Microsoft confirmó que Rusia está detrás del 58% de los ciberataques a gobiernos, entidades y empresas extranjeras

Rusia representó la mayor parte de los piratas informáticos patrocinados por el estado detectados por Microsoft durante el año pasado, con una participación del 58%, principalmente dirigida a agencias gubernamentales y grupos de expertos en los Estados Unidos, seguida de Ucrania, Gran Bretaña y miembros europeos de la OTAN, dijo la compañía.

La devastadora efectividad del hackeo de SolarWinds no detectado durante mucho tiempo, que principalmente violó empresas de tecnología de la información, incluida Microsoft, también aumentó la tasa de éxito de los piratas informáticos respaldados por el estado ruso al 32% en el año que finalizó el 30 de junio, en comparación con el 21% en los 12 meses anteriores.

Mientras tanto, China representó menos de 1 de cada 10 de los intentos de piratería informática respaldados por el estado detectados por Microsoft. Sin embargo, Beijing tuvo éxito el 44% de las veces en irrumpir en redes específicas, dijo Microsoft en su segundo Informe anual de defensa digital, que cubre desde julio de 2020 hasta junio 2021.

Si bien el prolífico pirateo patrocinado por el estado de Rusia es bien conocido, el informe de Microsoft ofrece detalles inusualmente específicos sobre cómo se compara con el de otros adversarios estadounidenses.Anuncios

El informe también citó los ataques de ransomware como una plaga grave y creciente, con Estados Unidos, con mucho, el país más atacado, golpeado por más del triple de los ataques de la siguiente nación más atacada. Los ataques de ransomware son criminales y están motivados económicamente.

Por el contrario, la piratería informática respaldada por el Estado se trata principalmente de la recopilación de inteligencia, ya sea para la seguridad nacional o para una ventaja comercial o estratégica, y, por lo tanto, generalmente es tolerada por los gobiernos, y los operadores cibernéticos de

Estados Unidos se encuentran entre los más capacitados. El informe de Microsoft, que trabaja en estrecha colaboración con las agencias del gobierno de Washington, no aborda la piratería del gobierno de Estados Unidos.

Sin embargo, el hackeo de SolarWinds fue tan embarazaoso para el gobierno de Estados Unidos que algunos legisladores de Washington exigieron algún tipo de represalia.

El presidente Joe Biden ha tenido dificultades para trazar una línea roja sobre qué actividad cibernética es tolerada. Ha emitido vagas advertencias al presidente Vladimir Putin para que tome medidas enérgicas contra los delincuentes de ransomware, pero varios altos funcionarios de seguridad cibernética de la administración dijeron esta semana que no han visto evidencia de que eso haya ocurrido.

En general, la piratería respaldada por un estado-nación tiene una tasa de éxito de entre el 10% y el 20%, dijo Cristin Goodwin, quien dirige la Unidad de Seguridad Digital de Microsoft, que se centra en los actores de los estado-nación. “Es algo que es realmente importante para nosotros tratar de mantenernos a la vanguardia, y seguir reduciendo ese número comprometido, porque cuanto más bajo, mejor lo estamos haciendo”, dijo Goodwin.Anuncios

Goodwin considera que los “objetivos geopolíticos” de China en su reciente ciberespionaje son especialmente notables, incluidos los ministerios de relaciones exteriores en países de América Central y del Sur, donde está realizando inversiones en infraestructura de la Iniciativa de la Franja y la Ruta, y universidades en Taiwán y Hong Kong donde la resistencia a las ambiciones regionales de Beijing es fuerte. Los hallazgos desmienten aún más como obsoleta cualquier sabiduría convencional de que los intereses de los ciberespías chinos se limitan a robar propiedad intelectual.

Los intentos de pirateo ruso aumentaron del 52% en el período 2019-20 como porcentaje de las ofertas de intrusión cibernética globales detectadas por el “servicio de notificación de estado-nación” que Microsoft emplea para alertar a sus clientes. Para el año que finalizó el 30 de junio, Corea del Norte ocupó el segundo lugar como país de origen con un 23%, frente a menos del 11% anterior. China bajó del 12% al 8%.

Pero el volumen de intentos y la eficacia son cuestiones diferentes. Microsoft descubrió que la tasa de fallas de Corea del Norte en el “spear-phishing” -dirigido a personas,

generalmente a través de correos electrónicos con trampas-, fue del 94% el año pasado.

Solo el 4% de todos los hackers respaldados por el estado que Microsoft detectó tenían como objetivo la infraestructura crítica, dijo la compañía con sede en Redmond, Washington, y los agentes rusos estaban mucho menos interesados en ella que los ciber-operativos chinos o iraníes.

Después de que se descubrió el hackeo de SolarWinds en diciembre, los rusos volvieron a centrarse principalmente en las agencias gubernamentales involucradas en la política exterior, la defensa y la seguridad nacional, seguidas de los think tanks y luego de la atención médica, donde se enfocaron en organizaciones que desarrollaban y probaban vacunas y tratamientos contra el COVID-19 en Estados Unidos, Australia, Canadá, Israel, India y Japón.

En el informe, Microsoft dijo que la reciente mayor eficacia de los piratas informáticos estatales rusos "podría presagiar más compromisos de alto impacto en el próximo año".

Más del 92% de la actividad rusa detectada fue el equipo de piratería de élite de la agencia de inteligencia extranjera SVR de Rusia, más conocida como Cozy Bear.

Cozy Bear, al que Microsoft llama Nobelium, estuvo detrás del hack de SolarWinds, que pasó desapercibido durante la mayor parte de 2020 y cuyo descubrimiento avergonzó mucho a Washington. Entre las agencias gubernamentales estadounidenses gravemente comprometidas se encontraba el Departamento de Justicia, del cual los ciberespías rusos exfiltraron el 80% de las cuentas de correo electrónico utilizadas por las oficinas de los fiscales estadounidenses en Nueva York.

Aún así, las notificaciones de ciberataques de Estados-nación de Microsoft, de las cuales alrededor de 7.500 se emitieron a nivel mundial en el período cubierto por el informe, no son de ninguna manera exhaustivas. Solo reflejan lo que detecta Microsoft.

Por Infobae