2.a-Taxonomía de Incidentes

Enlace al Repositorio

Github ->
https://github.com/IES-Rafael-Alberti/23-24-G1-Ciberseguridad/tree/main/Incidentes/2.a%20-%20Taxonom%C3%ADa%20de%20incidentes

Índice

Contenido Abusivo

Spam

¿Qué es?	Es cualquier comunicación no solicitada enviada en masa. Aunque suele enviarse por correo electrónico, el spam también se distribuye a través de mensajes de texto (SMS), soportes sociales o llamadas telefónicas
¿Cómo funciona?	Envían información en masa a un número amplio de usuarios
Cómo identificarlo	Chequeando que los mensajes o llamadas que nos llegan no son de remitentes deseados
Cómo protegernos	Utilizando dos correos, aplicando reglas, apuntandonos a la lista Robinson, filtros antispam (listas negras), utilizar la copia oculta CCO.

Noticia

URL	https://www.eldebate.com/tecnologia/20230201/peligroso-correo-suplantan-policia-acusarte-delito-cns_90384.html
Resumen	Los ciberdelincuentes utilizaban correo spam haciéndose pasar por la policía acusando de un delito de pornografía infantil, intentando hacerles pagar una multa a demás de sus datos.
Agrupación	Spam, Fraude
Origen	Externo, grupo de ciberdelincuentes
Categoría	Económica, confidencialidad y integridad de los datos del ciudadano
Usuarios afectados	Ciudadanía Española General
Número y tipología de sistemas afectados	No se ven afectados ningún sistema en específico, solo los usuarios de correo españoles.
Impacto	Alto, ya que se ve comprometido tanto la economía como muchos datos de españoles

Delito de odio

¿Qué es?	Es la motivación del autor que consiste en el rechazo u hostilidad hacia el que considera diferente.
¿Cómo funciona?	Cuando el autor comete una infracción motivado por el odio o discriminación que siente hacia la víctima.
Cómo identificarlo	Hay que comprobar que cumple las dos condiciones: que está recogido como delito y que se produce el delito por el rechazo que al agresor le produce la víctima al creer que pertenece a un grupo determinado.
Cómo protegernos	Bloqueando a dicho usuario, reportándose a las autoridades correspondientes.

Noticia

URL	https://www.elespanol.com/espana/tribunales/20231128/denuncian-delito-odio-responsable-lgtb-ugt-tuitear-gais-derechas-dan-asco/812918797_0.html
Resumen	Denunciaron a un alto cargo de la UGT por un presunto delito de odio al postear en su Twitter que los gais de derecha daban asco.
Agrupación	Delito de odio
Origen	Interno, una persona ha insultado directamente a un colectivo.
Categoría	Discriminación
Usuarios afectados	Todo el colectivo LGTB con ideologías de derechas
Número y tipología de sistemas afectados	No se ven afectados ningún sistema ya que es un incidente que involucra a personas.
Impacto	Bajo, ya que solo afecta a un grupo pequeño de ciudadanos y no desemboca ninguna pérdida económica ni personal.

Pornografía infantil, contenido sexual o violento inadecuado

Descripción	Material que represente de manera visual contenido relacionado con pornografía infantil, apología del odio, etc.
Funcionamiento	Puede propagarse de diversas maneras en la web, a menudo a través de sitios web, foros, redes sociales y correo electrónico.
Identificación	Este tipo de contenido puede estar presente de muchas formas, algunas de ellas pueden ser: ● Contenido que parece inapropiado o te haga estar incómodo. ● Solicitudes de información personal o imágenes/videos privados. ● Mensajes o publicaciones que promueven odio o violencia. ● Cualquier contenido que involucre a menores en actividades sexuales
Protección	Algunas medidas que se pueden tomar son: ● No compartir información personal con desconocidos en línea. ● Utilizar configuraciones de privacidad en redes sociales. ● Informar de actividades sospechosas a las autoridades pertinentes. ● En caso de menores, enseñarles los peligros existentes en internet

Noticia sobre Pornografía infantil, contenido sexual o violento inadecuado

URL	https://www.europapress.es/illes-balears/noticia-detenido-menor-edad-distribucion-pornografia-infantil-20231208101106.html
Agrupación	Pornografía infantil
Origen	Videoconsola/red social

Categoría	Distribución de pornografía infantil online
Perfiles usuarios afectados	Usuarios de la red social por el cual fue compartida
Número y tipología de sistemas afectados	Persona que ha recibido el video
Impacto del incidente	Exposición de contenido ilegal, puede tener acciones legales.

Contenido Dañino

Sistema infectado

Descripción	Sistema infectado con malware. Ejemplo: sistema, computadora o teléfono móvil infectado con un rootkit.
Funcionamiento	El malware se propaga e infecta el sistema.
Identificación	• El equipo funciona más lento de lo normal. • La velocidad de internet es más lenta. • Aumenta la cantidad de anuncios que aparecen, ventanas emergentes, reenvío a ciertas direcciones, etc. • Se instalan programas no deseados
Protección	• Mantener todos los sistemas actualizados. • Instalar un antivirus. • Descargar aplicaciones de desarrolladores confiables. • Evitar hacer clic en enlaces sospechosos. • No visitar sitios web no seguros. • Realizar análisis constantemente en busca de malware

Noticia sobre Sistema infectado

URL	https://www.elespanol.com/omicrono/software/20200122/virus-informatico-desconectado-hospital-torrejon/461704059_0.html

Agrupación	Contenido dañino: ransomware
Origen	Externo, por hackers internacionales.
Categoría	Ataque de ransomware
Perfiles usuarios afectados	Personal del hospital, pacientes y otros usuarios del sistema del hospital.
Número y tipología de sistemas afectados	Todos los sistemas informáticos del hospital.
Impacto del incidente	Alto, ha dejado sin acceso a los sistemas informáticos del hospital, además de comprometer información sensible respecto a los pacientes.

Servidor C&C

TIPO DE INCIDENTES	DESCRIPCIÓN	FUNCIONAMIENTO	IDENTIFICACIÓN	PROTECCIÓN
Servidor C&C (Mando y Control)	Es la capacidad de gestionar de manera perjudicial y malintencionada de un sistema que controla acciones de un conjuntos de dispositivos comprometidos	Se lleva a cabo una serie de técnicas y procesos diseñados para mantener el control malicioso sobre la red de dispositivos.	• El análisis de tráfico de red con, por ejemplo, la búsqueda de conexiones no autorizadas • Observar el comportamiento de los sistemas, por si hay algo sospechoso. • Utilizar Bases de Datos de firmas de malware para identificar patrones de servidores C&C. • Investigar los dominios y las direcciones IP para identificar servidores maliciosos. • Observar las consultas frecuentes a dominios, por si se hace de forma aleatoria	• Configurar firewalls, incluyendo restricciones de conexiones no autorizadas. • Implementar sistemas de detección de anomalías para controlar el comportamiento del sistema. • Bloquear el acceso a sitios web maliciosos. • Mantener el antivirus y el antimalware, e igual que todos los sistemas y software, siempre actualizado. • Controlar el tráfico de DNS para identificar consultas sospechosas.

Noticia sobre el Servidor C&C

URL de la Noticia	Agrupación	Origen	Categoría	Perfiles de usuario afectados	Número y tipología de sistema afectado	Impacto del incidente
https://www.elespanol.com/omicrono/software/20231122/litterdrifter-peligroso-virus-ruso-infectado-miles-equipos-robar-informacion/811669178_0.html	Contenido Malicioso	A través USB dentro de ficheros ocultos y por ahí se puede conectar a los servidores C&C	Confidencialidad y privacidad de los usuarios	Afectó a equipos de Ucrania, Chile, Vietnam, Polonia o Estados Unidos.	Sistemas de equipos personales por todo el mundo y se infecta a través de USB con archivos ocultos	Crítico debido a que afectó varios países.

Distribución de Malware

TIPO DE INCIDENTES	DESCRIPCIÓN	FUNCIONAMIENTO	IDENTIFICACIÓN	PROTECCIÓN
Distribución de malware	Son los métodos usados por los atacantes para extender su software malicioso en otros sistemas	El atacante utiliza tácticas o estrategias para hacer que el malware se extienda y se mantenga activo en distintos equipos.	• Utilizar antivirus y antimalware que estén actualizados. • Configurar firewalls para controlar el tráfico de entrada y salida. • Monitorear el tráfico de red en busca de patrones inusuales. • Observar el sistema por si hay algún comportamiento inusual. • Utilizar firmas y hashes de malwares conocidos para identificar algún fichero malicioso.	• Utilizar antivirus y antimalware que estén actualizados. • Otorgar a los usuarios y sistemas solo los privilegios necesarios. • Utilizar filtrado de contenido de web para bloquear acceso a webs maliciosas. • Implementar medidas de seguridad para el correo electrónico.

Noticia de la distribución de malware

URL de la Noticia	Agrupación	Origen	Categoría	Perfiles de usuario afectados	Número y tipología de sistema afectado	Impacto del incidente
https://www.europapress.es/la-rioja/noticia-detectada-campana-distribucion-malware-suplanta-identidad-policia-nacional-20230913122957.html	Contenido Malicioso	A través de correos de electrónicos	Confidencialidad, y robo de datos del usuario	Equipos personales de España	Sistemas de equipos personales de España	Medio, debido a que se comunicó rápidamente que era falso.

Configuración de Malware

¿Qué es?	Ejemplo	¿Posible uso?	¿Cómo se identifica?	¿Cómo evitar el peligro?
Es un tipo de recurso que aloja ficheros de configuración de malware.	Una incorporación de ataque DDoS en un troyano.	Incorporación del malware en diversas aplicaciones legales en su configuración para obtener datos o causar estragos.	Si te pide permisos que normalmente la aplicación no debería pedirte.	Asegurarse de que das los permisos justos al uso de las aplicaciones, y en caso de dinero, asegurarte de no vincular las cuentas bancarias o tarjetas al dispositivo.

Noticia del Configuración de Malware

URL	Titular	Agrupación	Origen	Categoría	Usuarios afectados	Número y tipología infectados	Impacto
https://www.europapress.es/portaltic/ciberseguridad/noticia-malware-cherryblos-int	El malware CherryBlos se integra en apps de	Configuración de Malware	Externo	Económica, confidencialidad e integridad	Todos los usuarios de las aplicaciones GPTalk, Happy	Ciudadanía española en general	Alto

egra-apps-android-usa-reconocimiento-optico-caracteres-robar-contrasenas-20230731121817.html	Android y usa reconocimiento óptico de caracteres para robar contraseñas				Miner, Robot 999 y SynthNet.		

Malware dominio DGA

¿Qué es?	Ejemplo	¿Posible uso?	¿Cómo se identifica?	¿Cómo evitar el peligro?
Es un tipo de recurso que aloja ficheros de configuración de malware.	Una incorporación de ataque DDoS en un troyano.	Incorporación del malware en diversas aplicaciones legales en su configuración para obtener datos o causar estragos.	Si te pide permisos que normalmente la aplicación no debería pedirte.	Asegurarse de que das los permisos justos al uso de las aplicaciones, y en caso de dinero, asegurarte de no vincular las cuentas bancarias o tarjetas al dispositivo.

Noticia del Malware dominio DGA

URL	Titular	Agrupación	Origen	Categoría	Usuarios afectados	Número y tipología infectados	Impacto
https://unaaldia.hispasec.com/2020/07/el-malware-de-robo-de-datos-qsnatch-infecto-mas-de-62-000-dispositivos-nas-qnap.html	El malware de robo de datos QSnatch infectó más de 62.000 dispositivos NAS QNAP	Malware dominio DGA	Externo	Confidencialidad e integridad	Usuarios de dispositivos QNAP.	Más de 62000 dispositivos NAS QNAP	Alto