El grupo de amenazas persistentes avanzadas (APT) Kimsuky (también conocido como Springtail), asociado con la Oficina General de Reconocimiento (RGB) de Corea del Norte, ha sido detectado implementando una versión para Linux de su puerta trasera GoBear en una campaña dirigida a organizaciones surcoreanas.

La puerta trasera, denominada Gomir, es *«estructuralmente casi idéntica a GoBear, con un amplio intercambio de código entre las variantes de malware. Cualquier funcionalidad de GoBear que depende del sistema operativo está ausente o ha sido reimplementada en Gomir»*, según el equipo de cazadores de amenazas de Symantec, parte de Broadcom, en un nuevo informe.

GoBear fue documentado por primera vez por la firma de seguridad surcoreana S2W a principios de febrero de 2024 en relación con una campaña que distribuyó un malware llamado Troll Stealer (también conocido como TrollAgent), el cual comparte características con familias de malware conocidas de Kimsuky como AppleSeed y AlphaSeed.

Un análisis posterior realizado por el Centro de Inteligencia de Seguridad de AhnLab (ASEC) reveló que el malware se distribuye a través de programas de seguridad troyanizados descargados desde un sitio web no especificado de una asociación surcoreana relacionada con la construcción.

Esto incluye nProtect Online Security, NX_PRNMAN, TrustPKI, UbiReport y WIZVERA VeraPort, este último previamente sometido a un ataque a la cadena de suministro de software por el grupo Lazarus en 2020.

Symantec también observó que el malware Troll Stealer se distribuye a través de instaladores fraudulentos para Wizvera VeraPort, aunque el mecanismo exacto de distribución de los paquetes de instalación aún se desconoce.

> *«GoBear también contiene nombres de funciones similares a una antigua puerta trasera de Springtail conocida como BetaSeed, escrita en C++, lo que sugiere que*

> *ambas amenazas tienen un origen común»,* indicó la compañía.

Se informa que el malware, que tiene la capacidad de ejecutar comandos recibidos de un servidor remoto, también se propaga a través de droppers que se hacen pasar por un instalador falso de una aplicación para una organización de transporte coreana.

Su contraparte en Linux, Gomir, soporta hasta 17 comandos, permitiendo a sus operadores realizar operaciones de archivos, iniciar un proxy inverso, pausar las comunicaciones de comando y control (C2) durante un tiempo determinado, ejecutar comandos de shell y finalizar su propio proceso.

> *«Esta última campaña de Springtail proporciona más evidencia de que los paquetes de instalación de software y las actualizaciones son ahora uno de los vectores de infección preferidos por los actores de espionaje de Corea del Norte»,* dijo Symantec.
>
> *«El software objetivo parece haber sido cuidadosamente seleccionado para maximizar las posibilidades de infectar a sus objetivos en Corea del Sur.»*