PASOS TRAS UN CIBERINCIDENTE

01 Identificación, primeras acciones y coordinación

02 Contención

03 Informar a la dirección

04 Acciones legales

05 Denuncia

06 Investigación y análisis forense

07 Lecciones aprendidas

IDENTIFICACIÓN, PRIMEROS PASOS Y ACCIONES DE COORDINACIÓN 01

A **Mantener la calma y no "tirar del cable (de tensión)"**

Si se están cifrando los archivos es ya demasiado tarde, el atacante ya ha terminado de realizar su trabajo.

B **No apagar las máquinas físicas**

ya que un apagado podría impedir el posterior arranque de dicha máquina. Mejor aislar a nivel de red.

C **Se debería realizar un snapshot...**

Y en el caso de que se traten de máquinas virtuales. Después pueden pausarse si se considera necesario.

D **Realizar una desconexión a nivel de red entre centros de datos o diferentes segmentos de red**

puede resultar mucho más útil.

E **Identificar de qué atacante se trata**

Los atacantes de ransomware son grupos organizados y presentan modus operandis característicos de cada grupo.

*En algunos casos será necesario ejecutar F para identificar al atacante

F **Obtener la nota de rescate y algunos ficheros cifrados para identificar al atacante**

Es posible usar recursos online para averiguar de qué tipo de ransomware se trata, y en algunos casos particulares es posible que exista alguna opción de recuperación (pero no es lo habitual).

G **Identificar si se trata de un grupo RaaS (Ransomware as a Service) o uno independiente**

una vez identificado el tipo de ransomware.

H **Realizar la comunicación mediante un partner experto familiarizado con negociaciones**

(incluido el pago si fuese necesario).

I **Coordinación de los diferentes equipos intervinientes y Gestión de reuniones y seguimiento de los avances durante el incidente.**

Recursos online para identificar tipo de ransomware:

- https://id-ransomware.malwarehunterteam.com
- https://www.nomoreransom.org

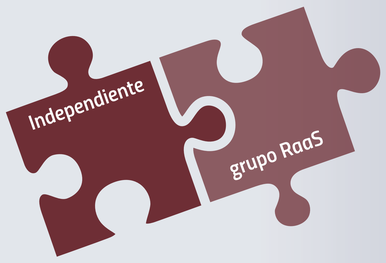
Escanea el código QR para acceder a los recursos

- **Si se trata de un grupo independiente**

  La información de inteligencia que obtengamos sobre el atacante nos indicará bastante bien cómo suelen operar. Esto puede indicarnos cuáles son las vías o vectores de entrada más habituales. Qué herramientas suelen utilizar, cómo suelen moverse lateralmente en la infraestructura, cómo suelen elevar privilegios y si suelen exfiltrar información

- **Si se trata de un grupo RaaS**

  No será tan sencillo, dado que aunque existen procedimientos comunes, cada grupo de operadores puede tener características algo diferentes.



CONTENCIÓN 02

Disponer capacidades de contención a nivel de host y red que permitan bloquear y controlar actividades consideradas maliciosas o sospechosas.

Las capacidades deben ser tecnológicas (herramientas: EDR, Firewall, etc) y humanas (conocimiento, capacidad de decisión, procedimientos, workflows, etc).

Tratar de aplicar políticas restrictivas que permitan tráfico hacia direcciones conocidas (whitelist) y confiables y monitorizar el trafico bloqueado para detectar posibles compromisos en la infraestructura

Proteger los sistemas de *Backup* aislando las copias realizadas del resto de la infraestructura *(Backups offline)* y verificar el estado de las posibles copias de seguridad.

Desconectar los unidades compartidas, servidores de ficheros o NAS de la red interna

Deshabilitar la exposición hacia Internet de servicios no esenciales que puedan haber sido explotados

Forzar el cambio de credenciales de los usuarios potencialmente comprometidos o sospechosos

Considerar el cambio de credenciales del usuario del KRBTGT (siguiendo el procedimiento de Microsoft) en caso de que haya indicios de acceso a dichas credenciales (Golden Ticket)

Aplicar mecanismos de 2FA para el acceso a los servicios corporativos (VPN, correo electrónico, servicios de gestión...)

En cada paso bloquear los diferentes IOC obtenidos durante la investigación del incidente (usuarios, dominios, IPs, ficheros maliciosos)

INFORMAR A LA DIRECCIÓN 03

Esta comunicación no debe esconder la realidad ni debe de suavizarse dado que las decisiones de negocio deben tomarse con toda la información en la mano. Hay que hacerlo de forma clara y sin tecnicismos y se deben de proporcionar todos los detalles posibles. La información debe suministrarse de forma continua según avanzan las horas y días trás el incidente.

Hay que tratar de responder a cuestiones como las siguientes: cuándo comenzó el ataque, cuánto tiempo estuvo el atacante, cómo consiguieron entrar, qué tipo y volumen de información ha sido accedida, si hay evidencias de exfiltración, etc

04 ACCIONES LEGALES

Notificar a la AEPD <72h

Cuando se detecta una brecha de seguridad de los sistemas que afecte a datos personales se deberá notificar a la AEPD durante las 72 horas siguientes a la **detección**

https://www.ismsforum.es/ficheros/descargas/guia-gestion-brechas-datos-20231676503894.pdf

Con posterioridad, se podrá aportar más información

Con posterioridad a dicha comunicación se podrá aportar información complementaria como por ejemplo un informe forense detallado del incidente

DENUNCIA 05

Si se aportan ciertos datos se podrán iniciar acciones judiciales que ayuden a identitificar a los atacantes, etc.

¿POR QUÉ?

Si suben las estadísticas de incidentes, el estado podrá dedicar más recursos a la persecución de estos delitos.

06 INVESTIGACIÓN Y ANÁLISIS FORENSE

La investigación forense se encarga de analizar con un gran nivel de profundidad diferentes aspectos clave del incidente.

Siempre que sea posible lo debe realizar un tercero experto.

- Localizar el vector de entrada usado por el atacante — 01
- Determinar las acciones llevadas a cabo en el sistema incluida la potencial exfiltración de información — 02
- Identificación de la familia de ransomware — 03
- Evaluación de la amenaza, para determinar si sigue activa — 04
- Identificar los sistemas afectados — 05
- Cadena de custodia de las fuentes de información relevantes — 06
- Triage y priorización del análisis en función de las debilidades de la infraestructura, información del grupo atacante y sistemas afectados — 07
- Documentar los resultados y evidencias analizadas y presentar reportar final — 08

LECCIONES APRENDIDAS 07

A **PUESTA EN COMÚN**

Tras la finalización del incidente y vuelta a la normalidad es fundamental realizar el ejercicio de poner en común entre todos los participantes aquellas cuestiones relevantes del incidente que permitan definir elementos de mejora de cara a evitar que se produzcan incidentes similares en el futuro.

B **IDENTIFICAR PUNTOS A MEJORAR**

Mejoras en la monitorización para detectar el ataque en fases previas, mejoras en la respuesta, mejoras en la comunicación interna, mejoras en la securización de la infraestructura, parcheado de sistemas,...