El individuo amenazante identificado como COLDRIVER ha persistido en llevar a cabo actividades de sustracción de credenciales dirigidas a entidades de importancia estratégica para Rusia, al mismo tiempo que perfecciona sus habilidades para evadir la detección.

El equipo de Inteligencia de Amenazas de Microsoft está monitoreando a este actor bajo el nombre de Star Blizzard (anteriormente conocido como SEABORGIUM). También es conocido como Blue Callisto, BlueCharlie (o TAG-53), Calisto (alternativamente escrito Callisto) y TA446.

> El adversario «*continúa de manera abundante atacando a individuos y organizaciones involucradas en asuntos internacionales, defensa y apoyo logístico a Ucrania, así como a instituciones académicas, empresas de seguridad informática y otras entidades alineadas con los intereses estatales rusos*», según lo expresado por Redmond.

Star Blizzard, vinculado al Servicio Federal de Seguridad (FSB) de Rusia, tiene un historial de establecer dominios falsos que imitan las páginas de inicio de sesión de empresas objetivo. Se tiene constancia de su actividad desde al menos 2017.

En agosto de 2023, Recorded Future reveló 94 nuevos dominios que forman parte de la infraestructura de ataque de este actor, la mayoría de los cuales incluyen términos relacionados con tecnología de la información y criptomonedas.

Microsoft señaló que observó al adversario utilizando scripts del lado del servidor para evitar el escaneo automatizado de la infraestructura controlada por el actor desde abril de 2023, cambiando de hCaptcha para determinar objetivos de interés y redirigiendo la sesión de navegación al servidor Evilginx.

El código JavaScript del lado del servidor está diseñado para comprobar si el navegador tiene instalados complementos, si la página está siendo accedida por una herramienta de automatización como Selenium o PhantomJS, y enviar los resultados al servidor en forma de

una solicitud POST HTTP.

> *«Después de la solicitud POST, el servidor de redirección evalúa los datos recopilados del navegador y decide si permitir la continuación de la redirección del navegador»*, informó Microsoft.

> *«Cuando se obtiene un veredicto positivo, el navegador recibe una respuesta del servidor de redirección, redirigiéndolo a la siguiente etapa de la cadena, que puede ser un hCaptcha para que lo resuelva el usuario, o la redirección directa al servidor Evilginx».*

Star Blizzard también ha comenzado a emplear servicios de marketing por correo electrónico como HubSpot y MailerLite para diseñar campañas que sirven como el punto inicial de la cadena de redirección, que culmina en el servidor Evilginx que aloja la página de sustracción de credenciales.

Además, se ha notado que el actor amenazante utiliza un servicio de nombres de dominio (DNS) para resolver la infraestructura de dominio registrada por el actor, enviando señuelos en archivos PDF protegidos por contraseña que contienen enlaces para evadir los procesos de seguridad por correo electrónico, así como para alojar los archivos en Proton Drive.

Y eso no es todo. Como indicador de que el actor amenazante sigue atentamente los informes públicos sobre sus tácticas y técnicas, ha actualizado su algoritmo de generación de dominios (DGA) para incluir una lista más aleatoria de palabras al nombrarlos.

> A pesar de estas modificaciones, Microsoft señala que *«las operaciones de Star Blizzard siguen enfocándose en el robo de credenciales de correo electrónico, dirigiéndose principalmente a proveedores de correo electrónico basados en la*

> *nube que alojan cuentas de correo electrónico tanto organizativas como personales».*

> *«Star Blizzard persiste en utilizar pares de servidores virtuales privados (VPS) dedicados para alojar la infraestructura controlada por el actor (servidores de redirección + servidores Evilginx) utilizada en actividades de spear-phishing, donde cada servidor generalmente alberga un dominio registrado por el actor».*

Sanciones del Reino Unido a Dos Integrantes de Star Blizzard

Esto surge a raíz de que el Reino Unido denunciara a Star Blizzard por sus *«intentos sostenidos y no exitosos de interferir en procesos políticos en el Reino Unido»,* al dirigirse a individuos y entidades de alto perfil mediante operaciones cibernéticas.

Además de asociar a Star Blizzard con el Centro 18, un elemento subordinado dentro del FSB, el gobierno del Reino Unido impuso sanciones a dos miembros del grupo de piratería: Ruslan Aleksandrovich Peretyatko y Andrey Stanislavovich Korinets (también conocido como Alexey Doguzhiev), por su participación en las campañas de spear-phishing.

> La actividad *«resultó en el acceso no autorizado y extracción de datos sensibles, con la intención de socavar a las organizaciones del Reino Unido y, de manera más amplia, al gobierno del Reino Unido»,* según lo expresado.