Se encontró una amenaza con un nexo de Corea del Norte que aprovecha una *«metodología novedosa de phishing de lanza»* que implica el uso de versiones troyanizadas del cliente PuTTY SSH y Telnet.

La compañía de inteligencia de amenazas propiedad de Google, Mandiant, atribuyó la nueva campaña a un grupo de amenazas emergentes que se rastrea bajo el nombre UNC4034.

> *«UNC4034 estableció comunicación con la víctima por medio de WhatsApp y la atrajo para que descargara un paquete ISO malicioso con respecto a una oferta de trabajo falsa que condujo a la implementación de la puerta trasera AIRDRY.V2 por medio de una instancia troyana de la utilidad PuTTY»,* dijeron los investigadores de Mandiant.

La utilización de señuelos laborales fabricados como vía para la distribución de malware es una táctica utilizada con frecuencia por atacantes patrocinados por el estado de Corea del Norte, incluyendo Lazarus Group, como parte de una campaña duradera llamada Operation Dream Job.

El punto de entrada del ataque es un archivo ISO que se hace pasar por una evaluación de Amazon como parte de una posible oportunidad laboral en el gigante tecnológico. El archivo se compartió a través de WhatsApp después de establecer el contacto inicial por correo electrónico.

El archivo, por su parte, contiene un archivo de texto que contiene una dirección IP y credenciales de inicio de sesión, y una versión alterada de PuTTY, que a su vez, carga un cuentagotas llamado DAVESHELL, que implementa una variante más nueva de una backdoor llamada AIRDRY.

Es probable que el atacante haya convencido a la víctima para que inicie una sesión de PuTTY y utilice las credenciales provistas en el archivo TXT para conectarse al host remoto, activando efectivamente la infección.

AIRDRY, también conocido como BLINDINGCAN, ha sido utilizado en el pasado por hackers vinculados a Corea del Norte para atacar a contratistas y entidades de defensa estadounidenses en Corea del Sur y Letonia.

Aunque las versiones anteriores del malware venían con casi 30 comandos para la transferencia de archivos, la administración de archivos y la ejecución de comandos, se descubrió que la última versión evita el enfoque basado en comandos a favor de los complementos que se descargan y ejecutan en la memoria.

Mandiant dijo que pudo contener el compromiso antes de que pudieran llevarse a cabo más actividades posteriores a la explotación después del despliegue del implante.

El desarrollo es otra señal más de que el uso de archivos ISO para el acceso inicial está ganando terreno entre los actores de amenazas para entregar tanto malware básico como dirigido.

El cambio también se puede atribuir a la decisión de Microsoft de bloquear las macros de Excel 4.0 (XLM o XL4) y Visual Basic para aplicaciones (VBA) para las aplicaciones de Office descargadas de Internet de forma predeterminada.