VPNFilter

Malware con capacidad destructiva

BCSC_ALERTA_VPNFilter

www.basquecybersecurity.eus

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

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

Mayo de 2018

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se facilita a título meramente informativo y orientativo. En ningún caso el Basque Cybersecurity Centre será o podrá ser responsable solidaria o subsidiariamente, de cualesquiera responsabilidades, daños, pérdidas y costos sufridos o incurridos, directos o indirectos, fortuitos o extraordinarios que pudieran derivarse del uso de la información que en el mismo se contiene.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

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

Cisco Talos ha informado de una variante de malware llamado VPNFilter creado específicamente para infectar routers de uso doméstico y de pequeñas empresas utilizando para ello credenciales por defecto y vulnerabilidades conocidas.

VPNFilter tiene la capacidad de llevar a cabo la recopilación de información u operaciones destructivas y ha demostrado métodos novedosos para la persistencia del dispositivo después de reinicios y una estructura de comando y control robusta. Aunque, según se informa, comparte código con el malware "BlackEnergy" utilizado anteriormente para atacar a las empresas energéticas ucranianas, esta información no ha sido corroborada de forma independiente.

Los investigadores estiman que desde 2016 ha infectado entre 500.000 y 1.000.000 de routers en 54 países.

3. ANÁLISIS TÉCNICO

3.2 Descripción

El 23 de mayo de 2018, Cisco Talos informó de que se había identificado un malware modular denominado "VPNFilter" en más de 500.000 dispositivos de 54 países.

Los atacantes se han dirigido esta vez a routers de uso doméstico y pequeñas empresas (SOHO) incluyendo Linksys, MikroTik, NETGEAR y equipos de red TP-Link y dispositivos de almacenamiento en red (NAS) QNAP.

VPNFilter tiene capacidades para extraer datos como credenciales de sitios web y un plugin específico para monitorizar los protocolos Modbus SCADA, además de tener funcionalidades potencialmente destructivas.

Según se informa, la campaña está activa desde 2016.

3.3 Detalle Técnico

El malware VPNFilter consta de tres fases con las siguientes funcionalidades:

- Fase 1: Esta etapa asegura la persistencia en el dispositivo añadiéndose al programador de trabajos de Linux (crontab). Este malware tiene varias vías de comunicación con el C&C, incluido el acceso a un dominio específico o la espera de un paquete de activación específico. El malware descarga las etapas siguientes a través de canales SSL.
- Fase 2: Esta variante de malware no persistente recupera comandos del C&C y tiene funcionalidades que incluyen la posibilidad de reiniciar un dispositivo sobrescribiéndolo, ejecutar un comando shell o plugin, así como establecer URLs proxy y otras funciones. Esta etapa crea una carpeta de módulos y un directorio de trabajo antes de ejecutarse, y utiliza las IPs configuradas para la comunicación inicial C&C.
- Fase 3: En esta etapa se añaden plugins para dotar de funcionalidad adicional al malware. Entre ellos, los más destacables son un sniffer para monitorizar el tráfico de red con el fin de obtener credenciales y un módulo de comunicación a través de TOR.

El malware comparte código con BlackEnergy, una variante de malware utilizada para dirigir ataques destructivos contra las infraestructuras críticas de Ucrania.

El grupo tras el VPNFilter parece estar llevando a cabo una campaña de recopilación de información y reconocimiento a gran escala.

Es probable que se estén enfocados en sistemas de control industrial ya que el malware incluye funcionalidades de análisis de tráfico Modbus, un protocolo de intercambio de información entre dispositivos utilizados habitualmente en este tipo de sistemas.

3.4 Recursos afectados

Los siguientes dispositivos fueron identificados como objetivo de esta actividad:

- LINKSYS DEVICES:
  - E1200
  - E2500
  - WRVS4400N
- MIKROTIK ROUTEROS VERSIONS FOR CLOUD CORE ROUTERS:
  - 1016
  - 1036
  - 1072
- NETGEAR DEVICES:
  - DGN2200
  - R6400
  - R7000
  - R8000
  - WNR1000
  - WNR2000
- QNAP DEVICES:
  - TS251
  - TS439 Pro
- TP-LINK DEVICES:
  - R600VPN

4. MITIGACIÓN / SOLUCIÓN

Para mitigar el impacto del malware, los routers deben ser reiniciados para eliminar los plugins instalados en la segunda y tercera etapa ya que no tienen persistencia.

Así mismo, se recomienda instalar la última actualización disponible y modificar las credenciales por defecto.

4.1. Indicadores de compromiso

- URLs:

photobucket[.]com/user/nikkireed11/library

photobucket[.]com/user/kmila302/library

photobucket[.]com/user/lisabraun87/library

photobucket[.]com/user/eva_green1/library

photobucket[.]com/user/monicabelci4/library

photobucket[.]com/user/katyperry45/library

photobucket[.]com/user/saragray1/library

photobucket[.]com/user/millerfred/library

photobucket[.]com/user/jeniferaniston1/library

photobucket[.]com/user/amandaseyfried1/library

photobucket[.]com/user/suwe8/library

photobucket[.]com/user/bob7301/library

toknowall[.]com

- IPs:

91.121.109[.]209

217.12.202[.]40

94.242.222[.]68

82.118.242[.]124

46.151.209[.]33

217.79.179[.]14

91.214.203[.]144

95.211.198[.]231

195.154.180[.]60

5.149.250[.]54

91.200.13[.]76

94.185.80[.]82

62.210.180[.]229

- Dominios:

zuh3vcyskd4gipkm[.]onion

- Hashes:

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec

0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92

9683b04123d7e9fe4c8c26c69b09c2233f7e1440f828837422ce330040782d17

d6097e942dd0fdc1fb28ec1814780e6ecc169ec6d24f9954e71954eedbc4c70e

4b03288e9e44d214426a02327223b5e516b1ea29ce72fa25a2fcef9aa65c4b0b

9eb6c779dbad1b717caa462d8e040852759436ed79cc2172692339bc62432387

37e29b0ea7a9b97597385a12f525e13c3a7d02ba4161a6946f2a7d978cc045b4

776cb9a7a9f5afbaffdd4dbd052c6420030b2c7c3058c1455e0a79df0e6f7a1d

8a20dc9538d639623878a3d3d18d88da8b635ea52e5e2d0c2cce4a8c5a703db1

0649fda8888d701eb2f91e6e0a05a2e2be714f564497c44a3813082ef8ff250b

f8286e29faa67ec765ae0244862f6b7914fcdde10423f96595cb84ad5cc6b344

Afd281639e26a717aead65b1886f98d6d6c258736016023b4e59de30b7348719

d113ce61ab1e4bfcb32fb3c53bd3cdeee81108d02d3886f6e2286e0b6a006747

c52b3901a26df1680acbfb9e6184b321f0b22dd6c4bb107e5e071553d375c851

f372ebe8277b78d50c5600d0e2af3fe29b1e04b5435a7149f04edd165743c16d

be4715b029cbd3f8e2f37bc525005b2cb9cad977117a26fac94339a721e3f2a5

27af4b890db1a611d0054d5d4a7d9a36c9f52dffeb67a053be9ea03a495a9302

110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8

fb47ba27dceea486aab7a0f8ec5674332ca1f6af962a1724df89d658d470348f

b25336c2dd388459dec37fa8d0467cf2ac3c81a272176128338a2c1d7c083c78

cd75d3a70e3218688bdd23a0f618add964603736f7c899265b1d8386b9902526

110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8

909cf80d3ef4c52abc95d286df8d218462739889b6be4762a1d2fac1adb2ec2b

044bfa11ea91b5559f7502c3a504b19ee3c555e95907a98508825b4aa56294e4

c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412

8f1d0cd5dd6585c3d5d478e18a85e7109c8a88489c46987621e01d21fab5095d

d5dec646c957305d91303a1d7931b30e7fb2f38d54a1102e14fd7a4b9f6e0806

C0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412

- Regla de SNORT detectada para VPNFilter

45563 45564 46782 46783

- Regla de SNORT que protege contra las vulnerabilidades

25589 26276 26277 26278 26279 29830 29831 44743 46080 46081 46082 46083 46084 46085 46086 46287 46121 46122 46123 46124 41445 44971 46297 46298 46299 46300 46301 46305 46306 46307 46308 46309 46310 46315 46335 46340 46341 46342 46376 46377 37963 45555 46076 40063 44643 44790 26275 35734 41095 41096 41504 41698 41699 41700 41748 41749 41750 41751 44687 44688 44698 44699 45001 46312 46313 46314 46317 46318 46322 46323 40866 40907 45157

5. REFERENCIAS

https://blog.talosintelligence.com/2018/05/VPNFilter.html

https://www.cnet.com/news/hackers-infected-over-500000-routers-with-potential-to-cutoff-internet-access/

https://www.us-cert.gov/ncas/current-activity/2018/05/23/VPNFilter-Destructive-Malware

https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

https://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/