Un grupo de espionaje cibernético con presuntos vínculos con los gobiernos kazajo y libanés, ha desatado una nueva ola de ataques contra una multitud de industrias con una versión renovada de un troyano de puerta trasera de 13 años.

Check Point Research llamó a los piratas informáticos afiliados a un grupo llamado Dark Caracal en un nuevo informe publicado ayer, en sus esfuerzos para implementar *«docenas de variantes firmadas digitalmente»* del troyano Bandook Windows durante el año pasado, por lo que una vez más *«reavivó el interés en esta vieja familia de malware»*.

Los objetivos señalados por el actor de la amenaza incluyen instituciones gubernamentales, financieras, energéticas, alimentarias, educativas, informáticas y legales ubicadas en Chile, Chipre, Alemania, Indonesia, Italia, Singapur, Suiza, Turquía y Estados Unidos.

La variedad inusualmente grande de mercados y ubicaciones objetivo *«refuerza la hipótesis anterior de que el malware no es desarrollado internamente y utilizado por una sola entidad, sino que es parte de una infraestructura ofensiva vendida por un tercero a gobiernos y actores de amenazas en todo el mundo, para facilitar las operaciones cibernéticas ofensivas»*, dijeron los investigadores.

El uso extensivo del RAT Bandook por parte de Dark Caracal, para ejecutar espionaje a escala global fue documentado por primera vez por Electronic Frontier Foundation (EFF) y Lookout a inicios de 2018, y el grupo se atribuyó al robo de propiedad intelectual empresarial e información de identificación personal de miles de víctimas que abarca más de 21 países.

El grupo, que ha operado al menos desde 2012, ha estado vinculado a la Dirección General de Seguridad General del Líbano (GDGS), considerándolo una amenaza persistente avanzada a nivel estado-nación.

El uso concurrente de la misma infraestructura de malware por distintos grupos para campañas aparentemente no relacionadas llevó a la EFF y Lookout a suponer que el actor APT *«o usa o administra la infraestructura que alberga una serie de campañas de ciberespionaje globales generalizadas».*

Ahora, el mismo grupo está de vuelta con una nueva cepa de Bandook, con esfuerzos adicionales para frustrar la detección y el análisis, según Check Point Research.

Cadena de infección en tres etapas

La cadena de infección es un proceso de tres etapas que comienza con un documento atractivo de Microsoft Word (por ejemplo, *Documentos certificados.docx*) entregado dentro de un archivo ZIP que, cuando se abre, descarga macros maliciosas, que posteriormente procede a soltar y ejecutar una segunda etapa secundaria de comandos de PowerShell cifrada dentro del documento de Word original.

En la última fase del ataque, este script de PowerShell se utiliza para descargar partes ejecutable codificadas de servicios de almacenamiento en la nube como Dropbox o Bitbucket para ensamblar el cargador Bandook, que luego asume la responsabilidad de inyectar el RAT en un nuevo proceso de Internet Explorer.

Bandook RAT, disponible comercialmente a partir de 2007, cuenta con las capacidades típicamente asociadas con las puertas traseras, ya que establece contacto con un servidor controlado de forma remota para recibir comandos adicionales que van desde la toma de capturas de pantalla hasta la realización de distintas operaciones relacionadas con archivos.

Pero según la compañía de ciberseguridad, la nueva variante de Bandook es una versión reducida del malware con soporte para solo 11 comandos, mientras que se sabía que las versiones anteriores presentaban hasta 120 comandos, lo que sugiere el deseo de los operadores de reducir la huella del malware y evadir la detección contra objetivos de alto perfil.

Además, no solo se usaron certificados válidos emitidos por Certum para firmar esta versión recortada del ejecutable del malware, los investigadores de Check Point descubrieron dos muestras más, variantes completas, firmadas digitalmente y sin firmar, que creen que son operadas y vendidas por una sola entidad.

> *«Aunque no es tan capaz ni tan practicado en seguridad operativa como otras empresas de seguridad ofensiva, el grupo detrás de la infraestructura en estos ataques parece mejorar con el tiempo, agregando varias capas de seguridad, certificados válidos y otras técnicas, para dificultar la detección y el análisis de sus operaciones»,* agregaron los investigadores.