Expertos en ciberseguridad han detectado dos paquetes maliciosos subidos al repositorio Python Package Index (PyPI), diseñados para extraer información sensible de sistemas comprometidos, según un informe reciente de Fortinet FortiGuard Labs.

Los paquetes, denominados zebo y cometlogger, acumularon 118 y 164 descargas respectivamente antes de ser retirados. Según los datos de ClickPy, la mayoría de estas descargas provino de países como Estados Unidos, China, Rusia e India.

Zebo es descrito como un *«ejemplo típico de malware, con funcionalidades orientadas a la vigilancia, robo de datos y control no autorizado»,* explicó la investigadora de seguridad Jenna Wang. Por su parte, cometlogger *«también muestra comportamientos dañinos, como manipulación dinámica de archivos, inyección de webhooks, robo de información y detección de entornos virtuales»*, añadió.

El paquete zebo emplea técnicas de ofuscación, como el uso de cadenas codificadas en formato hexadecimal, para ocultar la dirección del servidor de comando y control (C2) con el que establece comunicación a través de solicitudes HTTP.

Además, incluye múltiples herramientas para recopilar información, como la biblioteca pynput para registrar pulsaciones de teclado y ImageGrab para tomar capturas de pantalla cada hora. Estas imágenes se guardan localmente antes de ser enviadas al servicio de alojamiento de imágenes ImgBB mediante una clave API obtenida del servidor C2.

El malware también asegura su persistencia en el sistema creando un script en formato batch que ejecuta el código de Python y lo añade a la carpeta de Inicio de Windows, garantizando su ejecución automática tras cada reinicio.

Por otro lado, cometlogger cuenta con un conjunto de funcionalidades más amplio, enfocadas en recopilar datos como cookies, contraseñas, tokens y credenciales de aplicaciones como Discord, Steam, Instagram, X, TikTok, Reddit, Twitch, Spotify y Roblox.

También extrae información del sistema, datos de red y Wi-Fi, lista de procesos activos y

contenido del portapapeles. Adicionalmente, integra métodos para evitar ser ejecutado en entornos virtuales y cierra procesos relacionados con navegadores web para obtener acceso sin restricciones a los archivos.

> *«Mediante la ejecución asíncrona de tareas, el script optimiza su capacidad para robar grandes volúmenes de datos en poco tiempo»,* indicó Wang.
>
> *«Aunque algunas funciones podrían ser propias de herramientas legítimas, la falta de transparencia y las actividades sospechosas hacen que no sea seguro usarlo. Siempre revisen el código antes de ejecutarlo y eviten interactuar con scripts provenientes de fuentes no confiables».*