Ransomware mitigación

Autor

CERTuy - Centro Nacional de Respuesta a Incidentes de Seguridad Informática

Fecha de creación

16/04/2024

Tipo de publicación

Guías

Resumen

Guía de respuesta para ataques de ransomware tras la infección

Introducción

En el presente documento se describen acciones a tomar en caso de ser infectado por un ataque de ransomware.

Recomendaciones para mitigar un ataque de ransomware

En primer lugar, se debe reportar al CERTuy y al equipo de respuesta ante incidente de seguridad perteneciente a la organización, en el cuál, se brindarán las medidas de seguridad para estos casos.

Información de contacto CERTuy

Correo: cert@cert.uy
Acceder al formulario de reporte de incidente
Teléfono: (+598) 150 2378
Horario de atención: todos los días las 24 Horas

Identificar equipos comprometidos y su aislamiento

Es importante identificar qué equipos fueron comprometidos, se cifraron archivos o se bloqueó el acceso; para luego aislarlos de la red y evitar que se propague hacia aquellos equipos que están en la misma red.

En el caso de contar con un Active Directory o Lightweight Directory Access Protocol (LDAP) en la misma red, también aislarlo, realizar una búsqueda de posibles modificaciones en las contraseñas, roles o grupos de los usuarios con permisos administrativos.

Búsqueda con indicadores de compromiso (IOC)

- Revisar las Group Policy Object (GPO) que se crearon o modificaron con origen desconocido.
- Escanear con un antivirus los equipos de la red donde se encontraban los equipos comprometidos.
- En estos casos se pueden utilizar las reglas Yara para identificar posibles artefactos maliciosos.Yara es una herramienta destinada a identificar y clasificar muestras de malware.
- En caso de detectar un posible artefacto verificar el hash enVirustotal, es importante no subir el binario para no dejar un registro en el sitio sobre esta detección y de esta manera estaremos alertando a quien ataca de que ha sido detectado su compromiso.
- Revisar si hubo algún incremento de tráfico de red saliente a una IP de destino desconocido para verificar si hubo una posible fuga de información.

Identificar la variante del ransomware

Realizar una búsqueda por la extensión de los archivos cifrados, como de Indicator of Compromise (IOC) que incluyen nota de rescate, correo electrónico, sitio web, dirección TOR y monedero de Bitcoin.

A parte de identificar la variante, en algunos casos, se realiza una búsqueda de las herramientas de descifrados disponibles a la fecha.

Medidas para mitigar

Después de identificar y aislar los equipos comprometidos se pueden tomar las siguientes medidas para mitigar este tipo de ataque:

- Determinar qué sistemas se vieron afectados y aislarlos inmediatamente.
- Detectar cuál fue la causa inicial del ataque para que al momento de realizar la recuperación no se vuelva a comprometer los sistemas.
- Con su equipo puede desarrollar y documentar una comprensión inicial de lo ocurrido basado en el análisis inicial.
- Si varios sistemas o subredes aparecen afectados, desconectar de la red a nivel de switch. Puede que no sea factible desconectar sistemas individuales durante un incidente.
- Priorizar el aislamiento de sistemas críticos que son esenciales para las operaciones diarias.
- Si no es posible desconectar la red temporalmente, se debe localizar el cable de red (por ejemplo, ethernet) y desconectar los dispositivos afectados de la red.
- Para los recursos en la nube, deberá tomar una instantánea de los volúmenes para obtener una copia puntual que podrá revisar más tarde para la investigación forense.
- Aislar las copias de seguridad o respaldos que estén en línea para que no sean cifrados.
- Aislar los sistemas de Active Directory o LDAP para evitar una elevación de privilegios o que otras cuentas sean comprometidas.
- Modificar las contraseñas de los usuarios de los equipos comprometidos y de administradores de sistemas.
- Después de un compromiso inicial, los actores pueden monitorear la actividad o las comunicaciones de su organización para comprender si se detectaron sus acciones.
- Aislar los sistemas de manera coordinada y utilice métodos de comunicación como llamadas telefónicas para evitar avisar a los actores de que han sido descubiertos y que se están llevando a cabo acciones de mitigación. No hacerlo podría hacer que los actores se muevan lateralmente para preservar su acceso o implementar ransomware antes de que las redes se desconecten.
- Apagar los dispositivos si no pueden descontectarse de la red para evitar una mayor propagación de la infección. Este paso evitará que su organización mantenga artefactos de infección y evidencia potencial almacenado en la memoria volátil. Debe llevarse a cabo solo si no es posible apagar temporalmente la red o desconectar los hosts afectados de la red utilizando otros medios.
- Durante los casos de respuesta a incidentes se pueden encontrar eventos donde los medios de almacenamiento son extremadamente grandes y su recolección completa se hace ineficiente. El Triage se refiere a la recolección específica de elementos del sistema, este proceso ahorra tiempo en el procedimiento de recolección, traslado y análisis, obteniendo resultados más eficientes enfocados en el análisis forense. Por esto es necesario realizar un triage de los sistemas afectados para la restauración y recuperación.
- Esta actividad puede resaltar la evidencia de sistemas adicionales o malware involucrados en etapas anteriores del ataque.
- Buscar evidencia de malware precursor, un evento de ransomware puede ser evidencia de un compromiso de red anterior no resuelto.
- Estas variantes avanzadas de malware a menudo venden acceso a una red. Con este acceso se busca filtrar datos y amenazar con divulgarlos públicamente antes de rescatar la red para extorsionar aún más a la víctima y presionarla para que pague.
- Realizar una copia de los equipos infectados, a pesar de estar encriptados es posible que dentro de un tiempo se desarrolle una herramienta que lo pueda desencriptar. Luego formatear los equipos infectados y reinstalar los sistemas operativos.
- Implementar una recuperación por etapas, dando prioridad a los sistemas críticos necesarios para mantener la operativa que puedan afectar a la organización para luego continuar con otros sistemas de menor criticidad.
- Luego de restaurar los respaldos realizar un escaneo con antivirus en los equipos, para realizar un chequeo de que los respaldos no estén infectados.

- Revisar la actividad de antivirus en equipos que no fueron comprometidos y si es posible el escaneo con otro software de antivirus para mitigar un posible movimiento lateral.

Sobre el pago del rescate

Desde el CERTuy no se recomienda realizar el pago de la nota de rescate que deja la persona atacante, algunas de las razones son las siguientes:

- El pago no asegura que la información sea desencriptada de forma parcial o total, en algunos casos se descifran los datos de forma parcial y de esta forma se vuelve a pedir otro pago, continuando con el delito de extorsión.
- El pago también deja un antecedente para los grupos de quienes atacan como futuro objetivo para este tipo de ataques por la respuesta de pago de los mismos.
- Existen casos en que los ataques fueron detenidos por investigaciones policiales y ya no existen los servidores donde se realizó la filtración y cifrado de los datos.

Referencias

Acceder a NCSC UK – Mitigating Malware and Ransomware esta guía ayuda a las organizaciones de los sectores público y privado a lidiar con los efectos del malware. Brinda acciones para orientar a las organizaciones a prevenir una infección de malware y pasos a seguir si ya están infectadas.

Por más información acceder al Centro Nacional de Respuesta a Incidentes de Seguridad Informática