Análisis de ataques: una guía para crear arquetipos y casos de estudio

Junio de 2020

THE ENGINE ROOM

Contenido

Introducción

Esta guía busca contribuir al trabajo de las personas apoyando en seguridad organizacional en analizar los ataques de seguridad digital, con el fin de ayudar a una comunidad más amplia de profesionales y organizaciones de derechos humanos a identificar tendencias de ataques y aprender estrategias de mitigación.

Esta guía proporciona dos herramientas: arquetipos de ataques y estudios de caso.

Los arquetipos de ataques ilustran patrones y escenarios de amenazas comúnmente vistos. Pueden ayudar a las organizaciones de derechos humanos a identificar las prácticas recomendadas de protección digital, según el perfil de la organización y el tipo de ataques que están experimentando (o podrían experimentar algún día debido a su perfil).

Los casos de estudios buscan apoyar a los profesionales y organizaciones de la sociedad civil al ilustrar las consecuencias de los ataques y los beneficios de implementar tácticas de mitigación, a través de una descripción detallada de un escenario del mundo real.

En general, los incidentes que son la base del análisis son recopilados mediante informes de incidentes y otras fuentes, como medios de comunicación, fuentes comunitarias y la investigación de amenazas.

Construcción de un arquetipo de ataque

Recopilación de información

Para identificar patrones de amenazas típicos, es importante recopilar la siguiente información básica que **describa los ataques:**

- Fecha del ataque (mes y año, como mínimo).
- El perfil de las personas u organizaciones afectadas, incluyendo información relativa a sus metas, tamaño, tipo de trabajo (periodistas, activistas, defensoras de derechos humanos, abogadas, por ejemplo) y en qué sector están trabajando (anticorrupción, transparencia, rendición de cuentas, derechos de las mujeres, derechos LGBTQI+, derechos a la tierra, por ejemplo).
- Localización de los destinatarios del ataque (región o país, como mínimo). El nivel de detalle dependerá de la sensibilidad de la información y de dónde se compartirá.
- Descripción del ataque. El nivel de detalle dependerá de la sensibilidad de la información y de dónde se compartirá.
- Tipo de ataque, por ejemplo: secuestro de cuenta, DDoS, malware, phishing, spear-phishing, ataque físico, watering hole (abrevadero), hackeo de sitios web o bloqueo de sitios web debido a censura.
- Información sobre cómo se detectó el incidente.

La información adicional relevante sobre **los grupos objetivo** incluye:

- ¿Qué señales le indicaron a las personas u organización que fueron atacados?
- ¿Hay señales que indiquen que el grupo fue el objetivo de este ataque? Para los ataques de spear-phishing, por ejemplo, ¿qué hizo exactamente que el individuo / organización objetivo supiera o sospechara que se trataba de ese tipo de ataque?
- ¿Existe documentación o conocimiento acerca de que el grupo ha sido atacado en el pasado?
- Más específicamente sobre los antecedentes del grupo o individuo, ¿qué tipo de trabajo están haciendo? Si se trata de un grupo activista, ¿en qué temas trabajan? Si es periodista, ¿qué temas cubre?

Información adicional relevante sobre **el contexto** en el que se desarrollaron los ataques:

- Eventos políticos, económicos o sociales importantes que ocurrieron en el país / ciudad / lugar durante el ataque. Por ejemplo, elecciones o nuevas políticas que se estén implementando en ese momento.
- Considerar si el ataque ocurrió durante un momento crítico en el país o región, como aniversarios de revueltas sociales, protestas o acciones importantes lideradas por grupos de la sociedad civil (como acciones legales).

- ¿Hubo incidentes similares en las comunidades o grupos en los que participa la defensora de derechos humanos, activista o periodista? ¿Hubo otros incidentes, incluso si parecen no estar relacionados, en el mismo período?

Análisis de la información

Luego de recopilar la información sobre el incidente, es posible que puedas identificar tendencias sobre cómo se desarrollan los ataques: patrones relacionados con la organización, grupo o personas objetivo. Para determinar estas tendencias, puedes comenzar examinando organizaciones que trabajan en contextos y sectores similares, o que comparten otros elementos y luego revisar los ataques que experimentan. O puedes comenzar revisando los ataques y sus objetivos. Por ejemplo, ¿el/los ataque/s pretenden impedir la publicación de determinadas investigaciones? ¿O interceptar comunicaciones? ¿O acceder a información relevante que posee la organización?

Otra forma en que las personas pueden apoyar su propio análisis es agregando etiquetas a la información recopilada, para luego poder aplicar filtros y buscar documentos, amenazas, registros e incidentes.

Para desarrollar estas tendencias, identificar la forma del arquetipo de ataque y compartir los arquetipos, sugerimos seguir la siguiente estructura:

Plantilla para arquetipos de ataque

A. Introducción con información del contexto que llevó a desarrollar el siguiente arquetipo de ataque.
B. Tipos de ataques.
C. Descripción de las personas u organizaciones objetivo.
D. Información del contexto imperante al momento de los ataques, incluidos eventos políticos, económicos o sociales importantes. Por ejemplo, si estos ataques ocurren durante elecciones a nivel nacional o protestas organizadas.
E. Información del contexto de la comunidad, si es relevante. Por ejemplo, un ataque puede ocurrir mientras otros miembros de la comunidad están siendo blanco de ataques o amenazas similares. Estos ataques pueden ser semejantes, o bien diferentes al descrito en el arquetipo.
F. Información contextual de la organización, si es relevante. Por ejemplo, los ataques pueden ocurrir durante un período de transición o rotación de personal.
G. Proceso típico explicando el modo en que se desarrolló el o los ataques dentro de la organización o contra un individuo, lo que implica cómo se puede detectar el ataque, qué pasos puede tomar el individuo u organización después del ataque y cuándo el profesional de seguridad organizacional comienza su apoyo. Además, puede ser útil incluir si la respuesta de la comunidad fue relevante para mitigar los efectos de los ataques.

Un ejemplo no exhaustivo de un arquetipo de ataques

Introducción
El propósito de este arquetipo es representar un patrón y escenario de amenaza típicos, que describa el perfil de organización y los tipos de ataque que experimenta, para ayudar a las organizaciones de derechos humanos a identificar las prácticas recomendadas de protección digital.

Este arquetipo se concentrará en los ataques que buscan impedir que una organización o medio de comunicación publique en línea información relevante, con un foco en los ataques DDoS.

Tipos de ataque
Un ataque DDoS se mantiene como una de las formas más efectivas de forzar el cierre de un sitio web. “Un ataque distribuido de denegación de servicio (DDoS) es un intento malicioso de interrumpir el tráfico normal de un servidor, servicio o red objetivo, al abrumar al objetivo o a su infraestructura circundante con una avalancha de tráfico de internet”[1]. En los ataques DDoS, los sitios (o páginas específicas) se ven inundados por una abrumadora carga de solicitudes, lo que ocasiona que el servidor en el que se aloja el sitio web ya no pueda aceptar más solicitudes.

Otros ataques que tienen como fin interrumpir la publicación en línea de información relevante por parte de una organización o medio pueden incluir:

- Secuestro de cuentas, ataques de spear-phishing o ataques físicos a dispositivos, con el objetivo de acceder a la administración de sitios web para eliminar o modificar información.
- Defacement de sitio web.
- Redirigir el sitio a otro contenido, como sitios web fraudulentos o maliciosos.
- Ataques de fuerza bruta.
- Acoso en las redes sociales, mediante denuncias de contenido que es consecutivamente eliminado de las plataformas.
- Intentos de censura para bloquear sitios web o cuentas de redes sociales.

Descripción de las personas u organizaciones objetivo

- Organizaciones de medios independientes
- Consorcios o agrupaciones de medios independientes
- Organizaciones de derechos humanos que expresan su desacuerdo con el gobierno o las autoridades actuales

Contexto social, político y económico relevante
Muchos casos indican que los ataques ocurren durante o alrededor de fechas importantes, incluso en aniversarios de eventos asociados con disturbios sociales o fechas que tienen especial relevancia para los movimientos de oposición del gobierno. En cuanto a los medios de comunicación, los ataques suelen coincidir con la publicación de reportajes o historias con perspectiva crítica.

Contexto comunitario relevante

[1] "What is a DSoS Attack?" Cloudflare https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Date Accessed: 06 April 2020)

Los informes sobre ataques o amenazas que buscan silenciar a las organizaciones o los medios de comunicación muestran que otras personas de la comunidad también pueden ser atacadas. Los ataques pueden ocurrir digital y/o físicamente, y pueden incluir acoso en línea, amenazas de muerte, intimidación, ataques a sitios web, revocación de registro o negativa de renovación de franquicia, abuso verbal y vigilancia policial.

Contexto organizacional relevante
No hay suficiente información.

Proceso típico del modo en que se desarrolló el ataque dentro de la organización o contra una persona.
El método de detección de estos ataques varía. En el caso de un ataque DDoS, los profesionales de seguridad digital generalmente se enteran de un posible ataque después de ser contactados por alguien cuyo sitio web fue atacado, como un descubrimiento accidental mientras solucionan otros problemas o debido a una notificación de un sistema de monitoreo que les informa sobre un alto consumo de recursos (muchos ataques más allá de los DDoS se manifiestan a través de problemas de rendimiento). Estas alertas también pueden llegar de terceros (por ejemplo, una plataforma de alojamiento), o el sitio web puede simplemente dejar de funcionar.

Los pasos a seguir después de saber del ataque también varían, pero de acuerdo con un Informe de tendencias de ataques publicado por The Engine Room en 2020, pueden incluir:

Para ataques DDoS:
- Restablecer la configuración de Cloudflare mediante[2]:
  - Cierre de la IP de Cloudflare al servidor VPS de alojamiento.
  - Bloqueo de la fuente de ataque mediante geolocalización[3].
  - Habilitación del limitador de frecuencia[4].
- Migrar el sitio web de Cloudflare a Deflect[5].
- Seguir un proceso de mitigación liderado por Deflect.
- Brindar consultoría técnica para futuros litigios.
- Cambio a un plan de alojamiento diferente (debido a un ataque que incrementó el tráfico por encima del presupuesto de alojamiento de la organización).

Para ataques relacionados con secuestro de cuentas:
- Recuperar la cuenta perdida, con la asistencia de profesionales de la línea de ayuda de seguridad digital de Access Now.
- Evaluar y fortalecer la configuración de la cuenta de usuario, como la autenticación de 2-factores o Multifactor.
- Realizar capacitaciones sobre seguridad de cuentas y seguridad digital, así como desarrollar un plan de emergencia en caso de que los ataques continúen para adoptar una estrategia de mitigación a más largo plazo.

[2] https://support.cloudflare.com/hc/en-us/articles/200170196-Responding-to-DDoS-attacks
[3] https://support.cloudflare.com/hc/en-us/articles/217074967
[4] https://www.cloudflare.com/rate-limiting/
[5] https://deflect.ca/

Creación de casos de estudio basados en las consecuencias de ataques

Recopilación de información

Para crear esta herramienta, información básica para recopilar que **describe el ataque**:

- Fecha del ataque (mes y año, como mínimo).
- El perfil de las personas u organizaciones afectadas, incluyendo información relativa a sus metas, tamaño, tipo de trabajo (periodistas, activistas, defensoras de derechos humanos, abogadas, por ejemplo) y en qué sector están trabajando (anticorrupción, transparencia, rendición de cuentas, derechos de las mujeres, derechos LGBTQI+, derechos a la tierra, por ejemplo).
- Localización de los destinatarios del ataque (región o país, como mínimo). El nivel de detalle dependerá de la sensibilidad de la información y de dónde se compartirá.
- Descripción del ataque. El nivel de detalle dependerá de la sensibilidad de la información y de dónde se compartirá.
- Tipo de ataque, por ejemplo: secuestro de cuenta, DDoS, malware, phishing, spear-phishing, ataque físico, watering hole (abrevadero), hackeo de sitios web o bloqueo de sitios web debido a censura.
- Información sobre cómo se detectó el incidente.

Información adicional relevante sobre **la respuesta al ataque**, incluyendo:

- Si el intento fue exitoso o no.
- Estrategias utilizadas para responder a ataques y técnicas de mitigación, comprendiendo tanto acciones inmediatas como medidas preventivas para protegerse de ataques futuros, y detalles sobre cualquier análisis forense posterior que se haya realizado.
- Información relacionada con la colaboración con otros profesionales, comunidades, empresas u organizaciones para detectar o desarrollar próximos pasos de mitigación.
- Si se elaboraron informes o alertas y/o cómo se compartieron los indicadores (por ejemplo, en grupos Slack o Mattermost, mediante un contacto del sector privado, grupo Signal, MISP u otros).

Información adicional relevante sobre **el impacto del ataque**, incluyendo:

- Información sobre las consecuencias sociales, políticas o legales, posteriores al ataque.
- Información relacionada con el impacto del incidente en las personas y la organización:
    a. Si reportaron el incidente, ¿parecían las personas estresadas, asustadas o preocupadas?
    b. Si el incidente se resolvió, ¿cómo logró la persona u organización recuperarse?

c. ¿Tomaron medidas para evitar que se repitiera el mismo ataque? Si es así, ¿cuáles fueron esas medidas?
d. ¿Cuáles fueron las consecuencias del ataque para el individuo objetivo? Intenta responder esta pregunta de manera integral. Un ataque digital puede afectar a una persona a nivel físico y dar lugar a un cambio de residencia o a toda una organización a nivel psicosocial, lo que resulta en que todo el personal requiera apoyo psicosocial profesional. El ataque podría dar lugar a un incremento de disputas legales en nombre de la organización.

Plantilla para estudios de caso de consecuencias de ataques

En base a la información recopilada anteriormente, se puede desarrollar un estudio de caso que siga la historia de una organización, grupo o individuo en particular, utilizando la siguiente estructura:

A. Introducción con información contextual para el desarrollo del estudio de caso.
B. Tipo de ataque, y en qué consiste.
C. Descripción del ataque particular del caso.
D. Información sobre cómo se detectó el ataque.
E. Impacto del ataque.
F. Estrategias y técnicas de mitigación.
G. Recursos para complementar las estrategias y técnicas de mitigación.

Cómo compartir estas herramientas de forma segura con la comunidad

1. Si estás recopilando datos específicamente para crear cualquiera de estas herramientas, primero comparte con el grupo objetivo información acerca de lo que planeas hacer con los datos y acerca de cómo compartirás su historia con otros.
2. En algunos casos, los profesionales elaboran los reportes usando nombres en clave, diferenciándolos para poder detallar mejor su análisis.
3. Realiza una investigación sobre el contexto que te permita evitar que identifiquen a un grupo o individuo si el caso con el que estás trabajando no es público. Por ejemplo, si solo hay un representante del movimiento Black Lives Matter (BLM) en una ciudad determinada, hacer referencia a la ciudad y a un grupo BLM podría facilitar la identificación de la persona.
4. Si la información que estás recopilando no es pública, asegúrate de obtener el consentimiento de los grupos objetivo antes de compartir la información con otros profesionales o con una red.
5. Lee la información y verifica si hay nombres, información de contacto u otros detalles identificables que, si se comparten con la persona equivocada, podrían dañar al grupo objetivo. El uso de seudónimos no siempre alcanza para proteger a tus fuentes.
6. Comparte la información solo con grupos de confianza y, cuando lo hagas, especifica las pautas para compartir con otros.

7. Debes saber que si escribes datos identificatorios y/o compartes información detallada con otros, es posible que termine en manos equivocadas. Omite los detalles para proteger a los objetivos del ataque y toma precauciones adicionales cuando sea necesario.
8. Si necesitas omitir grandes secciones del estudio de caso para preservar la seguridad del objetivo, quizás lo más adecuado sea convertirlo en un arquetipo, que requiere información considerablemente menos detallada para ser útil.