La industria del transporte y las agencias gubernamentales relacionadas con el sector son víctimas de una campaña en curso desde julio de 2020, por parte de un grupo de ciberespionaje sofisticado y bien equipado en lo que parece ser otro repunte en las actividades maliciosas que son *«solo la punta del iceberg».*

> *«El grupo intentó acceder a algunos documentos internos (como horarios de vuelo y documentos para planes financieros) e información personal sobre los hosts comprometidos (como los historiales de búsqueda)»,* dijeron los investigadores de Trend Micro, Nick Dai, Ted Lee y Vickie Su.

Earth Centaur, también conocido como Pirate Panda y Tropic Trooper, es un grupo de amenazas de largo historial centrado en el robo de información y el espionaje que ha liderado campañas dirigidas contra el gobierno, la atención médica, el transporte y las industrias de alta tecnología en Taiwán, Filipinas y Hong Kong, estas campañas se remontan a 2011.

Los agentes hostiles, que se cree que son actores de habla china, son conocidos por su uso de correos electrónicos de phishing con archivos adjuntos armados para explotar vulnerabilidades conocidas, mientras que de forma simultánea, avanzan su herramientas maliciosas con ofuscación, sigilo y poder de ataque.

> *«Este grupo de amenazas es competente en el trabajo en equipo rojo. El grupo sabe cómo eludir la configuración de seguridad y mantener su operación sin obstáculos. El uso de los marcos de código abierto también le permite al grupo desarrollar nuevas variantes de puerta trasera de forma eficiente»,* dijeron los investigadores.

En mayo de 2020, se observó que los operadores ajustaban sus estrategias de ataque con nuevos comportamientos mediante el despliegue de un troyano USB denominado USBFerry, para atacar redes físicamente aisladas pertenecientes a instituciones gubernamentales y entidades militares en Taiwán y Filipinas en un intento por desviar datos confidenciales por

medio de dispositivos extraíbles.

La última secuencia de intrusión de múltiples etapas detallada por Trend Micro involucra al grupo que recurre para explotar los servidores vulnerables de Internet Information Services (IIS) y las vulnerabilidades del servidor Exchange como puntos de entrada para instalar un shell web que luego se aprovecha para entregar un cargador Nerapack basado en .NET y una puerta trasera de primera etapa conocida como Quasar en el sistema comprometido.

A partir de ahí, los atacantes le siguen agregando un arsenal de implantes de segunda etapa como ChiserClient, SmileSvr, ChiserClient, HTShell y versiones a medida de Lilith RAT y Gh0st RAT, dependiendo de la víctima para recuperar más instrucciones de un servidor remoto, descargar más cargas útiles, realizar operaciones de archivos, ejecutar comandos arbitrarios y exfiltrar los resultados al servidor.

Además, luego de la explotación exitosa del sistema, Tropic Trooper también intenta violar la Intranet, volcar credenciales y borrar los registros de eventos de las máquinas infectadas utilizando un conjunto específico de herramientas. También se utiliza un programa de línea de comandos llamado Reclone, que permite al actor copiar los datos recolectados a diferentes proveedores de almacenamiento en la nube.

> *«Actualmente no hemos descubierto daños sustanciales a estas víctimas causados por el grupo de amenazas. Sin embargo, creemos que seguirá recopilando información interna de las víctimas comprometidas y que simplemente está esperando una oportunidad para utilizar estos datos»,* dijeron los investigadores de Trend Micro.

Los pasos de esta amenaza persistente avanzada (APT) para evitar la detección y la naturaleza crítica de las entidades objetivo, son dignas de mencionar, además de las nuevas

capacidades desarrolladas para que su software malicioso permanezca en los hosts infectados y evite la detección.

> *«El grupo puede mapear la infraestructura de red de su objetivo y evitar los cortafuegos. Utiliza puertas traseras con diferentes protocolos, que se implementan según la víctima. También tiene la capacidad de desarrollar herramientas personalizadas para evadir el monitoreo de seguridad en diferentes entornos, y explota sitios web vulnerables y los usa como servidores»,* agregaron los investigadores.