FORTIBLEED

La campaña de ciberespionaje que comprometió más de 73.000 firewalls Fortinet alrededor del mundo

BeyGoo

Índice de contenidos

1. Resumen ejecutivo 3
2. Descripción General 3
3. Países, sectores y organizaciones afectadas 4
4. Factores que facilitaron la campaña 5
5. Tácticas, técnicas y procedimientos (TTPs) 5
6. Recomendaciones 6
7. Conclusión 7

1. Resumen ejecutivo

En junio de 2026 se identificó una de las **campañas de ciberespionaje automatizadas de mayor escala registradas hasta la fecha** contra infraestructura de acceso perimetral. La operación, denominada **FortiBleed**, tuvo como objetivo dispositivos **FortiGate y servicios SSL VPN expuestos a Internet**, aprovechando credenciales previamente comprometidas para obtener acceso no autorizado a redes corporativas.

De acuerdo con las investigaciones publicadas, la campaña habría afectado más de **73.900 dispositivos Fortinet distribuidos en 194 países, comprometiendo aproximadamente 21.600 dominios únicos**. La magnitud de la operación, junto con el uso de técnicas automatizadas de validación de credenciales y movimiento lateral hacia entornos internos, posiciona a FortiBleed como uno de los incidentes más relevantes del año para organizaciones que utilizan soluciones Fortinet como parte de su infraestructura de seguridad.

2. Descripción General

FortiBleed es una campaña de ciberespionaje atribuida a un grupo de actores de amenaza rusoparlantes que habrían aprovechado credenciales previamente comprometidas por infostealers para obtener acceso masivo a dispositivos FortiGate y gateways SSL VPN de Fortinet expuestos a Internet.

De acuerdo con las investigaciones publicadas, la campaña se caracterizó por una elevada capacidad operativa y un alto grado de automatización, destacándose los siguientes indicadores:

- **1,16 billones** de intentos de credential stuffing contra más de **320.000** dispositivos FortiGate
- **2,1 billones** de intentos de fuerza bruta dirigidos a más de **160.000** servidores Microsoft SQL Server.
- Se estima que entre **30.791** y **75.000** dispositivos habrían sido comprometidos mediante credenciales válidas.
- Infraestructura especializada para el descifrado de credenciales, compuesta por un clúster de 45 GPU gestionado mediante Hashtopolis, utilizado para procesar grandes volúmenes de hashes de autenticación.

Los atacantes habrían interceptado hashes de autenticación asociados a servicios SSL VPN y utilizado capacidades de procesamiento masivo para intentar descifrarlos.

Una vez obtenido el acceso inicial, los operadores realizaron movimientos laterales hacia entornos internos, particularmente infraestructuras Active Directory, con el objetivo de escalar privilegios, establecer mecanismos de persistencia y mantener acceso prolongado a las redes comprometidas.

3. Países, sectores y organizaciones afectadas

De acuerdo con la información disponible, los países con mayor cantidad de dispositivos presuntamente comprometidos fueron:

- **India**: 9.629 dispositivos.
- **Estados Unidos**: 6.352 dispositivos.
- **Taiwán**: 3.637 dispositivos.
- **México**: 3.197 dispositivos.
- **Turquía**: 3.032 dispositivos.

En cuanto a los sectores afectados, la campaña tuvo un impacto significativo sobre organizaciones de **servicios tecnológicos, telecomunicaciones, construcción, servicios financieros y entidades gubernamentales**, evidenciando el interés de los actores de amenaza por organizaciones que gestionan información crítica o desempeñan funciones estratégicas.

Uno de los incidentes más relevantes asociados a la campaña corresponde al presunto compromiso de un contratista de defensa vinculado a la OTAN en Turquía, donde se habría producido la exfiltración de documentación clasificada. Asimismo, investigadores reportaron compromisos de red en organizaciones ubicadas en Japón, Taiwán, Vietnam, Irak y Turquía, lo que demuestra el alcance global de la operación.

4. Factores que facilitaron la campaña

Uno de los principales factores que habría contribuido al éxito de la campaña está relacionado con la **gestión de credenciales en determinadas versiones de FortiOS.** Fortinet incorporó un **nuevo mecanismo de protección basado en PBKDF2** en las versiones 7.2.11, 7.4.8 y 7.6.1, sustituyendo el esquema heredado basado en SHA-256.

Sin embargo, al actualizar desde versiones anteriores, las contraseñas de administrador ya existentes pueden continuar almacenadas utilizando el mecanismo heredado hasta que cada usuario vuelva a autenticarse correctamente tras la actualización. Como consecuencia, determinados hashes podrían permanecer expuestos a técnicas de descifrado más eficientes en comparación con el nuevo esquema de protección.

De acuerdo con los investigadores, esta situación **podría afectar a dispositivos FortiGate que hayan sido actualizados desde versiones previas sin que se haya realizado una renovación efectiva de las credenciales administrativas.** Debido a que no se trata de una vulnerabilidad tradicional sino de una condición asociada a la gestión de credenciales heredadas, no existiría un parche específico para mitigar el riesgo, siendo necesaria la rotación de contraseñas y la revisión de los mecanismos de autenticación implementados.

5. Tácticas, técnicas y procedimientos (TTPs)

- **Credential Access (TA0006)**
  - Brute Force - Password Guessing (T1110.001)
  - Brute Force - Credential Stuffing (T1110.004)
  - Adversary-in-the-Middle (T1557)
  - Network Sniffing (T1040)

- **Defense Evasion (TA0030)**
  - Valid Accounts (T1078)

- **Lateral Movement (TA0109)**
  - Remote Services (T1021)

- **Discovery (TA0102)**
  - Remote System Discovery (T1018)

- **Reconnaissance (TA0043)**
  - Gather Victim Network Information (T1590)

- **Impact (TA0105)**
  - Data Encrypted for Impact (T1486)

- **Exfiltration (TA0010)**

- Exfiltration Over C2 Channel (T1041)

Herramienta asociada a la campaña, utilizada en las tácticas TA0006:

Hashtopolis es una plataforma de administración y distribución de tareas utilizada para la gestión centralizada de procesos de recuperación y descifrado de credenciales. Se basa en la arquitectura cliente-servidor, permite distribuir cargas de trabajo entre múltiples equipos o GPU, optimizando el procesamiento de grandes volúmenes de hashes de autenticación.

Si bien se trata de una herramienta legítima utilizada en entornos de auditoría y pruebas de seguridad, también puede ser empleada con fines maliciosos para acelerar procesos de descifrado de contraseñas a gran escala. Su capacidad para distribuir tareas entre múltiples sistemas permite incrementar significativamente la velocidad y eficiencia de los ataques dirigidos a credenciales comprometidas.

6. Recomendaciones

Con el objetivo de reducir el riesgo de compromiso y detectar posibles accesos no autorizados, se recomienda implementar las siguientes medidas:

- Rotar de forma inmediata todas las credenciales administrativas de dispositivos Fortinet, independientemente de su nivel de complejidad o fecha de creación.

- Habilitar autenticación multifactor (MFA) para todos los accesos remotos, especialmente aquellos asociados a servicios SSL VPN y cuentas privilegiadas.

- Verificar si dominios corporativos o credenciales de la organización se encuentran incluidos en conjuntos de datos comprometidos, utilizando herramientas de validación y monitoreo especializadas.

- Revisar los registros de autenticación y administración de dispositivos FortiGate en busca de accesos inusuales, intentos de autenticación reiterados o actividades realizadas fuera de los patrones habituales.

- Auditar los registros de eventos de seguridad y monitorear la actividad de red para identificar comportamientos anómalos, movimientos laterales o comunicaciones sospechosas.

- Revisar las cuentas con privilegios elevados y validar que únicamente los usuarios autorizados mantengan acceso administrativo a los dispositivos.

- Evaluar la exposición de servicios de administración y acceso remoto a Internet, aplicando restricciones de acceso cuando sea posible.

7. Conclusión

FortiBleed pone de manifiesto el impacto que puede tener la exposición de credenciales sobre dispositivos de acceso perimetral utilizados por organizaciones de todo el mundo. De acuerdo con las investigaciones disponibles, una parte significativa de los dispositivos comprometidos continúa accesible desde Internet, lo que podría permitir a los actores de amenaza mantener o recuperar acceso a redes corporativas e infraestructuras críticas mediante credenciales previamente comprometidas.

La campaña evidencia que el riesgo no se limita a vulnerabilidades de software, sino que también depende de la adecuada gestión de credenciales, la implementación de mecanismos de autenticación robustos y el monitoreo continuo de accesos privilegiados. Asimismo, demuestra cómo el compromiso de dispositivos perimetrales puede proporcionar una vía de acceso persistente a entornos internos, incluso mucho tiempo después de la filtración inicial de credenciales.

En este contexto, la revisión de credenciales administrativas, la adopción de autenticación multifactor y la supervisión constante de la actividad en dispositivos expuestos a Internet resultan medidas fundamentales para reducir la superficie de ataque y fortalecer la seguridad de las organizaciones.

Seguinos en LinkedIn

y enterate de todas las novedades

beygooapp beygoo.io