Preparación 1

- Se precisa de un buen conocimiento de las políticas usuales de seguridad de los sistemas operativos.
- Se precisa también de un buen conocimiento de las políticas habitualesde perfiles de usuario.
- Asegúrese de que los productos de seguridad de los equipos de cómputo y perímétricos (gateways de correo electrónico, caché de proxy) estén actualizados
- Dado que esta amenaza suele ser detectada por los usuarios finales, aumente su conocimiento de soporte de TI con respecto a la amenaza de ransomware
- Asegúrese de tener copias de seguridad minuciosas, recientes y fiables de los datos de los usuarios locales y de la red.

Identificación 2

Pricipales indicios de presencia de ransomware

Son varias las pistas pueden indicar que el sistema podría verse comprometido por el ransomware:

- Se reciben mensajes de correo electrónico inusuales (a menudo enmascarados como facturas) que contienen archivos adjuntos
- Aparece en el escritorio del usuario una “nota de secuestro” que explica que los documentos han sido cifrados y solicita el rescate con dinero.

- Los usuarios se quejan de que sus archivos no están disponibles o están dañados en sus equipos o sus carpetas compartidas en red y tienen extensiones inusuales (.abc, .xyz, .aaa, etc.).
- En las carpetas compartidas en red se están modificando numerosos archivos en un período muy corto de tiempo.

Identificación 2

Identificación basada en el host

- Busque binarios ejecutables inusuales en los perfiles de los usuarios (% ALLUSERSPROFILE% o% APPDATA%) y% SystemDrive%
- Busque las extensiones o notas de rescate antes mencionadas
- Capture una imagen de memoria de la computadora (si es posible)
- Busque procesos inusuales
- Busque patrones de adjuntos de correo electrónico inusuales
- Busque actividades inusuales en la red o navegación por Internet; Especialmente las conexiones a Tor o I2P IP, las puertas de enlace Tor (tor2web, etc) o los sitios web de pago de Bitcoin

Identificación basada en la red

- Busque patrones de conexión en los Kits Exploit
- Busque patrones de conexión a ransomware C & C
- Busque actividades inusuales en la red o navegación por Internet; Especialmente las conexiones a Tor o I2P IP, las puertas de enlace Tor (tor2web, etc) o los sitios web de pago de Bitcoin
- Busque patrones de adjuntos de correo electrónico inusuales

Contención 3

- Desconectar de la red todos los equipos que se hayan detectado como comprometidos
- Si no puede aislar el equipo, desconecte / cancele las unidades compartidas (NET USE x: \\ unc \ path \ / DELETE)
- Bloquear el tráfico a los servidores identificados de C&C del ransomware
- Enviar las muestras no detectadas al proveedor de seguridad de los equipos de cómputo.
- Enviar la URL maliciosa sin clasificar, nombres de dominio e IP a su proveedor de seguridad perimetral.

Remedio 4

- Elimine los binarios y las entradas de registro relacionadas (si las hubiera) de perfiles comprometidos (% ALLUSERSPROFILE% o % APPDATA%) y %SystemDrive%
- Si el paso anterior no es factible reinstale de una magen el equipo con una instalación limpia.

Recuperación 5

Objetivo: Restaurar el sistema a operaciones normales.

1. Actualizar las firmas antivirus para que los binarios maliciosos identificados sean bloqueados
2. Asegurarse que no haya binarios maliciosos presentes en los sistemas antes de volver a conectarlos
3. Asegurarse que el tráfico de red vuelva a la normalidad
4. Restaurar los documentos del usuario desde copias de seguridad

Todos estos pasos se realizarán paso a paso y con monitoreo del técnico.

Repercusiones 6

Informe

Un informe de incidente debe ser escrito y puesto a disposición de todos los interesados.
Deben describirse los siguientes temas:

- Detección inicial.
- Acciones y plazos.
- Lo que salió bien.
- Lo que salió mal.
- Costo del incidente.

Capitalizar

Para capitalizar esta experiencia deben definirse las acciones para mejorar los procesos de detección de intrusos de red y de malware,

- Considere los pasos que podría haber adoptado 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 apoyar en futuros incidentes.
- Colabore con los equipos jurídicos si se requiere una acción legal.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM # 17

Ransomware

Lineamientos para manejar y responder incidentes de infección por ransomware

Autor IRM: CERT SG / Jean-Philippe Teissier
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, mantenga la calma, siga el IRM y tome notas. Si es necesario contacte inmediatamente con su CSIRT.

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 proces