Preparación 1

Objetivo: Establecer contactos, definir procedimientos, obtener información y familiarizarse con las herramientas de detección de intrusos para ahorrar tiempo durante un ataque.

Sistemas de Detección de Intrusos

- Asegúrese que las herramientas de monitoreo estén actualizadas y vigentes;
- Establezca contacto con los equipos de operación de red y de seguridad;
- Asegúrese que esté definido un proceso de notificación de alerta y que se conozca por todos.

Red

- Asegúrese que el inventario de puntos de acceso a la red esté disponible y actualizado;
- Asegúrese de que los equipos de red tengan mapas de red y configuraciones actualizados;
- Busque de forma regular y cierre posibles puntos de acceso de red no deseados (xDSL, WiFi, módem, ...);
- Asegúrese que estén en funcionamiento las herramientas de gestión de tráfico.

Línea de base tráfico

- Identifique la línea de base del tráfico y de los flujos;
- Identifique los flujos críticos de operaciones.

Identificación 2

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

Fuentes de detección:

- Notificación por el usuario / mesa de ayuda;
- Alerta del IDS;
- Detección por personal de red;
- Queja de una fuente externa.

Registre la actividad sospechosa en la red

Se puede conservar tramas de red en un archivo y transmitirlo a su equipo de respuesta a incidentes para su posterior análisis.

Para volcar el tráfico malicioso utilice herramientas de captura de red (tshark, WinDump, tcpdump ...). Utilice un "hub" o "port mirroring" en una LAN afectada para recopilar datos importantes.

La forensia de red requiere experiencia y conocimientos. Pida asistencia o consejo a su equipo de respuesta a incidentes.

Analice el ataque

- Analice las alertas generadas por el IDS;
- Revise las estadísticas y los "logs" de los dispositivos de red;
- Trate de entender el objetivo del tráfico malicioso e identifique los componentes de la infraestructura afectada por ella;
- Identifique las características técnicas del tráfico:
    - Dirección IP de origen (es)
    - Puertos utilizados, TTL, ID Paquete, ...
    - Protocolos utilizados
    - Máquinas específicas / servicios
    - Exploit (s)
    - Cuentas remotas logueadas

Al final de este paso, debería de haberse identificado las máquinas afectadas y el modus operandi del ataque. Lo ideal sería que se hubiera identificado también el origen del ataque. Aquí es donde usted debe hacer sus investigaciones forenses, si es necesario.

Si se identifica que un equipo ha sido comprometido, recurra a la IRM dedicada a la intrusión.

Contención 3

Objetivo: Mitigar los efectos de ataque en recursos de TI cercanos.

Si el asunto se considera como estratégico (acceso a recursos sensibles), deberá activarse una célula específica de gestión de crisis.

Dependiendo de la criticidad de los recursos afectados, se pueden realizar y monitorear los siguientes pasos:

Desconectar de la red la zona afectada.

Aislar el origen del ataque. Desconectar la computadora(s) para realizar investigación posterior.

- Encontrar medidas de mitigación aceptables para el tráfico crítico para el negocio en acuerdo con los administradores de las líneas de negocio.
- Terminar las conexiones no deseadas o procesos en las máquinas afectadas.
- Utilice las reglas de firewall / IPS para bloquear el ataque.
- Utilice reglas de IDS para que coincida con este comportamiento malicioso e informar al personal técnico sobre los nuevos eventos.
- Aplique acciones ad hoc en caso de problemas estratégicos:
    - Bloquee en los filtros de Internet el destino de exfiltración o ubicación remota;
    - Restrinja servidores de archivos estratégicos para que rechacen conexiones desde la computadora comprometida;
    - Seleccione el tipo de archivos pueden ser perdidos / robados y restringir el acceso a los archivos confidenciales;
    - Cree documentos falsos con marca de agua que puedan ser utilizados como una prueba de robo;
    - Notifique a los usuarios de negocio dirigidas sobre lo que debe hacerse y lo que está prohibido;
    - Configurar capacidades de registro en modo detallado sobre el medio ambiente específico y guárdelas en un servidor remoto seguro.

Remedio 4

Objetivo: Adoptar medidas para detener el comportamiento malicioso.

Bloquee la fuente

Empleando el análisis de los pasos anteriores de identificación y contención, encuentre todos los canales de comunicación utilizados por el atacante y bloquéelos en todos los perímetros de su red.

Si el origen ha sido identificado como un “insider”, tome las acciones apropiadas e involucre a su gerencia y/o equipo de RRHH y/o equipo legal.

Si el origen ha sido identificado como un delincuente externo, considere la participación de los equipos de abuso y fuerzas policiales si es necesario.

Remediación técnica

Defina un proceso de reparación. Si es necesario, este proceso puede ser validado por otra estructura, como su equipo de respuesta a incidentes, por ejemplo.

También pueden ser útiles los pasos de corrección del IRM sobre intrusión.

Probar y hacer cumplir (“enforce”)

Pruebe el proceso de remediación y asegúrese de que funciona correctamente, sin dañar ningún servicio.

Aplique el proceso de remediación una vez que las pruebas hayan sido aprobadas tanto por TI como por el negocio.

Recuperación 5

Objetivo: Restaurar el sistema a las operaciones normales.

Asegúrese que el tráfico de la red vuelve a la normalidad
Vuelva a permitir el tráfico de red que se utilizó como un vector de propagación por el atacante
Vuelva a conectar las sub-redes en conjunto si es necesario
Vuelva a conectar el área a su red local si es necesario
Vuelva a conectar la zona a Internet si es necesario
Todos estos pasos se darán uno por uno y con monitoreo técnico.

Repercusiones 6

Informe

Deberá de escribirse un informe de incidente y ponerlo a disposición de todos los interesados. Deberán de describirse los siguientes temas:

- La detección inicial.
- Las acciones y línea de tiempo.
- Lo que sí funcionó.
- ¿Qué salió mal?
- Costo del incidente

Capitalice

Deberán de definirse acciones para mejorar los procesos de detección de malware de Windows para sacar provecho de esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM #5

Comportamiento malicioso en red

Lineamientos para manejar actividad sospechosa en una red

Autores IRM: CERT SG / David Bizeul & Vincent Ferran-Lacome
Versión IRM: 1.3
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