Un grupo de hackers con presuntos vínculos chinos ha aprovechado una reciente vulnerabilidad de día cero en los dispositivos de Barracuda Networks Email Security Gateway (ESG) para infiltrarse en sectores como el gubernamental, militar, de defensa, aeroespacial, tecnológico y de telecomunicaciones como parte de una campaña global de espionaje.

Mandiant, que sigue la actividad bajo el nombre UNC4841, describió al actor de amenazas como *«altamente receptivo a los esfuerzos defensivos»* y capaz de modificar activamente su modus operandi para mantener el acceso constante a sus objetivos.

> *«UNC4841 ha desplegado un malware nuevo y novedoso diseñado para mantener una presencia en un pequeño grupo selecto de objetivos de alta prioridad que comprometieron antes de que se lanzara el parche, o poco después de que Barracuda emitiera pautas de remediación»,* informó la firma de inteligencia de amenazas propiedad de Google en un nuevo informe técnico publicado hoy.

Cerca de un tercio de las organizaciones afectadas identificadas son agencias gubernamentales. Curiosamente, algunas de las intrusiones iniciales parecen haber ocurrido en un número reducido de dispositivos ubicados en la China continental.

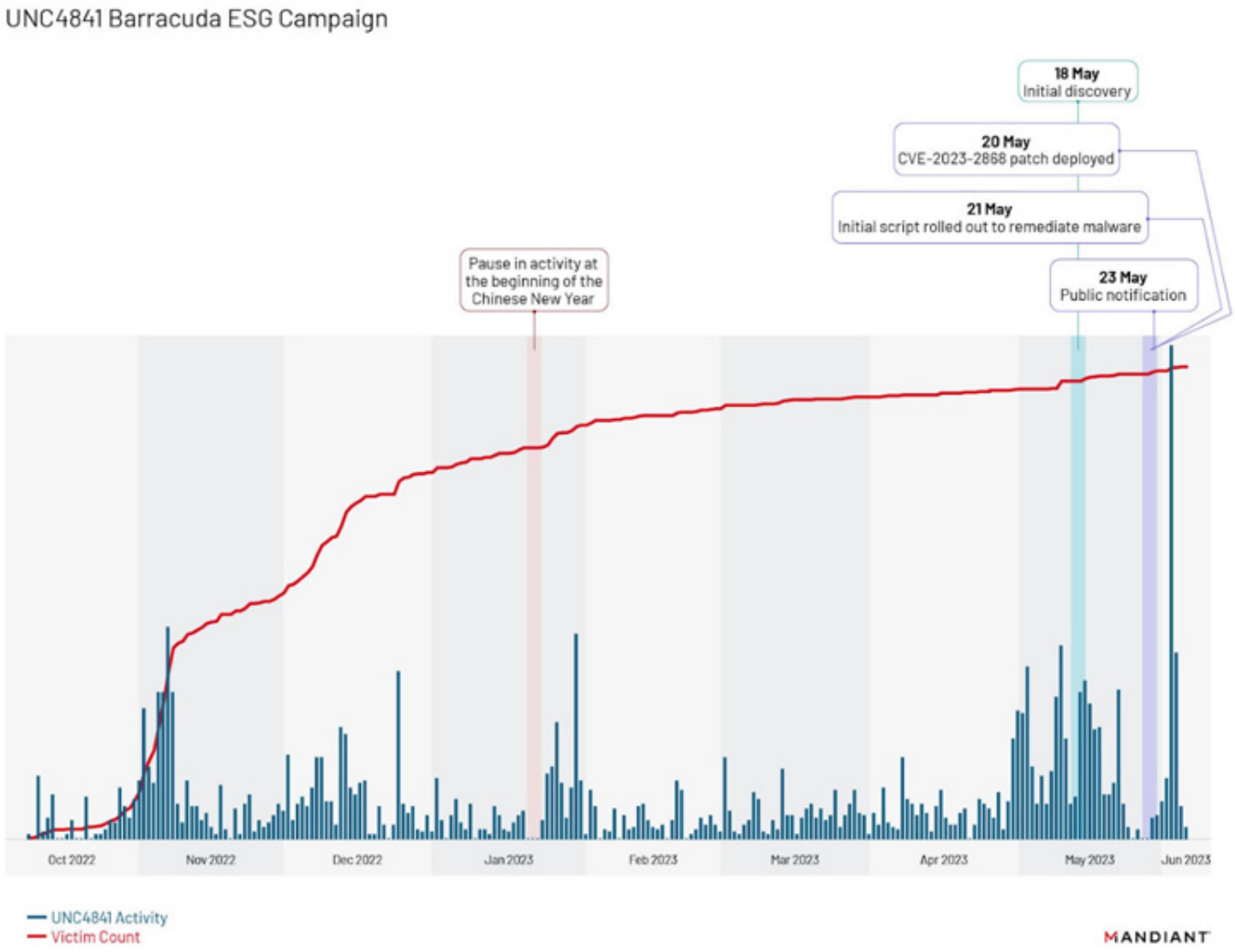
Los ataques implican la explotación de la CVE-2023-2868 para desplegar malware y llevar a cabo actividades posteriores a la explotación. En casos específicos, las intrusiones han resultado en la implementación de malware adicional, como SUBMARINE (también conocido como DEPTHCHARGE), para mantener la persistencia en respuesta a los esfuerzos de remediación.

Un análisis adicional de la campaña ha revelado una *«notable disminución en la actividad desde aproximadamente el 20 hasta el 22 de enero de 2023»,* coincidiendo con el comienzo del Año Nuevo Chino, seguida de dos oleadas, una después de la notificación pública de Barracuda el 23 de mayo de 2023 y otra a principios de junio de 2023.

Se dice que esta última involucró al atacante *«intentando mantener el acceso a entornos*

comprometidos mediante la implementación de nuevas familias de malware como SKIPJACK, DEPTHCHARGE y FOXTROT / FOXGLOVE».

Mientras SKIPJACK es un implante pasivo que registra un receptor para encabezados de correo electrónico específicos antes de descifrar y ejecutar su contenido, DEPTHCHARGE se carga previamente en el daemon Barracuda SMTP (BSMTP) utilizando la variable de entorno LD_PRELOAD y recopila comandos cifrados para su ejecución.



El primer registro de uso de DEPTHCHARGE se remonta al 30 de mayo de 2023, apenas unos días después de que Barracuda hiciera pública la vulnerabilidad. Mandiant informó que observó cómo el malware se propagaba rápidamente en un grupo limitado de objetivos, indicando un alto grado de preparación y un intento de mantenerse dentro de entornos de alto valor.

> *«Esto también sugiere que a pesar de que esta operación tenía alcance global, no fue oportunista, y que UNC4841 había planificado y financiado adecuadamente para anticipar y prepararse para posibles contingencias que pudieran interrumpir su acceso a las redes objetivo»*, explicó la empresa.

Se estima que alrededor del 2.64 por ciento del total de dispositivos comprometidos fueron infectados con DEPTHCHARGE. Estos objetivos abarcan entidades gubernamentales tanto de Estados Unidos como de otros países, además de proveedores de tecnología de la información y empresas de alta tecnología.

La tercera variedad de malware, también distribuida de forma selectiva entre los objetivos, es FOXTROT, un implante en C++ que se pone en marcha mediante un programa en C denominado FOXGLOVE. Utilizando TCP para comunicarse, este malware incluye funciones para registrar pulsaciones de teclas, ejecutar comandos de shell, transferir archivos y establecer una conexión de shell inversa.

Además, FOXTROT presenta similitudes con un rootkit de código abierto llamado Reptile, el cual ha sido ampliamente utilizado por varios grupos de hackers chinos en los últimos meses. Esto también incluye a UNC3886, un actor de amenazas relacionado con la explotación de una vulnerabilidad de seguridad de gravedad media, ya corregida, en el sistema operativo Fortinet FortiOS.

> *«FOXTROT y FOXGLOVE también destacan en que son las únicas familias de malware observadas utilizadas por UNC4841 que no fueron diseñadas*

> *específicamente para Barracuda ESGs. Por sus capacidades, es probable que FOXTROT también estuviera destinado a ser desplegado en otros dispositivos basados en Linux dentro de una red para facilitar el movimiento lateral y el robo de credenciales»,* señaló Mandiant.

Otro aspecto destacado de FOXTROT y FOXGLOVE es que fueron los más selectivamente utilizados entre todas las familias de malware empleadas por UNC4841, utilizándolos exclusivamente para dirigirse a organizaciones gubernamentales o relacionadas con el gobierno.

También se ha detectado que este grupo ha llevado a cabo tareas de reconocimiento interno y acciones posteriores de movimiento lateral en un número limitado de entornos de víctimas. En más de un caso, utilizaron Microsoft Outlook Web Access (OWA) para intentar acceder a las cuentas de correo de los usuarios dentro de las organizaciones.

Como una forma alternativa de acceso remoto, este actor de amenazas avanzadas (APT) creó cuentas que contenían cuatro caracteres generados aleatoriamente en el archivo etc/passwd en aproximadamente el cinco por ciento de los dispositivos que previamente habían sido afectados.

La conexión de UNC4841 con China se refuerza aún más por las similitudes en la infraestructura compartida entre este grupo y otro conjunto sin categorizar conocido como UNC2286, que a su vez comparte similitudes con otras campañas de espionaje chinas identificadas como FamousSparrow y GhostEmperor.

Esta última revelación se produce en un contexto en el que el Buró Federal de Investigación de los Estados Unidos (FBI) está instando a los clientes afectados a reemplazar sus dispositivos ESG de manera inmediata, citando un riesgo continuo.

«UNC4841 es un actor con abundantes recursos que ha utilizado una amplia gama de malware y herramientas diseñadas específicamente para facilitar sus operaciones globales

de espionaje», afirmó la empresa, resaltando la capacidad de este actor de amenazas para desplegar selectivamente más cargas útiles en entornos de víctimas específicos.

> *«La infraestructura compartida y las técnicas de anonimización son comunes entre los actores de espionaje cibernético chinos, así como el uso de herramientas compartidas y recursos de desarrollo de malware. Es probable que continuemos observando operaciones de espionaje cibernético chinas dirigidas a la infraestructura de borde con vulnerabilidades de día cero y el despliegue de malware personalizado para sistemas de dispositivos específicos».*