Microsoft descubrió ataques cibernéticos dirigidos a los think tanks europeos por parte de hackers vinculados al gobierno ruso, subrayando las preocupaciones de una posible interferencia en las elecciones de la Unión Europea en mayo.

La compañía estadounidense afirmó que estaba «confiada» de que los ataques dirigidos a los empleados de organizaciones como el Consejo Alemán de Relaciones Exteriores, el Instituto Aspen y el Fondo Marshall Alemá, se originaron en un grupo llamado Strontium, también conocido como Fancy Bear o APT 28.

Microsoft, que sigue investigando el origen de los ataques, afirmó anteriormente que el grupo está ampliamente asociado con el gobierno ruso.

El Consejo alemán de Relaciones Exteriores fue hackeado *«por un tiempo limitado»* el año pasado y desde entonces ha reforzado sus defensas digitales, afirmó Eva-María McCormack, portavoz del grupo de expertos de Berlín.

El anunció de Microsoft se llevó a cabo cuando los funcionarios de la UE se preparan para un intento de entremeterse en línea por parte de agentes respaldados por Rusia antes del bloque de elecciones, donde los partidos de extrema derecha están listos para obtener ganancias.

Los funcionarios están preocupados por los posibles ataques dirigidos a la tecnología de votación y aquellos diseñados para tratar de manipular el comportamiento de la votación.

> *«Los ataques validan las advertencias de los líderes europeos sobre el nivel de amenaza que deberíamos esperar ver en Europa este año»*, dijo Tom Burt, vicepresidente corporativo de Microsoft.

En un intento por obtener acceso a las credenciales de los empleados y entregar el malware, los atacantes crearon enlaces maliciosos y falsificaron direcciones de correo electrónico que parecían legítimas, mismas que apuntaban a 104 cuentas de empleados de think tanks

ubicados en Bélgica, Francia, Alemania, Polonia, Rumania y Serbia. Los ataques tuvieron lugar entre septiembre y diciembre del año pasado, aseguró Microsoft.

«Estos ataques no fueron sorpresa», dijo el presidente de German Marshall Fund Karen Donfried en un comunicado. Ella afirmó que la organización está constantemente revisando y actualizando sus protocolos a la luz de los desarrollos de seguridad cibernética. El Instituto Aspen no respondió de inmediato a solicitudes de comentarios por parte de Bloomberg.

Microsoft dijo el año pasado que descubrió la actividad de Strontium, que intentaba imitar a las organizaciones conservadores en los Estados Unidos, como el Instituto Republicano Internacional y el Instituto Hudson, en un intento aparente de interrumpir las elecciones a medio plazo de los Estados Unidos.

La compañía de ciberseguridad FireEye Inc. informó anteriormente que el grupo de piratería es un operador de recopilación de inteligencia, cuya misión principal es recopilar información en silencio para proporcionar a los responsables políticos rusos ideas.

Las redes sociales y plataformas tecnológicas, incluidas Twitter y Facebook, afirman que están intensificando los esfuerzos para detectar amenazas potenciales y proporcionar más transparencia sobre quién paga los anuncios políticos.

Alemania ha tenido una buena cantidad de ataques cibernéticos. Los hackers publicaron datos privados vinculados a la canciller Angela Merkel y muchos otros políticos alemanes en enero pasado, en lo que se llamó la mayor filtración de datos de ese país.

Los hackers también intentaron infiltrarse en las computadoras de los think tanks asociados con los partidos de la CDU y el SPD que gobernaron en 2017. Un año atrás, los piratas crearon un servidor falso en Letonia para enviar miles de correos electrónicos de phishing a los legisladores alemanes.

En 2015, los atacantes rompieron la red del parlamento del Bundestag y robaron 16 gigabytes de datos. La compañía de seguridad Trend Micro Inc. vinculó el ataque del

Bundestag y otros a Pawn Storm, otro alias para Strontium. El gobierno ruso negó repetidamente que esté pirateando poderes extranjeros.

Desde 2007, Strontium se ha dirigido a organismos gubernamentales, instituciones diplomáticas, fuerzas e instalaciones militares, periodistas y asesores políticos y organizaciones, según informes de Microsoft.