El viernes pasado, se dio a conocer que tanto la República Checa como Alemania fueron el blanco de una campaña de espionaje cibernético a largo plazo perpetrada por un actor estatal vinculado a Rusia conocido como APT28, lo que generó críticas por parte de la Unión Europea (UE), la Organización del Tratado del Atlántico Norte (OTAN), el Reino Unido y Estados Unidos.

El Ministerio de Relaciones Exteriores de la República Checa (MFA), en un comunicado, informó que algunas entidades no identificadas en el país fueron atacadas utilizando una vulnerabilidad de seguridad en Microsoft Outlook que se descubrió a principios del año pasado.

El MFA destacó que los ciberataques dirigidos a entidades políticas, instituciones estatales e infraestructura crítica no solo representan una amenaza para la seguridad nacional, sino que también perturban los procesos democráticos en los que se basa nuestra sociedad libre.

La vulnerabilidad en cuestión es CVE-2023-23397, un error crítico de escalada de privilegios en Outlook que ahora está parcheado y que podría permitir que un adversario accediera a hashes Net-NTLMv2 y luego los utilizara para autenticarse mediante un ataque de relé.

El Gobierno Federal de Alemania (también conocido como Bundesregierung) atribuyó al actor de amenazas un ataque cibernético dirigido al Comité Ejecutivo del Partido Socialdemócrata utilizando la misma vulnerabilidad de Outlook durante un *«período relativamente largo»,* lo que permitió *«comprometer numerosas cuentas de correo electrónico».*

Algunos de los sectores industriales objetivo de la campaña incluyen logística, armamentos, la industria aérea y espacial, servicios de tecnología de la información, fundaciones y asociaciones ubicadas en Alemania, Ucrania y Europa, con el Bundesregierung también implicando al grupo en el ataque al parlamento federal alemán (Bundestag) en 2015.

APT28, identificado como vinculado a la Unidad Militar 26165 de la agencia de inteligencia militar de Rusia GRU, también es conocido como BlueDelta, Fancy Bear, Forest Blizzard (antes Strontium), FROZENLAKE, Iron Twilight, Pawn Storm, Sednit, Sofacy y TA422 por la

comunidad de ciberseguridad.

A fines del mes pasado, Microsoft atribuyó al grupo de piratería la explotación de un componente del Spooler de Impresión de Microsoft Windows (CVE-2022-38028, puntuación CVSS: 7.8) como un día cero para entregar un malware personalizado previamente desconocido llamado GooseEgg e infiltrarse en organizaciones gubernamentales, no gubernamentales, educativas y del sector del transporte en Ucrania, Europa Occidental y América del Norte.

La OTAN afirmó que las acciones híbridas de Rusia *«constituyen una amenaza para la seguridad de los aliados».* El Consejo de la Unión Europea también señaló que la *«campaña de ciberataques maliciosos muestra el patrón continuo de comportamiento irresponsable de Rusia en el ciberespacio».*

> *«La reciente actividad del grupo cibernético ruso GRU APT28, incluido el ataque al ejecutivo del Partido Socialdemócrata alemán, es el último ejemplo de un patrón de comportamiento conocido por parte de los Servicios de Inteligencia Rusos para socavar los procesos democráticos en todo el mundo»*, declaró el gobierno del Reino Unido.

El Departamento de Estado de EE. UU. describió a APT28 como conocido por participar en un comportamiento *«malicioso, nefasto, desestabilizador y disruptivo»* y afirmó su compromiso con la *«seguridad de nuestros aliados y socios y en mantener el orden internacional basado en reglas, incluso en el ciberespacio».*

A principios de febrero, una acción coordinada de aplicación de la ley interrumpió una botnet que comprendía cientos de routers de oficinas pequeñas y domésticas (SOHO) en EE. UU. y Alemania que se cree que los actores de APT28 utilizaron para ocultar sus actividades maliciosas, como la explotación de CVE-2023-23397 contra objetivos de interés.

Según un informe de la firma de ciberseguridad Trend Micro de esta semana, la botnet de

proxy criminal de terceros se remonta a 2016 y consta de más que solo routers de Ubiquiti, abarcando otros routers basados en Linux, Raspberry Pi y servidores privados virtuales (VPS).

> *«El individuo amenazante [detrás de la red de bots] logró transferir algunos de los bots de EdgeRouter desde el servidor de mando y control (C&C) que fue desmantelado el 26 de enero de 2024, a una nueva infraestructura de mando y control configurada a principios de febrero de 2024»*, mencionó la empresa, indicando que restricciones legales y desafíos técnicos impidieron una limpieza exhaustiva de todos los routers atrapados.

Se anticipa que la actividad cibernética patrocinada por el estado ruso, como el robo de datos, los ataques destructivos, las campañas de denegación de servicio (DDoS) y las operaciones de influencia, también representará un riesgo significativo para las elecciones en regiones como Estados Unidos, el Reino Unido y la Unión Europea, por parte de varios grupos como APT44 (también conocido como Sandworm), COLDRIVER, KillNet, APT29 y APT28, según una evaluación publicada por la subsidiaria de Google Cloud, Mandiant, la semana pasada.

> *«En 2016, APT28 vinculado a la GRU comprometió objetivos de organizaciones del Partido Demócrata de Estados Unidos, así como la cuenta personal del jefe de campaña del candidato presidencial demócrata y orquestó una campaña de filtraciones antes de las elecciones presidenciales de Estados Unidos de 2016»*, señalaron los investigadores Kelli Vanderlee y Jamie Collier.

Además, datos de Cloudflare y NETSCOUT muestran un aumento en los ataques DDoS dirigidos a Suecia después de su adhesión a la alianza de la OTAN, reflejando el patrón observado durante la adhesión de Finlandia a la OTAN en 2023.

> «Los presuntos responsables de estos ataques incluyeron a los grupos de hackers

> NoName057, Anonymous Sudan, Russian Cyber Army Team y KillNet. Todos estos grupos están motivados políticamente, apoyando ideales rusos», informó NETSCOUT.

Estos acontecimientos se producen mientras que agencias gubernamentales de Canadá, el Reino Unido y Estados Unidos han emitido un nuevo folleto conjunto para ayudar a proteger a las organizaciones de infraestructuras críticas de los ataques continuos lanzados por aparentes hacktivistas pro-rusos contra sistemas de control industrial (ICS) y sistemas de tecnología operativa (OT) de pequeña escala desde 2022.

> *«La actividad de hacktivistas pro-rusos parece estar en su mayoría limitada a técnicas poco sofisticadas que manipulan equipos de ICS para crear efectos molestos. Sin embargo, las investigaciones han revelado que estos actores son capaces de técnicas que representan amenazas físicas contra entornos OT inseguros y mal configurados»,* afirmaron las agencias.

Los objetivos de estos ataques incluyen organizaciones en los sectores de infraestructuras críticas de América del Norte y Europa, como sistemas de agua y alcantarillado, presas, energía, y sectores de alimentos y agricultura.

Se ha observado que los grupos de hacktivistas obtienen acceso remoto explotando conexiones expuestas a Internet y contraseñas predeterminadas asociadas con interfaces hombre-máquina (HMI) en tales entornos, seguido por la manipulación de parámetros críticos, desactivación de mecanismos de alarma y bloqueo de operadores mediante el cambio de contraseñas administrativas.

Las recomendaciones para mitigar la amenaza incluyen fortalecer las interfaces hombre-máquina, reducir la exposición de los sistemas OT a Internet, usar contraseñas sólidas y únicas e implementar la autenticación multifactor para todo el acceso a la red OT.

> *«Estos hacktivistas buscan comprometer sistemas de control industrial (ICS) modulares y expuestos a Internet a través de sus componentes de software, como las interfaces hombre-máquina (HMI), mediante la explotación del software de acceso remoto de computación virtual (VNC) y contraseñas predeterminadas»*, señaló la alerta.