Al menos nueve entidades de las industrias de tecnología, defensa, atención médica, energía y educación, se vieron comprometidas al haberse explotado una vulnerabilidad crítica recientemente parcheada en la solución de autoservicio de administración de contraseñas e inicio de sesión único (SSO) ManageEngine ADSelfService Plus de Zoho.

La campaña de espionaje, que se observó a partir del 22 de septiembre de 2021, involucró al actor de la amenaza que aprovechó la falla para obtener acceso inicial a las organizaciones objetivo, antes de moverse lateralmente a través de la red para realizar actividades posteriores a la explotación mediante el despliegue de herramientas maliciosas diseñadas para recolectar credenciales y exfiltrar información confidencial a través de una puerta trasera.

> *«El actor confía en gran medida en el shell web de Godzilla, cargando varias variaciones del shell web de código abierto al servidor comprometido durante el transcurso de la operación. Varias otras herramientas que tienen características novedosas o no se han discutido públicamente como utilizadas en ataques anteriores, específicamente la puerta trasera NGLite y el ladrón de KdcSponge»,* dijeron investigadores del equipo de inteligencia de amenazas Unit42 de Palo Alto Networks.

Rastreada como CVE-2021-40539, la vulnerabilidad se relaciona con una falla de omisión de autenticación que afecta a las URL de la API REST, que podría permitir la ejecución remota de código, lo que provocó que la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), advirtiera sobre intentos de explotación activos en la naturaleza. La vulnerabilidad de seguridad ha recibido una calificación de 9.8 sobre 10 en gravedad.

Se dice que los ataques en el mundo real que utilizan el error como arma comenzaron en agosto de 2021, según CISA, la Oficina Federal de Investigaciones (FBI) de Estados Unidos y el Comando Cibernético de la Guardia Costera (CGCYBER).

La investigación de Unit42 sobre la campaña de ataque encontró que la explotación inicial

exitosa fue seguida por la instalación de un shell web JSP en idioma chino llamado «Godzilla», con víctimas seleccionadas también infectadas con un troyano de código abierto personalizado basado en Golang llamado «NGLite».

> *«NGLite se caracteriza por su autor como un 'programa anónimo de control remoto multiplataforma basado en tecnología blockchain'. Aprovecha la infraestructura de New Kind of Network (NKN) para sus comunicaciones de comando y control (C2), lo que teóricamente da como resultado el anonimato para sus usuarios»,* dijeron los investigadores Robert Falcone, Jeff White y Peter Renalds.

En los pasos posteriores, el conjunto de herramientas permitió al atacante ejecutar comandos y moverse de forma lateral a otros sistemas en la red, mientras simultáneamente transmitía archivos de interés. También se implementó en la cadena de eliminación un novedoso ladrón de contraseñas denominado «KdcSponge» orquestado para robar las credenciales de los controladores de dominio.

En última instancia, se cree que el adversario apuntó al menos a 370 servidores de Zoho ManageEngine en Estados Unidos solo a partir del 17 de septiembre. Si bien la identidad del actor de la amenaza sigue sin estar clara, Unit 42 dijo que observó correlaciones en las tácticas y herramientas entre el atacante y el de Emissary Panda, también conocido como APT27, TG-3390, BRONZE UNION, Iron Tiger o LuckyMouse.

> *«Las organizaciones que identifican cualquier actividad relacionada con los indicadores de compromiso ADSelfService Plus de ManageEngine dentro de sus redes deben tomar medidas de inmediato. Además de utilizar restablecimientos de contraseñas en todo el dominio y restablecimientos dobles de contraseñas de Kerberos Ticket Granting Ticket (TGT) si hay alguna indicación que afirme que el archivo NTDS.dit estaba comprometido»*, dijo CISA.