Ghost DNS Malware

BCSC_ALERTA_GHOST_DNS_MALWARE

www.basquecybersecurity.eus

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

Octubre de 2018

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

Cláusula de prohibición de venta

1. SOBRE EL BCSC

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca en la Agencia Vasca de Desarrollo Empresarial (en adelante Grupo SPRI), sociedad dependiente del Departamento de desarrollo Económico e Infraestructuras del Gobierno Vasco. El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Desarrollo Económico e Infraestructuras, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad incluye proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de su Comité Permanente.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

2. RESUMEN EJECUTIVO

Los investigadores de seguridad Netlab han descubierto un malware que se ha apoderado de más de 100.000 routers en Sudamérica y 50 páginas web, accediendo así a credenciales de inicio de sesión en múltiples plataformas, incluyendo instituciones bancarias.

Los routers afectados por este ataque son inyectados con código malicioso que redirige el tráfico a páginas de phishing o de malware, webs que parecen legítimas pero que en realidad no lo son, engañando a miles de usuarios que ingresaron sus credenciales en las mencionadas páginas falsas.

3. ANÁLISIS TÉCNICO

3.1. Recursos afectados

Más de 100.000 routers se han visto afectados por este malware, estando el 87.8% ubicados en Brasil. Así mismo, más de 50 dominios han sido secuestrados, incluyendo Netflix, Citibank.br y grandes entidades bancarias. La mayoría de los equipos afectados son Windows.

Los siguientes son los modelos de routers y/o Firmwares afectados por el malware:

- 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. Detalles generales

Se ha desarrollado un nuevo tipo de DNS changer, más potente y con mayor capacidad de propagación que los que se ha visto hasta el momento en otros tipos de ataques similares. Un DNS changer es un malware que modifica la configuración de un dispositivo o equipo, y en el caso concreto de un router redirigiendo el tráfico legitimo a webs ilegitimas.

Para poner esto en perspectiva, DNS es un servicio de Internet que convierte los nombres de dominio fáciles de usar en las direcciones IP numéricas que los ordenadores usan para comunicarse entre sí. Cuando se ingresa un nombre de dominio en la barra de direcciones del navegador, el ordenador se comunica con los servidores DNS para determinar la dirección IP de la web que desea visitar, así el ordenador usa esta dirección para conectarse. Los servidores DNS son operados por los proveedores de servicios de Internet (ISP) y están incluidos en la configuración de red del ordenador.

Lo primero que hace el malware es escanear direcciones IP en busca de routers que tengan contraseñas débiles o inexistentes, de modo que o bien la averigua o bien la elude a través de un exploit conocido como *dnscfg.cgi*. Una vez que accede a los routers, modifica la configuración DNS de los mismos.

El sistema GhostDNS consta de cuatro partes: módulo DNSChanger, módulo web de phishing, módulo Web Admin, módulo Rogue DNS.

DNSChanger es el módulo principal de GhostDNS, siendo el responsable de la recopilación y explotación de la información. Este módulo incluye más de 100 scripts maliciosos que afectan a 70 modelos de router diferentes.

El Shell DNSChanger es una combinación de 25 scripts maliciosos de Shell que afectan al firmware de 21 modelos distintos de router. Este submódulo utiliza un programa de terceros, Fast HTTP Auth Scanner v0.6 (FScan) para realizar la exploración. Se configura con una gran cantidad de reglas de escaneo, una lista de contraseñas de usuario y algunos scripts de inicio. El rango de direcciones IP de exploración de Fscan es una lista de segmentos de red seleccionados, la mayoría de los cuales se atribuyen a Brasil, lo que no evita que se pueda modificar y añadir rangos IP de otros países o sectores en el futuro.

Después de la exploración inicial, este submódulo utiliza la información recopilada para evadir las medidas de autenticación de los routers y acceder así a su configuración. En caso de tener éxito, la dirección de DNS predeterminada en el router se cambiará por otra correspondiente a un servidor de DNS fraudulento.

La estructura del Shell DNSChanger es la siguiente:

```
├── 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
```

Por otro lado, Js DNSChanger, escrito principalmente en Javascript, está compuesto por 10 scripts de ataque, que pueden infectar 6 modelos diferentes de routers. Su estructura funcional se divide principalmente en escáneres, generadores de carga útil y programas de ataque.

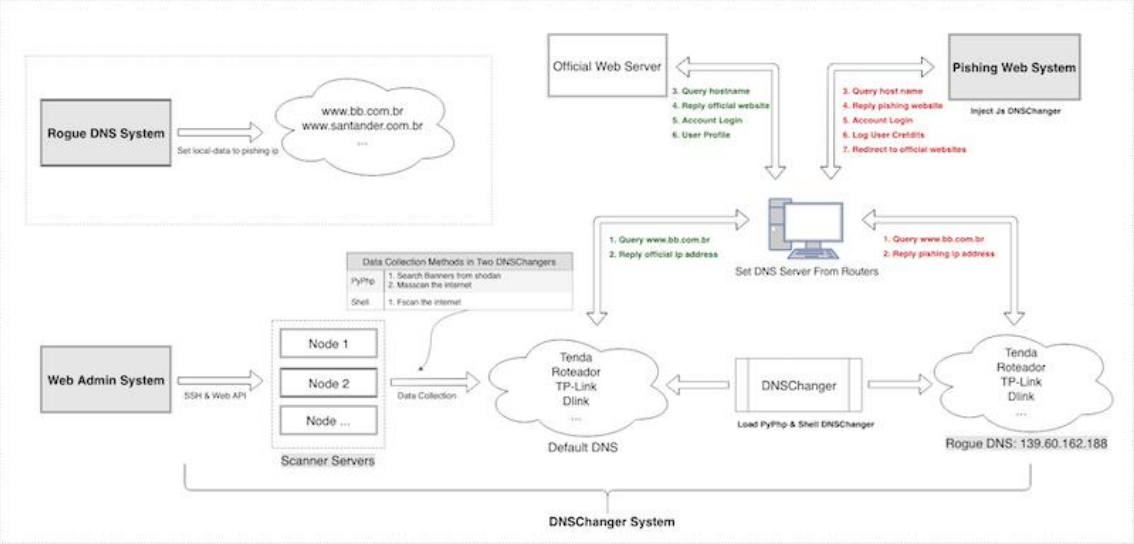
Por último está el módulo PyPhp DNSChanger, el cual es el módulo principal DNSChanger. Se ha descubierto que el/los atacante/s ha/n implementado este

programa en más de 100 servidores, la mayoría de los cuales están alojados en Google Cloud. Este submódulo se desarrolló en abril del 2018, utilizando python y php, y se compone principalmente de tres partes:

- **API web:** A través de la cual el atacante puede controlar el programa de manera conveniente.
- **Escáner:** El escáner utiliza tanto el escaneo de puertos de Masscan como el servicio de API de Shodan.

  Módulo de ataque: El módulo de ataque incluye 69 scripts de ataque contra 47 routers diferentes.

La siguiente imagen muestra el proceso de la infección:



Se han descubierto 52 dominios que han sido secuestrados por el malware. A continuación, se muestran los detalles de los mismos:


```
{"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"]}
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."
```

El malware modifica el registro del sistema e incluye las siguientes entradas:

- [HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces] "NameServer"
- HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{random} DhcpNameServer = 85.255.xx.xxx,85.255.xxx.xxx
- HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{random} NameServer = 85.255.xxx.133,85.255.xxx.xxx
- HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ DhcpNameServer = 85.255.xxx.xxx,85.255.xxx.xxx
- HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ NameServer = 85.255.xxx.xxx,85.255.xxx.xxx

3.3. Vector de entrada

El vector de entrada del malware es a través de las credenciales inseguras de los routers.

4. MITIGACIÓN / SOLUCIÓN

4.1. Indicadores de compromiso

Si hemos sido infectados por este malware lo que debemos hacer es restaurar la lista DNS de todos los dispositivos afectados. Casi todos los routers en el mercado tienen una página de configuración donde se pueden definir los servidores DNS. En la mayoría de los casos, los servidores DNS son dictados por el proveedor de servicios de Internet (ISP) y la configuración de DNS en el router estará vacía, pero es posible anular los servidores DNS del ISP configurando servidores DNS específicos en el router, que es exactamente lo que el malware del DNS Changer busca hacer. Hay dos pasos para determinar si el router ha sido infectado:

1. Comprobar la configuración de DNS en el router. Si no están vacíos, entonces:
2. Confirmar si los servidores DNS listados son maliciosos o al menos desconocidos.

El DNS predeterminado podría ser 8.8.8.8 o 8.8.4.4.

Es recomendable también comprobar los ajustes DNS del propio ordenador. Para ello debemos:

Apple

Apple → Preferencias del Sistema → Red → *Seleccionar la red* → Advance

Windows

Panel de control → Red e Internet → Conexiones de Red → Propiedades

A continuación, se enumeran los Indicadores de Compromiso más relevantes descubiertos por la investigación llevada a cabo por Netlab:

```
#Pishing Web Server
[takendown] 193.70.95.89                "AS16276 OVH SAS"
[takendown] 198.27.121.241              "AS16276 OVH SAS"
[takendown] 35.237.127.167              "AS15169 Google LLC"

#Rogue DNS Server
139.60.162.188              "AS395839 HOSTKEY"
139.60.162.201              "AS395839 HOSTKEY"
173.82.168.104              "AS35916 MULTACOM CORPORATION"
18.223.2.98                 "AS16509 Amazon.com, Inc."
185.70.186.4                "AS57043 Hostkey B.v."
200.196.240.104             "AS11419 Telefonica Data S.A."
200.196.240.120             "AS11419 Telefonica Data S.A."
80.211.37.41                "AS31034 Aruba S.p.A."
```

```
[takendown] 35.185.9.164                "AS15169 Google LLC"
[takendown] 144.22.104.185              "AS7160 Oracle Corporation"
[takendown] 192.99.187.193              "AS16276 OVH SAS"
[takendown] 198.27.121.241              "AS16276 OVH SAS"

#Web Admin Server
[takendown] 198.50.222.139             "AS16276 OVH SAS"
#DNSChanger Scanner Server
[takendown] 104.196.177.180             "AS15169 Google LLC"
[takendown] 104.196.232.200             "AS15169 Google LLC"
[takendown] 104.197.106.6               "AS15169 Google LLC"
[takendown] 104.198.54.181              "AS15169 Google LLC"
[takendown] 104.198.77.60               "AS15169 Google LLC"
[takendown] 198.50.222.139              "AS16276 OVH SAS"
[takendown] 35.185.127.39               "AS15169 Google LLC"
[takendown] 35.185.9.164                "AS15169 Google LLC"
[takendown] 35.187.149.224              "AS15169 Google LLC"
[takendown] 35.187.202.208              "AS15169 Google LLC"
[takendown] 35.187.238.80               "AS15169 Google LLC"
[takendown] 35.188.134.185              "AS15169 Google LLC"
[takendown] 35.189.101.217              "AS15169 Google LLC"
[takendown] 35.189.125.149              "AS15169 Google LLC"
[takendown] 35.189.30.127               "AS15169 Google LLC"
[takendown] 35.189.59.155               "AS15169 Google LLC"
[takendown] 35.189.63.168               "AS15169 Google LLC"
[takendown] 35.189.92.68                "AS15169 Google LLC"
[takendown] 35.194.197.94               "AS15169 Google LLC"
[takendown] 35.195.116.90               "AS15169 Google LLC"
[takendown] 35.195.176.44               "AS15169 Google LLC"
[takendown] 35.196.101.227              "AS15169 Google LLC"
[takendown] 35.197.148.253              "AS15169 Google LLC"
[takendown] 35.197.172.214              "AS15169 Google LLC"
[takendown] 35.198.11.42                "AS15169 Google LLC"
[takendown] 35.198.31.197               "AS15169 Google LLC"
[takendown] 35.198.5.34                 "AS15169 Google LLC"
[takendown] 35.198.56.227               "AS15169 Google LLC"
[takendown] 35.199.106.0                "AS15169 Google LLC"
[takendown] 35.199.2.186                "AS15169 Google LLC"
```

```
[takendown] 35.199.61.19                "AS15169 Google LLC"
[takendown] 35.199.66.147               "AS15169 Google LLC"
[takendown] 35.199.77.82                "AS15169 Google LLC"
[takendown] 35.200.179.26               "AS15169 Google LLC"
[takendown] 35.200.28.69                "AS15169 Google LLC"
[takendown] 35.203.111.239              "AS15169 Google LLC"
[takendown] 35.203.135.65               "AS15169 Google LLC"
[takendown] 35.203.143.138              "AS15169 Google LLC"
[takendown] 35.203.167.224              "AS15169 Google LLC"
[takendown] 35.203.18.30                "AS15169 Google LLC"
[takendown] 35.203.183.182              "AS15169 Google LLC"
[takendown] 35.203.25.136               "AS15169 Google LLC"
[takendown] 35.203.3.16                 "AS15169 Google LLC"
[takendown] 35.203.48.110               "AS15169 Google LLC"
[takendown] 35.203.5.160                "AS15169 Google LLC"
[takendown] 35.203.8.203                "AS15169 Google LLC"
[takendown] 35.204.146.109              "AS15169 Google LLC"
[takendown] 35.204.51.103               "AS15169 Google LLC"
[takendown] 35.204.77.160               "AS15169 Google LLC"
[takendown] 35.204.80.189               "AS15169 Google LLC"
[takendown] 35.205.148.72               "AS15169 Google LLC"
[takendown] 35.205.24.104               "AS15169 Google LLC"
[takendown] 35.221.110.75               "AS19527 Google LLC"
[takendown] 35.221.71.123               "AS19527 Google LLC"
[takendown] 35.227.25.22                "AS15169 Google LLC"
[takendown] 35.228.156.223              "AS15169 Google LLC"
[takendown] 35.228.156.99               "AS15169 Google LLC"
[takendown] 35.228.240.14               "AS15169 Google LLC"
[takendown] 35.228.244.19               "AS15169 Google LLC"
[takendown] 35.228.73.198               "AS15169 Google LLC"
[takendown] 35.228.90.15                "AS15169 Google LLC"
[takendown] 35.230.104.237              "AS15169 Google LLC"
[takendown] 35.230.158.25               "AS15169 Google LLC"
[takendown] 35.230.162.54               "AS15169 Google LLC"
[takendown] 35.230.165.35               "AS15169 Google LLC"
[takendown] 35.231.163.40               "AS15169 Google LLC"
[takendown] 35.231.60.255               "AS15169 Google LLC"
[takendown] 35.231.68.186               "AS15169 Google LLC"
```

```
[takendown] 35.232.10.244                "AS15169 Google LLC"
[takendown] 35.234.131.31                "AS15169 Google LLC"
[takendown] 35.234.136.116               "AS15169 Google LLC"
[takendown] 35.234.156.85                "AS15169 Google LLC"
[takendown] 35.234.158.120               "AS15169 Google LLC"
[takendown] 35.234.77.117                "AS15169 Google LLC"
[takendown] 35.234.89.25                 "AS15169 Google LLC"
[takendown] 35.234.94.97                 "AS15169 Google LLC"
[takendown] 35.236.117.108               "AS15169 Google LLC"
[takendown] 35.236.2.49                  "AS15169 Google LLC"
[takendown] 35.236.222.1                 "AS15169 Google LLC"
[takendown] 35.236.246.82                "AS15169 Google LLC"
[takendown] 35.236.25.247                "AS15169 Google LLC"
[takendown] 35.236.254.11                "AS15169 Google LLC"
[takendown] 35.236.34.51                 "AS15169 Google LLC"
[takendown] 35.237.127.167               "AS15169 Google LLC"
[takendown] 35.237.204.11                "AS15169 Google LLC"
[takendown] 35.237.215.211               "AS15169 Google LLC"
[takendown] 35.237.32.144                "AS15169 Google LLC"
[takendown] 35.237.68.143                "AS15169 Google LLC"
[takendown] 35.238.4.122                 "AS15169 Google LLC"
[takendown] 35.238.74.24                 "AS15169 Google LLC"
[takendown] 35.240.156.17                "AS15169 Google LLC"
[takendown] 35.240.212.106               "AS15169 Google LLC"
[takendown] 35.240.234.169               "AS15169 Google LLC"
[takendown] 35.240.94.181                "AS15169 Google LLC"
[takendown] 35.241.151.23                "AS15169 Google LLC"
[takendown] 35.242.134.99                "AS15169 Google LLC"
[takendown] 35.242.140.13                "AS15169 Google LLC"
[takendown] 35.242.143.117               "AS15169 Google LLC"
[takendown] 35.242.152.241               "AS15169 Google LLC"
[takendown] 35.242.203.94                "AS15169 Google LLC"
[takendown] 35.242.245.109               "AS15169 Google LLC"
[takendown] 40.74.85.45                  "AS8075 Microsoft Corporation"
```

4.2. Protección

No se debe confiar siempre del todo en la resolución DNS que realiza el dispositivo de red. Siempre se debe emplear correctamente los DNS corporativos o bien emplear DNS fiables, como OpendNS o Google DNS.

Se debe actualizar la versión del firmware en los dispositivos afectados por las marcas y modelos indicados. Aun limpiando adecuadamente el ordenador con un escaneo anti-malware si continuamos con la misma versión, corremos el riesgo de infectarnos de nuevo.

Por el momento, los fabricantes de dichos routers no han publicado un parche concreto, por ello debemos mantener nuestros sistemas actualizados tan reciente como sea posible.

Otra medida de protección importante para cualquier ataque Phishing es usar siempre https. Los atacantes no deberían obtener un certificado legítimo de dominios que no les pertenecen, por lo que los usuarios que habiliten esta opción como restricción de acceso, serán en gran medida protegidos de ellos.

Es importante que los usuarios sean conscientes de estas amenazas para que puedan tomar las medidas de protección básicas al navegar. Debemos comprobar siempre las URL de las páginas webs que visitamos, que efectivamente correspondan al DNS legítimo. Para ello puede añadirse alguna extensión al navegador, como por ejemplo HTTP Everywhere que garanticen una conexión https fiable.

Recordar igualmente que la mejor protección es cambiar la contraseña de administrador del router periódicamente y emplear sistemas complejos.

Si se ha sido infectado y se ha encontrado servidores DNS maliciosos en el router o en la configuración local de DNS, es probable que igualmente se encuentre instalado malware en el sistema. Se deberá escanear el ordenador con algún programa anti-malware fiable y asegurarse de su limpieza. Una vez hecho, se deberá volver a comprobar los ajustes DNS del router y el equipo.

Se debera llevar a cabo los siguientes pasos para la eliminación completa en un dispositivo infectado:

1. Deshabilitar System Restore (Windows Me/XP).
2. Actualizar la base de datos de virus
3. Ejecutar un escaneo completo del equipo
4. Borrar posibles valores añadidos en el registro
5. Borrar entradas añadidas en la lista del archivo RAS

5. REFERENCIAS

http://blog.netlab.360.com/70-different-types-of-home-routers-all-together-100000-are-being-hijacked-by-ghostdns-en/

https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html

https://www.symantec.com/connect/

https://www.symantec.com/security-center/writeup/2007-011811-1222-99?tabid=3

https://www.symantec.com/connect/forums/dns-changer-malware

https://www.firstpost.com/business/home-router-infected-dns-changer-malware-2272672.html

https://asector.org/2018/10/02/ghostdns-botnet-malware-affecting-100000-routers-so-far/

https://asector.org/2018/10/02/ghostdns-botnet-malware-affecting-100000-routers-so-far/

https://www.enigmasoftware.com/ghostdns-removal/

https://amp.thehackernews.com/thn/2018/10/ghostdns-botnet-router-hacking.html?__twitter_impression=true

https://securityboulevard.com/2018/10/100k-routers-hijacked-for-phishing-in-ghostdns-campaign/

https://www.f-secure.com/v-descs/dnschang.shtml