I. DATOS GENERALES:

Clase de alerta: Ciberamenaza
Tipo de Incidente: Compromiso de credenciales / Acceso no autorizado
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Campaña FortiBleed compromete credenciales de dispositivos Fortinet expuestos a Internet - Figura referencial

FortiBleed es una campaña de ciberataque de compromiso de credenciales que afecta a dispositivos Fortinet/FortiGate expuestos a Internet. Los actores de amenaza emplean técnicas de Credential Stuffing y reutilización de credenciales previamente filtradas para obtener acceso no autorizado a servicios SSL VPN e interfaces administrativas, comprometiendo principalmente dispositivos perimetrales.

III. INTRODUCCIÓN

Investigadores de SOCRadar y Hudson Rock alertaron de una campaña de ciberataques denominada FortiBleed, en el que actores de amenaza aprovechan credenciales comprometidas, contraseñas reutilizadas y configuraciones inseguras para obtener acceso no autorizado a firewalls y concentradores VPN Fortinet. Según las investigacio-

nes publicadas hasta el momento, se estima que entre 30.000 y 74.000 urls del firewall FortiGate a nivel mundial podrían encontrarse comprometidos con 21.632 dominios afectados únicos en 194 países.

De los datos expuestos, se tiene que incluyen organizaciones de alto perfil como Samsung, Oracle, Foxconn, Comcast, Siemens, Lenovo, Spotify, Sony, así como también de objetivos gubernamentales, de telecomunicaciones, de fabricación, minoristas, logísticos y de infraestructura crítica.

IV. VECTOR DE ATAQUE

Informes de la investigación identifican al actor de amenaza como un grupo de cibercriminales de habla rusa, quienes realizaban escaneos automatizados para localizar dispositivos FortiGate y VPN accesibles públicamente, donde luego ejecutaron aproximadamente 1.16 mil millones de intentos de credenciales (Credential Stuffing) contra más de 320.000 objetivos FortiGate, junto con 2.1 mil millones de intentos adicionales de fuerza bruta dirigido a más de 160.000 servidores MySQL. Interceptaron hashes SSL VPN, los descifraron con un clúster de 45 GPU gestionado vía Hashtopolis y se movieron lateralmente hacia Active Directory.

Una vez obtenido el inicio de sesión, los atacantes lo registraron en una base de datos verificada. Posteriormente, la operación podría alimentarse por sí misma, incluido el acceso de firewall FortiGate comprometido, que puede permitir a los atacantes monitorear el tráfico VPN o de la puerta de enlace, recopilar más credenciales y reutilizarlas en ataques posteriores, método conocido como self-feeding (autopropagado).

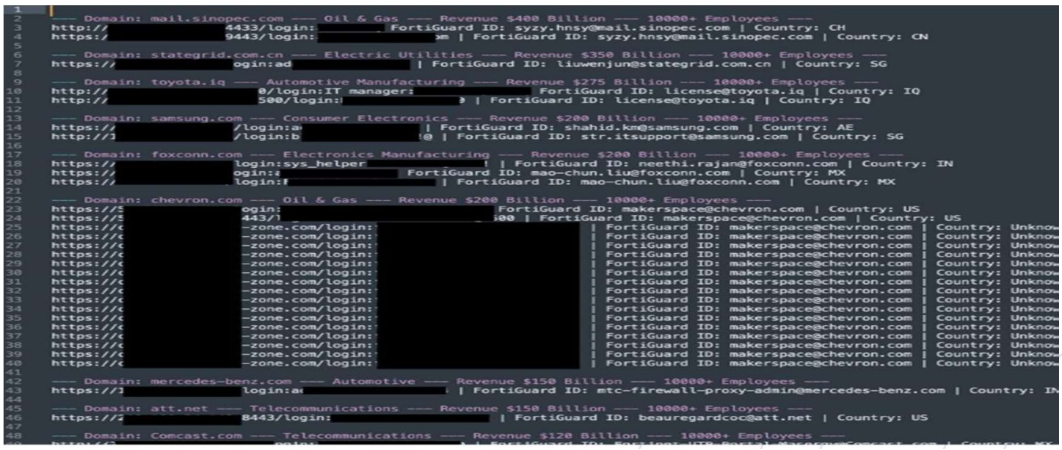

Figura 2.- Lista de entradas de inicio de sesión del firewall FortiGate, dominios afectados, ID de FortiGuard, industrias y códigos de país.

V. IMPACTO

- Fortinet FortiGate Firewalls
- Fortinet SSL-VPN
- Fortinet VPN Gateways

VI. INDICADORES DE COMPROMISO

- Inicios de sesión VPN desde ubicaciones inusuales.
- Accesos administrativos no reconocidos.
- Creación inesperada de cuentas administrativas.
- Cambios no autorizados en configuraciones FortiGate.
- Incremento anómalo de autenticaciones exitosas.
- Conexiones desde direcciones IP no habituales.
- Tráfico saliente inusual desde dispositivos Fortinet

VII. RECOMENDACIONES:

- Verificar si la organización se encuentra entre los dominios o dispositivos potencialmente comprometidos mediante la herramienta de verificación en https://www.hudsonrock.com/fortinet?page=2.
- Cambiar inmediatamente todas las credenciales VPN y administrativas asociadas a dispositivos Fortinet.
- Implementar autenticación multifactor (MFA) para accesos remotos, interfaces administrativas y cuentas privilegiadas.
- Revisar todas las cuentas administrativas configuradas y eliminar aquellas que no sean necesarias o que resulten sospechosas.
- Deshabilitar la exposición directa a Internet de las interfaces de administración de FortiGate y restringir su acceso mediante listas de IP autorizadas, hosts de confianza o VPN administrativas.
- Verificar la exposición de servicios accesibles desde Internet, incluyendo SSL VPN, HTTPS, SSH, IPsec y otros servicios de administración remota.
- Auditar los registros de acceso VPN y administrativos para identificar inicios de sesión desde ubicaciones inusuales, accesos fuera de horario, múltiples intentos fallidos seguidos de autenticaciones exitosas y cualquier actividad sospechosa.

- Revisar cambios recientes en usuarios, políticas de firewall, objetos, rutas, túneles VPN y configuraciones de seguridad para detectar modificaciones no autorizadas.
- Aplicar políticas robustas de contraseñas que eviten la reutilización de credenciales y reduzcan el riesgo de ataques de Credential Stuffing.
- Verificar si las credenciales corporativas aparecen en filtraciones conocidas y forzar su restablecimiento cuando corresponda.
- Monitorear continuamente la actividad de los dispositivos Fortinet para detectar comportamientos anómalos, tráfico inusual o intentos de acceso no autorizados.
- Mantener FortiOS y demás componentes Fortinet actualizados a las versiones más recientes recomendadas por el fabricante.
- Realizar una revisión integral de seguridad e integridad de los dispositivos potencialmente afectados para detectar accesos persistentes, configuraciones alteradas o indicadores de compromiso.
- En caso de identificar actividad maliciosa o accesos no autorizados, activar los procedimientos de respuesta a incidentes, contención, erradicación y análisis forense correspondientes.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

INFOSTEALERS (2026). *FortiBleed: 75,000 Fortinet Firewalls Compromised, Global Enterprises Exposed – Claim Your Ethical Disclosure*. https://www.infostealers.com/article/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure/

HACKREAD (2026). *FortiBleed Attack Targets Fortinet Firewalls Using Stolen Credentials*. https://hackread.com/fortibleed-attack-fortinet-firewalls-credentials/

CSIRT TELCONET (2026). *Campaña masiva de espionaje cibernético FortiBleed compromete más de 73.900 dispositivos Fortinet*. https://csirt.telconet.net/comunicacion/boletines-servicios/campana-masiva-de-espionaje-cibernetico-fortibleed-compromete-mas-de-73900-dispositivos-fortinet/

CENTRO VASCO DE CIBERSEGURIDAD (2026). *FortiBleed: 75.000 Firewalls Fortinet comprometidos a nivel mundial*. https://ciberseguridad.euskadi.eus/noticia/2026/fortibleed-75-000-firewalls-fortinet-comprometidos-a-nivel-mundial/webcyb00-contcibglos/es/