Taxonomía de incidentes

Grupo formado por:

- Israel Valderrama
- Alejandro Seoane
- Victor Jiménez

Enlace a la presentación

Índice

Taxonomía de incidentes **1**
Índice **1**
1. Introducción **2**
2. Incidentes **2**
2.1. Contenido malicioso 2
2.1.1. Sistema infectado 2
2.1.2. Distribución de malware 3
2.1.3. Configuración de malware 5
2.2. Disponibilidad 6
2.2.1. Mala configuración 6
2.2.2. Interrupción 7
2.3. Compromiso de la información 8
2.3.1. Modificación no autorizada de información 8
2.4. Fraude 9
2.4.1. Suplantación 9
2.5. Vulnerable 11
2.5.1. Amplificador DDoS 11
3. Conclusión **12**
4. Bibliografía **12**

1. Introducción

Los incidentes de ciberseguridad representan eventos que comprometen la confidencialidad, integridad o disponibilidad de los sistemas de información. Este trabajo presenta una taxonomía de incidentes, describiéndolos y presentando ejemplos reales. Para ello se han desarrollado 8 incidentes de los presentes en la Matriz de taxonomía de INCIBE-CERT.

2. Incidentes

En este apartado se muestran las tablas referentes a cada uno de los incidentes.

2.1. Contenido malicioso

2.1.1. Sistema infectado

Información general	
Descripción	Equipo o dispositivo comprometido con malware como pueden ser los virus, ransomware o spyware.
Funcionamiento	El malware entra al sistema a través de medios como correos electrónicos, descargas maliciosas, vulnerabilidades sin parches o USB infectados.
Identificación	Lentitud del sistema, comportamiento extraño, aparición de ventanas emergentes, procesos desconocidos ejecutándose, o archivos corruptos.
Protección	Mantener el software actualizado, utilizar un antivirus confiable, evitar enlaces sospechosos y realizar análisis regulares del sistema.

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
Breve descripción	Malware dirigido al programa nuclear de Irán mediante USBs infectados, afectando sistemas críticos. El virus Stuxnet tomó control de 1.000 máquinas en la planta nuclear de Natanz, ordenándo se autodestruirse.
Agrupación/Tipo	Gusano.

Origen	EE.UU. e Israel (según expertos, aunque no confirmado oficialmente).
Perfiles usuarios afectados	Infraestructura nuclear y sistemas industriales
Número y tipología de sistemas afectados	Miles de máquinas de producción de materiales nucleares. Específicamente, 1.000 centrifugadoras para enriquecer uranio.
Categoría (Importancia de los sistemas afectados)	Crítico (infraestructura nacional).
Peligrosidad e Impacto del incidente	Alta. Logró dañar físicamente la infraestructura del "mundo real", siendo el primer ataque cibernético de este tipo.
Prioridad que tu le darías	Máxima.

2.1.2. Distribución de malware

Información general	
Descripción	Propagar software malicioso a través de redes, dispositivos o plataformas para afectar otros sistemas.
Funcionamiento	Los atacantes distribuyen malware mediante phishing, redes P2P (Peer-to-peer), sitios web comprometidos, o dispositivos infectados.
Identificación	Recibir correos o mensajes sospechosos con enlaces o archivos adjuntos, o encontrar aplicaciones que descargaste de fuentes no confiables.
Protección	No abrir enlaces o archivos adjuntos de fuentes desconocidas, configurar filtros de correo para evitar spam y correos no deseados y descargar aplicaciones solo de tiendas oficiales.

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://www.cloudflare.com/es-es/learning/security/ransomware/wannacry-ransomware/
Breve descripción	Ataque ransomware que explotó una vulnerabilidad de Windows, paralizando hospitales, empresas y universidades.

Agrupación/Tipo	Ransomware
Origen	Hackers del Grupo Lazarus (Corea del Norte)
Perfiles usuarios afectados	Usuarios corporativos e instituciones de salud.
Número y tipología de sistemas afectados	Más de 200,000 ordenadores en más de 150 países.
Categoría (Importancia de los sistemas afectados)	Alta
Peligrosidad e Impacto del incidente	Muy alto
Prioridad que tu le darías	Máxima

2.1.3. Configuración de malware

Información general	
Descripción	Recurso que aloje ficheros de configuración de malware.
Funcionamiento	Los atacantes configuran el malware para elegir objetivos específicos, modificar rutas de infección o establecer formas de comunicación encubierta.
Identificación	Cambios no autorizados en configuraciones del sistema, scripts sospechosos o herramientas de administración remota no instaladas por el usuario.
Protección	Monitorea cambios en la configuración de sistemas, emplea herramientas de detección de anomalías, y asegúrate de restringir accesos no autorizados.

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://www.bbc.com/mundo/noticias-55836181
Breve descripción	Troyano utilizado para robar información financiera mediante correos electrónicos maliciosos y phishing.
Agrupación/Tipo	Troyano

Origen	Desconocido
Perfiles usuarios afectados	Bancos, pequeñas empresas y usuarios corporativos.
Número y tipología de sistemas afectados	Miles de ordenadores
Categoría (Importancia de los sistemas afectados)	Alta
Peligrosidad e Impacto del incidente	Muy alto
Prioridad que tu le darías	Alta

2.2. Disponibilidad

2.2.1. Mala configuración

Información general	
Descripción	Fallo de configuración en el software que está directamente asociado con una pérdida de disponibilidad de un servicio. Esto desencadena en problemas de funcionamiento, seguridad o rendimiento.
Funcionamiento	Los sistemas o servicios no funcionan correctamente debido a malas configuraciones, causando así interrupciones o accesos limitados.
Identificación	Funcionamiento incorrecto de un servicio, problemas al acceder, rendimiento fuera de lo normal, etc.
Protección	Para mayor protección se debería implementar algún proceso de revisión de las configuraciones, realizar auditorías, etc.

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://www.xatakamovil.com/aplicaciones/peor-fallo-whatsapp-fecha-se-debio-a-mala-configuracion-routers-facebook

Breve descripción	WhatsApp, Instagram y Facebook sufrieron una caída global de más de seis horas debido a una mala configuración de los routers de Facebook.
Agrupación/Tipo	Disponibilidad / Mala configuración
Origen	Error interno en la configuración de los routers de Facebook
Perfiles usuarios afectados	Millones de usuarios de WhatsApp, Instagram y Facebook en todo el mundo
Número y tipología de sistemas afectados	Servidores y sistemas de red de Facebook, afectando a múltiples plataformas
Categoría (Importancia de los sistemas afectados)	Crítico (afectó servicios de comunicación global)
Peligrosidad e Impacto del incidente	Muy alto (interrupción prolongada de servicios esenciales de comunicación)
Prioridad que tu le darías	Máxima

2.2.2. Interrupción

Información general	
Descripción	Es un evento que causa la indisponibilidad de un servicio o sistema, impidiendo el acceso a los usuarios temporalmente.
Funcionamiento	Puede deberse a ataques DDoS, fallos técnicos, eventos externos que afecten al sistema…
Identificación	Se identifica cuando el servicio no da respuesta, los tiempos de carga son excesivos, fallos en la conexión, mensajes del propio servicio (como por ejemplo “servicio no disponible temporalmente”).
Protección	Implementación de redundancia (alta disponibilidad y continuidad del servicio), sistema de monitoreo y detección, mantenimiento preventivo, planes de continuidad del negocio…

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://elpais.com/tecnologia/2024-07-19/un-fallo-de-microsoft-provoca-incidencias-a-nivel-global-en-aerolineas-bancos-y-otros-sistemas.html

Breve descripción	El problema, que ha afectado desde aeropuertos a hospitales, surgió de una actualización en un antivirus de la firma de ciberseguridad CrowdStrike que bloquea el sistema Windows.
Agrupación/Tipo	Disponibilidad / Interrupción
Origen	Error en actualización de software de seguridad
Perfiles usuarios afectados	Empresas y usuarios finales de múltiples sectores (hospitales, aeropuertos, bancos…)
Número y tipología de sistemas afectados	Sistemas operativos Windows en ordenadores de todo el mundo
Categoría (Importancia de los sistemas afectados)	Crítico (afectó infraestructuras y servicios esenciales)
Peligrosidad e Impacto del incidente	Muy alto (interrupción de servicios a nivel global)
Prioridad que tu le darías	Máxima

2.3. Compromiso de la información

2.3.1. Modificación no autorizada de información

Información general	
Descripción	Es una vulnerabilidad de seguridad que ocurre cuando se modifican datos sin el permiso correspondiente.
Funcionamiento	Mediante vulnerabilidades un atacante consigue modificar los datos sin los permisos necesarios .
Identificación	Para la modificación autorizada de información debemos tener sistemas de autenticación multifactor.
Protección	Para la protección podemos implementar un sistema MFA, utilizar registros de auditorías para poder controlar todas las modificaciones que se realicen.

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://elpais.com/tecnologia/2024-08-01/y-si-estan-usando-fotos-de-su-hijo-para-entrenar-una-inteligencia-artificial.html
Breve descripción	El problema es que LAION-5B que es un repositorio de imágenes utilizaba imágenes de menores sin consentimiento los cuales incluían datos identificables.
Agrupación/Tipo	Uso no autorizado de datos personales para entrenamiento de IA
Origen	LAION-5B
Perfiles usuarios afectados	Menores de edad (principalmente de Brasil y Australia)
Número y tipología de sistemas afectados	Se ha encontrado 360 fotos en las que aparecen niños australianos y brasileños
Categoría (Importancia de los sistemas afectados)	Alta por la sensibilidad de los datos de los menores.
Peligrosidad e Impacto del incidente	Alta, ya que compromete la privacidad de los menores.
Prioridad que tu le darías	Alta ya que tienen que proteger los datos de los menores y prevenir futuros incidentes.

2.4. Fraude

2.4.1. Suplantación

Información general	
Descripción	Consiste en hacerse pasar por otra persona o empresa para obtener información confidencial o cometer delitos a nombre de otras personas o empresas.
Funcionamiento	Mediante técnicas como phising obtienen los datos de una persona y una vez los tienen se crean perfiles falsos y hacen el delito que el ciberdelincuente necesite.
Identificación	Se consigue detectar debido a la actividad sospechosa en correos, cuentas etc.

Protección	Implementar autenticación de dos factores, usar contraseñas fuertes, mantener el software actualizado, etc.

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://www.cope.es/programas/mediodia-cope/noticias/alejandro-victima-una-suplantacion-identidad-empezaron-llegar-denuncias-casa-20220505_2065547
Breve descripción	Un ciberdelincuente obtuvo la copia del DNI de la víctima y lo utilizó para contratar líneas telefónicas, después puso varios anuncios de ventas de perros y estafó a los compradores.
Agrupación/Tipo	Suplantación de identidad con DNI
Origen	Copia de DNI
Perfiles usuarios afectados	Ciudadanos
Número y tipología de sistemas afectados	Sistemas de contratación de telefonía.
Categoría (Importancia de los sistemas afectados)	Alta. Ya que afecta a los sistemas de identificación de personas.
Peligrosidad e Impacto del incidente	Alto ya que la persona que fué afectada tuvo varias denuncias y gastos de hasta 20000 €.
Prioridad que tu le darías	Alta. Debido al impacto tanto legal como financiero que tuvo la víctima

2.5. Vulnerable

2.5.1. Amplificador DDoS

Información general	
Descripción	Un ataque DDoS por amplificación de DNS es cuando un atacante usa servidores de DNS para enviar una gran cantidad de tráfico a un objetivo, haciendo que su servicio se caiga.

Funcionamiento	El atacante manda solicitudes a servidores DNS abiertos usando la dirección IP de la víctima.
Identificación	Tráfico que viene de direcciones IP falsificadas.
Protección	Limitar el uso de servidores DNS abiertos. Usar herramientas que puedan detectar y detener esos ataques DDoS.

Ejemplo de caso real	
URL de la noticia/descripción del incidente	https://www.genbeta.com/actualidad/github-acaba-de-sobrevivir-el-ataque-ddos-mas-grande-de-la-historia
Breve descripción	Github sufrió el mayor ataque DDoS registrado hasta el momento, llegando a un pico de tráfico 1.35 Terabits por segundo.
Agrupación/Tipo	Ataque DDoS port amplificación de Memcached.
Origen	Servidores que no estaban preparados y además aceptaban todo tipo de solicitudes.
Perfiles usuarios afectados	Usuarios de github en todo el mundo.
Número y tipología de sistemas afectados	Servidores e infraestructura de red.
Categoría (Importancia de los sistemas afectados)	Alta. Debido a que github es una plataforma para el desarrollo de software.
Peligrosidad e Impacto del incidente	Alto. Se interrumpió el servicio durante 10 minutos.
Prioridad que tu le darías	Muy alta. Debido a la importancia que tiene github.

3. Conclusión

En resumen, el análisis de los incidentes de ciberseguridad muestra como de vulnerables son los sistemas hoy en día. A lo largo del trabajo, hemos visto diferentes tipos de problemas, como malware, configuraciones erróneas y ataques DDoS. Un caso importante

fue el ataque DDoS a GitHub, que generó un tráfico enorme y afectó a millones de usuarios en todo el mundo.
Con esto hemos visto lo importante que es tener buena seguridad y estar atentos a las posibles nuevas amenazas.

4. Bibliografía

https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
https://www.cloudflare.com/es-es/learning/security/ransomware/wannacry-ransomware/
https://www.bbc.com/mundo/noticias-55836181
https://www.xatakamovil.com/aplicaciones/peor-fallo-whatsapp-fecha-se-debio-a-mala-configuracion-routers-facebook
https://elpais.com/tecnologia/2024-07-19/un-fallo-de-microsoft-provoca-incidencias-a-nivel-global-en-aerolineas-bancos-y-otros-sistemas.html
https://elpais.com/tecnologia/2024-08-01/y-si-estan-usando-fotos-de-su-hijo-para-entrenar-una-inteligencia-artificial.html
https://www.cope.es/programas/mediodia-cope/noticias/alejandro-victima-una-suplantacion-identidad-empezaron-llegar-denuncias-casa-20220505_2065547
https://www.genbeta.com/actualidad/github-acaba-de-sobrevivir-el-ataque-ddos-mas-grande-de-la-historia