El Threat Analysis Group (TAG) de Google reveló este jueves que había actuado para bloquear hasta 36 dominios maliciosos operados por grupos de hacking de India, Rusia y los Emiratos Árabes Unidos.

De forma análoga al ecosistema de software de vigilancia, las compañías de hacking equipan a sus clientes con capacidades para permitir ataques dirigidos a empresas, activistas, periodistas, políticos y otros usuarios de alto riesgo.

Ambos se diferencian en que los clientes compran el software espía a proveedores comerciales y después lo implementan ellos mismos, se sabe que los operadores detrás de los ataques de hacking a sueldo realizan las intrusiones en nombre de sus clientes para ocultar su papel.

> *«El panorama de piratería a sueldo es fluido, tanto en la forma en que los atacantes se organizan como en la amplia gama de objetivos que persiguen en una sola campaña a instancias de clientes dispares»,* dijo Shane Huntley, director de Google TAG.

> *«Algunos atacantes de hacking anuncian abiertamente sus productos y servicios a cualquiera que esté dispuesto a pagar, mientras que otros operan de forma más discreta vendiendo a una audiencia limitada».*

Se cree que una campaña recientemente montada por un operador indio de piratería informática se centró en una empresa de TI en Chipre, una institución educativa en Nigeria, una compañía de tecnología financiera en los Balcanes y una empresa de compras en Israel, lo que indica la amplitud de las víctimas.

El equipo, que Google TAG dijo que ha estado rastreando desde 2012, se ha relacionado con una serie de ataques de phishing de credenciales con el objetivo de recopilar información de

inicio de sesión asociada con agencias gubernamentales, Amazon Web Services (AWS) y cuentas de Gmail.

La campaña consiste en enviar correos electrónicos de phishing selectivo que contienen un enlace falso que, al darle clic, abre una página de phishing controlada por el atacante y diseñada para desviar las credenciales ingresadas por usuarios desprevenidos. Los objetivos incluyeron los sectores de gobierno, salud y telecomunicaciones en Arabia Saudita, Emiratos Árabes Unidos y Bahrein.

Google TAG atribuyó las actividades de los actores indios de pirateo a sueldo a una empresa llamada Rebsec, que, según su cuenta ahora inactiva de Twitter, es la abreviatura de *«Rebellion Securities»* y tiene su sede en la ciudad de Amritsar. El sitio web de la compañía, inactivo también *«por mantenimiento»* en este momento, también asegura ofrecer servicios de espionaje corporativo.

Un conjunto similar de ataques de robo de credenciales dirigidos a periodistas, políticos europeos y organizaciones sin fines de lucro, se ha relacionado con un atacante ruso llamado Void Balaur, un grupo de delincuentes cibernéticos documentado por primera vez por Trend Micro en noviembre de 2021.

En los últimos cinco años, se cree que el grupo ha seleccionado cuentas en los principales proveedores de correo web como Gmail, Hotmail y Yahoo!, además de proveedores regionales de correo electrónico como abv.bg, mail.ru, invox.lv y UKR.net.

Finalmente, TAG detalló las actividades de un grupo con sede en los Emiratos Árabes Unidos y tiene conexiones con los desarrolladores originales de un troyano de acceso remoto llamado njRAT (también conocido como H-Worm o Houdini).

Los ataques de phishing, como descubrió antes Amnistía Internacional en 2018, implican el uso de señuelos de restablecimiento de contraseña para robar credenciales de objetivos en organizaciones gubernamentales, educativas y políticas en el Medio Oriente y África del Norte.

Después del compromiso de la cuenta, el atacante mantiene la persistencia otorgando un token OAuth a una aplicación de correo electrónico legítima como Thunderbird, generando una contraseña de aplicación para acceder a la cuenta por medio de IMAP o vinculando la cuenta de Gmail de la víctima a una cuenta propiedad del adversario en un proveedor de correo tercero.

Los hallazgos llegan una semana después de que Google TAG revelara los detalles de una compañía italiana de software espía llamada RCS Lab, cuya herramienta de hacking «Hermit» se utilizó para atacar a los usuarios de Android e iOS en Italia y Kazajstán.