Preparación 1

Objetivo: Establecer contactos, definir procedimientos, reunir información para ahorrar tiempo durante un ataque.

- Cree una lista de todos los dominios legítimos que pertenecen a su empresa. Esto le ayudará a analizar la situación y evitar que se inicie un procedimiento de baja de un sitio web legítimo "olvidado".
- Prepare una página web alojada en la infraestructura, lista para ser publicada en cualquier momento, para advertir a sus clientes sobre un ataque de estafa en curso. Prepare y pruebe un procedimiento de implementación claro.
- Prepare formatos de correo electrónico de pedido de baja, de ser posible en varios idiomas. Los va a utilizar en todos los casos de estafa. Esto acelerará las cosas cuando trate de llegar a empresas que operan en Internet durante el proceso de baja.
- Tenga varias maneras de ser contactado de manera oportuna (si es posible 24/7):
  - Dirección de email, fácil de recordar para todos (por ejemplo: seguridad @ suorganizacion)
  - Formulario web en el sitio web de su empresa (el lugar es importante, a no más de 2 clics de distancia de la página principal)
  - Cuenta de Twitter visible

Contactos

- Mantenga una lista de todas las personas acreditadas para tomar decisiones sobre lciberdelincuencia y una eventual acción sobre el tema. De ser posible, establezca un contrato con procesos claramente establecidos..
- Establezca y mantenga una lista de contactos para baja en:
  - Las compañías de hosting
  - Registradores
  - Registro de empresas
  - Los proveedores de correo electrónico
- Establezca y mantenga contactos en los CERT a nivel mundial, pues siempre serán capaces de ayudarle si procede.

Sensibilice al cliente

No espere los incidentes de estafa para comunicarse con sus clientes. Sensibilice sobre varios tipos de estafa (fraude de lotería, estafa 419 etc.), explique lo que es y haga que sus clientes sepan que usted nunca va a contactarlos por esos temas por e-mail.

Identificación 2

Objetivo: Detectar el incidente, determinar su alcance, e involucrar a las partes apropiadas.

Detección de la estafa

- Controle de cerca todos los puntos de contacto (e-mail, formularios web, etc.)
- Implemente trampas de spam y trate de reunir spam de asociados y terceros.
- Implemente vigilancia activa de los repositorios de estafa, como por ejemplo Millersmiles o 419scam.
- Monitoree cualquier lista de correo especializado, feed RSS o Twitter al que pueda tener acceso, que pueda reportar cartas de estafa.

Utilice sistemas automatizados de control con todas estas fuentes, de manera que cada detección active una alerta para tener una reacción inmediata.

Involucre a las partes correspondientes

Tan pronto como detecte una campaña de estafa, contacte con las personas en su organización que estén acreditadas para tomar una decisión, si es que no es usted.

La decisión de actuar sobre la dirección de e-mail fraudulento debe tomarse tan pronto como sea posible, en cuestión de minutos.

Reúna evidencia

Tome muestras de los e-mails fraudulentos enviados por los estafadores. Tenga cuidado de recoger los encabezados de correo electrónico además del contenido correo. Recoja varios e-mails, si es posible, para verificar si la dirección IP del remitente real. Esto ayudará a la investigación y el análisis de si la campaña se envía de una máquina o de una botnet.

Si usted no está seguro sobre la recolección de encabezados de email, visite http://spamcop.net/fom-serve/cache/19.html

Contención 3

Objetivo: Mitigar los efectos del ataque sobre el entorno objeto.

- Difunda el contenido del correo electrónico fraudulento en los sitios web de spam y fraude así como son sus asociados.
- Comuníquese con sus clientes.

Si la marca se ve afectada, implemente la página de alerta / advertencia con información del ataque en curso.

En caso de que se vean afectados varias veces a la semana, no despliegue un mensaje de alerta, sino más bien una página muy informativa sobre la estafa, para crear conciencia.

Remedio 4

Objetivo: Adoptar medidas para detener el fraude.

- En caso de que haya una página web fraudulenta relacionada con el fraude, alojada en un sitio web comprometido, trate de ponerse en contacto con el propietario del sitio web. Explíquele claramente el fraude al propietario, de manera que tome las acciones apropiadas: eliminar el contenido fraudulento, y sobre todo mejorar la seguridad, para que el estafador no pueda volver a explotar la misma vulnerabilidad.
- En todo caso, contacte también con la empresa de alojamiento de la página web. Envíe emails a las direcciones de contacto de la empresa de alojamiento (generalmente hay una abuse @ empresadehosting) luego trate de contactar a alguien por teléfono, para acelerar las cosas.
- Contacte a las empresa de alojamiento de correo electrónico para cancelar la cuenta fraudulenta del estafador. No olvide de enviar una copia del e-mail fraudulento.

En caso que no obtenga respuesta o no se tomen medidas, llame y envíe mensajes de correo electrónico regularmente. Si la baja es demasiado lenta, póngase en contacto con un CERT local en el país en cuestión, que lo ayudará a dar de baja el fraude, y explíqueles las dificultades que enfrenta.

Recuperación 5

Objetivo: Volver al estado de funcionamiento anterior.

Evalúe el cierre del caso

- Asegúrese de que la dirección de correo electrónico fraudulento se ha cerrado.
- Si hay alguna página web fraudulenta asociada al fraude, manténgala en observación.
- Al final de la campaña de estafa, retire la página de advertencia asociada de su sitio web.

Repercusiones 6

Objetivo: Documentar los detalles del incidente, discutir las lecciones aprendidas, y ajustar los planes y las defensas.

- Considere cuáles pasos podría haber dado para responder al incidente más rápida o eficientemente.
- Actualice sus listas de contactos y agregue notas sobre la forma más eficaz de comunicarse con cada parte implicada.
- Considere cuáles relaciones dentro y fuera de la organización podrían ayudar en futuros incidentes.
- Colabore con los equipos jurídicos si se requiere una acción legal.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM # 14

Respuesta a incidentes de estafa

Lineamientos para manejar incidentes de estafa

Autor IRM: CERT SG / Cedric PERNET
Versión IRM: 1.0
email: cert.sg@socgen.com
web: http://cert.societegenerale.com
Traducción: Francisco Neira
email: neira.francisco@gmail.com
Twitter: @neirafrancisco

Extracto

Esta “Metodología de Respuesta a Incidentes” (IRM, por sus siglas en inglés) es una hoja resumen dedicada a los manejadores de incidentes que investigan un asunto de seguridad específico. Quién debe de usar estas hojas IRM?

- Administradores
- Centro de Operaciones de Seguridad (SOC)
- CISOs y sus delegados
- CSIRT (equipos de respuesta a incidentes informáticos)

Recuerde: Si usted afronta un incidente, siga el IRM, tome notas y no pierda el control. Contacte su CSIRT inmediamente si es necesario.

Pasos del manejo de incidentes

Se definen 6 pasos para manejar los incidentes de seguridad:

- Preparación: Alistarse para manejar el incidente
- Identificación: Detectar el incidente
- Contención: Limitar el impacto del incidente
- Remedio: Remover la amenaza
- Recuperación: Recobrar a una etapa normal
- Repercusiones: Delinear y mejorar el proceso