزعبورکاربران مورد سوءاستفاده قرار گرفته بودند، شناسایی شده اند.

2 محصولات تحت تاثیر

بیش از 70 نوع مسیریاب، از جمله مدل‌های مسیریاب/firmware های زیر که نسبت به این باتنت آسیب‌پذیر هستند و در ایران نیز موجود می‌باشند عبارتند از:

ردیف	شرکت	مدل
1	TP-Link	TD-W8901G
2	TP-Link	TD-W8961ND

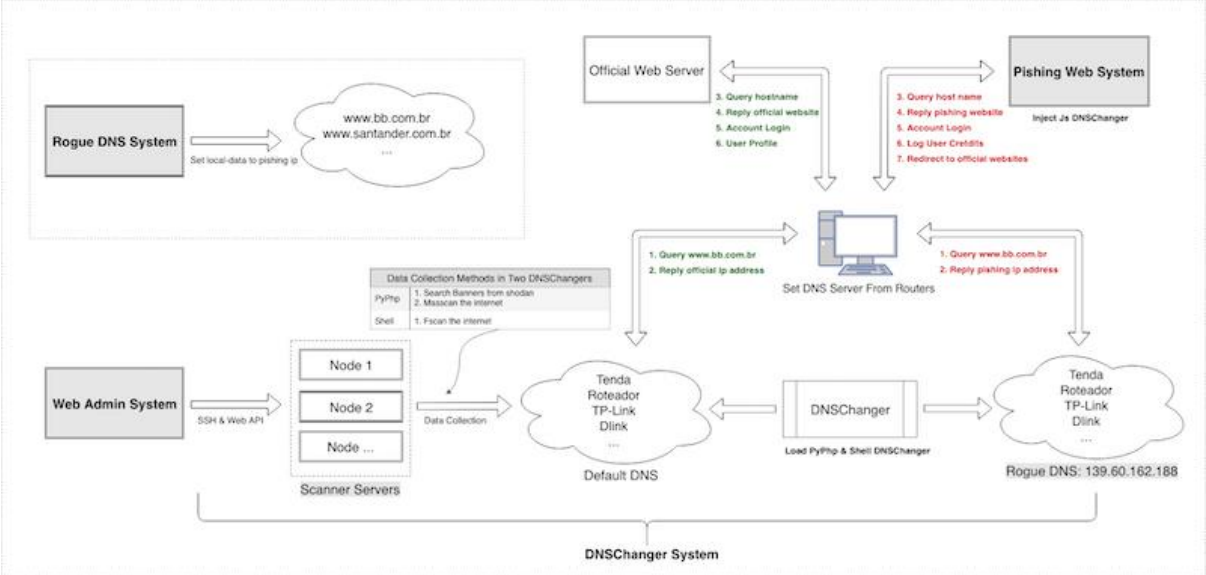
TD-8816	TP-Link	**3**
TD-W8960N	TP-Link	**4**
TL-WR740N	TP-Link	**5**
Archer C7	TP-Link	**6**
TL-WR1043ND	TP-Link	**7**
TL-WR720N	TP-Link	**8**
TL-WR740N	TP-Link	**9**
TL-WR840N	TP-Link	**10**
TP-LINK Nano WR702N	TP-Link	**11**
TP-LINK TL-WR941HP	TP-Link	**12**
TP-LINK Wireless AP WA5210G	TP-Link	**13**
TP-LINK Wireless Lite N Router WR740N	TP-Link	**14**
TP-LINK Wireless N Router WR841N/WR841ND	TP-Link	**15**
TP-LINK Wireless N Router WR845N	TP-Link	**16**
TP-LINK Wireless N Router WR941ND	TP-Link	**17**
TP-LINK Wireless Router	TP-Link	**18**
TP-LINK WR340G	TP-Link	**19**
TP-LINK WR720N	TP-Link	**20**
TP-LINK WR740N	TP-Link	**21**
TP-LINK WR741N	TP-Link	**22**
TP-LINK WR743ND	TP-Link	**23**
TP-LINK WR840N	TP-Link	**24**
TP-LINK WR841HP	TP-Link	**25**
TP-LINK WR841N	TP-Link	**26**
TP-LINK WR940N	TP-Link	**27**
TP-LINK WR941N	TP-Link	**28**
TL-WR840N	TP-Link	**29**
TL-WR841N	TP-Link	**30**
TL-WR845N	TP-Link	**31**
TL-WR941ND	TP-Link	**32**
DIR600	D-Link	**33**
DIR-615	D-Link	**34**

همچنین مدل‌های D-LINK DSL-2640T، D-LINK DSL-2740R و Huawei SmartAX MT880a، مدل‌های آسیب‌پذیری هستند که در برزیل موجود بوده‌اند و سری U از آن‌ها در ایران نیز استفاده می‌شود. لذا این احتمال وجود دارد که firmware آن‌ها یکسان بوده و مدل‌های مورد استفاده در ایران نیز تحت تاثیر این آسیب‌پذیری باشند.

علاوه بر موارد فوق، انواعی از مدل مسیریاب/firmware های شرکت سیسکو، میکروتیک و Tenda نیز احتمال آسیب‌پذیری دارند ولی تاکنون مدل‌های آسیب‌پذیر این شرکت‌ها شناسایی نشده است.

3 بررسی اجزای کمپین بدافزار GhostDNS

این سیستم شامل چهار بخش است: ماژول تغییردهنده DNS، ماژول فیشینگ وب، ماژول مدیریت وب و ماژول DNS مخرب، که در میان آنها، ماژول DNSChanger مسئول جمع‌آوری و بهره‌برداری از اطلاعات است.



شکل۱- نمودار جریان GhostDNS

ماژول تغییر DNS، ماژول اصلی GhostDNS است. مهاجم از سه زیرگروه DNSChanger برای حمله به مسیریاب‌ها در شبکه‌های اینترنت و اینترانت استفاده می‌کند. این ماژول شامل مجموعاً بیش از 100 حمله اسکریپتی است که بیش از 70 نوع مسیریاب مختلف را تحت تاثیر قرار داده‌اند.

3-1 ماژول DNSChanger

زیرگروه‌های DNSChanger در جدول ۱ ذکر شده‌اند.

DNSChanger	Attack Surface	Attack Vector(s)	Attack Script Count	Affect Device Count
Shell	Wan	Web Auth Bruteforce	25	21
Js	Lan	Web Auth Bruteforce	10	6
PyPhp	Wan	Web Auth Bruteforce & dnscfg.cgi Exploit	69	47

جدول۱- زیرگروه‌های ماژول DNSChanger

3-1-1 زیرگروه Shell DNSChanger

Shell DNSChanger برای اولین بار در حدود ژوئن 2016 در دسترس قرار گرفته است. این DNSChanger اساساً ترکیبی از 25 حمله اسکریپتی شل (پوسته) است که روی 21 مسیریاب/ firmware تاثیرگذار است. این زیرمجموعه بصورت محدود توسط مهاجم مورد استفاده قرار می‌گیرد.

این زیرگروه از یک برنامه دیگر، با نام Fast HTTP Auth Scanner v0.6 (FScan) برای انجام اسکن استفاده می‌کند. این اسکنر با تعداد زیادی از قوانین اسکن، لیستی از رمز عبورهای کاربران و برخی از اسکریپت‌های راه‌اندازی، پیکربندی شده است.

پس از اسکن اولیه، این زیرگروه از اطلاعات جمع‌آوری شده دستگاه مسیریاب برای شکستن رمز عبور بر روی صفحات احراز هویت وب این مسیریاب‌ها استفاده می‌کند. اگر موفقیت‌آمیز باشد، آدرس پیش فرض DNS در مسیریاب به سرور DNS مخرب تغییر خواهد کرد.

ساختار زیر، ساختار اصلی کد Shell DNSChanger را نمایش می‌دهد.

```
├── brasil
├── changers
│   ├── 3com1
│   ├── aprouter
│   ├── dlink1
│   ├── dlink2
│   ├── dlink3
│   ├── dlink4
│   ├── dlink5
│   ├── dlink6
│   ├── dlink7
│   ├── dlink7_
│   ├── globaltronic
│   ├── huawei
│   ├── intelbrass
```

```
│   ├── kaiomy
│   ├── mikrotik
│   ├── oiwtech
│   ├── ralink
│   ├── realtek
│   ├── speedstream
│   ├── speedtouch
│   ├── speedtouch2
│   ├── tplink1
│   ├── tplink2
│   ├── tplink3
│   ├── triz
│   └── viking
├── configs
├── logs
├── mdetector
├── mikrotik
├── ralink
├── src
│   ├── BasicAuth.cpp
│   ├── Makefile
│   ├── Net-Telnet-3.03.tar.gz
│   ├── base64.cpp
│   ├── config.cpp
│   ├── fscan.cpp
│   ├── md5.cpp
│   ├── md5.h
│   ├── sockets.cpp
│   ├── sslscanner.h
│   ├── ulimit
│   └── webforms.cpp
├── .fscan
└── .timeout
```

انواع مسیریاب/firmware که در ادامه ذکر شده‌اند، مدل‌های آسیب‌پذیری هستند که تاکنون شناخته شده‌اند.

3COM OCR-812
AP-ROUTER
D-LINK
D-LINK DSL-2640T
D-LINK DSL-2740R
D-LINK DSL-500
D-LINK DSL-500G/DSL-502G
Huawei SmartAX MT880a
Intelbras WRN240-1
Kaiomy Router
MikroTiK Routers
OIWTECH OIW-2415CPE
Ralink Routers
SpeedStream
SpeedTouch
Tenda
TP-LINK TD-W8901G/TD-W8961ND/TD-8816
TP-LINK TD-W8960N
TP-LINK TL-WR740N
TRIZ TZ5500E/VIKING
VIKING/DSLINK 200 U/E

3-1-2 زیرگروه JS DNSChanger

JS DNSChanger عمدتاً به زبان Javascript نوشته شده است. این زیرگروه شامل 10 حمله اسکریپتی است که می تواند 6 مدل مسیریاب/ firmware را آلوده کند. ساختار عملکردی آن عمدتا به اسکنرها، تولبدکننده Payload (پی‌لود در امنیت سایبری، به محموله داده‌ای گفته می‌شود که توسط بدافزار و از طریق وسایل یا شبکه‌های آسیب‌دیده منتقل می‌شود) و برنامه‌های حمله تقسیم می‌شود. برنامه Js DNSChanger معمولاً به وب‌سایت‌های فیشینگ تزریق می‌شود.

برای مثال، یک کد JS DNSChanger در صفحه اصلی آی‌پی 35.236.25.247 وجود دارد (عنوان وب سایت: Convertidor Youtube Mp3 | Mp3 youtube).

ساختار زیر بخشی از ساختار کد JS DNSChanger است:

```
├── api.init.php
├── index.php
└── index2.php
```

موارد ذیل، انواع مسیریاب/firmwareهای شناسایی شده‌اند که تحت تاثیر این زیرگروه از DNSChanger می‌باشند.

```
A-Link WL54AP3 / WL54AP2
D-Link DIR-905L
Roteador GWR-120
Secutech RiS Firmware
SMARTGATE
TP-Link TL-WR841N / TL-WR841ND  **/**
```

محدوده اسکن آی‌پی برای اسکنر این زیرگروه به صورت زیر است:

```
192.168.0.1
192.168.15.1
192.168.1.1
192.168.25.1
192.168.100.1
10.0.0.1
192.168.2.1
```

3-1-3 زیرمجموعه PyPhp DNSChanger

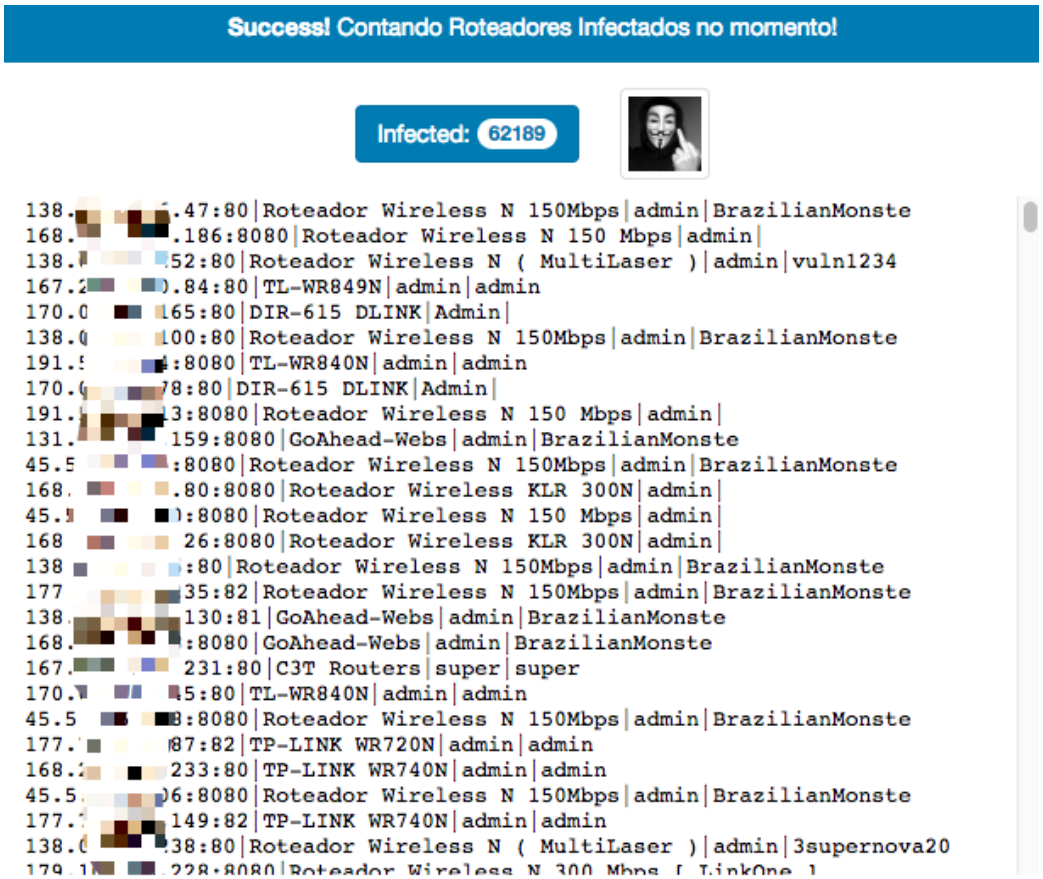
PyPhp DNSChanger ماژول اصلی DNSChanger است، مشاهده شده که مهاجم این برنامه را بر روی بیش از 100 سرور قرار داده است که بیشتر آنها در ابر گوگل هستند. این زیرمجموعه در سال 2018، با استفاده از هر دو زبان پایتون و پی اچ پی توسعه داده شده است. این زیرگروه عمدتاً از سه بخش تشکیل شده است:

- **API (رابط کاربری برنامه نویسی) وب:** از طریق این بخش مهاجم می‌تواند کنترل و برنامه ریزی برای اجرای برنامه را به راحتی انجام دهد.
- **اسکنر:** اسکنر از هر دو اسکن پورت Masscan و سرویس API Shodan استفاده می‌کند تا IP های مسیریاب مقصد را فقط در برزیل قرار دهد. جالب است که کلید API Shodan در اینجا نیز توسط یکی دیگر از پروژه های آموزشی و تحقیقاتی در Github استفاده می‌شود.

اطلاعات کلیدی API سایت Shodan به شرح زیر است:

```
API key: LI****Lg9P8****X5iy****AaRO
Created: 2017-11-03T16:55:13.425000
Plan: EDU
```

- **ماژول حمله:** ماژول حمله شامل 69 اسکریپت حمله برای 47 مدل مسیریاب/ firmware مختلف است. این پروتکل، IP های فعال مسیریاب را از اسکنر جمع آوری کرده و از این طریق حمله بروت‌فورس احراز هویت را صورت می‌دهد و یا از اکسپلویت‌های آسیب پذیری dnscfg.cgi برای دور زدن احراز هویت استفاده می‌کند. پس از آن DNS resolver پیش‌فرض مسیریاب‌ها را به سرور DNS جعلی(که برای سرقت وب سایت‌های خاص در فیشینگ استفاده می‌شود) تغییر می‌دهد.



تصویر 2: نمایی از آمار آلودگی‌ها در سایت PyPhp DNSChanger

ساختار کد PyPhp DNSChnger به شرح زیر است:

```
├── api
├── application
│   ├── class
```

```
│   │   ├── routers
│   │   │   ├── routers.28ZE.php
│   │   │   ├── routers.AN5506-02-B.php
│   │   │   ├── routers.ELSYSCPE-2N.php
│   │   │   ├── routers.PQWS2401.php
│   │   │   ├── routers.TLWR840N.php
│   │   │   ├── routers.WR941ND.php
│   │   │   ├── routers.airos.php
│   │   │   ├── routers.c3t.php
│   │   │   ├── routers.cisconew.php
│   │   │   ├── routers.dlink.905.php
│   │   │   ├── routers.dlink.dir600.php
│   │   │   ├── routers.dlink.dir610.php
│   │   │   ├── routers.dlink.dir610o.php
│   │   │   ├── routers.dlink.dir615.php
│   │   │   ├── routers.fiberhome.php
│   │   │   ├── routers.fiberhomenew.php
│   │   │   ├── routers.ghotanboa.php
│   │   │   ├── routers.goahed.php
│   │   │   ├── routers.greatek.php
│   │   │   ├── routers.greatek2.php
│   │   │   ├── routers.gwr120.php
│   │   │   ├── routers.huawei.php
│   │   │   ├── routers.intelbras.php
│   │   │   ├── routers.intelbras.wrn240.php
│   │   │   ├── routers.intelbras.wrn300.php
│   │   │   ├── routers.intelbrasN150.php
│   │   │   ├── routers.linkone.php
│   │   │   ├── routers.livetimdslbasic.php
│   │   │   ├── routers.livetimsagecom.php
│   │   │   ├── routers.mikrotkit.php
│   │   │   ├── routers.multilaser.php
│   │   │   ├── routers.oiwtech.php
```

```
│   │   │   ├── routers.othermodels.php
│   │   │   ├── routers.sharecenter.php
│   │   │   ├── routers.thomson.php
│   │   │   ├── routers.timdsl.php
│   │   │   ├── routers.timvmg3312.php
│   │   │   ├── routers.wirelessnrouter.php
│   │   │   ├── routers.wrn1043nd.php
│   │   │   ├── routers.wrn342.php
│   │   │   ├── routers.wrn720n.php
│   │   │   ├── routers.wrn740n.php
│   │   │   ├── routers.wrn749n.php
│   │   │   ├── routers.wrn840n.php
│   │   │   ├── routers.wrn841n.php
│   │   │   └── routers.wrn845n.php
│   │   ├── routers_py
│   │   │   ├── WR300build8333.py
│   │   │   ├── install.sh
│   │   │   ├── router.ArcherC7.py
│   │   │   ├── router.FiberLink101.py
│   │   │   ├── router.GEPONONU.py
│   │   │   ├── router.PNRT150M.py
│   │   │   ├── router.QBR1041WU.py
│   │   │   ├── router.RoteadorWirelessN300Mbps.py
│   │   │   ├── router.SAPIDORB1830.py
│   │   │   ├── router.TENDAWirelessNBroadbandrouter.py
│   │   │   ├── router.TLWR840N.py
│   │   │   ├── router.TLWR841N.py
│   │   │   ├── router.TLWR849N.py
│   │   │   ├── router.TPLINKWR841N.py
│   │   │   ├── router.TechnicLanWAR54GSv2.py
│   │   │   ├── router.TendaWirelessRouter.py
│   │   │   ├── router.WEBManagementSystem.py
│   │   │   ├── router.WLANBroadbandRouter.py
```

```
│   │   │   ├── router.WebUI.py
│   │   │   ├── router.WirelessNWRN150R.py
│   │   │   ├── router.WirelessRouter.py
│   │   │   ├── router.WiveNGMTrouterfirmware.py
│   │   │   ├── router.ZXHNH208N.py
│   │   │   └── scan
│   │   │       ├── __init__.py
│   │   │       └── password.py
│   │   ├── scanner
│   │   │   └── class.scanner.utils.php
│   │   ├── shodan
│   │   │   ├── class.shodan.php
│   │   │   └── cookie.txt
│   │   ├── utils
│   │   │   ├── class.colors.php
│   │   │   ├── class.utils.php
│   │   │   └── class.webrequest.php
│   │   └── web
│   │       ├── blockedtitles
│   │       ├── class.web.api.php
│   │       └── class.web.interface.php
│   ├── config.bruteforce.php
│   ├── config.init.php
│   ├── config.layout.php
│   ├── config.rangelist - bkp.php
│   ├── config.rangelist.php
│   ├── config.routers.php
│   ├── config.scanner.php
│   ├── launchers
│   │   └── attack
│   │       └── launch
│   └── logs
├── logs
```

```
│   ├── change.log
│   └── gravar.php
├── parse_logs
└── scanner
    ├── api.php
    ├── extrator.php
    ├── ranged_scanner.php
    ├── rodar.php
    ├── rodarlista.php
    ├── shodan.php
    └── teste.py
```

مدل‌های مسیریاب/ firmware آسیب‌پذیر به این زیرگروه از DNSChanger در ادامه لیست شده‌اند.

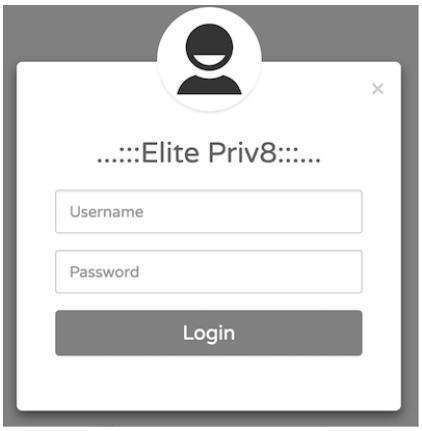
AirRouter AirOS

Antena PQWS2401
C3-TECH Router
Cisco Router
D-Link DIR-600
D-Link DIR-610
D-Link DIR-615
D-Link DIR-905L
D-Link ShareCenter
Elsys CPE-2n
Fiberhome
Fiberhome AN5506-02-B
Fiberlink 101
GPON ONU
Greatek
GWR 120
Huawei
Intelbras WRN 150
Intelbras WRN 240
Intelbras WRN 300
LINKONE
MikroTik
Multilaser
OIWTECH
PFTP-WR300
QBR-1041 WU
Roteador PNRT150M
Roteador Wireless N 300Mbps
Roteador WRN150
Roteador WRN342
Sapido RB-1830

TECHNIC LAN WAR-54GS
Tenda Wireless-N Broadband Router
Thomson
TP-Link Archer C7
TP-Link TL-WR1043ND
TP-Link TL-WR720N
TP-Link TL-WR740N
TP-Link TL-WR749N
TP-Link TL-WR840N
TP-Link TL-WR841N
TP-Link TL-WR845N
TP-Link TL-WR849N
TP-Link TL-WR941ND
Wive-NG routers firmware
ZXHN H208N
Zyxel VMG3312

3-2 سیستم مدیریت تحت وب

یک وب سایت مدیر وب بر روی یک گره PyPhp DNSChanger شناسایی شده است. هنوز اطلاعات زیادی درباره این سیستم در دست نیست، اما کارشناسان بر این باورند که این یک سیستم مدیریت کمپین است.



تصویر 3: وب سایت مدیریتی روی یکی از گره‌های PyPhp DNSChanger

در صفحه ورود سیستم مدیریت وب، یک برچسب ویژه"Elite Priv8" دیده می‌شود. با کمی جستجو، می‌توان یک توصیف مشابه را در پستی با عنوان "testador santander banking 2.1 versao beta elitepriv8" در یک انجمن امنیتی برزیلی پیدا کرد.

آدرس IP سرور مدیریت وب به شرح زیر است:

198.50.222.139 "AS16276 OVH SAS"

3-3 سیستم DNS مخرب

با توجه به عدم دسترسی به سرور DNS مخرب، نمی‌توان به طور دقیق گفت که چه تعداد از نام‌های دامنه ربوده شده است، اما با بررسی دامنه‌های یک میلیون بالای الکسا و DNSMon در برابر سرور DNS مخرب (139.60.162.188)، مجموع 52 دامنه سوء استفاده شده شناسایی شده است. دامنه‌های ربوده شده عمدتا شامل بانک، سرویس میزبانی ابری و همچنین شرکت امنیتی Avira می‌باشد.

در ادامه جزئیات سوءاستفاده سرور DNS مخرب (139.60.162.188) آمده است. دامنه‌ی شرکت امنیتی avira.com.br نیز روی 0.0.0.0 تنظیم شده است.

{"domain": "avira.com.br", "rdata": ["0.0.0.0"]}
{"domain": "banco.bradesco", "rdata": ["198.27.121.241"]}
{"domain": "bancobrasil.com.br", "rdata": ["193.70.95.89"]}
{"domain": "bancodobrasil.com.br", "rdata": ["193.70.95.89"]}
{"domain": "bb.com.br", "rdata": ["193.70.95.89"]}
{"domain": "bradesco.com.br", "rdata": ["193.70.95.89"]}
{"domain": "bradesconetempresa.b.br", "rdata": ["193.70.95.89"]}
{"domain": "bradescopj.com.br", "rdata": ["193.70.95.89"]}
{"domain": "br.wordpress.com", "rdata": ["193.70.95.89"]}
{"domain": "caixa.gov.br", "rdata": ["193.70.95.89"]}
{"domain": "citibank.com.br", "rdata": ["193.70.95.89"]}
{"domain": "clickconta.com.br", "rdata": ["193.70.95.89"]}
{"domain": "contasuper.com.br", "rdata": ["193.70.95.89"]}
{"domain": "credicard.com.br", "rdata": ["198.27.121.241"]}
{"domain": "hostgator.com.br", "rdata": ["193.70.95.89"]}
{"domain": "itau.com.br", "rdata": ["193.70.95.89"]}
{"domain": "itaupersonnalite.com.br", "rdata": ["193.70.95.89"]}
{"domain": "kinghost.com.br", "rdata": ["193.70.95.89"]}
{"domain": "locaweb.com.br", "rdata": ["193.70.95.89"]}
{"domain": "netflix.com.br", "rdata": ["35.237.127.167"]}
{"domain": "netflix.com", "rdata": ["35.237.127.167"]}
{"domain": "painelhost.uol.com.br", "rdata": ["193.70.95.89"]}
{"domain": "santander.com.br", "rdata": ["193.70.95.89"]}
{"domain": "santandernet.com.br", "rdata": ["193.70.95.89"]}
{"domain": "sicredi.com.br", "rdata": ["193.70.95.89"]}
{"domain": "superdigital.com.br", "rdata": ["193.70.95.89"]}
{"domain": "umbler.com", "rdata": ["193.70.95.89"]}
{"domain": "uolhost.uol.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.banco.bradesco", "rdata": ["198.27.121.241"]}
{"domain": "www.bancobrasil.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.bb.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.bradesco.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.bradesconetempresa.b.br", "rdata": ["193.70.95.89"]}
{"domain": "www.bradescopj.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.br.wordpress.com", "rdata": ["193.70.95.89"]}
{"domain": "www.caixa.gov.br", "rdata": ["193.70.95.89"]}
{"domain": "www.citibank.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.credicard.com.br", "rdata": ["193.70.95.89"]}

{"domain": "www.hostgator.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.itau.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.kinghost.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.locaweb.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.netflix.com", "rdata": ["193.70.95.89"]}
{"domain": "www.netflix.net", "rdata": ["193.70.95.89"]}
{"domain": "www.painelhost.uol.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.santander.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.santandernet.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.sicredi.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.superdigital.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.umbler.com", "rdata": ["193.70.95.89"]}
{"domain": "www.uolhost.com.br", "rdata": ["193.70.95.89"]}
{"domain": "www.uolhost.uol.com.br", "rdata": ["193.70.95.89"]}

در ادامه لیستی از سرورهای DNS مخرب شناسایی شده، آمده است:

139.60.162.188	"AS395839 HOSTKEY"
139.60.162.201	"AS395839 HOSTKEY"
144.22.104.185	"AS7160 Oracle Corporation"
173.82.168.104	"AS35916 MULTACOM CORPORATION"
18.223.2.98	"AS16509 Amazon.com, Inc."
185.70.186.4	"AS57043 Hostkey B.v."
192.99.187.193	"AS16276 OVH SAS"
198.27.121.241	"AS16276 OVH SAS"
200.196.240.104	"AS11419 Telefonica Data S.A."
200.196.240.120	"AS11419 Telefonica Data S.A."
35.185.9.164	"AS15169 Google LLC"
80.211.37.41	"AS31034 Aruba S.p.A."

3-4 سیستم فیشینگ وب

سرورDNS مخرب، دامنه‌های خاصی را مورد سوء استفاده قرار می دهد و آدرس‌هایIP آنها را روی وب‌سرور فیشینگ قرار می‌دهد، که در نتیجه برای قربانیان هنگام درخواست نام میزبان مربوطه، سایت‌های فیشینگ خاص، در پاسخ برگردانده می‌شود.

با پیگیری سرور فیشینگ با 52 دامنه ربوده شده، 19 سایت مختلف فیشینگ شناسایی شده اند که در ادامه لیست شده‌اند.

```
md5, url, hostname, pishing web api
```

42c3c9b4207b930b414dd6bd64335945 http://193.70.95.89 itau.com.br ['http://193.70.95.89/processar1.php']

42c3c9b4207b930b414dd6bd64335945 http://193.70.95.89 itaupersonnalite.com.br ['http://193.70.95.89/processar1.php']

42c3c9b4207b930b414dd6bd64335945 http://193.70.95.89 www.itau.com.br ['http://193.70.95.89/processar1.php']

4398ceb11b79cbf49a9d300095923382 http://193.70.95.89/login.php umbler.com ['http://193.70.95.89/processa_1.php']

4398ceb11b79cbf49a9d300095923382 http://193.70.95.89/login.php www.umbler.com ['http://193.70.95.89/processa_1.php']

492188f294d0adeb309b4d2dd076f1ac http://193.70.95.89 www.credicard.com.br ['http://193.70.95.89/acesso.php']

492c7af618bd8dcbc791037548f1f8e6 http://193.70.95.89 sicredi.com.br ['http://193.70.95.89/salvar.php']

492c7af618bd8dcbc791037548f1f8e6 http://193.70.95.89 www.sicredi.com.br ['http://193.70.95.89/salvar.php']

5838b749436a5730b0112a81d6818915 http://193.70.95.89 bradesconetempresa.b.br ['http://193.70.95.89/processa_2.php', 'http://193.70.95.89/enviar_certificado_1.php']

70b8d0f46502d34ab376a02eab8b5ad7 http://193.70.95.89/default.html locaweb.com.br ['http://193.70.95.89/salvar.php']

70b8d0f46502d34ab376a02eab8b5ad7 http://193.70.95.89/default.html www.locaweb.com.br ['http://193.70.95.89/salvar.php']

748322f4b63efbb9032d52e60a87837d http://193.70.95.89/login.html bancobrasil.com.br ['http://193.70.95.89/processar_1.php']

748322f4b63efbb9032d52e60a87837d http://193.70.95.89/login.html bancodobrasil.com.br ['http://193.70.95.89/processar_1.php']

748322f4b63efbb9032d52e60a87837d http://193.70.95.89/login.html bb.com.br ['http://193.70.95.89/processar_1.php']

748322f4b63efbb9032d52e60a87837d http://193.70.95.89/login.html www.bancobrasil.com.br ['http://193.70.95.89/processar_1.php']

748322f4b63efbb9032d52e60a87837d http://193.70.95.89/login.html www.bb.com.br ['http://193.70.95.89/processar_1.php']

8e94b7700dde45fbb42cdecb9ca3ac4e http://193.70.95.89/BRGCB/JPS/portal/Index.do.shtml citibank.com.br ['http://193.70.95.89/BRGCB/JPS/portal/Home.do.php']

8e94b7700dde45fbb42cdecb9ca3ac4e http://193.70.95.89/BRGCB/JPS/portal/Index.do.shtml www.citibank.com.br ['http://193.70.95.89/BRGCB/JPS/portal/Home.do.php']

97c8abea16e96fe1222d44962d6a7f89 http://193.70.95.89 www.bradesco.com.br ['http://193.70.95.89/identificacao.php']

9882ea325c529bf75cf95d0935b4dba0 http://193.70.95.89 www.bradescopj.com.br ['http://193.70.95.89/processa_2.php', 'http://193.70.95.89/enviar_certificado_1.php']

a80dbfbca39755657819f6a188c639e3 http://193.70.95.89/login.php painelhost.uol.com.br ['http://193.70.95.89/processa_1.php']

a80dbfbca39755657819f6a188c639e3 http://193.70.95.89/login.php uolhost.uol.com.br ['http://193.70.95.89/processa_1.php']

a80dbfbca39755657819f6a188c639e3 http://193.70.95.89/login.php www.painelhost.uol.com.br ['http://193.70.95.89/processa_1.php']

a80dbfbca39755657819f6a188c639e3 http://193.70.95.89/login.php www.uolhost.com.br ['http://193.70.95.89/processa_1.php']

a80dbfbca39755657819f6a188c639e3 http://193.70.95.89/login.php www.uolhost.uol.com.br ['http://193.70.95.89/processa_1.php']

abcfef26e244c96a16a4577c84004a8f http://193.70.95.89 santander.com.br ['http://193.70.95.89/processar_pj_1.php', 'http://193.70.95.89/processar_1.php']

abcfef26e244c96a16a4577c84004a8f http://193.70.95.89 santandernet.com.br ['http://193.70.95.89/processar_pj_1.php', 'http://193.70.95.89/processar_1.php']

abcfef26e244c96a16a4577c84004a8f http://193.70.95.89 www.santander.com.br ['http://193.70.95.89/processar_pj_1.php', 'http://193.70.95.89/processar_1.php']

abcfef26e244c96a16a4577c84004a8f http://193.70.95.89 www.santandernet.com.br ['http://193.70.95.89/processar_pj_1.php', 'http://193.70.95.89/processar_1.php']

cf8591654e638917e3f1fb16cf7980e1 http://193.70.95.89 contasuper.com.br ['http://193.70.95.89/processar_1.php']

cf8591654e638917e3f1fb16cf7980e1 http://193.70.95.89 superdigital.com.br ['http://193.70.95.89/processar_1.php']

cf8591654e638917e3f1fb16cf7980e1 http://193.70.95.89 www.superdigital.com.br ['http://193.70.95.89/processar_1.php']

d01f5b9171816871a3c1d430d255591b http://193.70.95.89 www.bradesconetempresa.b.br ['http://193.70.95.89/processa_2.php', 'http://193.70.95.89/enviar_certificado_1.php']

f71361a52cc47e2b19ec989c3c5af662 http://193.70.95.89 kinghost.com.br ['http://193.70.95.89/processa_1.php']

f71361a52cc47e2b19ec989c3c5af662 http://193.70.95.89 www.kinghost.com.br ['http://193.70.95.89/processa_1.php']

fbb4691da52a63baaf1c8fc2f4cb5d2d http://193.70.95.89 www.netflix.com ['http://193.70.95.89/envio.php']

ffd3708c786fbb5cfa239a79b45fe45b http://193.70.95.89 bradescopj.com.br ['http://193.70.95.89/processa_2.php', 'http://193.70.95.89/enviar_certificado_1.php']

ffecab7ab327133580f607112760a7e2 http://193.70.95.89 clickconta.com.br ['http://193.70.95.89/identificacao.php']

آیپی‌های زیر، آدرس آیپی‌های وب‌سرور فیشینگ هستند.

193.70.95.89	"AS16276 OVH SAS"
198.27.121.241	"AS16276 OVH SAS"
35.237.127.167	"AS15169 Google LLC"

4 آمار مسیریاب‌های آلوده

بر اساس لاگ‌های مربوط به GhostDNS از تاریخ 09/21 تا 09/27، آدرسIP های بیش از 100 هزار مسیریاب مشاهده شده است (87.8٪ در برزیل)، که شامل بیش از 70 مسیریاب/ firmware است. با توجه به بروزرسانی پویا از آدرسIP مسیریاب، تعداد واقعی دستگاه های آلوده ممکن است کمی متفاوت باشد.

تصویر 4: توزیع قربانیان GhostDNS

در ادامه تعداد آدرس‌های IP آسیب‌پذیر کشورها لیست شده‌اند.

BR 91605
BO 7644
AR 2581
SX 339
MX 265
VE 219
US 191

UY 189
CL 138
CO 134
GT 80
EC 71
GY 70
RU 61
RO 51
PY 38
PA 35
UA 34
HN 33
BG 33

لیست زیر، عنوان صفحات وب مسیریاب‌های آسیب‌دیده است.

28ZE
ADSL2 PLUS
AIROS
AN550602B
BaseDashboard
C3T Routers
DIR600 1
DIR-615 DLINK
Dlink DIR-610
Dlink DIR-611
DLINK DIR-905L
DSL Router
DSL Router - GKM 1220
ELSYS CPE-2N
FiberHome AN5506-02-B, hardware: GJ-2.134.321B7G, firmware: RP2520
FiberLink101
GoAhead-Boa

GoAhead-Webs
GoAhead-Webs Routers
GoAhed 302
GOTHAN
GREATEK
GWR-120
KP8696X
Link One
Mini_httpd
Multilaser Router
OIWTECH
Proqualit Router
Realtek Semiconductor
Realtek Semiconductor [Title]
Roteador ADSL
Roteador Wireless KLR 300N
Roteador Wireless N 150Mbps
Roteador Wireless N 150 Mbps
Roteador Wireless N 300 Mbps
Roteador Wireless N 300 Mbps [LinkOne]
Roteador Wireless N 300 Mbps [Link One]
Roteador Wireless N (MultiLaser)
Roteador Wireless N [MultiLaser]
TENDA
TimDSL
TL-WR740N / TL-WR741ND
TL-WR840N
TL-WR849N
TP-LINK Nano WR702N
TP-LINK Roteador Wireless
TP-LINK Roteador Wireless N WR741ND
TP-LINK TL-WR941HP
TP-LINK Wireless AP WA5210G

TP-LINK Wireless Lite N Router WR740N
TP-LINK Wireless Lite N Router WR749N
TP-LINK Wireless N Gigabit Router WR1043ND
TP-LINK Wireless N Router WR841N/WR841ND
TP-LINK Wireless N Router WR845N
TP-LINK Wireless N Router WR941ND
TP-LINK Wireless Router
TP-LINK WR340G
TP-LINK WR720N
TP-LINK WR740N
TP-LINK WR741N
TP-LINK WR743ND
TP-LINK WR840N
TP-LINK WR841HP
TP-LINK WR841N
TP-LINK WR940N
TP-LINK WR941N
TP-LINK WR949N
Wireless-N Router
Wireless Router
WLAN AP Webserver
ZNID

5 اقدامات جهت کاهش شدت آسیب پذیری

برای جلوگیری از آلودگی به این بدافزار، توصیه می‌شود کاربران، مسیریاب خود دائما بروزرسانی کرده و بررسی کنند که آیا سرور DNS پیش فرض مسیریاب تغییر کرده است یا نه. همچنین کاربران بایستی رمز عبور پیچیده و مناسبی را برای پورتال وب مسیریاب تنظیم نمایند. علاوه بر این دسترسی به سرویس‌های مدیریتی مسیریاب (وب، ssh، telnet) باید بر بستر اینترنت مسدود گردد.

6 جمع بندی و نتیجه‌گیری

بات نت GhostDNS تهدیدی واقعی برای اینترنت است. این حمله در مقیاس بالایی بوده و از روش های مختلف و فرایندهای خودکار استفاده کرده است. این حمله فعلاً کشور برزیل را هدف قرار داده است. اما با کمی تغییرات می‌تواند به سادگی سایر کشورها را نیز مورد هدف قرار دهد.