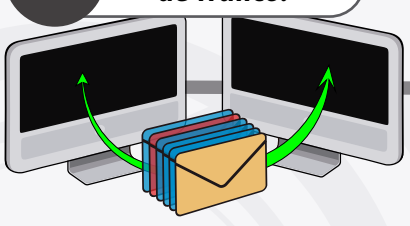
EVENTO 21/02/2019

Ataque en el medio sobre correo electrónico

0 Reunión de Entendimiento.

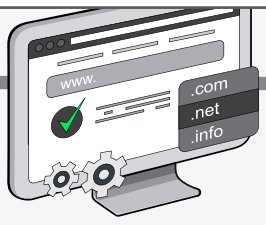
Esta reunión busca entrar en conciencia a un equipo. Se ha sufrido un evento de seguridad.

1 Identificar Flujos de Tráfico.



Se busca identificar el flujo del trafico y aislar a las partes que participan del mismo.

2 Validar Reputación de Dominios.



Se busca determinar que los dominios involucrados en el evento sean dominios validos y que no hayan sido reportados con anterioridad.

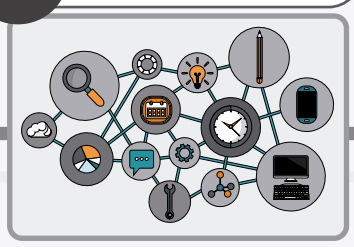
3 Identificar Contenido y Estructura de Correo.

Se busca determinar si la estructura del correo efectivamente permitía un engaño.

4 Analizar Logs Disponibles.

Se busca obtener la evidencia referente al tráfico dejado por el evento.

5 Diagramar el Evento.



Se busca mediante una infografía clarificar el evento para diferentes perfiles profesionales.

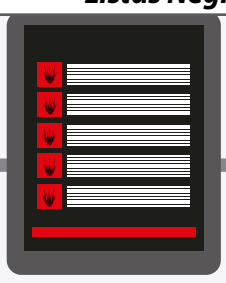
6 Denunciar a las Autoridades.

Se busca determinar si el evento va a ser comunicado a las autoridades o va a ser manejado de manera interna.

7 Bloquear Dominios Falsos.

Se bloquean en la red interna todos los dominios utilizados en el evento.

8 Reportar Dominios Falsos en Listas Negras.



Se reportan en listas negras los dominios considerados como causa raíz.

9 Configurar Controles Adicionales.

Se busca configurar controles adicionales de seguridad en las plataformas actuales para proteger las cuentas comprometidas y las que podrían llegar a ser comprometidas.

10 Gráfica de entendimiento

Se realiza una infografía para el entendimiento del proceso de identificación, control y entendimiento del evento.

BLACK HAT ARCHETYPE
DESMANTELANDO AL HACKER