El Buró Federal de Investigación (FBI) de los Estados Unidos está emitiendo una advertencia de que los dispositivos de Barracuda Networks Email Security Gateway (ESG) que fueron actualizados para solucionar una vulnerabilidad crítica recientemente revelada siguen siendo susceptibles a posibles ataques de grupos de hackeo chinos sospechosos.

El FBI también ha calificado las correcciones como *«ineficaces»* y continúa observando intrusiones activas, considerando que todos los dispositivos Barracuda ESG afectados están comprometidos y vulnerables a este exploit.

Identificada como *CVE-2023-2868* (con una puntuación CVSS de 9.8), se afirma que esta vulnerabilidad de día cero fue utilizada como arma tan temprano como octubre de 2022, más de siete meses antes de que se solucionara el agujero de seguridad. La actividad relacionada con China en este contexto está siendo rastreada por Mandiant, una empresa propiedad de Google, bajo el nombre *UNC4841*.

Esta vulnerabilidad de inyección remota de comandos afecta a las versiones 5.1.3.001 a 9.2.0.006 y permite la ejecución no autorizada de comandos del sistema con privilegios de administrador en el producto ESG.

En los ataques observados hasta el momento, una intrusión exitosa sirve como punto de entrada para desplegar múltiples tipos de malware, como SALTWATER, SEASIDE, SEASPY, SANDBAR, SEASPRAY, SKIPJACK, WHIRLPOOL y SUBMARINE (también conocido como DEPTHCHARGE). Estos permiten la ejecución de comandos arbitrarios y evasión de las medidas de seguridad.

IP Addresses			
101.229.146.218	23.224.42.29	139.84.227.9	107.173.62.158
103.146.179.101	23.224.78.130	155.94.160.72	137.175.19.25
103.27.108.62	23.224.78.131	182.239.114.135	137.175.28.251
103.77.192.13	23.224.78.132	182.239.114.254	137.175.30.36
103.77.192.88	23.224.78.133	192.74.226.142	137.175.30.86
103.93.78.142	23.224.78.134	192.74.254.229	137.175.51.147
104.156.229.226	37.9.35.217	198.2.254.219	137.175.53.17
104.223.20.222	38.54.113.205	198.2.254.220	137.175.53.170
107.148.149.156	38.54.1.82	198.2.254.221	137.175.53.218
107.148.219.227	38.60.254.165	198.2.254.222	137.175.60.252
107.148.219.53	45.63.76.67	198.2.254.223	137.175.60.253
107.148.219.54	52.23.241.105	199.247.23.80	137.175.78.66
107.148.219.55	64.176.4.234	213.156.153.34	216.238.112.82
107.148.223.196	64.176.7.59	195.234.82.132	**54.197.109.223***
185.243.41.209*	**155.94.160.95***	**45.154.253.153***	**45.154.253.154***
173.201.39.85*			

Note: Bolded IPs are previously unidentified IOCs discovered through an FBI investigation.

> *«Los actores cibernéticos utilizaron esta vulnerabilidad para insertar cargas maliciosas en el dispositivo ESG con diversas capacidades que les permitieron mantener un acceso persistente, escanear correos electrónicos, recolectar credenciales y filtrar datos»,* declaró el FBI.

La firma de inteligencia de amenazas ha caracterizado a UNC4841 como un grupo agresivo y hábil, que demuestra sofisticación y se adapta rápidamente a su arsenal personalizado para utilizar mecanismos adicionales de persistencia y mantener su presencia en objetivos de alta prioridad.

La agencia federal está recomendando a los clientes que aíslen y reemplacen de inmediato

todos los dispositivos ESG afectados, además de escanear las redes en busca de tráfico saliente sospechoso.

Actualización:

Barracuda Networks compartió la siguiente declaración con The Hacker News:

> *«Barracuda mantiene su orientación constante para los clientes. Como medida de precaución y para apoyar nuestra estrategia de contención, recomendamos a los clientes afectados que reemplacen su dispositivo comprometido. Si un cliente ha recibido una notificación en la interfaz de usuario o ha sido contactado por un representante de soporte técnico de Barracuda, debe ponerse en contacto con support@barracuda[.]com para obtener un dispositivo ESG de reemplazo. Barracuda proporciona el producto de reemplazo a los clientes afectados sin costo alguno».*

> *«Hemos notificado a los clientes afectados por este incidente. Si un dispositivo ESG muestra una notificación en la interfaz de usuario, el dispositivo ESG tenía indicadores de compromiso. Si no se muestra ninguna notificación, no tenemos motivos para creer que el dispositivo haya sido comprometido en este momento. Nuevamente, solo un subconjunto de dispositivos ESG se vio afectado por este incidente.»*