Anuncio de Servicio Público

FBI & CISA

Número de alerta: I-073124-PSA
31 de julio de 2024

Para su conocimiento: Los ataques DDoS pueden dificultar el acceso a la información

La Oficina Federal de Investigación (FBI) y la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) publican este anuncio para concientizar acerca de los ataques de denegación de servicio distribuido (DDoS) contra la infraestructura electoral, o la infraestructura de soporte que apoya las operaciones electorales, los cuales podrían obstaculizar el acceso público a la información electoral, pero no afectarían la seguridad o integridad de los procesos electorales.

Se espera que estos ataques de bajo nivel continúen a medida que nos acercamos a las elecciones generales de 2024 en los Estados Unidos, y pudiesen interrumpir la disponibilidad de algunas funciones relacionadas con las elecciones durante el ciclo electoral, tales como las herramientas de búsqueda de votantes o los informes no oficiales durante la noche de elecciones, pero no afectarán la votación en sí. Los actores de amenaza pueden afirmar falsamente que los ataques DDoS indican un riesgo relacionado con el proceso electoral, con el fin de socavar la confianza en las elecciones estadounidenses. En los últimos años, los ataques DDoS han sido una táctica popular utilizada por hacktivistas y delincuentes cibernéticos que buscan promover una causa social, política o ideológica.

Los ataques DDoS se producen cuando los atacantes cibernéticos maliciosos sobrecargan un servidor público accesible por Internet, haciendo que el servidor en cuestión se ponga lento o sea inaccesible. Esto impide temporalmente a los usuarios legítimos acceder a información o recursos en línea, como páginas web y servicios en línea, y puede interrumpir las actividades comerciales por cierto periodo de tiempo. En el caso concreto de las elecciones, los ataques DDoS dirigidos a la infraestructura electoral pueden impedir que un votante acceda a sitios web que contengan información sobre dónde y cómo votar, servicios electorales en línea como el registro de votantes o resultados electorales no oficiales.

En el evento de que actores extranjeros o delincuentes cibernéticos lleven a cabo ataques DDoS contra la infraestructura electoral u otra infraestructura de soporte a la administración electoral, los datos subyacentes y los sistemas internos permanecerían intactos, y cualquier persona con derecho a votar podría emitir su voto. En el pasado, los actores cibernéticos han expresado falsamente que los ataques DDoS han comprometido la integridad de los sistemas de votación con el fin de engañar al público con la idea de que su ataque impediría a un votante emitir su voto o podría cambiar los votos ya emitidos. El FBI y CISA no poseen información que sugiera que un ataque DDoS haya impedido alguna vez que un votante emita su voto, haya puesto en riesgo la integridad de los votos emitidos o haya interrumpido la capacidad de tabular votos o transmitir resultados electorales a tiempo.

Además de los canales de comunicación directa, como los sitios web oficiales, las oficinas electorales a lo largo de todo el país han identificado canales alternos para difundir información a los votantes, como los medios de comunicación tradicionales, los mensajes directos a los votantes y otros recursos previstos. Los funcionarios electorales disponen de múltiples salvaguardias, procesos de copia de seguridad y planes de respuesta a incidentes para limitar el impacto de un incidente DDoS y recuperarse de él con una interrupción mínima en las operaciones electorales.

Recomendaciones:

El FBI y CISA recomiendan a los votantes que tomen las siguientes precauciones:

- Buscar información en fuentes oficiales, como los funcionarios electorales estatales y locales, sobre cómo inscribirse para votar, los colegios electorales, el voto por correo y los resultados finales de las elecciones.
- Si el sitio web oficial de su oficina electoral no está disponible, póngase en contacto con su funcionario electoral estatal o local.
- Recuerde que los ataques DDoS no pueden afectar la seguridad o integridad de los sistemas electorales existentes.

CISA y el FBI coordinan estrechamente con colaboradores electorales federales, estatales y locales y proporcionan servicios e información para salvaguardar los procesos de votación en los Estados Unidos y mantener la resiliencia de las elecciones estadounidenses. El FBI es responsable de investigar y perseguir los delitos electorales, las operaciones malignas de influencia extranjera y las actividades cibernéticas maliciosas dirigidas contra la infraestructura electoral y otras instituciones democráticas estadounidenses. CISA, en su rol de Agencia Sectorial de Manejo de Riesgos a la Infraestructura Electoral, ayuda a los propietarios y operadores de infraestructuras críticas, incluyendo a aquellos en comunidad electoral, a garantizar la seguridad y resilencia de la infraestructura electoral frente a las amenazas físicas y cibernéticas.

Denuncia de víctimas e información adicional

El FBI y CISA animan al público a comunicar información acerca de actividades sospechosas o delictivas, como ataques DDoS, a su oficina local del FBI (www.fbi.gov/contact-us/field-offices-offices), llamando al 1-800-CALL-FBI (1-800-225-5324), o en línea en ic3.gov.

Los ataques DDoS que afectan la infraestructura electoral también pueden comunicarse a CISA llamando al 1-844-Say-CISA (1- 844-729-2472) o enviando un correo electrónico a report@cisa.dhs.gov. Para obtener ayuda adicional que incluya términos comunes y mejores prácticas, tales como la alfabetización mediática, visite los siguientes sitios web:

- Voces protegidas: www.fbi.gov/investigate/counterintelligence/foreign- influence/protected- voices;
- Delitos electorales y seguridad: www.fbi.gov/scams-and-safety/common-scams- and- crimes/election-crimes-and-security.
- CISA #Protect2024: https://www.cisa.gov/protect2024