Los hackers están usando instaladores de VPN corruptos para implementar un software de vigilancia denominado EyeSpy como parte de una campaña de malware que comenzó en mayo de 2022.

> *«Utiliza componentes de SecondEye, una aplicación de monitoreo legítima, para espiar a los usuarios de 20Speed VPN, un servicio VPN con sede en Irán, a través de instaladores troyanos»,* dijo Bitdefender.

Se ha notado que la mayoría de las infecciones se originan en Irán, con detecciones menores en Alemania y Estados Unidos.

SecondEye, según las instantáneas capturadas por medio de Internet Archive, afirma ser un software de monitoreo comercial que puede funcionar como un *«sistema de control parental o como un perro guardián en línea».* A partir de noviembre de 2021, se ofrece a la venta entre 99 y 200 dólares.

Cuenta con una amplia gama de funciones que le permiten tomar capturas de pantalla, grabar micrófonos, registrar pulsaciones de teclas, recopilar archivos y contraseñas guardadas de navegadores web y controlar de forma remota las máquinas para ejecutar comandos arbitrarios.

SecondEye pasó desapercibido antes en agosto de 2022, cuando BlackPoint Cyber reveló el uso que los atacantes hacían de sus módulos de software espía y su infraestructura para el almacenamiento de datos y carga útil.

La última cadena de ataque comienza cuando un usuario desprevenido descarga un ejecutable malicioso del sitio web de 20Speed VPN, lo que indica dos escenarios: sus servidores fueron violados para alojar el spyware o es un intento deliberado de espiar a las personas que podrían descargar aplicaciones VPN para eludir apagones de Internet en el

país.

Una vez instalado, se inicia el servicio VPN legítimo, al mismo tiempo que inicia sigilosamente un conjunto de actividades maliciosas en segundo plano para establecer la persistencia y descargar las cargas útiles de siguiente etapa para recopilar datos personales del host.

> *«EyeSpy tiene la capacidad de comprometer completamente la privacidad en línea a través del registro de teclas y el robo de información confidencial, como documentos, imágenes, billeteras criptográficas y contraseñas. Esto puede conducir a adquisiciones de cuentas completas, robo de identidad y pérdidas financieras»,* dijo Janos Gergo Szeles, investigador de Bitdefender.