Se descubrió una operación que involucra hackers a sueldo que utilizan una variedad de malware previamente indocumentado para apuntar a instituciones financieras del sur de Asia y empresas de entretenimiento globales.

Apodada como CostaRicto por los investigadores de BlackBerry, la campaña parece ser obra de hackers de APT que poseen herramientas de malware a medida y capacidades complejas de proxy VPN y tunelización SSH.

> *«Los objetivos de CostaRicto se encuentran dispersos en distintos países de Europa, América, Asia, Australia y África, pero la mayor concentración parece estar en el sur de Asia, lo que sugiere que el actor de la amenaza podría estar basado en esa región, pero trabajando en una amplia gama de comisiones de diversos clientes»,* dijeron los investigadores.

El modus operandi es sencillo, según los investigadores. Al obtener un punto de apoyo inicial en el entorno del objetivo a través de credenciales robadas el atacante procede a configurar un túnel SSH para descargar una puerta trasera y un cargador de carga útil llamado CostaBricks que implementa un mecanismo de máquina virtual C++ para decodificar e inyectar la carga útil del código de bytes en la memoria.

Además de administrar servidores de comando y control (C2) a travésde un túnel de DNS, la puerta trasera entregada por los cargadores mencionados anteriormente es un ejecutable compilado en C++ llamado SombRAT, llamado así por Sombra, un hacker mexicano e infiltrado del popular juego Overwatch.

La puerta trasera está equipada con 50 comandos distintos para llevar a cabo tareas específicas que van desde inyección de DLL maliciosas en la memoria, hasta enumerar archivos almacenados y extraer los datos capturados para un servidor controlado por un atacante.

En total, se han identificado seis versiones de SombRAT, la primera versión se remonta a

octubre de 2019 y la última variante observada a principios de agosto, lo que implica que la puerta trasera está en desarrollo activo.

Si bien aún se desconocen las identidades de los delincuentes detrás de la operación, una de las direcciones IP a las que se registraron los dominios de puerta trasera se ha vinculado a una campaña de phishing anterior atribuida al grupo de hackers APT28 vinculado a Rusia, lo que sugiere la posibilidad de que las campañas de phishing podrían haber sido subcontratando al mercenario en nombre del actor real de la amenaza.

Esta es la segunda operación de hackers a sueldo descubierta por Blackberry, la primera se trató de una serie de campañas de un grupo llamado Bahamut, que se descubrió que explotaba vulnerabilidades de día cero en el Medio Oriente y Asia meridional.

> *«Con el éxito innegable de Ransomware-as-a-service (RaaS), no es sorprendente que el mercado de los delincuentes cibernéticos haya ampliado su cartera para agregar campañas dedicadas de phishing y espionaje a la lista de servicios que se ofrecen»*, dijeron los investigadores a Blackberry.
>
> *«La subcontratación de ataques o ciertas partes de la cadena de ataque a grupos mercenarios no afiliados tiene varias ventajas para el adversario: ahorra tiempo y recursos y simplifica los procedimientos, pero lo más importante es que proporciona una capa adicional de indirecta, que ayuda a proteger la identidad real del actor de amenazas»,* agregaron.