Preparación 1

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

Apoyo del Proveedor de Servicio de Internet (ISP)

- Contacte con su ISP para entender cuáles son los servicios de mitigación para DDoS que ofrece (pagados y gratuitos) que qué procesos debe usted seguir.
- De ser posible, suscriba una conexión redundante a Internet.
- Establezca contactos con su ISP y entidades de cumplimiento de la Ley. Asegúrese que usted tiene la posibilidad de emplear una vía de comunicación 2fuera de banda", como una línea telefónica o una ADSL.

Inventario

- Prepare una lista blanca de las direcciones IP y protocolos que usted debe de permitir si prioriza el tráfico durante un ataque. No olvide incluir a sus clientes críticos, socios clave, etc.
- Documente los detalles de su infraestructura de TI, incluyendo los dueños de los negocios, direcciones IP e IDs de circuito, ajustes de ruteo (AS, etc.). Prepare un diagrama de topología de red y un inventario de activos.

Infraestructura de red

Diseñe una buena infraestructura de red sin puntos únicos de falla o cuellos de botella.

Distribuya sus servidores DNS así como otros servicios críticos en diferentes

Identificación 2

Detecte la infección

Se debe recopilar y analizar la información proveniente de diferentes fuentes:

- Bitácoras de antivirus,
- Sistemas de Detección de Intrusión (IDS),
- Intentos sospechosos de conexión a servidores,
- Gran cantidad de cuentas bloqueadas,
- Tráfico de red sospechoso,
- Intentos sospechosos de conexión a los firewalls,
- Gran incremento en llamadas a Soporte,
- Cargas altas o sistemas "colgados",
- Grandes volúmenes de email enviados,

Si se observan uno o mas de estos síntomas, deberán de contactarse a los actores definidos en la etapa "Preparación" y si es necesario, crear una célula de crisis.

Identifique la infección

Analice los síntomas para identificar el gusano, sus vectores de propagación y contramedidas.

Se pueden hallar pistas en:
Boletines de CERTs,
Contactos externos de soporte (casas de antivirus, etc.),
Sitios de Seguridad (Secunia, SecurityFocus, etc.)

Notifique al Jefe de Seguridad de la Información.
Contacte a su CSIRT si es necesario.

Evalúe el perímetro de la infección

Defina la extensión de la infección (p.e: infección global, limitada a una oficina, etc.)
De ser posible, identifique el impacto de la infección en las operaciones.

Contención 3

La célula de crisis deberá de realizar y monitorear las siguientes acciones:

1. Desconecte el área infectada de Internet
2. Aísle el área infectada. Desconéctela de cualquier red
3. Si no se puede desconectar del tráfico crítico, permítalo después de asegurarse que no es un vector de infección o después de aplicar técnicas validadas de elusión.
4. Neutralice los vectores de propagación. Un vector de propagación puede ser cualquier cosa desde el tráfico de red hasta una falla en el software. Se aplicarán contramedidas relevantes (parches, bloqueo de tráfico, deshabilitar dispositivos, etc.) Por ejemplo, se pueden emplear las siguientes:
   - Herramientas de despliegue de parches (WSUS),
   - Windows GPO,
   - Reglas de firewall,
   - Procedimientos operacionales.
5. Repita los pasos 2 al 4 en cada sub-área del área infectada hasta que el gusano deje de propagarse. Si es posible, monitoree la infección empleando herramientas de análisis (consola del antivirus, bitácoras de servidor, llamadas a Soporte)

Debe de monitorearse la dispersión del gusano.

Dispositivos móviles

Asegúrese que el gusano no pueda utilizar ninguna laptop, smartphone, PDA o dispositivo removible de almacenamiento como vector de propagación. De ser posible, bloquee las conexiones.

Pida a los usuarios finales que sigan estas instrucciones.

Remedio 4

Identifique
Identifique herramientas y métodos de remedio.
Deben de considerarse los siguientes recursos:

- Arreglos (fixes) del proveedor (Microsoft, Oracle, etc.)
- Base de datos de firmas del antivirus
- Contactos externos de Soporte
- Sitios web de Seguridad

Defina un proceso de desinfección. El proceso debe de ser validado por un órgano externo, como su CSIRT.

Pruebe
Pruebe el proceso de desinfección y asegúrese que funciona adecuadamente sin dañar algún servicio.

Despliegue
Despliegue las herramientas de desinfección. Se pueden usar varias opciones:

- Windows WSUS
- GPO
- Despliegue de firmas de antivirus
- Desinfección manual

Advertencia: Algunos gusanos podrían bloquear alguno de los métodos de despliegue de remedios. Si esto sucede, deberá de de aplicarse algún artificio.

El progreso del remedio debe de ser monitoreado por la célula de crisis.

Recuperación 5

Verifique que todos los pasos previos se hayan realizado correctamente y obtenga una aprobación de la jefatura antes de proceder con los siguientes pasos.

1. Reabra el tráfico de red que fue utilizado como método de propagación por el gusano.
2. Reconecte las sub-áreas entre sí.
3. Reconecte las laptops y móviles al área
4. Reconecte el área a su red local.
5. Reconecte el área a Internet.

Todos estos pasos deben de realizarse en una manera "paso a paso" y se debe de realizar un monitoreo técnico puesto en vigor por el equipo de crisis.

Repercusiones 6

Informe
Deberá de redactarse un informe de crisis que será distribuído entre todos los actores de la célula de manejo de crisis.

Deben de describirse los siguientes temas:
Causa inicial de la infección
Acciones y líneas de tiempo de cada evento importante
Qué salió bien
Qué salió mal
Costo del incidente

Capitalice
Deberán de definirse las acciones para mejorar los procesos de manejo de infecciones de gusanos para capitalizar esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM #4

Respuesta a Incidentes de DDoS

Lineamientos para el manejo de incidentes de Denegación Distribuída de Servicio

Autor IRM: CERT SG / 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