Un nuevo grupo de hackers denominado Void Balaur, se ha relacionado con una serie de actividades de espionaje cibernético y robo de datos dirigidas a miles de entidades, así como a activistas de derechos humanos, políticos y funcionarios gubernamentales de todo el mundo al menos desde 2015 para obtener beneficios económicos mientras acecha en las sombras.

Nombrado en honor a un dragón de muchas cabezas del folclore rumano, el adversario fue desenmascarado anunciando sus servicios en foros clandestinos de habla rusa que datan de 2017 y vendiendo tesoros de información confidencial como registros de teléfonos de torres celulares, registros de vuelos de pasajeros, informes de crédito, datos bancarios, mensajes SMS y detalles del pasaporte. El actor de amenazas se llama a sí mismo como Rockethack.

> *«Este grupo de hackers contratados no opera desde un edificio físico, ni tiene un prospecto brillante que describa sus servicios»,* dijo la investigadora de Trend Micro, Feike Hacquebord.

> *«El grupo no intenta escabullirse de una posición difícil justificando su negocio, ni está involucrado en juicios contra cualquiera que intente informar sobre sus actividades. En cambio, este grupo es bastante abierto sobre lo que hace: irrumpir en cuentas de correo electrónico y cuentas de redes sociales por dinero»,* agregó Hacquebord.

Además de obtener críticas positivas casi unánimes en los foros por su capacidad para ofrecer información de calidad, también se cree que Void Balaur se ha centrado en los intercambios de criptomonedas al crear numerosos sitios de phishing para engañar a los usuarios del intercambio de criptomonedas para obtener acceso no autorizado a sus billeteras.

Además, las campañas involucraron el despliegue de ladrones de información y software espía de Android como Z*Stealer y DroidWatcher contra sus objetivos.

Se ha observado que el conjunto de intrusión de Void Balaur se ha desplegado contra una amplia gama de personas y entidades, incluidos periodistas, activistas de derechos humanos, políticos, científicos, médicos que trabajan en clínicas de FIV, empresas de genómica y biotecnología e ingenieros de telecomunicaciones. Trend Micro dijo que descubrió más de 3500 direcciones de correo electrónico en las que el grupo se propuso.

Se dice que la mayoría de los objetivos del grupo están ubicados en Rusia y otros países vecinos como Ucrania, Eslovaquia y Kazajstán. También existen víctimas en Estados Unidos, Israel, Japón, India y naciones europeas. Las organizaciones atacadas abarcan desde proveedores de telecomunicaciones, corporaciones de comunicaciones por satélite y firmas de tecnología financiera, hasta proveedores de cajeros automáticos, proveedores de puntos de venta (PoS) y empresas de biotecnología.

> *«Void Balaur busca los datos más privados y personales de empresas e individuos y luego los vende a quien quiera pagar por ellos»,* dijeron los investigadores.

Tampoco se sabe cómo se adquieren los registros confidenciales de teléfonos y correos electrónicos de los objetivos sin interacción, aunque los investigadores sospechan que el actor de la amenaza podría haber involucrado directa o indirectamente a personas con información privilegiada en las empresas interesadas para vender los datos o comprometer las cuentas de empleados con clave de acceso a los buzones de correo electrónico específicos.

El análisis profundo de Trend Micro también encontró algo en común con otro grupo de amenazas persistentes avanzadas con sede en Rusia llamado Pawn Storm (también conocido como APT28, Sofacy o Iron Twilight), con superposiciones observadas en las direcciones de correo electrónico específicas entre los dos grupos, mientras que también difieren significativamente en varias formas, incluido el modus operandi de Void Balaur de llamar a

los usuarios de criptomonedas y sus horas de funcionamiento.

En todo caso, el desarrollo destaca una vez más el crecimiento desenfrenado de las actividades ilícitas relacionadas con los hackers y la demanda de dichos servicios, con una serie de operaciones: BellTroX (también conocido como Dark Basin), Bahamut, CostaRicto y PowerPepper, que han sido expuestas dirigiéndose a organizaciones sin fines de lucro, instituciones financieras y agencias gubernamentales en los últimos meses.

Para defenderse de los ataques de piratería, se recomienda habilitar la autenticación de dos factores (2FA) a través de una aplicación de autenticación o una clave de seguridad de hardware, confiar en aplicaciones con cifrado de extremo a extremo (E2EE) para correo electrónico y comunicaciones, y eliminar permanentemente mensajes no deseados para mitigar el riesgo de exposición de datos.

> *«La realidad es que los usuarios habituales de Internet no pueden disuadir fácilmente a un cibermercenario determinado. Si bien las herramientas ofensivas avanzadas contra el arsenal de un mercenario cibernético pueden estar destinadas a ser utilizadas en la lucha contra el terrorismo y el crimen organizado, la realidad es que, a sabiendas o no, terminan en manos de los actores de amenazas que las usan contra objetivos»,* dijeron los investigadores.