Preparación y mitigación de operaciones con influencia extranjera dirigidas en contra de la infraestructura crítica

Febrero de 2022

Compendio de amenazas

Los actores maliciosos utilizan operaciones de influencia, incluyendo tácticas como información errónea, desinformación e información maliciosa (MDM, por sus siglas en inglés) para moldear la opinión pública, socavar la confianza, aumentar la división y sembrar discordia. Los actores foráneos participan en dichas acciones para sesgar el desarrollo de políticas y socavar la seguridad de los EE. UU. y nuestros aliados, perturbar los mercados y fomentar disturbios.

Si bien las operaciones de influencia tienen precedente histórico, la evolución de la tecnología, las comunicaciones y los sistemas en red han creado nuevos vectores para su explotación.

Una sola narrativa de MDM puede parecer inocua, pero cuando se promueve de manera constante en audiencias específicas y es reforzada por gente cercana e individuos con influencia, puede tener efectos complejos. Las operaciones modernas de influencia foránea demuestran cómo la explotación estratégica y consistente de temas divisivos, y el conocimiento de la audiencia objetivo y en quién dicha audiencia confía, pueden aumentar el poder y el impacto de una narrativa de MDM para las Funciones Críticas Nacionales (NCF, por sus siglas en inglés) y la infraestructura crítica. Además, los factores sociales actuales, incluida la intensa polarización y la pandemia mundial, aumentan el riesgo y el impacto de las operaciones de influencia en la infraestructura crítica de los EE. UU., especialmente por parte de actores de amenazas expertos.

En los últimos años, los actores foráneos han utilizado operaciones de influencia para persuadir las audiencias estadounidenses e impactar funciones y servicios críticos en múltiples sectores. Las operaciones de influencia extranjera se han combinado con la actividad cibernética para derivar contenido, crear confusión, aumentar la ansiedad y distraer la atención de otros eventos. A la luz del desarrollo de las tensiones geopolíticas entre Rusia y Ucrania, el riesgo de que las operaciones de influencia extranjera afecten a las audiencias nacionales ha aumentado. Las operaciones de influencia foránea observadas recientemente en el extranjero demuestran que los gobiernos extranjeros y los actores vinculados con ellos, tienen la capacidad de emplear rápidamente técnicas de influencia sofisticadas para seleccionar las audiencias de los EE. UU. con el objetivo de interrumpir la infraestructura crítica de los EE. UU. y socavar los intereses y las autoridades de los EE. UU.

Este producto de Perspectivas CISA tiene como objetivo garantizar que los propietarios y operadores de infraestructura crítica sean conscientes de los riesgos de operaciones de influencia que se aprovechan de las redes sociales y las plataformas en línea. Las organizaciones pueden tomar medidas internas y externas para garantizar una coordinación rápida de intercambio de información, así como la capacidad de comunicar información precisa y confiable para reforzar la resiliencia. CISA anima a los líderes en todas las organizaciones a tomar medidas proactivas para evaluar los riesgos de la manipulación de la información, aumentar la resiliencia y mitigar el impacto de las posibles operaciones de influencia foránea.

Evaluar el entorno de información

- Evaluar el precedente de las narrativas de MDM dirigidas a su sector.
- Aprenda cómo y dónde las personas de interés y clientes reciben información.
- Rastree las personas clave que a usted le interesan y cómo se comunica con ellas. Considere cómo estos canales le permitirían a su organización identificar y responder a la actividad de MDM. Operar según el principio de empoderar a sus asociados (NCF, por sus siglas en inglés) de confianza con información precisa.

- Supervise cualquier cambio en la actividad en línea relacionado con su organización y sector, como un aumento repentino de etiquetas o seguidores, un aumento en las búsquedas o un gran volumen de consultas.

Identificar vulnerabilidades

- Identificar vulnerabilidades potenciales que MDM podría explotar. Piense en preguntas comunes o puntos de confusión que las personas tienen sobre su sector y operaciones.

Las organizaciones deben establecer sus propios criterios para evaluar la gravedad de las narrativas de MDM. Algunos ejemplos de indicadores podrían incluir:

Alto: ¿Una narrativa amenaza significativamente con socavar su función esencial? ¿Cuáles son algunos ejemplos conocidos?
Medio: ¿Tiene una narrativa o incidente el potencial de afectar negativamente su función esencial?
Bajo: ¿Qué narrativas son claramente refutables, inverosímiles o representan una amenaza limitada?

Su evaluación puede informar su intercambio de información y su respuesta a las narrativas de MDM, lo que ayuda a decidir si se debe responder y, de ser así, cuándo. También puede guiarlo en la selección de las partes que debe involucrar con el fin de amplificar los esfuerzos de respuesta.

- Educar al personal sobre cómo proteger sus cuentas personales de redes sociales. Animar a todos los miembros del personal a usar la autenticación de múltiples factores para las cuentas en redes sociales y a revisar la configuración de privacidad para asegurarse de que saben cuál información referente a ellos está visible en línea.
- Recordar al personal que practique higiene inteligente del correo electrónico y que esté alerta a los correos electrónicos de phishing, y desaconseje hacer clic en enlaces sospechosos y/o reenviar información cuestionable.

Actividades Cibernéticas y Operaciones de Influencia:

Los actores maliciosos pueden usar la piratería y otras actividades cibernéticas como parte de las operaciones de influencia. Los piratas informáticos ayudan en la vigilancia o el reconocimiento y brindan oportunidades para ataques destructivos. El secuestro de cuentas y la desfiguración de sitios públicos pueden usarse para influir en la opinión pública. Las organizaciones deben ser conscientes de los riesgos cibernéticos y tomar medidas para reducir la probabilidad y el impacto de un compromiso potencialmente dañino.

Fortalecer los canales de comunicación

Construya su red:

Preparar canales de comunicación y establecer contactos antes de que ocurran incidentes de MDM le permite responder rápidamente y compartir información.

- Involucrar a las partes que le interesan para establecer canales de comunicación claros y mecanismos de coordinación para compartir información.
- Revisar y actualizar el sitio web de su organización para que la información sea lo más clara, transparente y accesible posible.
- Revisar y actualizar la presencia de su organización en las plataformas de redes sociales y buscar los métodos de verificación que ofrecen las plataformas para las cuentas oficiales.
- Revisar los privilegios de acceso para las cuentas de redes sociales de la empresa. Activar la autenticación multifactorial y el uso contraseñas complejas.

Comprometerse en comunicación proactiva

- Si su organización ha establecido mecanismos de comunicación con sus integrantes, personas de interés y/o la comunidad, revise estas prácticas para identificar oportunidades de mejoramiento. Esto puede incluir boletines, informes, publicaciones de blog, eventos, contenido de redes sociales, podcasts u otras actividades.
- Evaluar el alcance y el compromiso de sus esfuerzos de comunicación y ajustar su estrategia según sea necesario.

La comunicación como herramienta:

El uso de comunicaciones claras, consistentes y relevantes que no solo respondan, sino que se anticipen a MDM es una forma importante y efectiva de mantener la seguridad y generar confianza pública en su organización.

- Coordinar con otras organizaciones en su sector para difundir y reforzar los mensajes, con el objetivo de construir una red sólida de voces confiables.
- Alentar a su equipo de comunicaciones a mantenerse en contacto con medios de comunicación clave.

Desarrollar un plan de respuesta a incidentes

- Asignar a una persona para que supervise el proceso de respuesta a incidentes de MDM y las comunicaciones de crisis asociadas.
- Establecer roles y responsabilidades para la respuesta de MDM, que incluyen, entre otros, responder a las consultas de los medios, emitir declaraciones públicas, comunicarse con su personal, involucrar a la red de personas que fueron previamente identificadas como personas de interés, e implementar medidas de seguridad física.
- Asegurarse de que sus sistemas de comunicación estén configurados para manejar las preguntas que reciban. Los teléfonos, las cuentas de redes sociales y las bandejas de entrada centralizadas deben ser monitoreadas por varias personas en un horario rotativo para evitar agotamiento.
- Identificar y capacitar al personal sobre los procedimientos de presentación de informes a las empresas de redes sociales, el gobierno y/o las fuerzas del orden.
- Considerar canales y procesos de coordinación internos para identificar incidentes, delinear el intercambio de información y la respuesta. Los actores foráneos pueden combinar operaciones de influencia con actividades cibernéticas, lo que requiere una coordinación adicional para facilitar una respuesta por parte de toda la organización.

Modelo TRUST (por sus siglas en inglés)

En el entorno de la información de hoy en día, los propietarios y operadores de infraestructura critica deben desempeñar un rol proactivo en la respuesta al MDM. Aunque las narrativas de MDM difieran, el modelo TRUST para la respuesta a incidentes puede ayudar a mitigar riesgos y a proteger a las personas de interés.