Investigadores de seguridad cibernética dieron a conocer este miércoles la interrupción de una red de publicidad maliciosa inteligente dirigida a AnyDesk, que entregó un instalador armado del software de escritorio remoto a través de anuncios de Google falsos que aparecían en las páginas de resultados del motor de búsqueda.

La campaña, que se cree que comenzó el 21 de abril de 2021, involucra un archivo malicioso que se hace pasar por un ejecutable de configuración para AnyDesk (*AnyDeskSetup.exe*), que al ejecutarse, descarga un implante de PowerShell para acumular y exfiltrar información del sistema.

> *«El script tenía algunas ofuscaciones y múltiples funciones que se asemejaban a un implante, así como un dominio codificado (zoomstatistic[.]com) para información de reconocimiento POST como nombre de usuario, nombre de host, sistema operativo, dirección IP y el nombre del proceso actual»,* dijeron los investigadores de CrowdStrike.

La solución de acceso a escritorio remoto de AnyDesk ha sido descargada por más de 300 millones de usuarios en todo el mundo, según el sitio web de la compañía. Aunque la empresa de seguridad cibernética no atribuyó la actividad maliciosa a un actor o nexo de amenaza específico, sospecha que se trata de *«una campaña generalizada a una amplia gama de clientes»* debido a la gran base de usuarios.

La secuencia de comandos de PowerShell puede tener todas las características de una puerta trasera típica, pero es la ruta de intrusión donde el ataque lanza una curva, lo que indica que está más allá de una operación de recopilación de datos de variedad de jardín: el instalador de AnyDesk se distribuye a través de anuncios maliciosos de Google colocados por el actor de la amenaza, que luego se sirven a personas desprevenidas que están usando Google para buscar *«AnyDesk»*.

El resultado del anuncio fraudulento, cuando se hace clic, redirige a los usuarios a una página de ingeniería social que es un clon del sitio web legítimo de AnyDesk, además de

proporcionar al usuario un enlace al instalador troyanizado.

CrowdStrike estima que el 40% de los clics en el anuncio malicioso se convirtieron en instalaciones del binario de AnyDesk, y el 20% de esas instalaciones incluyeron actividad de seguimiento con el teclado.

> *«Si bien se desconoce qué porcentaje de las búsquedas de AnyDesk en Google dieron como resultado clics en el anuncio, una tasa de instalación de troyanos del 40% a partir de un clic en un anuncio muestra que este es un método extremadamente exitoso para obtener acceso remoto en una amplia gama de objetivos potenciales»,* dijeron los investigadores.

La compañía también dijo que notificó a Google de sus hallazgos, que al parecer ya tomó medidas inmediatas para retirar el anuncio.

> *«Este uso malintencionado de Google Ads es una forma eficaz e inteligente de lograr la implementación masiva de shells, ya que proporciona al actor de amenazas la capacidad de elegir libremente sus objetivos de interés»*, agregaron los investigadores.
>
> *«Debido a la naturaleza de la plataforma de publicidad de Google, puede proporcionar una muy buena estimación de cuántas personas harán clic en el anuncio. A partir de ahí, el actor de amenazas puede planificar y presupuestar de forma adecuada en función de esta información. Además de las herramientas de orientación como AnyDesk u otras herramientas administrativas, el actor de amenazas puede apuntar a usuarios privilegiados/administrativos de una forma única».*