sedian

Seguridad Digital
de Andalucía

Ciberterrorismo y ciberdelitos.

Amenaza silenciosa a la seguridad de las Administraciones y el reto de la concienciación social.

Junta de Andalucía

Índice

1. Rompiendo mitos.
2. Análisis ciberdelincuencia y ciberterrorismo.
3. ¿Países terroristas o ciberdelincuentes?
4. Inteligencia en fuentes abiertas usadas por ciberdelincuentes.
5. Inteligencia en fuentes abiertas usadas por investigadores.
6. Conciencia y preparación de las Administraciones.
7. Coordinación de una respuesta mundial a las ciberamenazas.
8. Asistencia institucional.
9. Dudas y preguntas

Rompiendo mitos

Terrorismo /ciberterrorismo: Los grupos o colectivos asociados en esta categoría se podrían resumir en aquellos que ejercen o ejecutan (según la legislación comparada) acciones intencionadas para subvertir un Estado, y lo hacen usando herramientas informáticas y/o de carácter Ciber.

Rompiendo mitos

Delincuencia organizada: grupos o colectivos que tienen como objetivo parasitar o “fiscalizar” mediante procesos económicos a Estados o instituciones usando metodologías propias del ámbito penal, pudiendo trasladar esas metodologías a procesos ciber o informáticos.

Rompiendo mitos

Inteligencia /Ciberinteligencia: la diferencia está en el primer caso, cuando las acciones corresponden a una acción dirigida a la toma de decisiones como objetivo primario y usando la informática o metodología Ciber.

Mientras que en el segundo caso es más un ámbito operativo que se apoya o se imbrica en sistemas de inteligencia desde el punto de vista táctico. Se basa específicamente en procesos técnicos más que en planteamientos estratégicos.

Análisis ciberdelincuencia y ciberterrorismo.

Los analistas de *Thales y Verint* han definido cuatro categorías principales de atacantes en función de sus motivos y objetivos finales.

De aproximadamente sesenta grupos principales de atacantes analizados:

- El 49% son grupos que trabajan para los Estados, a menudo con el objetivo de robar datos sensibles de objetivos de interés geopolítico.
- El 26% son hacktivistas motivados ideológicamente.
- Los cibercriminales (20%) que están impulsados por ganancias financieras.
- Los ciberterroristas representan el 5% de los grupos analizados.

Análisis ciberdelincuencia y ciberterrorismo.

Todos los poderes económicos, políticos y militares del mundo son el objetivo prioritario de los ciberatacantes.

Los 12 países del mundo con el PIB más alto se encuentran en la parte superior de la lista de objetivos, encabezados por Estados Unidos, Rusia, la Unión Europea (particularmente el Reino Unido, Francia y Alemania) y China, seguidos por India, Corea del Sur y Japón.

Análisis ciberdelincuencia.

Informe de la INTERPOL sobre la evolución de las tendencias y amenazas en materia de ciberdelincuencia durante el año 2020.

Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada por la COVID-19

Jürgen Stock, Secretario General de INTERPOL

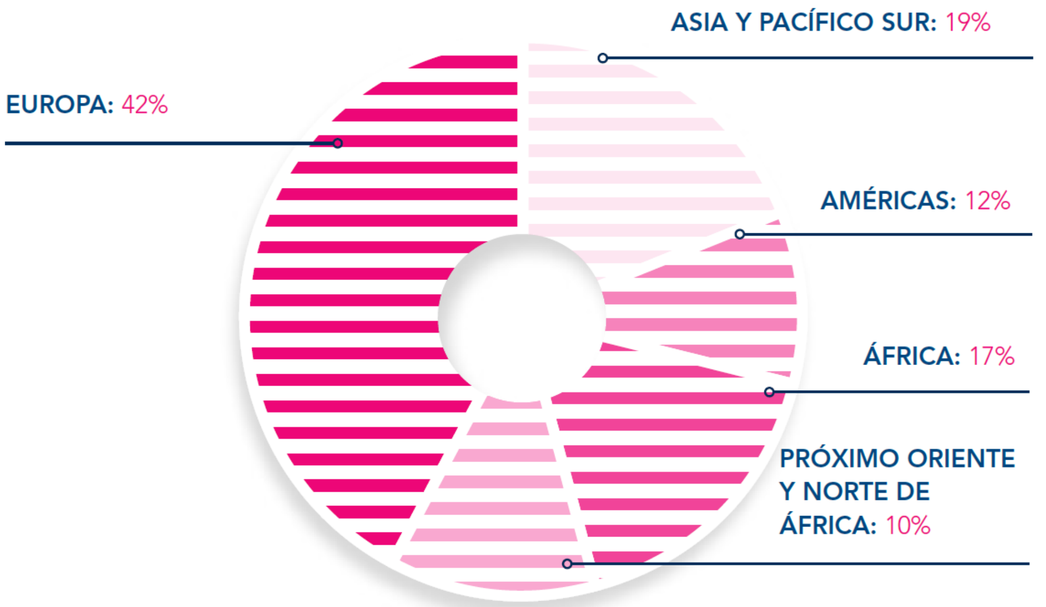
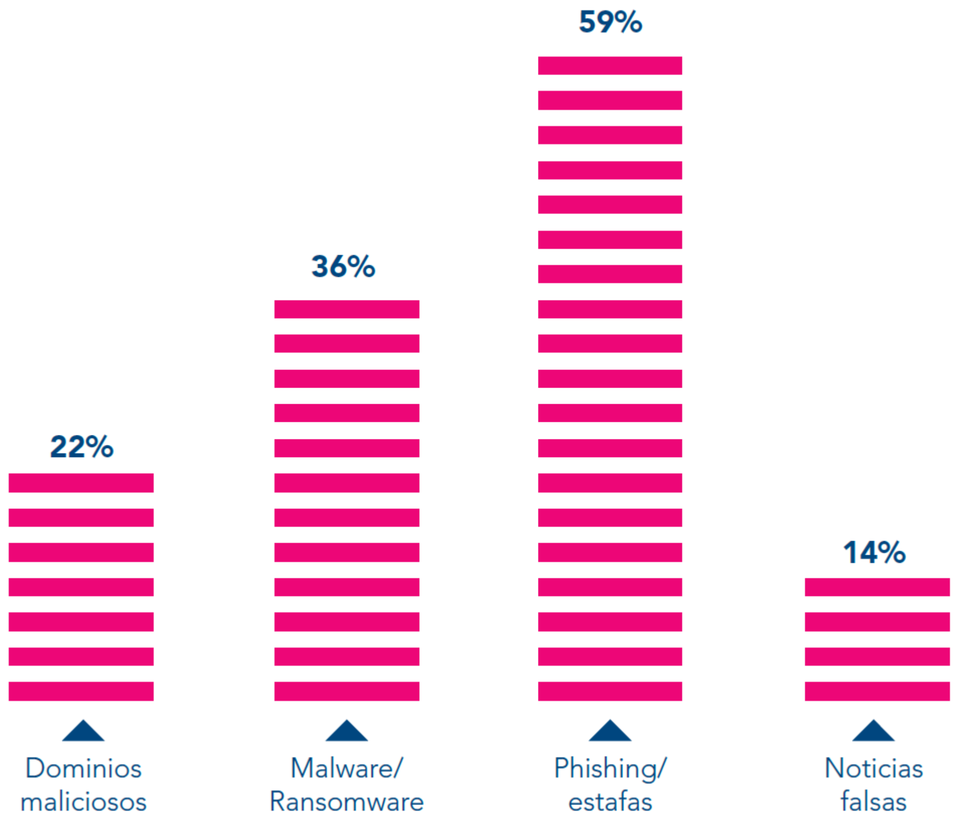


Fig. 1 Encuesta mundial de INTERPOL sobre ciberdelincuencia

Análisis ciberdelincuencia.

Se han observado que algunas tendencias y comportamientos de los cibercriminales se hacen cada vez más frecuentes y los datos arrojan un crecimiento constante en las víctimas de estos ataques.
Entre los delitos más recurrentes encontramos:

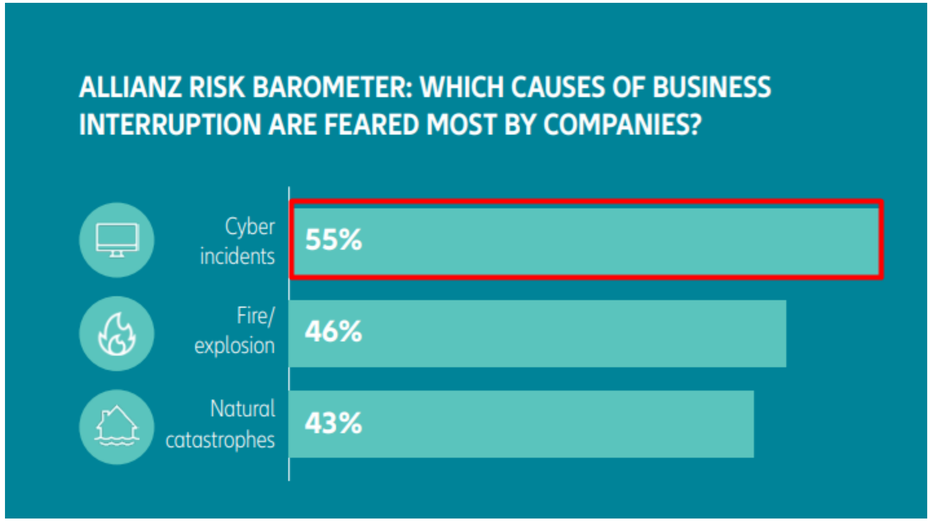
Phishing/estafas
Malware/Ransomware
Dominios maliciosos
Noticias falsas



Análisis ciberdelincuencia

Los datos anteriores coinciden en gran medida con el estudio realizado por la compañía ***Allianz Global Corporate & Specialty*** (AGCS), sobre el impacto del aumento de la interconectividad y el riesgo, la principal causa por la que se produce interrupciones en el servicio en las compañías, es causada por incidentes como los ataques de denegación de servicio (DDoS) o las campañas de phishing y ransomware.

A su vez, representan una mayoría significativa del valor de los siniestros cibernéticos hoy en día.



Análisis ciberdelincuencia.

Estafas por Internet y el phishing: Los ciberdelincuentes, haciéndose pasar por autoridades gubernamentales y sanitarias, envían a sus víctimas correos electrónicos de phishing sobre la COVID-19 en los que las incitan a facilitar datos personales y a descargar contenidos maliciosos.

Muchos de los ciberataques se están produciendo mediante perfiles falsos.

20bits ACTUALIDAD DISPOSITIVOS EMPRENDIMIENTO FABRICANTES EMPRESAS

BBVA, CaixaBank y Banco Santander alertan a sus clientes de un ataque de phishing para robar sus datos

POR **Raquel Holgado** NOTICIA 15.06.2021 - 11:26H

- Varios clientes de estos bancos han recibido correos o SMS de ciberdelincuentes que se hacían pasar por las entidades para conseguir sus datos personales.
- Descubren troyanos bancarios escondidos en apps maliciosas de Android que simulan ser de bancos

Los ciberdelincuentes redirigen a los usuarios a páginas web falsas. **Freepik**

Los correos electrónicos en la actualidad se han convertido en un nido de spam y de correos que ni siquiera abrimos, sin embargo, siempre estamos atentos a la bandeja de entrada por si acaso recibimos alguno importante. **Si encontramos un mensaje de nuestra entidad bancaria, posiblemente lo abramos para comprobar qué ocurre.**

MÁS INFORMACIÓN SOBRE:

SMS Banco Santander BBVA
spam correo electrónico
Redes sociales Bancos
CaixaBank Bankia Phishing
Contraseña Ciberseguridad

Ford apuesta por la mecánica híbrida autorrecargable para los S-Max y Galaxy
DIEGO PÉREZ

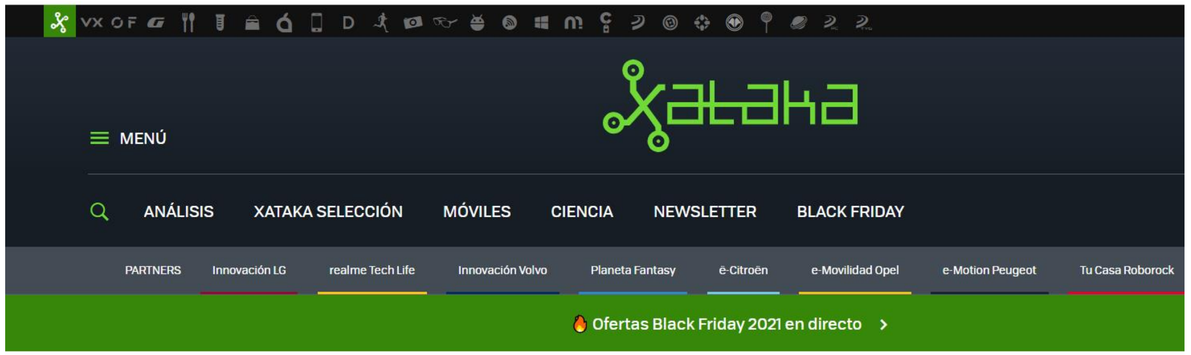
Las especies invasoras amenazan con extinguir la flora y fauna australianas para 2050
EFE

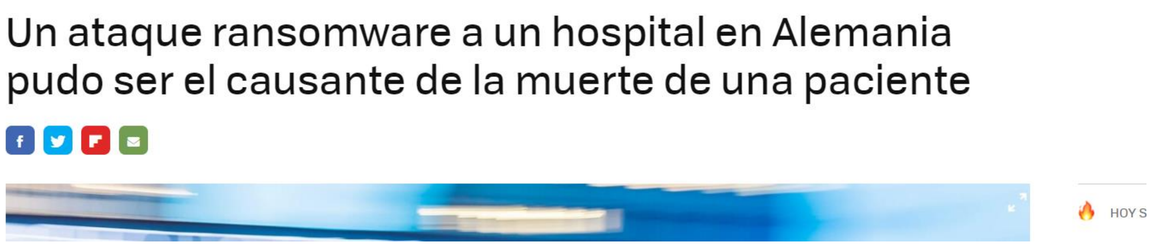
El sufrimiento de Antonio Lobato narrando el podio de Alonso en Cesar: "Esto se va a

Análisis ciberdelincuencia.

Malware disruptivos (ransomware y DDoS): Alentados por la probabilidad de causar graves problemas y obtener sustanciosas ganancias, los ciberdelincuentes multiplicaron el número de ataques con malware disruptivos contra las infraestructuras esenciales e instituciones sanitarias.

Las investigaciones de las fuerzas del orden muestran que la mayoría de los atacantes calculaban con bastante exactitud la cantidad máxima que podían solicitar como rescate a las organizaciones víctimas de sus ataques.





Análisis ciberdelincuencia.

Desinformación: Asistimos a una amplificación de la desinformación y las noticias falsas que se propagan rápidamente entre los ciudadanos.

La información no contrastada, las amenazas mal entendidas y las teorías de la conspiración han fomentado la ansiedad de la población y, en algunos casos, facilitado la ejecución de ciberataques.

Otros ciberdelitos…

Pharming: Se basa en la utilización de programas informáticos para alterar el servidor de nombres de dominio (DNS) encargado de transformar los nombres de dominio en direcciones IPs, de forma que redirigen al usuario a la máquina del atacante que de esta forma se hace con las claves. En el caso del malware, se trata de comprometer a los ordenadores para obtener la información personal y financiera de los usuarios, y realizar compras o transferencias electrónicas fraudulentas.

Ofertas de trabajo: Ya sea para mover el dinero producto de las transferencias fraudulentas (utilizando intermediarios captados mediante estas falsas ofertas de trabajo); o bien solicitando un anticipo de dinero para los primeros trámites con el fin de obtener un buen trabajo.

Carding: Es uso fraudulento de los números de tarjeta válidos en el comercio electrónico. Los números se obtienen de diferentes formas (programas generadores de números, puntos de venta presencial, compraventa de lotes de tarjetas a través de la red…).

¿Países terroristas o ciberdelincuentes?

Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. No obstante, podemos hablar de países donde esta actividad delictiva, se vuelve algo más común que en otros lugares.

Sistemas no democráticos : Países/instituciones o colectivos según ONU /organismos supranacionales o bajo definiciones reglamentarias comunes.

Sistemas teocráticos: Países/instituciones o colectivos que se rigen por principios propios en materia Ciber y no democráticos participativos.

Sistemas híbridos: Países/organizaciones o colectivos que acogen o toleran en su territorio las bases u operaciones desarrolladas por ciberatacantes de cualquier rango.

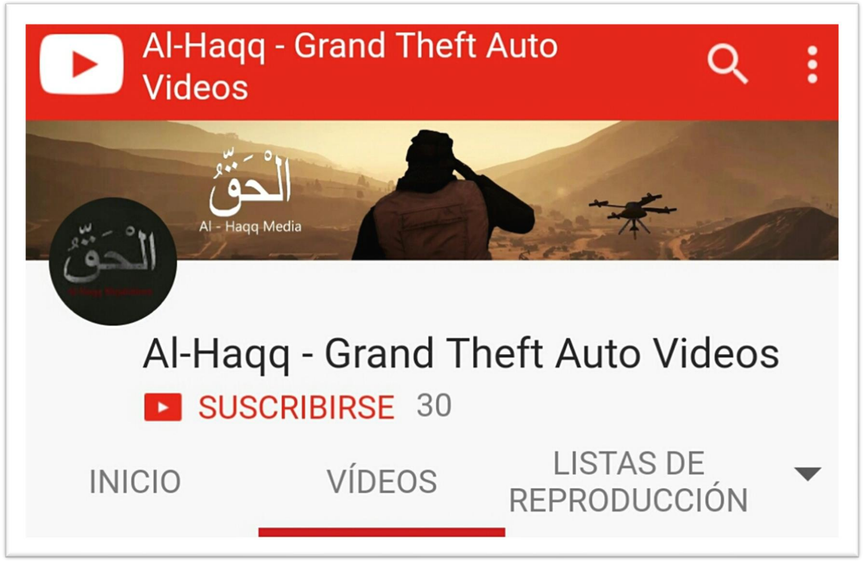
¿Países terroristas o ciberdelincuentes?

Sistemas focalizados: organizaciones transnacionales que tienen como base o como referencia un ámbito legislativo o fiscal más que una localización geográfica.

Sistemas para estatales: empresas/instituciones que controlan Estados fallidos o que influyen de forma directa en los mismos al ser estados fallidos o “satélite”.

Países nación: Estructuras jurídicas privadas de existencia física o jurídica que “venden” su estructura a organizaciones o colectivos “ciber”.

¿Cuál es el principal medio o técnica usada por ciberterroristas y para establecer comunicación y expandir su mensaje?



Las redes sociales y la **Dark web** se han convertido en los medios más comunes para establecer intercambiar información entre ciberterroristas.

Ejemplo de mensaje que podemos encontrar en la Dark web.

BABUK

!!ALL DATA !! Phone House España 13 millions customers data has been stolen, including passports and other privacy information

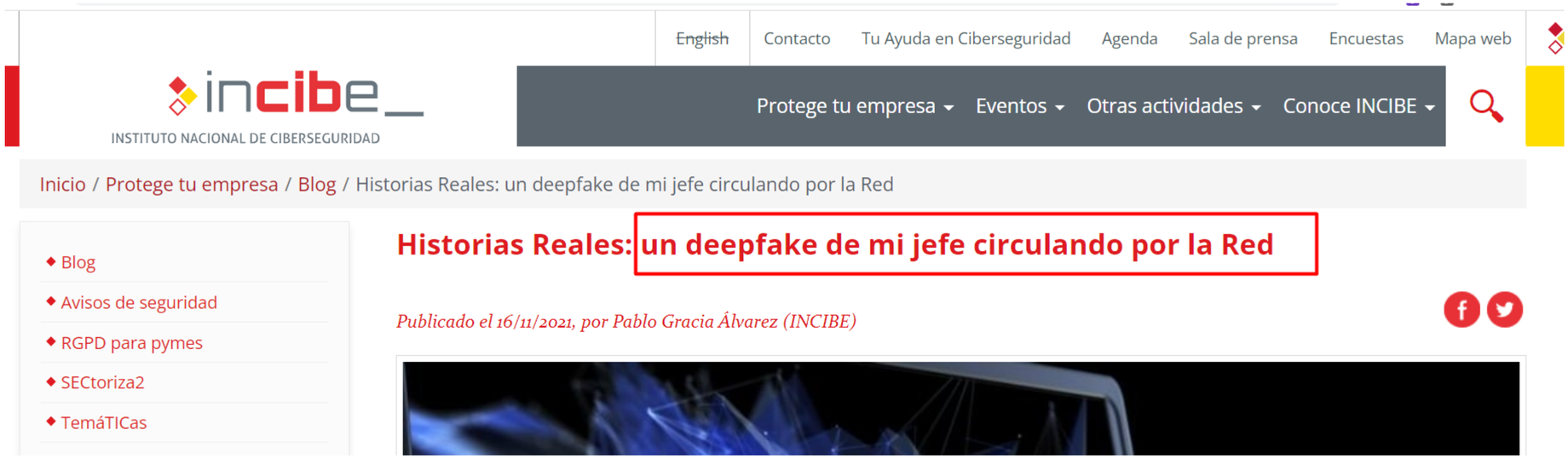
PHONEHOUSE.ES - MORE THEN 100GB OF SENSITIVE DATA

We have downloaded full dump of your 10 Oracle databases which containts GDPR information(full name, date of birth, email, phone, address, nationality, imei, etc) of more than 3 MILLION clients and employees.
If you do not pay - all this information will be published on our public blog, darknet forums, sended to all your partners and competitors.

DB names:

INFOVENTAS	SMARTHOUSE
PHONE	TARVAR
POS	VENTASONLINE
PP	VISIOFRANK
SEGUROSPH	MK_DWH

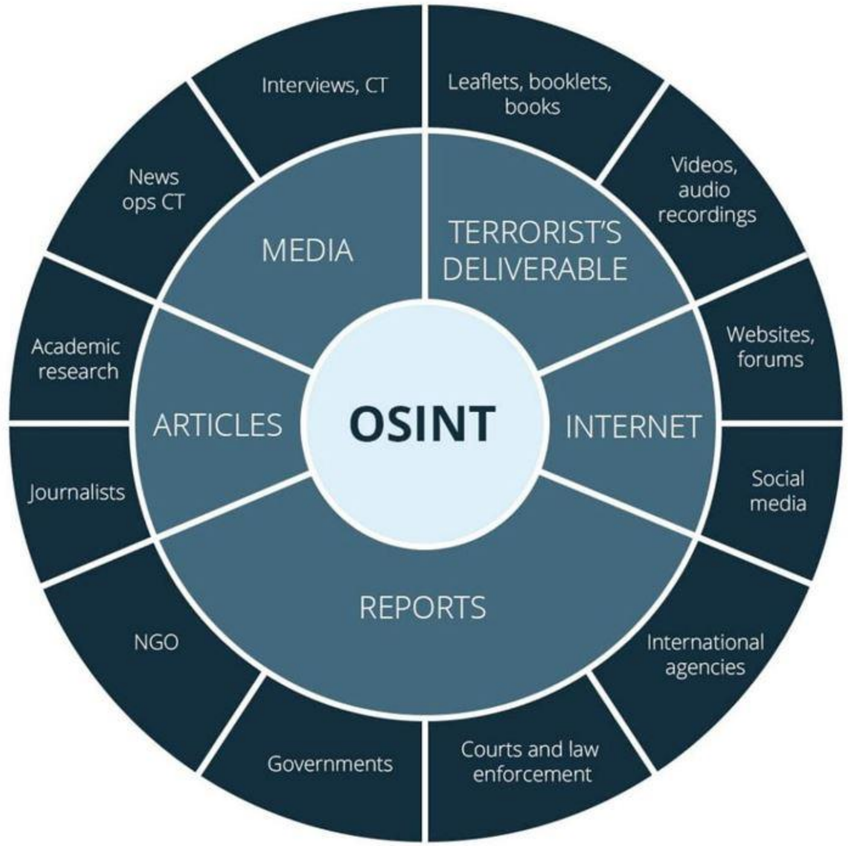
Además, las redes sociales se convierten en escenario perfecto para llevar a cabo sus ataques, debido a que hoy en día, la mayoría de los usuarios de internet, almacena fotos e información que queda expuesta públicamente en estos medios.



Inteligencia en ciberdelincuentes.

Las técnicas ***OSINT*** también son aplicadas por ciberdelincuentes para obtener **información de carácter no privado** que circula por la red y a la que se accede sin “seguridad“ en Internet y, sobre la cual se desarrolla una acción criminal.

Se aplicará un análisis a esa información pública, a fin de obtener información relevante para llevar a cabo el hecho delictivo. ¿Qué herramientas utilizan?



Por ejemplo:

OsintStalker (FBStalker y GeoStalker): Utilizan diferentes redes sociales como Facebook, LinkedIn, Flickr, Instagram y Twitter para recolectar gran cantidad de información sobre una persona.

Cree.py: Permite obtener datos de Twitter, Flickr e Instagram. A partir de la selección de una cuenta extrae fechas e información GPS, y crea una base de datos en formato csv o kmz para visualizarlos.

Theharvester: Esta herramienta obtiene emails, subdominios, host, nombres de empleados, puertos abiertos, etc. a través de diferentes servicios como Google, Bing, LinkedIn y Shodan.

Inteligencia en fuentes abiertas usadas por investigadores.

Las herramientas de uso técnico, policial o de agencias de inteligencia, son las mismas utilizadas por los delincuentes pero con extensiones diferentes.

Por la ley de protección de información clasificada no se pueden publicitar, al ser extensiones y programas protegidos por la ley.

Inteligencia en fuentes abiertas usadas por investigadores.

Ejemplo de herramientas utilizadas:

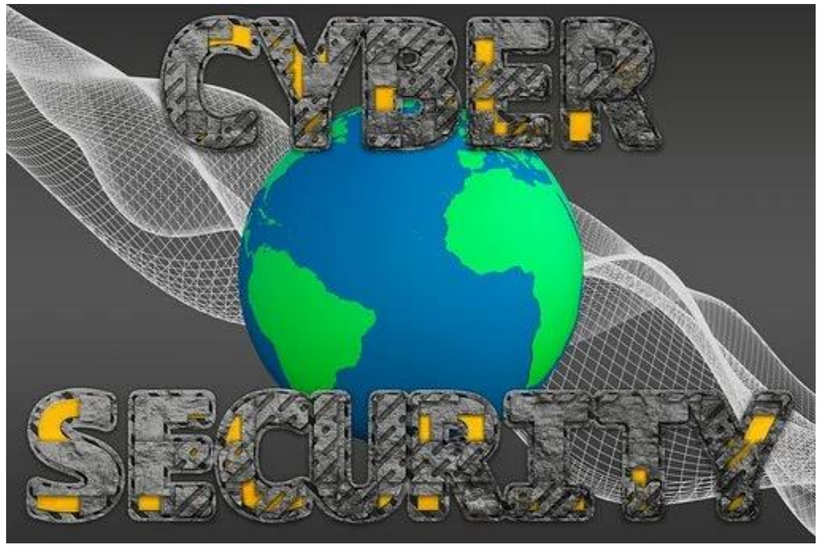
Tinfoleak: Herramienta open-source catalogada dentro de las disciplinas OSINT (Open Source Intelligence) y SOCMINT (Social Media Intelligence) que automatiza la extracción de información de Twitter y facilita su análisis posterior para la generación de inteligencia, desarrollada por la empresa Internet Security Auditors. La herramienta arroja resultados obtenidos del análisis de hahstags, tweets, likes, contenido multimedia, geolocalización, etc.

Conciencia y preparación de las Administraciones.

Las **Administraciones públicas** son objetivos de primera línea de los ciberataques.

Ya no sólo las atacan los empleados descontentos, los ciberdelincuentes o los grupos criminales, también los Estados. Ejemplo de Administraciones atacadas en los últimos años en España:

Ayuntamiento de Jerez, Ayuntamiento de Castellón, Ayuntamiento de Oviedo, el SEPE...



BUSINESS INSIDER

Economía Tecnología Estrategia Política Más temas

Suscríbete

Los atacantes del Ayuntamiento de Castellón reivindican la filtración de 119 gigas en datos robados: el 'ransomware' hace su agosto en las administraciones españolas

Alberto R. Aguiar 13 abr. 2021 7:30h.

SUSCRÍBETE 956 297 002 MARTES, 23 DE NOVIEMBRE, 2020 REGÍSTRATE | INICIAR SESIÓN

Diario de Jerez JEREZ

JEREZ PROVINCIA SEMANA SANTA ANDALUCÍA SOCIEDAD ESPAÑA ECONOMÍA DEPORTES CULTURA OPINIÓN TODAS LAS SECCIONES

JEREZ

AYUNTAMIENTO

Onda Jerez sufre un ciberataque informático

- Se han encriptado todos los servidores de la red interna de la radiotelevisión municipal
- La emisora continúa emitiendo, aunque con limitaciones
- El ataque no ha afectado, por el momento, al resto de la red informática del Ayuntamiento

La emisión en Onda Jerez no se ha visto interrumpida. / MIGUEL ANGEL GONZÁLEZ

REDACCIÓN
19 Mayo, 2021 - 19:28h

El Ayuntamiento de Jerez ha sufrido este miércoles **un nuevo ciberataque informático**. Esta vez solo ha afectado a los servidores internos de **Onda Jerez**, la radiotelevisión municipal, sin que haya alcanzado al resto de la red informática municipal, según ha informado el gobierno local en un comunicado. La emisora continúa emitiendo, aunque con limitaciones.

El ejecutivo ha explicado que, teniendo en cuenta los primeros análisis, se cree que ha podido ser un ataque de "**ransomware**" (impide a los usuarios acceder a su sistema o a sus archivos personales para luego el pago de un rescate para poder acceder de nuevo a ellos). Así, se ha detectado que se han encriptado los servidores adscritos a la red interna de la radiotelevisión municipal. En octubre de 2019 el Ayuntamiento jerezano ya sufrió un ciberataque similar que afectó a toda la red

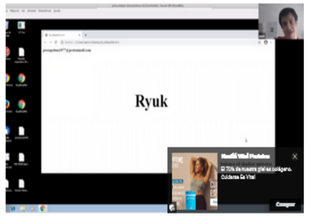
Economía | Tecnología

Así me hackea Ryuk, el virus ruso que ha colapsado al SEPE

Javier Espejo, director de ciberseguridad de Transparent Edge Services, hace una demostración para 'El Independiente' sobre cómo funciona una versión de este 'ransomware'

MIGUEL FITER

12/01/21 - 00: 11



Javier Espejo, director de ciberseguridad de Transport Edge, enseña cómo funciona el 'ransomware' Ryuk. EL INDEPENDIENTE

El martes, a las 10.26 horas, el Servicio Público de Empleo Estatal (SEPE), publicó un tuit desconcertante: «Por motivos ajenos, la *web* y la sede electrónica no se encuentran disponibles». Era una forma discreta de decir que acababan de ser atacados por un *ransomware*. Un virus que invade el ordenador, secuestra los archivos y exige un rescate a las víctimas. El ciberataque ha puesto patas arriba al organismo encargado de gestionar los ERTE. Hasta el punto de que sus funcionarios están atendiendo a los usuarios con cita previa a papel y boli.

Por causas ajenas al @empleo_SEPE , la web y la sede electrónica del

¿Qué tipo de organizaciones crees que realizaron dichos ataques?

¿Crees que han sido ataques internos del país o externos?

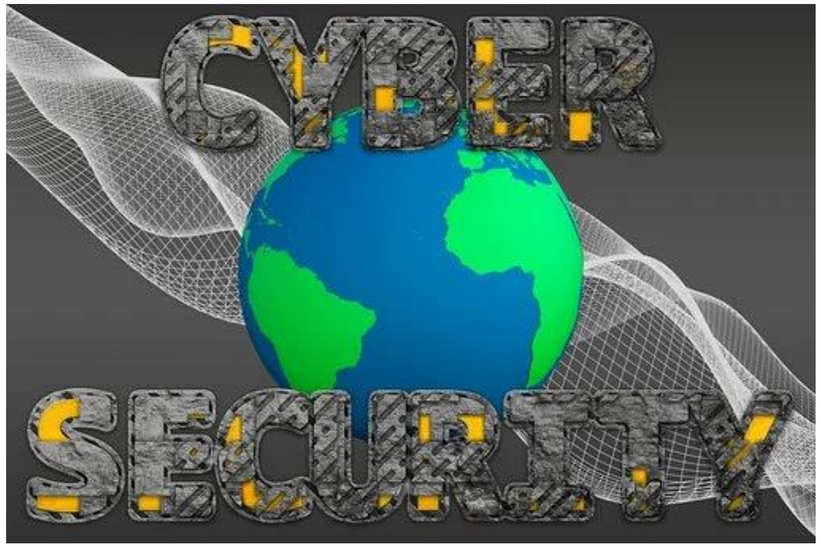
¿Cuál es el objetivo de este tipo de ataques?

¿Cómo protegernos desde la Administración de estos ataques informáticos?

Conciencia y preparación de las Administraciones.

Los dos retos más importantes con relación a la ciberseguridad son:

- La complejidad y sofisticación de los ciberataques.
- La falta de formación y concienciación en profesionales y directivos.



Procedimientos Administrativos.

La ciberseguridad debe ser tratada como un problema de gestión de riesgos. Los elementos clave de su gestión incluyen:

- Priorizar los activos más valiosos de la organización.
- Priorizar, conocer y entender a los adversarios y amenazas más relevantes.
- Conocer e implantar las mejores defensas preventivas contra las amenazas actuales y potenciales.
- Estar preparado cuando los atacantes consigan sobrepasar todas las tecnologías de seguridad y detectarlos, contenerlos y remediar sus acciones lo antes posible para minimizar el daño corporativo.
- Adoptar una postura de crisis continua buscando activamente amenazas que hayan entrado en el entorno corporativo y detectar aquellos puntos vulnerables.
- Gestionar a nivel corporativo la comunicación de la situación de violación.
- Definir y ejecutar constantemente iniciativas que minimicen el riesgo y así volver a empezar con el ciclo de mejora continua.

En cualquier empresa, sea grande o pequeña, se debe invertir en acciones de sensibilización de ciberseguridad.

Realmente es una cultura, el reto es conseguir que los empleados se identifiquen y se vuelquen en ella.

La prioridad es defender y proteger al usuario que está expuesto a ciberamenazas y facilitarle las conexiones seguras para minimizar los riesgos de seguridad.

Controles críticos de ciberseguridad.

Los controles críticos de seguridad del Centro de Seguridad de Internet ("Controles CIS") son un conjunto de defensas prácticas específicamente dirigidas a detener los ciberataques, estas defensas propuestas eran de naturaleza técnica y tenían la intención de definir pasos prácticos específicos diseñados para responder a la frecuente pregunta:

"¿Dónde debería comenzar cuando quiero mejorar mis defensas ante la ciberdelincuencia/terrorismo?"

Controles críticos de ciberseguridad.

CSC 1 | Inventario de dispositivos autorizados y no autorizados.

CSC 2 | Inventario de software autorizado y no autorizado.

CSC 3 | Configuraciones seguras de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores.

CSC 4 | Evaluación continua de la vulnerabilidad y remediación.

CSC 5 | Uso controlado de privilegios administrativos.

- Muchas organizaciones ya están siguiendo una arquitectura de seguridad utilizando otras normas o regulaciones de seguridad, regímenes de seguridad como el Framework de ciberseguridad NIST, la alineación del NIST y la serie ISO 27000.

- Las reglamentaciones como PCI DSS, HIPAA, NERC CIP y FISMA.

- Estándar como NIST 800-53.

Formación y concienciación.

(*) Ángeles El Centro Criptológico Nacional lanza **ÁNGELES**, su nuevo portal de formación y cultura de ciberseguridad.

En él se unifica todo el contenido de formación, concienciación y capacitación desarrollado por el Centro.

El objetivo es facilitar el acceso a todos los recursos elaborados por el organismo que buscan mejorar la cultura de ciberseguridad en nuestro país, a través de la formación, la concienciación y la capacitación de los profesionales.

En **ÁNGELES** se pueden encontrar todos los cursos del CCN, tanto presenciales como online; los diferentes itinerarios de formación a seguir en materia de ciberseguridad; un amplio catálogo de sesiones formativas a través de la plataforma Vanesa o los distintos retos de ***Atenea***.

Colaboración intrainstitucional.

Se refiere a todo proceso donde se involucre el trabajo de varias personas (o instituciones) en conjunto.

Para ello se establecen protocolos de acceso, control y difusión de información, además se establecen ***Normas*** que permitirán cumplir medidas de seguridad para la custodia, archivo, acceso, reproducción y distribución de la Información privilegiada.

Coordinación de una respuesta mundial a las ciberamenazas.

En el ciberespacio no existen fronteras: las amenazas y los ataques pueden provenir de cualquier lugar en cualquier momento, lo que supone un desafío para la policía, porque en los casos de ciberdelincuencia pueden estar implicados sospechosos, víctimas y delitos de múltiples países.

INTERPOL (Organización International de Policía Criminal) ayuda a los países miembros a identificar, seleccionar y coordinar la respuesta a las ciberamenazas. Para ello pone a nuestra disposición el resumen de la estrategia mundial contra la ciberdelincuencia en el que se recogen distintas líneas de acción.

Líneas de acción marcadas por INTERPOL.

Evaluación y análisis de amenazas, seguimiento de las tendencias.

Detectar e identificar positivamente la ciberdelincuencia, ciberdelincuentes y grupos de ciberdelincuencia, mediante evaluación de amenazas, análisis y seguimiento de las tendencias.

Líneas de acción marcadas por INTERPOL

Acceso a, y explotación de, datos digitales brutos.

Facilitar el acceso a datos relacionados con ataques cibernéticos, y a las herramientas y socios pertinentes, para consolidar la recopilación de datos y mejorar su explotación.

Líneas de acción marcadas por INTERPOL

Proceso de gestión de pruebas digitales.

Gestión de pruebas digitales encaminada a la investigación y el enjuiciamiento: recopilación legal de pistas informáticas, conservación de pruebas y hacer que estas sean inteligibles y aceptables para el sistema judicial.

Líneas de acción marcadas por INTERPOL

Correlación de información digital y física.

Establecer puentes entre las huellas informáticas y la identificación física, a fin de identificar la ubicación de los posibles perpetradores.

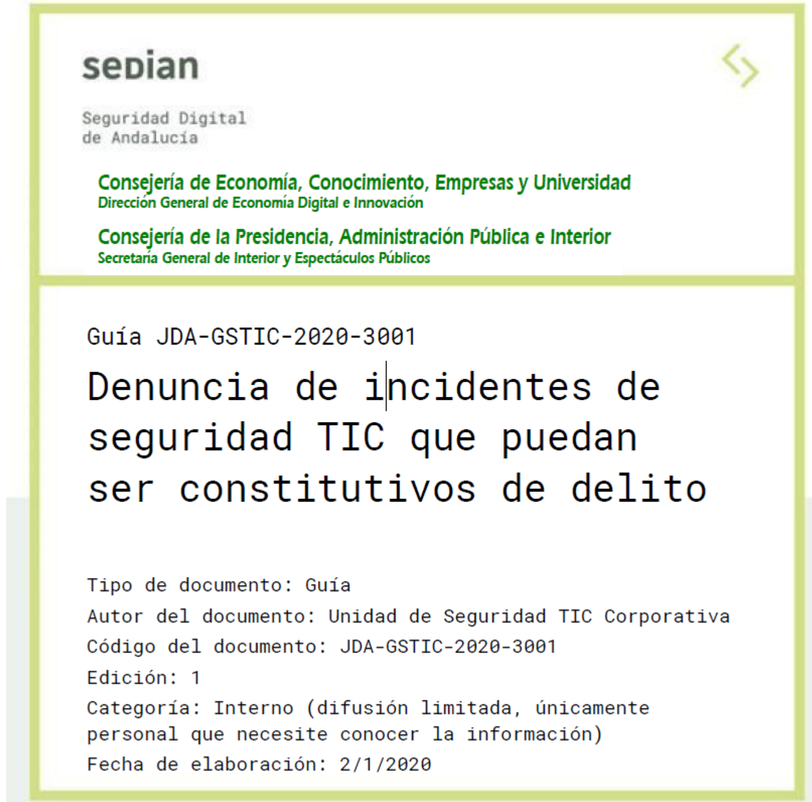
Líneas de acción marcadas por INTERPOL

Armonización e interoperabilidad.

Mejorar la interoperabilidad en las operaciones y la coordinación mundial, y alentar la armonización legislativa.

Asistencia institucional.

a) Instituciones de apoyo a los riesgos.
b) Defensa de la Administración.
c) Normativas.
d) CCN /INCIBE /CNI /CNP /GC.
e) Delitos telemáticos.
f) Apoyo a la restauración de sistemas.
g) Asistencia técnica.
h) Aviso a la ciudadanía , usuarios y demás cadena de valor implicada.



Conclusiones

Es altamente probable que la ciberdelincuencia siga aumentando a corto plazo. Debido a las vulnerabilidades asociadas al teletrabajo y la posibilidad de obtener mayores ganancias, los ciberdelincuentes seguirán ampliando sus actividades y concebirán unos modus operandi más avanzados y complejos.

También es posible que **aumenten las estafas a empresas por e-mail mediante suplantación de identidad**, como consecuencia de la recesión económica y los cambios que se han producido en el panorama empresarial, lo que generará nuevas oportunidades para la comisión de delitos.

Por lo tanto, es necesario destacar la necesidad de una cooperación más estrecha entre los sectores públicos y privados si nuestra intención es atajar con eficacia el peligro que se plantea a nuestra salud cibernética.

Referencias imágenes

1. https://www.istockphoto.com/es/search/2/image?page=11&phrase=seguridad%20informatica

2. https://cybercamp.es/sites/default/files/contenidos/videos/adjuntos/cybercamp19_cs_va_osint_e_ingenieria_social_min.pdf

3. https://pixabay.com/es/images/search/ciberseguridad/

4. https://www.stickpng.com/es/img/download/5b26a4398f68598d6f5a5e79#google_vignette

Referencias

1. https://www.thalesgroup.com/es/group/journalist/press-release/cyberthreat-handbook-thales-verint-lanzan-su-quien-es-quien-los
2. https://cybercamp.es/cybercamp2016/sites/default/files/contenidos/material/cybercamp2016-ciberamenaza-ccn_pablo_lopez.pdf
3. https://willistowerswatsonupdate.es/ciberseguridad/que-es-un-hacker-ciberdelincuentes/
4. https://www.interpol.int/es/Delitos/Ciberdelincuencia/Respuesta-a-las-ciberamenazas
5. https://angeles.ccn-cert.cni.es/index.php/es/
6. https://www.ccn-cert.cni.es/soluciones-seguridad.html
7. https://www.ccn-cert.cni.es/publico/ens/ens/topics/192.html
8. https://www.isecauditors.com/herramientas-tinfoleak

Referencias

1. https://www.incibe.es
2. https://www.ccn-cert.cni.es/
3. https://www.cert.fnmt.es/
4. https://www.ccn-cert.cni.es/guias.html
5. https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es
6. https://www.incibe.es › catalogo_ciberseguridad
7. https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php#
8. https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
9. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Cyber-Risk-Trends-2020.pdf
10. https://www.ibm.com/security/data-breach/threat-intelligence?mhsrc=ibmsearch_a&mhq=Threat%20Intelligence%20Index

Referencias

1. https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173&modo=2&nota=0&tab=2
2. https://www.ciberisciii.es/agenda/research-think-tank-focal-lesions-at-the-crossroads-of-vascular-liver-diseases
3. https://swisscyberthinktank.com/
4. https://www.inap.es/
5. https://www.csga-global.org/think-tank
6. https://ocsc.com.au/think-tank/
7. https://www.mimecast.com/company/cyber-resilience-think-tank/
8. https://www.cybersecurityintelligence.com/swiss-cyber-think-tank-sctt-5347.html
9. https://www.chathamhouse.org/topics/cyber-security
10. https://www.osce.org/es/countering-terrorism

Bibliografía y referencias

1. https://www.refworks.com/refworks2/default.aspx?lang=es&site=023921081742400000/1385746/CIBER%20Test
2. https://www.esedsl.com/blog/tag/base-de-datos
3. https://scholar.google.es/scholar?q=web+bibliografia+sobre+ciber&hl=es&as_sdt=0&as_vis=1&oi=scholart
4. https://ciberseguridad.blog/33-de-los-mejores-libros-de-ciberseguridad/
5. https://www.sec2crime.com/libros-ciberseguridad/
6. https://www.cibercorresponsales.org/pages/webgrafia-y-bibliografia
7. https://ciberseguridad.com/formacion/libros/

¿PREGUNTAS?

MUCHAS GRACIAS POR LA ATENCIÓN.

sedian Seguridad Digital de Andalucía