Un grupo de hackers previamente indocumentado y con motivaciones financieras se ha relacionado con una serie de ataques de robo de datos y extorsión en más de 40 entidades entre septiembre y noviembre de 2021.

El grupo de hackers, que se conoce con el nombre autoproclamado Karakurt y fue identificado por primera vez en junio de 2021, es capaz de modificar sus tácticas y técnicas para adaptarse al entorno objetivo, dijo el equipo de Cyber Investigations, Forensics and Response (CIFR) de Accenture en un comunicado del 10 de diciembre.

> *«El grupo está motivado económicamente, oportunista en la naturaleza, y hasta ahora, parece apuntar a las pequeñas empresas o filiales de las corporaciones contra el enfoque alternativo. Según el análisis de intrusiones hasta la fecha, el grupo de amenazas se centra únicamente en la exfiltración de datos y la extorsión posterior, en lugar de la implementación de ransomware más destructiva»,* dijo el equipo CIFR.

El 95% de las víctimas conocidas se encuentran en América del Norte, mientras que el 5% restante se encuentra en Europa. Los verticales de servicios profesionales, salud, industria, comercio minorista, tecnología y entretenimiento fueron los más seleccionados.

El objetivo, según los investigadores, es evitar llamar la atención sobre sus actividades maliciosas tanto como sea posible confiando en técnicas de vivir de la tierra (LotL), en las que los atacantes abusan del software legítimo y las funciones disponibles en un sistema, como los componentes del sistema operativo o software instalado para moverse lateralmente y exfiltrar datos, en lugar de implementar herramientas posteriores a la explotación como Cobalt Strike.

Con los ataques de ransomware ganando atención mundial a raíz de incidentes dirigidos a

Colonial Pipeline, JBS y Kaseya, así como las posteriores acciones policiales que han provocado que los grupos de hackers como DarkSide, BlackMatter y REvil, cierren sus operaciones, Karakurt parece estar intentando un rumbo diferente.

En lugar de implementar ransomware después de obtener acceso inicial a los sistemas de Internet de las víctimas por medio de credenciales VPN legítimas, el actor se centra casi exclusivamente en la exfiltración y extorsión de datos, una medida que es menos probable que paralice las actividades comerciales de los objetivos, y sin embargo, habilite Karakurt para exigir un «rescate» a cambio de la información robada.

Además del cifrado de datos en reposo donde corresponda, se recomienda a las organizaciones que activen la autenticación multifactor (MFA) para cuentas, deshabilitar RDP en dispositivos externos y actualizar la infraestructura a las últimas versiones para evitar que los adversarios exploten los sistemas no parcheados públicamente. Un grupo de hackers previamente indocumentado y con motivaciones financieras se ha relacionado con una serie de ataques de robo de datos y extorsión en más de 40 entidades entre septiembre y noviembre de 2021.