Un actor de amenazas persistentes avanzadas (APT) bajo el alias de ToddyCat, ha sido vinculado a una serie de ataques cibernéticos dirigidos a entidades de alto perfil en Europa y Asia desde al menos diciembre de 2020.

El grupo de hackers relativamente nuevo, comenzó sus operaciones apuntando a los servidores de Microsoft Exchange en Taiwán y Vietnam, utilizando un exploit desconocido para implementar el shell web de China Chopper y activar una cadena de infección de múltiples etapas.

Otros países prominentes a los que se dirigen son Afganistán, India, Indonesia, Irán, Kirguistán, Malasia, Pakistán, Rusia, Eslovaquia, Tailandia, Reino Unido y Uzbekistán, justo cuando los hackers evolucionaron su conjunto de herramientas en el transcurso de distintas campañas.

> *«La primera ola de ataques se dirigió exclusivamente a los servidores de Microsoft Exchange, que estaban comprometidos con Samurai, una puerta trasera pasiva sofisticada que generalmente funciona en los puertos 80 y 443»,* dijo la compañía de seguridad cibernética Kaspersky.

> *«El malware permite la ejecución de código C# arbitrario y se utiliza con múltiples módulos que permiten al atacante administrar el sistema remoto y moverse lateralmente dentro de la red objetivo».*

ToddyCat, también rastreado con el nombre de Websiic por la empresa de ciberseguridad ESET, salió a la luz por primera vez en marzo de 2021 por su explotación de las vulnerabilidades de ProxyLogon Exchange para apuntar a servidores de correo electrónico pertenecientes a empresas privadas en Asia y un organismo gubernamental en Europa.

La secuencia de ataque posterior al despliegue del shell web de China Chopper conduce a la

ejecución de un dropper que, a su vez, se utiliza para realizar modificaciones en el Registro de Windows para lanzar un cargador de segunda etapa, que por su parte, está diseñado para desencadenar un cargador .NET de tercera etapa que es responsable de ejecutar Samurai.

La backdoor, además de utilizar técnicas como la ofuscación y el aplanamiento del flujo de control para que sea resistente a la ingeniería inversa, es modular en el sentido de que los componentes permiten ejecutar comandos arbitrarios y extraer archivos de interés del host comprometido.

También se observó en incidentes específicos una herramienta sofisticada llamada Ninja, que se generó por el implante Samurai y probablemente funciona como una herramienta de colaboración que permite que varios operadores trabajen en la misma máquina de forma simultánea.

A pesar de sus características similares a otros kits de herramientas posteriores a la explotación como Cobalt Strike, el malware permite al atacante *«controlar sistemas remotos, evitar la detección y penetrar profundamente dentro de una red objetivo».*

Aunque las víctimas de ToddyCat están relacionadas con países y sectores tradicionalmente atacados por grupos de habla china, no existe evidencia que vincule el modus operandi con un actor de amenazas conocido.

> *«ToddyCat es un grupo APT sofisticado que utiliza múltiples técnicas para evitar la detección y, por lo tanto, mantiene un perfil bajo»,* dijo el investigador de Kaspersky, Giampaolo Dedola.

> *«Las organizaciones afectadas, tanto gubernamentales como militares, muestran*

> *que este grupo se centra en objetivos de muy alto perfil y probablemente se utiliza para lograr objetivos críticos, probablemente relacionados con intereses geopolíticos».*