Se detectó un servicio de malware de pago por instalación (PPI) conocido como PrivateLoader, que distribuye un marco *«bastante sofisticado»* llamado NetDooka, que otorga a los atacantes un control total sobre los dispositivos infectados.

> *«El marco se distribuye por medio de un servicio de pago por instalación (PPI) y contiene varias partes, incluido un cargador, un cuentagotas, un controlador de protección y un troyano de acceso remoto (RAT) con todas las funciones que implementa su propio protocolo de comunicación de red»,* dijo Trend Micro.

PrivateLoader, como lo documentó previamente Intel 471 en febrero de 2022, funciona como un descargador responsable de la instalación del malware adicional en el sistema infectado, incluyendo SmokeLoader, RedLine Stealer, Vidar, Raccoon, GCleaner y Anubis.

Con técnicas antianálisis, PrivateLoader está escrito en el lenguaje de programación C++ y se dice que está en desarrollo activo, con la familia de malware de descarga ganando terreno entre múltiples actores de amenazas.

Las infecciones de PrivateLoader generalmente se propagan a través de software pirateado descargado de sitios web no autorizados, que se colocan en la parte superior de los resultados de búsqueda a través de técnicas de envenenamiento de optimización de motores de búsqueda (SEO).

> *«PrivateLoader se utiliza actualmente para distribuir ransomware, ladrones, banqueros y otros programas maliciosos básicos. Es probable que el cargador siga actualizándose con nuevas características y funcionalidades para evadir la detección y entregar efectivamente cargas de malware de segunda etapa»,* dijo Zscaler.

El marco, aún en fase de desarrollo, contiene diferentes módulos: un cuentagotas, un

cargador, un controlador de protección de archivos y procesos en modo kernel, y un troyano de acceso remoto que utiliza un protocolo personalizado para comunicarse con el servidor de comando y control (C2).

El conjunto de infecciones recientemente observado que involucra el marco NetDooka comienza con PrivateLoader actuando como un conducto para implementar un componente cuentagotas, que luego descifra y ejecuta un cargador que, a su vez, recupera otro cuentagotas de un servidor remoto para instalar un troyano con funciones completas así como un controlador de kernel.

> *«El componente del controlador actúa como una protección a nivel de kernel para el componente RAT. Hace esto al intentar evitar la eliminación del archivo y la finalización del proceso del componente RAT»*, dijeron los investigadores Aliakbar Zahravi y Leandro Froes.

La backdoor, denominada NetDookaRAT, se destaca por su amplitud de funciones, lo que le permite ejecutar comandos en el dispositivo objetivo, llevar a cabo ataques de denegación de servicio distribuido (DDoS), acceder y enviar archivos, registrar pulsaciones de teclas y descargar y ejecutar cargas útiles adicionales.

Esto indica que las capacidades de NetDooka no solo le permiten actuar como un punto de entrada para otro malware, sino que también pueden convertirse en armas para robar información confidencial y formar botnets controladas remotamente.

> *«Los servicios de malware de PPI permiten a los creadores de malware implementar fácilmente sus cargas útiles»,* agregaron los investigadores.

> *«El uso de un controlador malicioso crea una gran superficie de ataque para que los atacantes la exploten, al mismo tiempo que les permite aprovechar enfoques como la protección de procesos y archivos, eludir los programas antivirus y ocultar el malware o sus comunicaciones de red del sistema».*