eurecat

"innovating for business"

Ciberseguridad en el sector turístico



Juan Caubet, PhD **Director de la Unidad de IT&OT Security**juan.caubet@eurecat.org
@juancaubet

www.eurecat.org



ÍNDICE

- ¿Qué es la Ciberseguridad? Ataques y amenazas.
- Casos reales (Incidentes)
- ¿Cómo protegerse? Firewall humano.
- Retos de la Ciberseguridad

eurecat

¿Qué es la Ciberseguridad? Ataques y amenazas.



¿QUÉ ES LA CIBERSEGURIDAD?



"La ciberseguridad es la práctica de **proteger los sistemas** antes, durante y después **de los ciberataques**".





PRINCIPIOS DE SEGURIDAD

- Auditabilidad
- Autenticación
- Autorización
- Confidencialidad
- Contabilización
- Disponibilidad
- Integridad
- No Repudio



Tríada CIA





La ciberseguridad, identificada como el principal riesgo de las empresas

Actualidad

20 NOV 2019



Los niveles de riesgo se están incrementando y las empresas tardar en responder y mitigar las amenazas. Según un nuevo estudio, menos de un tercio de las organizaciones pueden predecir con precisión el impacto de las amenazas y vulnerabilidades asociadas con la tecnología emergente.





GESTIÓN DE LA CIBERSEGURIDAD



https://adl.incibe.es/





DETECCIÓN Y RESPUESTA ANTE AMENAZAS





Datos del DBIR de 2016.



VULNERABILIDADES

Ejemplos de vulnerabilidades:

Diseño

 Debilidad en el diseño de los protocolos utilizados en las redes, políticas de seguridad deficientes e inexistentes...

Implementación

• Errores de programación, existencia de "puertas traseras", descuidos de los fabricantes...

Operación/Control

 Configuración inadecuada de los sistemas, desconocimiento y falta de sensibilización de los usuarios y de los responsables de los sistemas, disponibilidad de herramientas que facilitan los ataques...

Vulnerabilidades de día cero

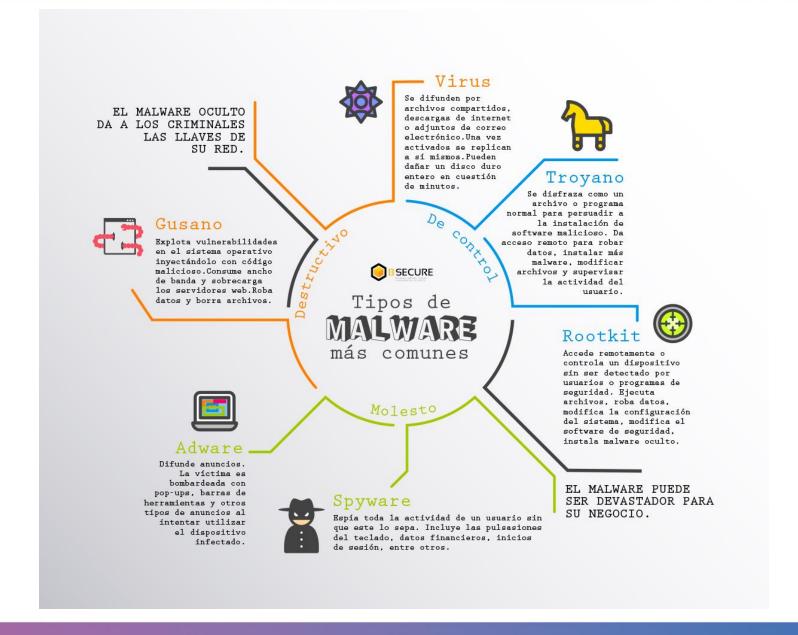




ATAQUES/AMENAZAS

- La mayoría de ataques o amenazas se pueden clasificar en una de estas categorías:
 - Secuestro de datos (Ransomware),
 - Suplantación de identidad (spoofing),
 - Phishing,
 - Denegación de servicio (DoS),
 - Manipulación (tampering),
 - Espionaje (eavesdropping),
 - Puerta trasera,
 - Ingeniería social,
 - Ataque directo,
 - Escalada de privilegios.







MERCADO NEGRO

Blog de GlobalSign



08 may 2019

Aviso: Kits de Phishing Avanzados Disponibles en la Dark Web

El auge de la *dark web*, o Internet oscura, ha implicado un gran cambio para los delincuentes. Según las últimas investigaciones, este espacio de Internet, que durante años sirvió de refugio para la compra-venta de drogas, armas, ID falsas y datos confidenciales, es también el lugar en el que encontrar fácilmente kits de *phishing* avanzados.

INDUSTRY NEWS

Researchers sifting the dark web uncover tools that turn fake news into real profit

② November 17, 2017 ■ 3 Min Read

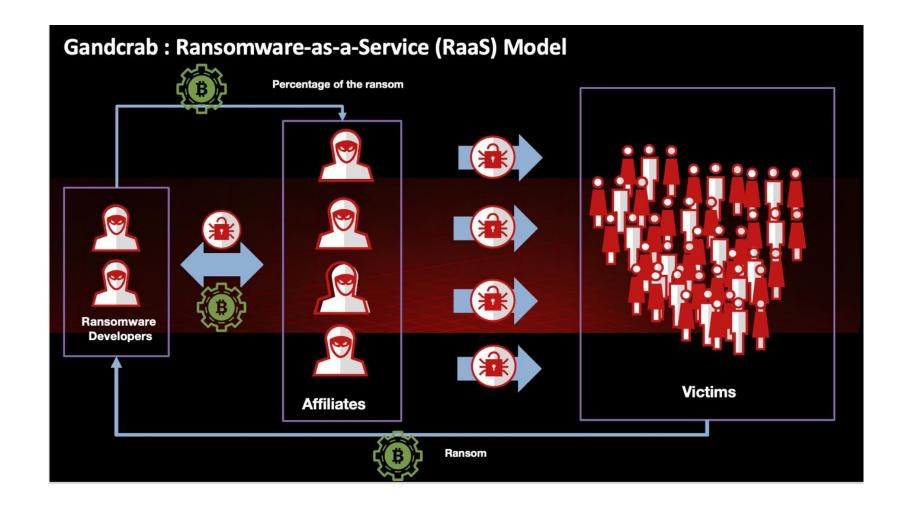


New research focusing on the growth of "fake news" has uncovered a booming business in using disinformation to generate profits. Cybercriminals are actively selling fake-news-generation tools and services on the dark web for as little as \$5.





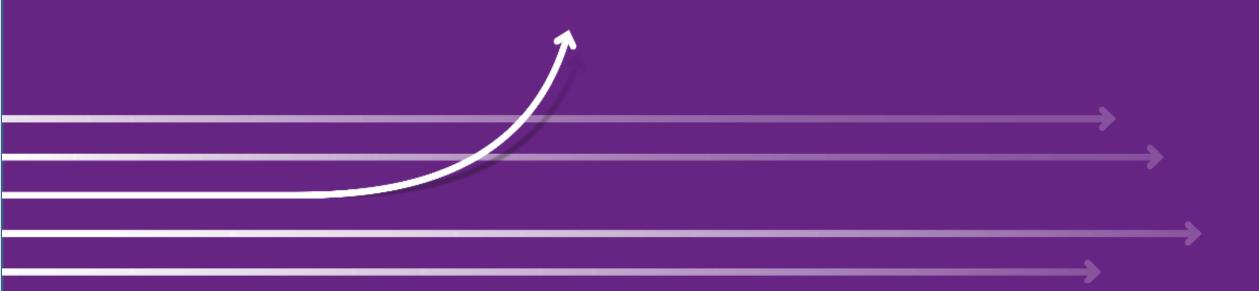
MERCADO NEGRO





eurecaț

Casos Reales (Incidentes)





BRECHAS DE DATOS

TECH CYBERSECURITY

Marriott discloses another security breach that may impact over 5 million guests

Marriott had a data breach less than two years ago





Tara Seals US/North America News Reporter, Infosecurity Magazine Email Tara



The data breach tidal wave continues: the Mandarin Oriental Hotel Group has confirmed that its hotels have been affected by a credit-card breach.



Banks told independent researcher Brian Krebs that they had noticed a pattern of fraudulent charges on customer cards that had all recently been used at Mandarin hotels. To boot, it appears that the attack happened just before Christmas, and that it likely affected most if not all of the company's two-dozen locations.



When Krebs reached out to the luxury chain, the company confirmed it is investigating a breach caused by malware used to infect its point-of-sale systems in the US and in Europe.

"We can confirm that Mandarin Oriental has been alerted to a potential credit card breach and is currently conducting a thorough investigation to identify and resolve the issue," the company told Krebs.

Photo by Justin Heiman / Getty Images

quests. This marks Marriott's second data breach in service launched.

Marriott says a security breach may have exposed t Hackers didn't waste any time and have started hijacking Disney+ user accounts hours after the



Marriott reveals massive database breach affecting up to 500 million hotel guests

A troubling BOOKING DOT CON Hackers target Booking.com in criminal bid to steal hundreds of thousands from customers

> The cyber crooks sent messages to Booking.com customers demanding full payment for holidays

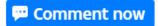
EXCLUSIVE

David Jarvis

3 Jun 2018, 2:57







CYBER crooks have targeted travel firm Booking.com in a bid to steal hundreds of thousands of pounds from customers.

Users were sent WhatsApp and text messages claiming a security breach meant they needed to change their password.





SECUESTRO DE DATOS

Un hacker «secuestra» un hotel inutilizando las llaves de las habitaciones con clientes

Los hoteles que tienen su sistema de aper blancos de criminales con 'ransomware', y

Por Manu Contreras 💆 @mcontreras, hace 3 años



Un hotel austriaco ha vivido su peor pesadilla er ransomware que les impedía acceder a sus orde puertas de sus habitaciones, impidiendo a sus h europa<mark>press</mark> / portaltic / ciberseguridad

El 'ransomware' asedia a 174 municipios en el mundo durante 2019



Ciberseguridad y derecho al olvido, recurso - PIXABAY - Archivo MADRID, 23 Dic. (Portaltic/EP) -

Los ciberataques de tipo **'ransomware'**, en los que los atacantes encriptan la información de dispositivos o redes y exigen a cambio un rescate económico, han afectado durante este año a **174 municipios en todo el mundo** con más de 3.000 organizaciones subsidiarias.

Publicado 23/12/2019 14:48:44 +01:00 CET

ÚLTIMAS NOTICIAS / PORTALTIC >>

Una vulnerabilidad en Microsoft Teams permite usar un GIF malicioso para robar datos

Facebook acusa a la empresa israelí NSO Group de usar servidores estadounidenses para espiar smartphones

Encuentran una vulnerabilidad en los programas antivirus más populares capaz de desactivarlos

ware Demand After

nal Airport, Albany International Airport New York, ack, ransomware attacks, Sodinokibi, Sodinokibi

Más leídas ofrecido por cellnex

- Una vulnerabilidad en Microsoft
 Teams permite usar un GIF malicioso
 para robar datos
- 2 Encuentran una vulnerabilidad en los programas antivirus más populares capaz de desactivarlos

1

Share

nto the news a lot recently. The evil e targets. And now, the latest : Airport.





MALWARE

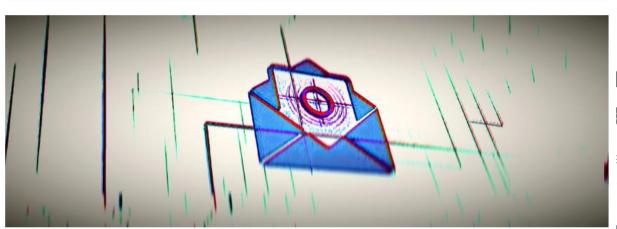
RevengeHotels una campaña de malware para robar datos de la tarjeta de crédito a los clientes de Home > News > Security > Hackers Target the North American Hotel Industry With a RAT

By Sergiu Gatlan

5 diciembre, 2019 Por Fernando Ramíre

Una campaña de malware denomir más de 20 hoteles en varios países y poder hacer compras con ellas po

Hackers Target the North American Hotel Industry With a RAT



A malspam campaign was spotted by security researchers that was targeting the financial staff of multiple entities from the North American hotel industry, using malicious attachments to drop the NetWiredRC Remote Access Trojan (RAT) on unsuspecting victims.

Malspam (short for malicious or malware spam) is a type of spam email designed to deliver malware payloads via malicious URLs or infected attachment.

npaña de espionaje Isiáticos

siglo 21.

August 13, 2019 (7) 01:34 PM 0

10 Nov 20

My Kaspersky v







OTROS

El fraude del CEO, un timo millonario silenciado por las propias empresas

Uno de los ciberdelitos más habituales es la suplantación de hacen pasar por otra persona para obtener un rendimiento directamente económico, de un usuario desprevenido.

Chipertextual

El Internet de las Cosas fue usado para el último gran ataque DDoS y no podemos hacer nada para impedirlo

Eduardo Arcos - Oct 23, 2016 - 17:02 (CET)

La situación de falta de seguridad en millones de dispositivos del internet de las cosas es tan grave que medio internet no solo es posible, sino

amente tienen grandes conocimientos

Hackean un casino a través de un termómetro de pecera conectado a Internet

By Jorge Quijije - Abr 16, 2018



ypor

ıdo



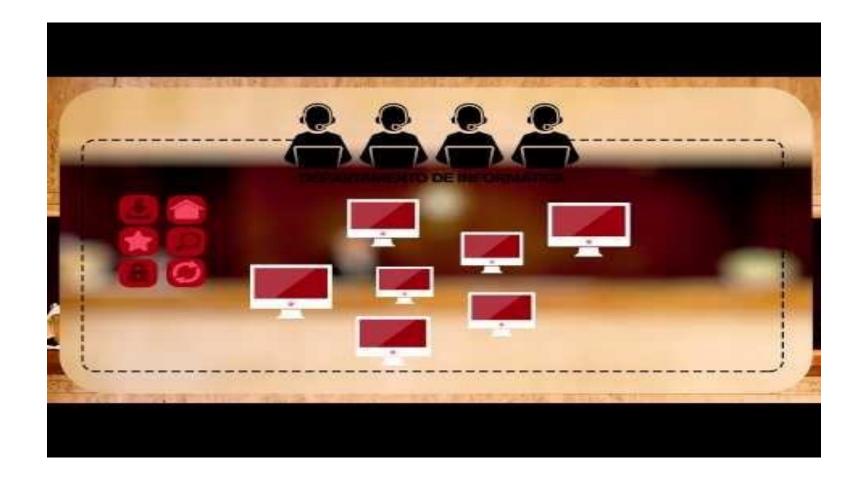


eurecat

¿Cómo protegerse? Firewall humano.



PLAN DIRECTOR DE CIBERSEGURIDAD





¿QUÉ DEBEMOS HACER?

SEREMOS VÍCTIMAS DE ATAQUES

Detección de intrusos

Realizar copias de seguridad

Monitorizar activos

NO HAY PERÍMETRO

Proteger la información

Proteger las comunicaciones

Securizar todos los sistemas

LA CADENA SE ROMPE POR EL ESLABÓN MÁS DÉBIL

Formar a los trabajadores

Exigir a proveedores

Gestionar el riesgo



BUENAS PRÁCTICAS

- Limitar el uso de herramientas no corporativas.
- Actualización de sistemas/dispositivos.
- Gestión segura de contraseñas.
- Desarrollo seguro de software.
- Etc.





FIREWALL HUMANO

El 95% de los ciberataques que logra su objetivo viene precedido de un error humano



Expertos de KPMG advierten de que para mejorar la seguridad informática de una compañía no basta con invertir en tecnología; es fundamental formar sobre los riesgos a los trabajadores

IRATXE BERNAL

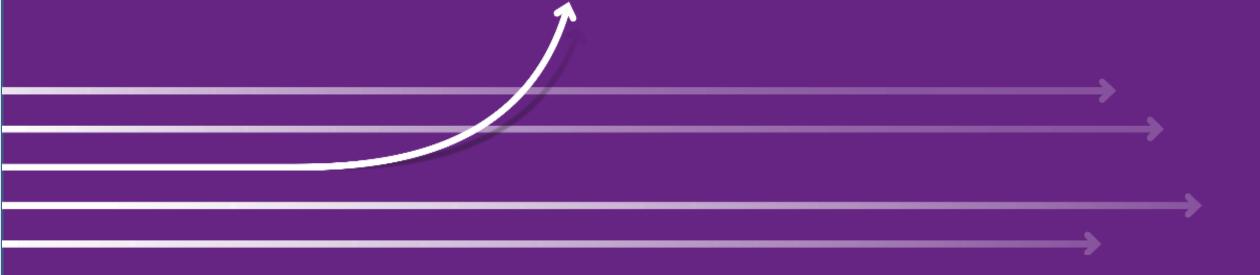
Martes, 21 abril 2020, 02:01





eurecat

Retos de la Ciberseguridad





RETOS DE LA CIBERSEGURIDAD

- Aplicación del modelo "Zero Trust".
 - Modelo de protección que promete ser altamente efectivo, empoderando a empresas a tener mayor control de sus activos.
- Esclavos del ransomware.
- Contrarrestar la Inteligencia Artificial y el Machine Learning.
- Efecto "Noise Canceling".
 - Enfocarse en las alertas que realmente importan mediante la implementación de procesos más eficientes de evaluación de compromisos.
- Encontrar la Inteligencia más buscada, la Humana.
- IoT, 5G y los ataques DDoS.





Gracias

Juan Caubet, PhD

<u>juan.caubet@eurecat.org</u> @juancaubet

Director de la Unidad de IT&OT Security

