Homeland Security

Mejores Prácticas para la Continuidad de las Operaciones (Manejo de Malware Destructivo)

según la Dirección de Programas y Protección Nacional
Departamento de Seguridad Nacional

26 de junio de 2018

Descripción general

Si bien es poco frecuente, el malware destructivo[1] puede presentar una amenaza directa para las operaciones diarias de una organización que afectan la disponibilidad de activos y datos críticos. Las organizaciones deben aumentar la vigilancia y evaluar sus capacidades que abarcan la planificación, preparación, detección y respuesta para tal evento. Esta publicación se centra en la amenaza de los métodos de propagación distribuida a escala empresarial para el malware y proporciona orientación y consideraciones recomendadas para que una organización las aborde como parte de su arquitectura de red, línea de base de seguridad, monitoreo continuo y prácticas de respuesta a incidentes. Este documento proporciona recomendaciones y estrategias que las organizaciones pueden emplear para prepararse activamente y responder a un evento disruptivo como el malware destructivo. Estas recomendaciones también se publicaron en el sitio web de US-CERT y están disponibles en https:// www.us- cert.gov/ncas.tips/ST13-003.

Vectores de distribución potencial

El malware destructivo tiene la capacidad de dirigirse a una gran variedad de sistemas y potencialmente puede ejecutarse en múltiples sistemas a lo largo de una red. Como resultado, es importante que una organización evalúe su entorno en busca de canales atípicos para la posible entrega y/o propagación de malware a través de sus sistemas. Los sistemas a evaluar incluyen:

- Aplicaciones empresariales, en particular aquellas que tienen la capacidad de interactuar directamente con múltiples hosts y puntos finales e impactar en ellos. Los ejemplos comunes incluyen:
    - Sistemas de gestión de parches
    - Sistemas de gestión de activos
    - Software de asistencia remota (usado generalmente por el departamente de apoyo corporativo Help Desk)
    - Antivirus (desactivado)
    - Sistemas asignados al personal administrativo de sistemas y redes
    - Servidores de respaldo centralizados
    - Recursos compartidos de archivos centralizados

Si bien no se aplica específicamente al malware, los actores de amenazas podrían comprometer recursos adicionales para afectar la disponibilidad de datos y aplicaciones críticos. Los ejemplos comunes incluyen:

- Dispositivo de almacenamiento centralizado
    - Riesgo potencial: acceso directo a particiones y almacenes de datos;
- Dispositivos de red
    - Capacidad de riesgo potencial para inyectar rutas falsas dentro de la tabla de enrutamiento, eliminar rutas específicas de la tabla de enrutamiento o eliminar/modificar atributos de configuración, lo que podría aislar o degradar la disponibilidad de recursos de red críticos.

Mejores prácticas y estrategias de planificación

Se pueden seguir estrategias comunes para fortalecer la resiliencia de una organización contra el malware destructivo. La evaluación específica y la aplicación de las mejores prácticas deben emplearse para los componentes empresariales susceptibles al malware destructivo.

- Flujo de comunicación
    - Garantice una segmentación adecuada de la red[2].
    - Asegúrese de que las listas de control de acceso (ACL) basadas en la red estén configuradas para permitir la conectividad de servidor a host y de host a host a través del alcance mínimo de puertos y protocolos y que los flujos direccionales para la conectividad se representen adecuadamente.
        - El flujo de comunicación debe estar completamente definido, documentado y autorizado.

---

1 https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B, Sitio web consultado por última vez el 22 de enero de 2015.
2 http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/De..., Sitio web consultado por última vez el 22 de enero de 2015.

- Aumente el conocimiento de los sistemas que se pueden utilizar como puerta de enlace para pivotar (movimiento lateral) o conectarse directamente a puntos finales adicionales en toda la empresa.
    - Asegúrese de que estos sistemas estén contenidos dentro de VLAN restrictivas, con segmentación adicional y controles de acceso a la red.
- Asegúrese de que la red centralizada y las interfaces de administración de los dispositivos de almacenamiento residan en VLAN restrictivas.
    - Control de acceso en capas, y
    - Cumplimiento del control de acceso a nivel de dispositivo, que restringe el acceso solo desde VLAN predefinidas y rangos de IP confiables.

- Control de acceso
    - Para sistemas empresariales que pueden interactuar directamente con múltiples puntos finales:
        - Requerir autenticación de dos factores para inicios de sesión interactivos.
        - Asegúrese de que los usuarios autorizados estén asignados a un subconjunto específico del personal de la empresa.
            - Si es posible, "Todos", "Usuarios del dominio" o "Autenticados
              A los grupos de usuarios no se les debe permitir la capacidad de acceder o autenticarse directamente en estos sistemas.
        - Asegúrese de que se utilicen y documenten cuentas de dominio únicas para cada servicio de aplicación empresarial.
            - El contexto del permiso asignado a estas cuentas debe estar completamente documentado y configurado según el concepto de privilegio mínimo.
            - Brinda a una empresa la capacidad de rastrear y monitorear acciones específicas que se correlacionan con la cuenta de servicio asignada de una aplicación.
        - Si es posible, no otorgue a una cuenta de servicio permisos de inicio de sesión interactivos o locales.
            - A las cuentas de servicio se les deben denegar explícitamente los permisos para acceder a recursos compartidos de red y ubicaciones de datos críticos.
        - Las cuentas que se utilizan para autenticarse en dispositivos o servidores de aplicaciones empresariales centralizados no deben contener permisos elevados en sistemas y recursos posteriores en toda la empresa.
    - Revise continuamente las listas de control de acceso a archivos compartidos centralizados y los permisos asignados.
        - Restrinja los permisos de Escritura/Modificación/Control total cuando sea posible.
- Monitoreo
    - Audite y revise los registros de seguridad en busca de referencias anómalas a cuentas administrativas (privilegiadas) y de servicio de nivel empresarial.
        - Intentos de inicio de sesión fallidos,
        - Acceso a archivos compartidos, y
        - Inicios de sesión interactivos a través de una sesión remota.

      Revise los datos de flujo de la red en busca de signos de actividad anómala.
        - Conexiones que utilizan puertos que no se correlacionan con el flujo de comunicación estándar con una aplicación,
        - Actividad relacionada con el escaneo o la enumeración de puertos, y
        - Conexiones repetidas usando puertos que se pueden utilizar para fines de comando y control.

- Asegúrese de que los dispositivos de red registren y auditen todos los cambios de configuración.
    - Revise continuamente las configuraciones de los dispositivos de red y los conjuntos de reglas para garantizar los flujos de comunicación están restringidos al subconjunto autorizado de reglas.

Distribución de archivos

- Al implementar parches o firmas AV en toda la empresa, organice las distribuciones para incluir un grupo específico de sistemas (escalonados durante un período de tiempo predefinido).
    - Esta acción puede minimizar el impacto general en el caso de que una gestión de parches empresarial o un sistema AV se aproveche como vector de distribución para una carga útil maliciosa.
- Supervise y evalúe la integridad de los parches y las firmas AV, que se distribuyen por toda la empresa.
    - Asegúrese de que las actualizaciones se reciban solo de fuentes confiables.
    - Realizar comprobaciones de integridad de archivos y datos.
    - Supervise y audite en relación con los datos que se distribuyen desde una aplicación empresarial.

Refuerzo de sistemas y aplicaciones

- Asegúrese de que el sistema operativo (SO) subyacente y las dependencias (por ejemplo, IIS, Apache, SQL) que admiten una aplicación estén configurados y reforzados según las recomendaciones de mejores prácticas estándar de la industria[3]. Implemente controles de seguridad a nivel de aplicación basados en la guía de mejores prácticas proporcionada por el proveedor. Las recomendaciones comunes incluyen:
    - Utilice el control de acceso basado en roles.
    - Evitar que las capacidades del usuario final eludan los controles de seguridad a nivel de aplicación,
    - Ejemplo: deshabilitar AV en una estación de trabajo local.
    - Deshabilite funciones o paquetes innecesarios o no utilizados.
    - Implemente registros y auditorías sólidos de aplicaciones.
- Probar e implementar exhaustivamente los parches de los proveedores de manera oportuna.

Planificación de recuperación y reconstitución

Un análisis de impacto comercial (BIA)[4] es un componente clave de la planificación y preparación para contingencias. El resultado general de un BIA proporcionará a una organización dos componentes clave (en relación con la misión crítica/operaciones comerciales):

- Caracterización y clasificación de los componentes del sistema, y
- Interdependencias.

Con base en la identificación de los activos de misión crítica de una organización (y sus interdependencias asociadas), en caso de que una organización se vea afectada por una condición potencialmente destructiva, se deben considerar los esfuerzos de recuperación y reconstitución. Para planificar este escenario, una organización debe abordar la disponibilidad y accesibilidad de los siguientes recursos (y debe incluir el alcance de estos elementos dentro de los ejercicios y escenarios de respuesta a incidentes):

- Inventario completo de todos los sistemas y aplicaciones de misión crítica:
    - Información de versiones,
    - Dependencias del sistema/aplicación,
    - Conectividad y configuración de partición/almacenamiento del sistema, y
    - Propietarios de activos/Puntos de contacto.

[3] http://web.nvd.nist.gov/view/ncp/repository, Sitio web consultado por última vez el 22 de enero de 2015.
[4] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_err...Sitio web consultado por última vez el 22 de enero de 2015.

- Información de contacto de todo el personal esencial dentro de la organización,
- Canal de comunicación seguro para los equipos de recuperación,
- Información de contacto para recursos externos dependientes de la organización:
    - Proveedores de comunicación,
    - Proveedores (hardware/software), y
    - Socios de divulgación/partes interesadas externas
- Números de contrato de servicio para contratar soporte de proveedores,
- Puntos de contacto de adquisiciones organizacionales,
- Archivos de imagen/ISO para la restauración de línea de base de sistemas y aplicaciones críticos:
    - Medios de instalación de sistemas operativos,
    - Paquetes de servicios/parches,
    - firmware y
    - Paquetes de instalación de software de aplicación.
- Licencias/claves de activación para Sistemas Operativos (Oss) y aplicaciones dependientes,
- Diagramas de arquitectura y topología de red empresarial,
- Documentación del sistema y de la aplicación,
- Copias impresas de listas de verificación operativas y libros de jugadas,
- Archivos de copia de seguridad de la configuración del sistema y de la aplicación,
- Archivos de respaldo de datos (completos/diferenciales),
- Línea de base de seguridad de sistemas y aplicaciones y listas de verificación/directrices de refuerzo, y
- Prueba de integridad del sistema y de la aplicación y lista de verificación de aceptación.

Contención

En el caso de que una organización observe un brote a gran escala que pueda reflejar un ataque de malware destructivo[5], de acuerdo con las mejores prácticas de respuesta a incidentes, el enfoque inmediato debe ser contener el brote y reducir el alcance de los sistemas adicionales que podrían verse más afectados.

Las estrategias de contención incluyen:

- Determinar un vector común a todos los sistemas que experimentan un comportamiento anómalo (o que no están disponibles) desde el cual se podría haber enviado una carga útil maliciosa:
    - Aplicación empresarial centralizada,
    - Recurso compartido de archivos centralizado (para el cual los sistemas identificados fueron asignados o tuvieron acceso),
    - Cuenta de usuario privilegiado común a los sistemas identificados,
    - Segmento de red o límite, y
    - Servidor DNS común para resolución de nombres.
- Con base en la determinación de un vector de distribución probable, se pueden aplicar controles de mitigación adicionales para minimizar aún más el impacto:
    - Implementar listas de control de acceso basadas en la red para denegar a las aplicaciones identificadas la capacidad de comunicarse directamente con sistemas adicionales.
        - Proporciona una capacidad inmediata para aislar y aislar sistemas o recursos específicos
    - Implemente rutas de red nulas para direcciones IP específicas (o rangos de IP) desde las cuales el la carga útil puede ser distribuida,
        - El DNS interno de una organización también se puede aprovechar para esta tarea, al igual que se puede agregar un registro de puntero nulo dentro de la zona DNS para un servidor o una aplicación identificados.

[5] http://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B, Sitio web consultado por última vez el 22 de enero de 2015.

- Deshabilite fácilmente el acceso para usuarios sospechosos o cuentas de servicio, y
- Para recursos compartidos de archivos sospechosos (que pueden albergar el vector de infección), elimine el acceso o inhabilite la ruta del recurso compartido para que otros sistemas no accedan.

Prácticas adicionales recomendadas

NCCIC/ICS-CERT alienta a los propietarios de activos a tomar medidas defensivas adicionales para protegerse contra este y otros riesgos de seguridad cibernética.

- Minimice la exposición de la red para todos los dispositivos y/o sistemas del sistema de control, y asegúrese de que no se pueda acceder a ellos desde Internet.
- Ubique las redes del sistema de control y los dispositivos remotos detrás de los firewalls y aíslelos de la red empresarial.
- Cuando se requiera acceso remoto, use métodos seguros, como redes privadas virtuales (VPN), reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible. También reconozca que la VPN es tan segura como los dispositivos conectados.

ICS-CERT también proporciona una sección para las prácticas recomendadas de seguridad de los sistemas de control en la página web: http://ics-cert.us-cert.gov/content/recommended-practices. Varias prácticas recomendadas están disponibles para leer y descargar, incluyendo Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ICS-CERT recuerda a las organizaciones que realicen un análisis de impacto y una evaluación de riesgos adecuados antes de implementar medidas defensivas.

La guía adicional de mitigación y las prácticas recomendadas están disponibles públicamente en el documento de información técnica de ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, que está disponible para su descarga desde el sitio web de ICS-CERT (http://ics-cert.us-cert.gov/).

Es posible que las organizaciones deseen leer las Mejores prácticas defensivas para malware destructivo, versión 1.0, MIT-001R-2015, con fecha del 16 de enero de 2015, disponible en: https://www.nsa.gov/ia/_files/factsheets/Defending_Against_Destructive_Malware.pdf

Las organizaciones que observan cualquier actividad maliciosa sospechosa deben seguir sus procedimientos internos establecidos e informar sus hallazgos a ICS-CERT para realizar un seguimiento y correlación con otros incidentes.

Además, ICS-CERT recomienda que los usuarios tomen las siguientes medidas para protegerse de los ataques de ingeniería social:

1. No haga clic en enlaces web ni abra archivos adjuntos no solicitados en mensajes de correo electrónico.
2. Consulte Cómo reconocer y evitar estafas por correo electrónico[6] para obtener más información sobre cómo evitar las estafas por correo electrónico.
3. Consulte Cómo evitar ataques de ingeniería social y phishing[7] para obtener más información sobre los ataques de ingeniería social.

[6]Reconocer y evitar las estafas por correo electrónico http://www.us-cert.gov/reading_room/emailscams_0905.pdf, sitio web consultado por última vez el 22 de enero de 2015.
[7]Consejo de Seguridad Cibernética del Sistema Nacional de Alerta Cibernética ST04-014 http://www.us-cert.gov/cas/tips/ST04-014.html, sitio web consultado por última vez el 22 de enero de 2015.

Contactar y reportar a ICS-CERT

ICS-CERT recomienda que las organizaciones informen los incidentes cibernéticos para su seguimiento y correlación. Esto permite que ICS-CERT cree una vista general de la actividad cibernética maliciosa e informe a la comunidad para una mayor conciencia de la situación.

ICS-CERT también puede brindar asistencia a las empresas con el análisis de discos duros, malware, archivos de registro y otros artefactos. Los indicadores derivados del análisis de esos datos se eliminan de la atribución de la empresa y se devuelven a la comunidad del sistema de control industrial para su detección. El informe de incidentes permite que fluya más información procesable a la comunidad de sistemas de control industrial y, en última instancia, crea conciencia sobre las amenazas cibernéticas y ayuda a proteger CIKR.

Para cualquier pregunta relacionada con este informe, comuníquese con ICS-CERT al:
Centro de operaciones de ICS-CERT
Número gratuito: 1-877-776-7585
Internacional: 1-208-526-0900
Correo electrónico: ics-cert@hq.dhs.gov

Para la información de seguridad de los sistemas de control industrial y el reporte de incidentes:
http://ics-cert.us-cert.gov/

ICS-CERT se esfuerza continuamente por mejorar sus productos y servicios. Puede ayudar respondiendo una breve serie de preguntas sobre este producto en la siguiente URL: https://www.us-cert.gov/forms/feedback.