Meta Platforms informó que tomó una serie de medidas para frenar la actividad maliciosa de ocho empresas diferentes con sede en Italia, España y los Emiratos Árabes Unidos (EAU) que operan en la industria de la vigilancia por contrato.

Estos hallazgos forman parte de su Informe de Amenazas Adversarias para el cuarto trimestre de 2023. El spyware estaba dirigido a dispositivos iOS, Android y Windows.

> *«Su variado malware incluía capacidades para recopilar y acceder a información del dispositivo, ubicación, fotos y medios, contactos, calendario, correo electrónico, SMS, redes sociales y aplicaciones de mensajería, y habilitar funciones de micrófono, cámara y captura de pantalla»,* dijo la empresa.

Las ocho empresas son Cy4Gate/ELT Group, RCS Labs, IPS Intelligence, Variston IT, TrueL IT, Protect Electronic Systems, Negg Group y Mollitiam Industries.

Estas empresas, según Meta, también se dedicaron al scraping, la ingeniería social y actividades de phishing que apuntaban a una amplia gama de plataformas como Facebook, Instagram, X (anteriormente Twitter), YouTube, Skype, GitHub, Reddit, Google, LinkedIn, Quora, Tumblr, VK, Flickr, TikTok, SnapChat, Gettr, Viber, Twitch y Telegram.

Específicamente, una red de identidades ficticias vinculadas a RCS Labs, propiedad de Cy4Gate, se dice que engañó a los usuarios para que proporcionaran sus números de teléfono y direcciones de correo electrónico, además de hacer clic en enlaces falsos para llevar a cabo reconocimientos.

Otro conjunto de cuentas de Facebook e Instagram ahora eliminadas, asociadas al proveedor de spyware español Variston IT, se utilizó para el desarrollo y prueba de exploits, incluida la compartición de enlaces maliciosos. La semana pasada, surgieron informes de que la empresa está cerrando sus operaciones.

Meta también comunicó que identificó cuentas utilizadas por Negg Group para poner a

prueba la distribución de su spyware, así como por Mollitiam Industries, una compañía española que promociona un servicio de recopilación de datos y spyware orientado a Windows, macOS y Android, con el fin de extraer información pública.

En otra instancia, el gigante de las redes sociales tomó medidas contra redes de China, Myanmar y Ucrania que mostraban comportamiento coordinado y no auténtico (CIB), eliminando más de 2,000 cuentas, páginas y grupos de Facebook e Instagram.

Mientras que el conjunto chino se enfocaba en las audiencias estadounidenses con contenido vinculado a la crítica de la política exterior de EE. UU. hacia Taiwán e Israel, y su respaldo a Ucrania, la red originaria de Myanmar centró su atención en sus propios residentes con artículos originales que elogiaban al ejército birmano y menospreciaban a las organizaciones armadas étnicas y a los grupos minoritarios.

El tercer conjunto es destacado por su empleo de páginas y grupos ficticios para publicar contenido que respaldaba al político ucraniano Viktor Razvadovskyi, al mismo tiempo que compartía *«comentarios de apoyo sobre el gobierno actual y comentarios críticos sobre la oposición»* en Kazajistán.

Estos acontecimientos se dan en un momento en el que una coalición de gobiernos y empresas tecnológicas, entre las que se incluye Meta, ha suscrito un acuerdo para frenar el abuso de spyware comercial con el propósito de cometer violaciones de derechos humanos.

Como medidas defensivas, la empresa ha introducido nuevas características, como la Integridad del Flujo de Control (CFI) activada en Messenger para Android y el aislamiento de memoria de VoIP para WhatsApp, con el objetivo de dificultar la explotación y reducir la superficie de ataque en general.

Dicho esto, la industria de la vigilancia sigue prosperando en diversas formas inesperadas. El mes pasado, 404 Media, basándose en investigaciones anteriores del Consejo Irlandés de Libertades Civiles (ICCL) en noviembre de 2023, reveló una herramienta de vigilancia denominada Patternz, que aprovecha datos de publicidad en tiempo real (RTB) recopilados

de aplicaciones populares como 9gag, Truecaller y Kik para rastrear dispositivos móviles.

> *«Patternz permite a las agencias de seguridad nacional utilizar datos generados por publicidad en tiempo real e históricos para detectar, monitorear y prever acciones de los usuarios, amenazas de seguridad y anomalías basadas en el comportamiento, patrones de ubicación y características de uso móvil de los usuarios»,* afirmó ISA, la empresa israelí detrás del producto, en su sitio web.

Luego, la semana pasada, Enea reveló un ataque de red móvil previamente desconocido denominado MMS Fingerprint, que se dice que fue utilizado por el fabricante de Pegasus, el Grupo NSO. Esta información se incluyó en un contrato de 2015 entre la empresa y el regulador de telecomunicaciones de Ghana.

Aunque la técnica exacta empleada sigue siendo algo enigmático, la firma sueca de seguridad en telecomunicaciones sospecha que probablemente involucre la utilización de MM1_notification.REQ, un tipo especial de mensaje SMS conocido como SMS binario, que alerta al dispositivo receptor sobre la existencia de un MMS que aguarda ser recuperado desde el Centro de Servicio de Mensajes Multimedia (MMSC).

La recuperación del MMS se realiza mediante MM1_retrieve.REQ y MM1_retrieve.RES, siendo el primero una solicitud HTTP GET a la dirección URL contenida en el mensaje MM1_notification.REQ.

Lo notable de este enfoque es que la información del dispositivo del usuario, como User-Agent (diferente de una cadena de agente de usuario de un navegador web) y x-wap-profile, se encuentra incrustada en la solicitud GET, sirviendo así como una suerte de identificador distintivo.

> *«El User-Agent (MMS) es una cadena que típicamente identifica el sistema operativo y el dispositivo. x-wap-profile apunta a un archivo UAProf (Perfil de Agente de*

> *Usuario) que describe las capacidades de un teléfono móvil»*, explicó Enea.

Un actor de amenazas que busque desplegar spyware podría utilizar esta información para explotar vulnerabilidades específicas, personalizar sus elementos maliciosos según el dispositivo objetivo o incluso diseñar campañas de phishing más eficaces. A pesar de esto, no hay evidencia de que esta vulnerabilidad de seguridad haya sido explotada en la práctica en los últimos meses.