Administradores Sistemas Prevención ante ransomware

Autor

CERTuy - Centro Nacional de Respuesta a Incidentes de Seguridad Informática

Fecha de creación

16/04/2024

Tipo de publicación

Guías

Resumen

Herramientas prácticas para prevenir, detectar y responder a ataques de ransomware. Dirigido a administradores de sistemas que buscan proteger sus redes y sistemas críticos.

¿Qué es el Ransomware?

Ransomware es un tipo de malware cibernético diseñado para bloquear o cifrar el acceso a archivos, carpetas o infraestructura, esto puede afectar a computadoras, dispositivos móviles o servidores. En la mayoría de los casos poseen la capacidad de exfiltrar información hacia los servidores del atacante previo al cifrado.

El cifrado impide a la persona usuaria acceder a su sistema o documentos. Una vez cifrado los archivos, se suelen exigir rescates, generalmente en forma de criptomonedas, a cambio de proporcionar la clave de cifrado necesaria para restaurar el acceso a los archivos afectados.

Este tipo de ataque busca doblegar a las víctimas mediante una doble extorsión: por un lado, exigiendo un rescate a cambio de recuperar la información, y por otro, amenazándolas con hacer públicos dichos datos en caso de negarse a pagar.

Es importante destacar que pagar el rescate no garantiza siempre la recuperación de los archivos e incentiva aún más esta actividad.

Para protegerse contra este tipo de amenazas, es imprescindible prevenir, educar sobre ciberseguridad y adoptar medidas de seguridad.

Modalidades de Ataque

1. Automatizado

Los ataques de ransomware, en su mayoría, suelen estar automatizados, propagándose de manera rápida dentro de una red.

Etapas de propagación en el proceso de ataque

En la primera etapa, emplean una variedad de técnicas para obtener acceso:

- Envían correos electrónicos que contienen documentos maliciosos.
- Aprovechan debilidades en el software.
- Explotan equipos vulnerables.
- Comprometen identidades.

En una segunda etapa, buscan credenciales de administrador u otras cuentas con acceso privilegiado.

En una tercera etapa es el movimiento lateral para descubrir puntos finales.

En una cuarta etapa el compromiso de los endpoint.

Técnicas comunes utilizadas en ataques de ransomware basados en MITRE ATT&CK.

Dentro de esta modalidad se puede distinguir:

Ransomware as a Service (RaaS), que sigue un modelo de negocio SaaS (Software as a Service)* en el cual las personas desarrolladoras de ransomware proporcionan herramientas para iniciar campañas de ataque. Esto implica contratar la creación de malware como un servicio o participar a través de un programa de afiliados, distribuyendo una familia de ransomware a cambio de un porcentaje de las ganancias.

Este servicio es ofrecido por grupos de ciberdelincuentes que desarrollan este tipo de códigos maliciosos y es promovido en foros clandestinos en los que buscan reclutar personas, que son quienes contratan el servicio. Esas personas tienen acceso a una infraestructura robusta y bien desarrollada con códigos maliciosos diseñados para evadir las defensas sin necesidad de tener conocimientos de programación.

Asimismo, quienes adquieren el servicio tienen acceso a un panel de control donde podrán establecer los montos que solicitarán a cada víctima por el rescate, así como el mensaje de rescate, entre otros detalles.

*SaaS (Software as a Service) es un modelo de distribución de software a través de la nube, donde los usuarios acceden a la aplicación mediante una suscripción periódica, sin necesidad de instalaciones locales. La responsabilidad de mantenimiento recae en el proveedor de servicios en la nube.

2. Dirigido por atacantes

El ransomware dirigido por atacantes se incrementó debido a que las soluciones de seguridad actuales han mejorado en técnicas de bloqueo de phishing o malware automatizado.

Este tipo de ataque se apoya en las mismas técnicas que el ransomware automatizado para realizar la etapa de reconocimiento por quien ataca, pero se diferencia en que utiliza otros métodos para las etapas de acceso y movimiento lateral desde una posición privilegiada.

Empleando cuentas comprometidas mediante ataques de phishing o malware, se obtienen credenciales adicionales que facilitan el desplazamiento lateral dentro de la red.

Dentro de la red se buscan credenciales administrativas así como también, acceso a equipos de almacenamiento o respaldo para eliminar copias de seguridad y dejar a la organización sin acceso a las herramientas de recuperación de sus sistemas.

Recomendaciones para prevenir ataques de ransomware

En este capítulo, se exploran estrategias enfocadas en la prevención y protección de los ataques de ransomware, desde la detección temprana hasta la salvaguarda de información crítica. Se presentan formas de identificar las señales de alerta, bloquear el acceso de atacantes, limitar su escalada de privilegios y blindar los datos más valiosos.

Detección

Es importante contar con un sistema de monitoreo y análisis continuo sobre los sistemas como son los EDR (Endpoint Detection and Response) o XDR (Extended Detection and Response) que alerte y permita prevenir este tipo de amenaza.

Supervisar los eventos de archivos creados, modificados o cambios de extensión en los directorios, control de los procesos y comandos de elevación de privilegios. Este proceso se desencadena únicamente cuando se detecta un comportamiento específico, asegurando así una respuesta contextualizada a eventos particulares.

Prevenir el acceso de quien ataca

El vector de ataque se puede iniciar a través de un acceso remoto como VPN, correo electrónico, computadoras y servidores.

Recomendaciones orientadas hacia personas administradoras de sistemas:

- Mantener actualizados el software y los sistemas operativos.
- Revisar que el software y el hardware no se encuentren en su EOL (End of Life), momento a partir del cual ya no cuentan con actualizaciones a nivel de seguridad.
- Utilizar los protocolos seguros donde el tráfico es cifrado, por ejemplo, HTTPS para navegación, en correo electrónico IMAPS o SMTPS, autenticación en dominios LDAPS o para transferencia de archivos FTPS.
- Implementar un sistema de seguridad sobre los servicios de correo electrónico para poder filtrar los casos de phishing o malware.
- Bloquear los medios de almacenamiento externo.
- No publicar en internet servicios administrativos como pueden ser RDP o de la consola de algún software interno, los cuales se deberían acceder a través de una VPN o red privada.
- En el caso del acceso al servidor web, se recomienda limitar el acceso solo a personas usuarias ubicadas en Uruguay. En situaciones donde sea necesario acceder desde el exterior, se aconseja hacerlo a través de una VPN. Es importante señalar que estas medidas se aplican específicamente al servidor web y no abarcan la recepción de correos electrónicos.
- Deshabilitar las macros como predeterminadas para reducir el riesgo que el ransomware se propague a través de los archivos adjuntos de Microsoft Office.
- Para VPN es recomendable utilizar el modelo de seguridad de la red “Zero Trust”, basado en no confiar en nada y verificarlo todo.
- Utilizar MFA (Multi-factor Autentication) para incrementar la robustez de la seguridad en las cuentas.
- Establecer una política de contraseñas sólida que incluya la expiración de las mismas en un plazo definido, cada 3 o 4 meses, con un máximo de 6 meses.
- Implementar el uso de un firewall de próxima generación (NGFW) ya que tienen características más sofisticadas que los firewalls de red tradicionales y de un firewall para aplicaciones web (WAF).
- Llevar a cabo un análisis de vulnerabilidades de manera regular posibilita la revisión y evaluación de las debilidades de seguridad presentes en la infraestructura de un sistema de información.

Prevenir que quienes atacan tengan más privilegios

Contar con una estrategia de mínimo privilegio que consiste en la asignación de permisos necesarios y suficientes a un usuario para desempeñar sus actividades dentro de una organización, por un tiempo limitado y con el mínimo de derechos necesarios para realizar sus tareas.

Monitorear sistemas de identidad como Active Directory o LDAP y prevenir ataques de escalación de privilegios, se recomienda configurar auditorías de eventos para registrar actividad relacionada con autenticación y cambios de privilegios. Además, establecer alertas y notificaciones personalizadas, implementar políticas de control de acceso rigurosas, utilizar soluciones de análisis de comportamiento para identificar actividades inusuales, utilizar herramientas de monitoreo en tiempo real.

Implementar un monitoreo activo de los roles y funcionalidades asignados a usuarios es crucial para evitar la posesión indebida de privilegios que puedan surgir debido a cambios en sus responsabilidades o grupos de pertenencia.

Para detectar posibles movimientos laterales de equipos comprometidos en la red, es esencial implementar un monitoreo exhaustivo de la actividad del sistema, incluyendo el análisis de patrones de comportamiento anómalos y el seguimiento de eventos en los endpoints. Además, el uso de soluciones de análisis de seguridad contribuirá a alertar sobre cualquier desplazamiento inusual en la red.

Utilizar herramientas de gestión de acceso privilegiado PAM (Privilege Access Management) que permite definir diferentes niveles de acceso para administradores y así tener un mayor control de las acciones que cada usuario realiza en el sistema.

Otros puntos a tener en cuenta:

- Monitoreo de ataques de fuerza bruta sobre las cuentas de usuarios.
- Monitoreo de alertas sobre la deshabilitación de herramientas o controles de seguridad.
- Supervisión de cambios en las credenciales de administradores de sistemas.
- Monitoreo de la eliminación de trazas de auditoria sobre eventos de sistema o de seguridad.
- Acción inmediata para mitigar o contener un equipo comprometido en la red.

Proteger el acceso y la destrucción de la información crítica

Para proteger la información crítica es necesario tener copias de seguridad de forma programada, pueden ser con periodicidad diaria (7 últimos días), semanal (4 últimas semanas), mensual (12 últimos meses), o con la frecuencia que el negocio requiera.

La regla de 3-2-1 en la gestión de copias de seguridad se refiere a contar con tres copias de tus datos. Estas tres copias deben almacenarse en dos tipos de soportes diferentes y, además, la tercera copia debe alojarse en un lugar físico distinto.

El término "soportes diferentes" se refiere a utilizar medios de almacenamiento distintos, como discos duros externos, cintas, servicios en la nube, entre otros. Esta práctica garantiza redundancia y diversidad en caso de pérdida o corrupción de datos en un medio específico. Además, colocar la tercera copia en un lugar físico diferente mejora la protección contra eventos como desastres naturales o situaciones que puedan afectar la integridad de los datos en un solo lugar.

También es recomendable realizar una prueba de restauración de estas copias de seguridad con su procedimiento documentado, y corroborar que las copias de seguridad se realizaron correctamente.

Definir políticas de gestión de la seguridad de la información, procurando responder al contexto de su organización, objetivos de negocio, misión y enfoque de su análisis de riesgos de seguridad de la información.

Desarrollar un plan de continuidad del negocio (BCP), un plan de recuperación de desastres (DRP) y hacer simulaciones del ejercicio para prevenir este tipo de incidentes.

Auditar y monitorear los permisos de escritura/eliminación de archivos compartidos que puedan ser críticos.

Un buen mecanismo de protección es la segmentación de la red, se realiza a través de VLANs y ACLs que controlan el tráfico entre VLANs. En referencia a esto y en caso de una infección de malware, u otro problema de seguridad, esto habilita el aislamiento sólo en el segmento de red en que ha sido infectado y así no se extienda por toda la organización. Es particularmente importante para las organizaciones que mantienen sistemas que ya están fuera de su ciclo de vida (end of life) y no pueden recibir actualizaciones de seguridad.

Otra medida de seguridad posible es el software de microsegmentación, que utiliza tecnología de virtualización de red para crear zonas seguras cada vez más detalladas. Se puede utilizar para proteger cada máquina virtual de una red empresarial con controles de seguridad a nivel de aplicación basados en políticas. Dado que las políticas de seguridad se aplican a cada carga de trabajo, el software de microsegmentación puede impulsar significativamente la resistencia de una empresa a los ataques.

Referencias

Acceder a Microsoft Security

Acceder a Microsoft – Ransomware operado por Humanos

Acceder a Microsoft – Ransomware protección para empresas

Acceder al Centro Nacional de Respuesta a Incidentes de Seguridad Informática