El Grupo de Análisis de Amenazas (TAG) de Google, reveló un nuevo corredor de acceso inicial que, según dijo la compañía, está estrechamente afiliado a un grupo ruso de hacking, conocido por sus operaciones de ransomware con Conti y Diavol.

Nombrado como Exotic Lily, se ha observado al actor de amenazas motivado financieramente explotando una vulnerabilidad crítica ya parcheada en la plataforma Microsoft Windows MSHTML (CVE-2021-40444) como parte de campañas de phishing generalizadas que involucraron el envío de no menos de 5000 correos electrónicos con propuestas comerciales con el objetivo de 650 organizaciones al día en todo el mundo.

> *«Los corredores de acceso inicial son los cerrajeros oportunistas del mundo de la seguridad, y es un trabajo completo. Estos grupos se especializan en violar un objetivo para abrir las puertas, o las ventanas, al actor malicioso con la oferta más alta»*, dijeron los investigadores de TAG.

Exotic Lily, detectada por primera vez en septiembre de 2021, estuvo involucrada en la exfiltración de datos y el despliegue de las cepas de ransomware Conti y Diavol, operadas por hackers, las cuales comparten superposiciones con Wizard Spider, el sindicato ciberdelincuente ruso que también es conocido por operar TrickBot, BazarBackdoor y Anchor.

> *«Sí, esta es una posibilidad, especialmente considerando que es más sofisticada y dirigida que una campaña de spam tradicional, pero no lo sabemos con certeza a partir de ahora»*, dijo Google a TAG.

> *«En las filtraciones de Conti, los miembros de Conti mencionan a los 'spammers' como alguien con quien trabajan (por ejemplo, proporcionan muestras de malware encriptadas personalizadas, etc.) a través de la subcontratación. Sin embargo, la mayoría de los 'spammers' no parecen estar presentes (o comunicarse*

> *activamente) en el chat, lo que lleva a la conclusión de que están operando como una entidad separada».*

Los señuelos de ingeniería social del actor de amenazas, enviados desde cuentas de correo electrónico falsificadas, se han centrado específicamente en los sectores de TI, ciberseguridad y atención médica, aunque después de noviembre de 2021, los ataques se han vuelto más indiscriminados y se dirigen a una amplia variedad de organizaciones e industrias.

Además de utilizar empresas e identidades ficticias como un medio para generar confianza con las entidades objetivo, Exotic Lily ha aprovechado los servicios legítimos de intercambio de archivos como WeTransfer, TransferNow y OneDrive para entregar cargas útiles de BazarBackdoor en un intento por evadir los mecanismos de detección.

Los ciberdelincuentes por lo general se hacían pasar por empleados de compañías como Amazon, con perfiles de redes sociales fraudulentos en LinkedIn, que presentaban imágenes de perfil falsas generadas por IA. También se cree que el grupo se hizo pasar por empleados reales de la empresa al extraer sus datos personales de las redes sociales y bases de datos comerciales como RocketReach y CrunchBase.

> *«En la etapa final, el atacante cargaría la carga útil en un servicio público de intercambio de archivos (TransferNow, TransferXL, WeTransfer o OneDrive) y luego usaría una función de notificación por correo electrónico integrada para compartir el archivo con el objetivo, permitiendo que el correo electrónico final se origine en la dirección de correo electrónico de un servicio legítimo de intercambio de archivos y no en el correo electrónico del atacante, lo que presenta desafíos de detección adicionales»*, dijeron los investigadores.

También se entrega utilizando el exploit MHTML, un cargador personalizado llamado Bumblebee que está diseñado para recopilar y filtrar información del sistema a un servidor remoto, que responde a los comandos para ejecutar shellcode y ejecutar archivos ejecutables de próxima etapa, incluido Cobalt Strike.

Un análisis de la actividad de comunicación de Exotic Lily indica que los atacantes tienen un *«trabajo típico de 9 a 5″* entre semana y es posible que trabajen desde una zona horaria de Europa Central o del Este.

> *«EXOTIC LILY parece operar como una entidad separada, enfocándose en adquirir acceso inicial a través de campañas de correo electrónico, con actividades de seguimiento que incluyen el despliegue de Conti y Diavol ransomware, que son realizadas por un conjunto diferente de actores»*, agregaron los investigadores.