Anuncio de servicio público

FBI & CISA

Número de aviso: I-081524-PSA

15 de agosto de 2024

Para su información: las interrupciones que causen los programas de cibersecuestro de datos durante los comicios no afectarán la seguridad ni la capacidad de recuperación de la votación o del conteo de votos

El Buró Federal de Investigaciones (FBI, por sus siglas en inglés) y la Agencia de Seguridad Cibernética y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) emiten este anuncio para informar al público que, si bien los ataques por parte de programas de cibersecuestro de datos a redes gubernamentales estatales o locales o a la infraestructura electoral podrían causar retrasos limitados, no comprometerán la seguridad o la precisión de los procesos de votación o del conteo de votos.

La amenaza que presentan los programas de cibersecuestro de datos es un desafío crítico en el panorama digital actual; agentes maliciosos hacen blanco de personas, empresas e incluso de infraestructuras como las redes gubernamentales. Los programas de cibersecuestro de datos que afectan los sistemas gubernamentales estatales o locales podrían dejar inaccesibles el acceso a ciertas funciones relacionadas con las elecciones temporalmente, y hacer que los funcionarios electorales se remitan a procesos y sistemas de respaldo. Si bien esto podría afectar la celeridad de ciertos procesos, no afectaría la seguridad o la exactitud de los procesos inherentes a la votación y el conteo de votos. Los funcionarios electorales emplean un esquema de seguridad de múltiples niveles, el mismo que emplea controles tecnológicos, físicos y de procedimentales para evitar que las intrusiones cibernéticas, como los programas de cibersecuestro de datos, afecten la seguridad y la capacidad de recuperación de la votación y del conteo de votos. De ocurrir un incidente de cibersecuestro de datos que afecte sus oficinas, los funcionarios electorales tendrán planes y sistemas redundantes que posibiliten la continuación de las operaciones electorales a fin de que los votantes legalmente capacitados para hacerlo puedan votar de manera segura.

Cualquier atentado de cibersecuestro de datos exitoso dirigido a la infraestructura electoral que haya sido detectado por el FBI y la CISA se ha mantenido restringido y gestionado exitosamente, sufriendo una interrupción mínima de las operaciones electorales, y sin ningún impacto a la seguridad y la precisión de los procesos o de los sistemas de votación o tabulación.

En elecciones anteriores en los Estados Unidos y en el extranjero, agentes maliciosos han tratado de difundir o amplificar afirmaciones falsas o exageradas sobre incidentes cibernéticos para manipular la opinión pública, desacreditar el proceso electoral o socavar la confianza en las instituciones democráticas estadounidenses. A la fecha de este informe, el FBI y la CISA no tienen **ningún** informe que sugiera que la actividad cibernética, incluso los programas de cibersecuestro de datos, haya impedido en ningún momento que un votante registrado vote, haya comprometido la integridad de los votos emitidos o haya afectado la precisión de la tabulación de votos o de la información del registro de los votantes.

Recomendaciones sobre la manera de comprender y mitigar los posibles impactos de un incidente de cibersecuestro de datos dirigido contra de la infraestructura electoral:

- Buscar información sobre el registro electoral, los lugares de votación, la votación por correo, el proceso de boleta provisional y los resultados finales de los comicios con antelación a las fechas limites principales o el día de las elecciones.
- Confiar en los funcionarios electorales del gobierno estatal y local, ya que son la fuente fiable de información electoral para usted. Visitar los sitios web de sus oficinas electorales estatal y local para obtener información correcta sobre el proceso electoral. Tener cuidado con los sitios web no afiliados al gobierno local o estatal. Algunos funcionarios electorales tienen sitios web que usan un dominio ".gov", lo que indica que son un sitio oficial del gobierno. Si tiene preguntas sobre la seguridad electoral en su jurisdicción, comuníquese directamente con la oficina electoral local.
- Estar atento a las tramas relacionadas con las elecciones que busquen impedir la gestión de los comicios o alegar que ha habido un incidente cibernético contra la infraestructura o los sistemas electorales.
- Tener cuidado con las publicaciones en redes sociales, así como correos electrónicos o llamadas telefónicas no solicitados que vengan de direcciones de correo electrónico o números de teléfono desconocidos. A menudo estas comunicaciones hacen declaraciones sospechosas sobre el proceso electoral o sobre atentados cibernéticos contra la infraestructura electoral. Si usted ve o recibe este tipo de información, verifíquela comparándola con la información proporcionada por su funcionario electoral estatal o local siendo este la fuente fiable de información electoral.

La CISA y el FBI coordinan con socios electorales federales, estatales, locales y territoriales estrechamente y brindan servicios e información para salvaguardar los procesos de los comicios estadounidenses y mantener la capacidad de recuperación de las elecciones de los EE. UU. El FBI es responsable por investigar y enjuiciar a los que cometan delitos electorales, operaciones de influencia extranjera maliciosa y actividades cibernéticas maliciosas en contra de la infraestructura electoral y de otras instituciones democráticas estadounidenses. La CISA, como la agencia de gestión de riesgos sectoriales a cargo del subsector de la infraestructura electoral, ayuda a los propietarios y los operadores de la infraestructura crítica, incluso aquellos en la comunidad electoral, a garantizar la seguridad y la capacidad de recuperación de la infraestructura electoral ante las amenazas físicas y cibernéticas.

Denuncias por víctimas e información adicional

El FBI y la CISA exhortan al público a denunciar las actividades sospechosas o delictivas —como los atentados de cibersecuestro de datos— al Centro de Denuncias de Delitos en Internet (IC3) del FBI en www.ic3.gov. Los atenados cibernéticos también pueden denunciarse a la CISA llamando al

1-844-Say-CISA (1-844-729-2472), enviando un mensaje por correo electrónico a report@dhs.cisa.gov o haciendo una denuncia en línea en cisa.gov/report.

Para obtener más ayuda, incluyendo los términos comunes y las mejores prácticas, visite:

- Stop Ransomware | CISA para más recursos a fin de enfrentar más eficazmente al cibersecuestro de datos;
- CISA #Protect2024 para más recursos para proteger la infraestructura electoral contra riesgos de seguridad cibernética, física y operacional; y
- Protected Voices para obtener recursos adicionales para protegerse contra las operaciones de influencia extranjera en línea, las amenazas cibernéticas y los delitos electorales federales.