MALWARE VPNFILTER

Bogotá D.C; Colombia, 28 de Mayo de 2018
CONFIDENCIAL

MALWARE VPNFILTER

NIVEL DE ALERTA

Muy Critica
Sin CVE asociado a la fecha

IMPACTO

Recopilación de credenciales de inicio de sesión y posiblemente el control de supervisión y adquisición del tráfico de datos.

PRODUCTOS AFECTADOS

A continuación, se relacionan los dispositivos que posiblemente pueden ser vulnerables:

- Linksys E1200
- Linksys E2500
- Linksys WRVS4400N
- Mikrotik RouterOS for Cloud Core Routers: Versions 1016, 1036,1072
- Netgear DGN2200
- Netgear R6400
- Netgear R7000
- Netgear R8000
- Netgear WNR1000
- Netgear WNR2000
- QNAP TS251
- QNAP TS439 Pro
- Otros QNAP NAS dispositivos corriendo en QTS software
- TP-Link R600VPN

DESCRIPCIÓN DEL MALWARE

El **Centro de Seguridad y Vigilancia Digital** de A3SEC ha sido alertado sobre un nuevo malware llamado “VPNFilter” que recopila las credenciales de inicio de sesión y posiblemente el control de supervisión y adquisición del tráfico de datos.

El malware hace posible que los atacantes puedan crear ofuscamiento en los dispositivos y generar problemas en la conexión a los puntos finales. Los investigadores afirman que al menos parte del malware incluye un comando para desactivar permanentemente el dispositivo, lo que permitiría a los atacantes deshabilitar el acceso a Internet para cientos de miles de personas en todo el mundo o en una región centrada.

El informe de Cisco indica que VPNFilter contiene una función defectuosa que involucra el cifrado RC4 que es idéntico al encontrado en el malware conocido como BlackEnergy. BlackEnergy se ha utilizado en una variedad de ataques vinculados al gobierno ruso, incluido uno en diciembre de 2016 que causó un corte de energía en Ucrania.

El malware actua de la siguiente manera:

Etapa 1
En la primera etapa infecta los dispositivos que ejecutan el firmware basado en Busybox y Linux, y se compila para varias arquitecturas de CPU. El objetivo principal es ubicar un servidor controlado por atacante en Internet para ejecutar la segunda etapa. La etapa 1 ubica el servidor descargando una imagen de Photobucket.com y extrayendo una dirección IP de seis valores enteros utilizados para la latitud y la longitud GPS almacenadas en el campo EXIF. En caso de que la descarga de Photobucket falle, la etapa 1 intentará descargar la imagen de toknowall.com.

Si esto llegase a fallar, la etapa 1 abre un "sniffer" que espera un paquete de activación específico de los atacantes. El sniffer comprueba su IP pública desde api.ipify.org y la almacena para su uso posterior. Esta es la etapa que persiste incluso después de reiniciar el dispositivo infectado.

Etapa 2
En la segunda etapa, el malware actua como una plataforma inteligente de recopilación de información" que realiza las siguientes acciones:

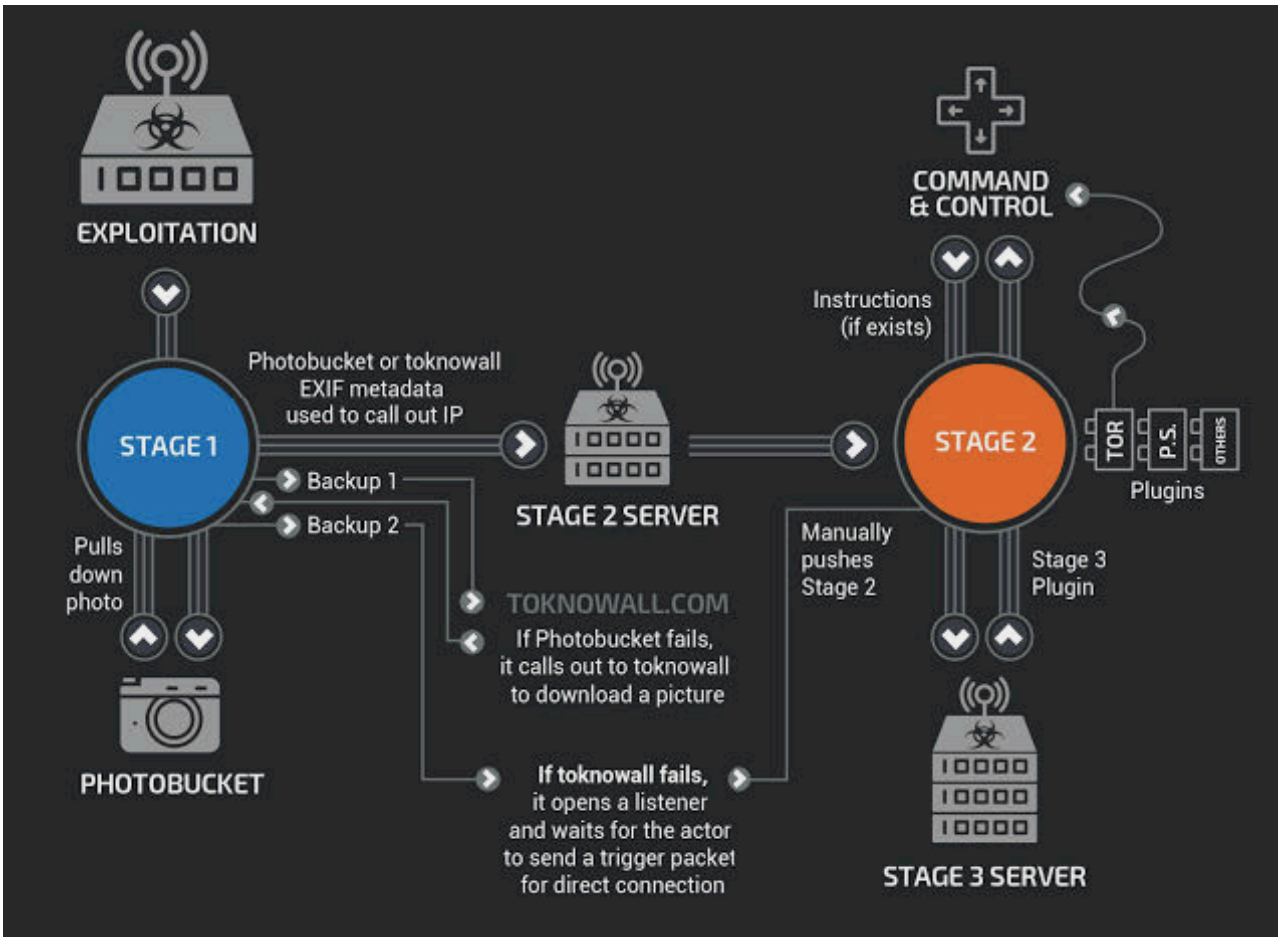
- Recopilación de archivos
- Ejecución de comandos y extracción de datos
- Administración de dispositivos.

Algunas versiones de la etapa 2, poseen una capacidad de autodestrucción que funciona sobrescribiendo una parte crítica del firmware del dispositivo y luego reiniciando, un proceso que inutiliza el dispositivo. Los investigadores de Cisco creen que, incluso sin el comando integrado kill, los atacantes pueden usar la etapa 2 para destruir dispositivos manualmente.

Etapa 3
La etapa 3 contiene al menos dos módulos de complemento de la siguiente manera:

- Un rastreador de paquetes para recoger el tráfico que pasa a través del dispositivo. El tráfico interceptado incluye credenciales del sitio web y protocolos Modbus SCADA.

- Un segundo módulo permite que la etapa 2 se comunique a través del servicio de privacidad de Tor.



SOLUCIÓN

A la fecha, **NO** se tiene una solución o parche de seguridad; los enrutadores y dispositivos NAS generalmente no reciben protección antivirus o de firewall y están conectados directamente a Internet. Si bien los investigadores todavía no saben con precisión cómo se infectan los dispositivos, casi todos los afectados tienen vulnerabilidades públicas conocidas o credenciales predeterminadas.

Cisco y Symantec aconsejan a los usuarios de los dispositivos mencionados ejecutar las siguientes accciones:

1. Restablecimiento de fábrica; con el problema de que estos restablecimientos borran todos los ajustes de configuración almacenados en el dispositivo, por lo que los usuarios tendrán que volver a ingresar la configuración una vez que el dispositivo se reinicie. Esta acción evitará que las etapas 2 y 3 se ejecuten, al menos hasta que la etapa 1 logre reinstalarlas.

2. Cambios de Contraseñas predeterminadas.

3. Actualización de los dispositivos a la última versión del firmware y si es posible deshabilitar la administración remota.

RECOMENDACIONES

Desde el Centro de Seguridad y Vigilancia Digital, se realizan las siguientes recomendaciones:

1. Si dentro de la organización se define que no se tiene la necesidad de ingresar a los dominios mencionados en el boletin, se recomienda generar el bloqueo de los mismos en el Firewall; esto como contención temporal mientras el proveedor genera el parche de seguridad o la solución definitiva para contrarestar el malware.

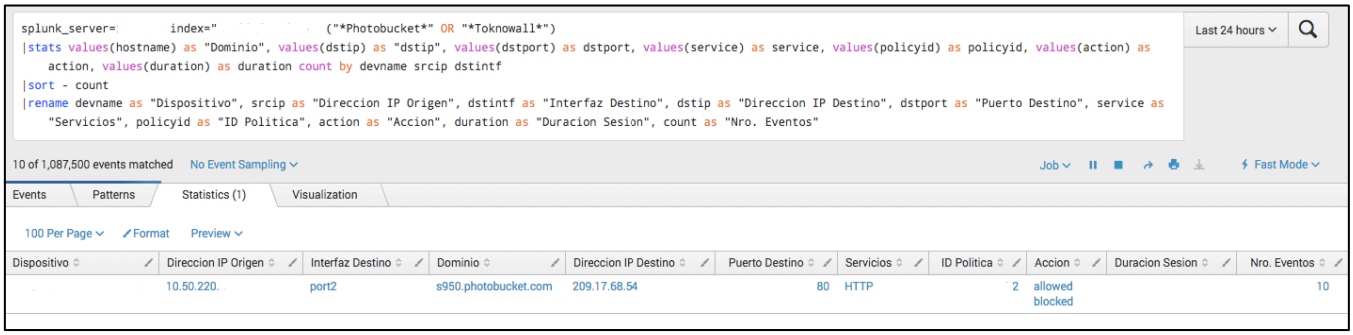
    a. Photobucket.com
    b. Toknowall.com

    Por otra parte, adjunto a este documento se comparte el listado de otros dominios, direcciones IP y hash de archivos identificados como maliciosos.

2. Si en la arquitectura de red, sus enrutadores se encuentran antes del Firewall, aplique los bloqueos de dominios y direcciones IP directamente sobre estos dispositivos en el Firewall de cada enrutador.

3. Agregue las direcciones IP y dominios mencionados del archivo adjunto a su lista de control de acceso de Botnets y Sitios maliciosos.

Desde el SIEM, se realizó la creación de una alerta que se dispare cuando se identifique trafico permitido a los dominios y direcciones IP utilizadas para la comunicación entre el atacante y el dispositivo.



REFERENCIAS

https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware

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

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

https://community.netgear.com/t5/General-WiFi-Routers/Security-Advisory-for-VPNFilter-Malware-on-Some-Routers/m-p/1576170

https://www.fortinet.com/blog/threat-research/defending-against-the-new-vpnfilter-botnet.html

A3SEC. ESPAÑA C/ Aravaca, 6 2º Piso 28040 Madrid, España T.+34 915330978	**A3SEC S.A.S** Carrera 49A # 94-76 Oficina 304 Edificio Empresarial Castellana Bogotá, COLOMBIA **T.**+57 1 3099533	**A3SEC USA** 1401 Brickell Ave #320 Miami, FL 33131, USA T. +1 786 556 90 32	**A3SEC. México** **Gral. Mariano Escobedo, 748 Piso 9 C.P. 11590 México D.F.** **T. +52 (55) 5980-3547**