Microsoft advierte sobre un repunte entre los estados nacionales y los actores criminales que aprovechan cada vez más las vulnerabilidades de día cero divulgadas públicamente para violar los entornos de destino.

La compañía, en su Informe de defensa digital de 114 páginas, dijo que *«ha observado una reducción en el tiempo entre el anuncio de una vulnerabilidad y la mercantilización de esa vulnerabilidad»*, por lo que es importante que las organizaciones corrijan dichas vulnerabilidades de forma oportuna.

Por otro lado, un aviso de abril de 2022 de la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), encontró que los hackers están atacando *«agresivamente»* los errores de software recientemente revelados contra objetivos amplios a nivel mundial.

Microsoft dijo que solo se necesitan 14 días en promedio para que un exploit esté disponible luego de la divulgación pública de una falla, y dijo que, aunque los ataques de día cero inicialmente tienen un alcance limitado, tienden a ser adoptados rápidamente por otros atacantes, lo que lleva a eventos de sondeo indiscriminados antes de que se instalen los parches.

Además, acusó a los grupos patrocinados por el estado chino de ser *«particularmente competentes»* en el descubrimiento y desarrollo de exploits de día cero.

Esto se ha visto agravado por el hecho de que la Administración del Ciberespacio de China (CAC) promulgó una nueva regulación de informes de vulnerabilidades en septiembre de 2021 que requiere que los fallos de seguridad se informen al gobierno antes de compartirlos con los desarrolladores de productos.

Microsoft dijo además que la ley podría permitir que elementos respaldados por el gobierno

almacenen y conviertan en armas los errores informados, lo que resultará en un mayor uso de días cero para actividades de espionaje diseñadas para promover los intereses económicos y militares de China.

Algunas de las vulnerabilidades que primero explotaron los atacantes chinos antes de ser detectadas por otros grupos adversarios incluyen:

- CVE-2021-35211 (puntaje CVSS: 10.0): Una vulnerabilidad de ejecución remota de código en el servidor de transferencia de archivos administrado SolarWinds Serv-U y el software Serv-U Secure FTP que fue explotado por DEV-0322.
- CVE-2021-40539 (puntaje CVSS: 9.8): Una falla de omisión de autenticación en Zoho ManageEngine ADSelfService Plus, que fue explotada por DEV-0322 (TiltedTemple).
- CVE-2021-44077 (puntaje CVSS: 9.8): Una falla de ejecución de código remoto no autenticado en Zoho ManageEngine ServiceDesk Plus, que fue explotada por DEV-0322 (TiltedTemple).
- CVE-2021-42321 (puntaje CVSS: 8.8): Una vulnerabilidad de ejecución remota de código en Microsoft Exchange Server que se explotó tres días después de que se revelara durante el concurso de hacking de la Copa Tianfu el 16 y 17 de octubre de 2021.
- CVE-2022-26134 (puntaje CVSS: 9.8): Una vulnerabilidad de inyección del lenguaje de navegación de gráficos de objetos (OGNL) en Atlassian Confluence que probablemente haya sido aprovechada por un atacante afiliado a China contra una entidad estadounidense no identificada días antes de la divulgación de la vulnerabilidad el 2 de junio.

Los hallazgos también se producen casi un mes después de que CISA publicara una lista de las principales vulnerabilidades armadas por hackers con sede en China desde 2020 para robar propiedad intelectual y desarrollar el acceso a redes sensibles.

> *«Las vulnerabilidades de día cero son un medio particularmente efectivo para la explotación inicial y, una vez expuestas públicamente, las vulnerabilidades pueden*

> *ser reutilizadas rápidamente por otros estados nacionales y actores criminales»,* dijo la compañía.