INSTITUCIÓN UNIVERSITARIA
COLEGIO MAYOR
DE ANTIOQUIA®

Acreditados
en ALTA CALIDAD

VI SIMPOSIO INTERNACIONAL

PARA LA INNOVACIÓN Y EL DESARROLLO EMPRESARIAL:

RETOS DE LA TRANSFORMACIÓN DIGITAL

VI SEMANA DE LA FACULTAD DE ADMINISTRACIÓN

Seguridad de la Información en la Sociedad de la Información

Juan G. Lalinde-Pulido, PhD
Universidad EAFIT
Profesor Investigador
Escuela de Ciencias Aplicadas e Ingeniería
Área de Ciencias Fundamentales

Agenda

- Introducción
- ¿Son reales las amenazas?
- ¿Qué es seguridad de la información?
- Guerra de Información
- Las organizaciones y la seguridad de la información

INTRODUCCIÓN

Introducción

El aislamiento por la pandemia del COVID-19 transformó la sociedad. Desde el inicio de la pandemia hasta finales de 2020, **el crecimiento de los cibercrímenes fue del 600%.**

- **30.000 sitios web** son hackeados cada día.
- **64% de las empresas del mundo** han sido víctimas de ciberataques.
- En marzo de 2021 fueron robados **20 Millones de registros de información**.
- En 2020 los casos de **ransomware** crecieron un **150%**.
- El **94% del malware** se distribuye por **email**.
- Cada **39 segundos** hay un ataque en la web
- En promedio, cada día se bloquean aproximadamente **24.000 aplicaciones móviles**.
- Cada día se crean **300.000 aplicaciones malware**.

Introducción

El aislamiento por la pandemia del COVID-19 transformó la sociedad. Desde el inicio de la pandemia hasta finales de 2020, **el crecimiento de los cibercrímenes fue del 600%.**

- En 2020 el **63% de los robos de información** fueron por motivos económicos.
- Las extensiones más utilizadas para enviar **malware por email** son .zip y .jar
- Cada día se envían **6.4 mil millones de correos falsos**.
- **El costo** por **ataques informáticos** en 2021 fue de **6 billones de dólares**.
- El **53% de las instituciones de salud** experimen-taron al menos un **robo de datos** en 2021.
- El **60% de los dominios maliciosos** de Internet están asociados con campañas de **spam**.
- El tiempo promedio requerido para **solucionar un robo de datos** es de **314 días**

Amenazas principales

ENISA clasificó las amenazas en 8 grupos. La frecuencia y el impacto determinan la importancia que siguen teniendo todas estas amenazas.

- **Ransomware:** El 60% de las organizaciones afectadas han pagado rescates.
- **Malware:** 66 revelaciones de vulnerabilidades de día cero observadas en 2021
- **Ingeniería social:** El phishing sigue siendo una técnica popular, pero vemos surgir nuevas formas de phishing, como el spear-phishing, el whaling, el smishing y el vishing
- **Amenazas contra los datos:** Aumentan en proporción al total de datos producidos

Amenazas principales

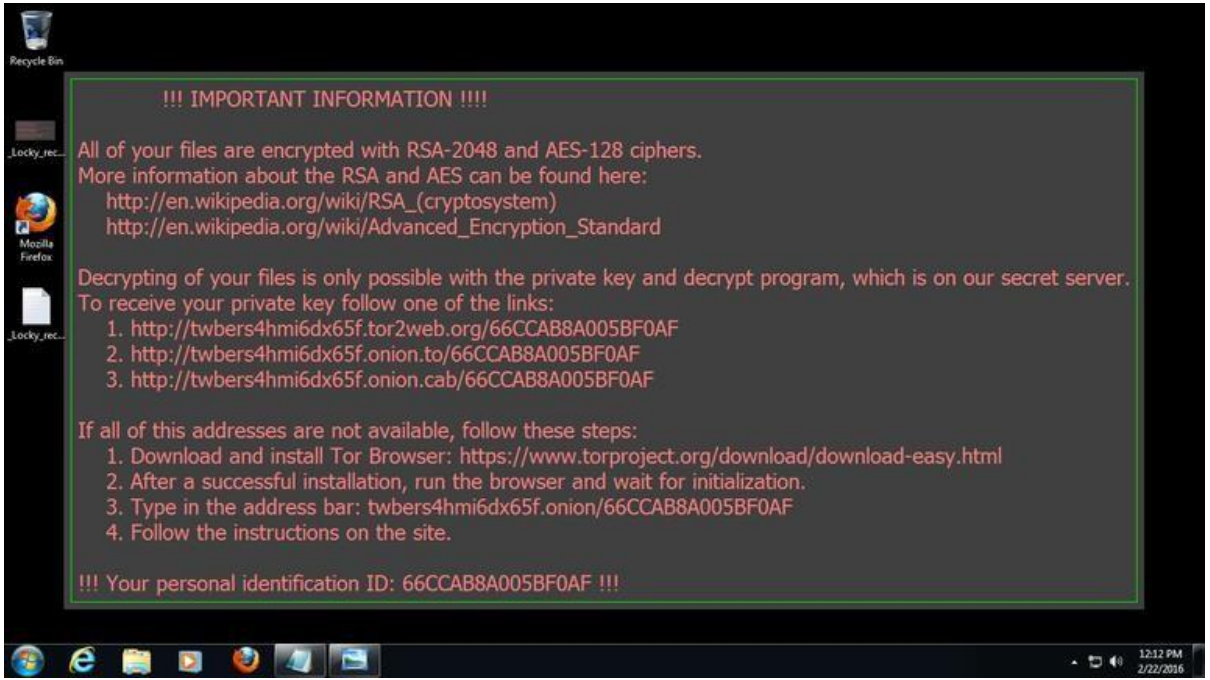
- **Amenazas contra la disponibilidad:** En julio de 2022 se lanzó en Europa el mayor ataque de denegación de servicio (DDoS) de la historia;
- **Internet:** destrucción de infraestructuras, cortes y desvío del tráfico de Internet.
- **Desinformación - desinformación:** Aumento de la desinformación basada en IA, deepfakes y desinformación como servicio.
- **Ataques a la cadena de suministro:** Los incidentes de terceros representan el 17 % de las intrusiones en 2021, frente a menos del 1 % en 2020

Principales tendencias

- Los exploits de día cero son el nuevo recurso utilizado actores ofensivos para lograr sus objetivos
- Desde la guerra entre Rusia y Ucrania se ha observado una nueva ola de hacktivismo.
- Los ataques DDoS son cada vez mayores y más complejos, desplazándose hacia las redes móviles y la Internet de las Cosas (IoT), que ahora se utilizan en la ciberguerra.
- Desinformación y deepfakes basados en IA.

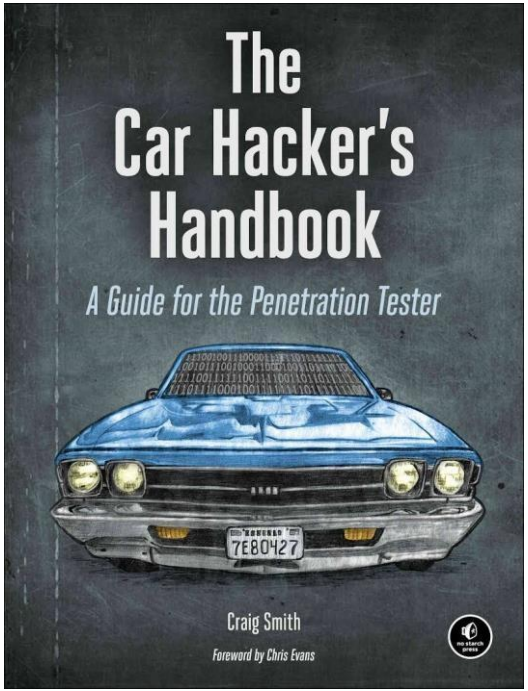
¿SON REALES LAS AMENAZAS?

¿Son reales las amenazas?



¿Son reales las amenazas?

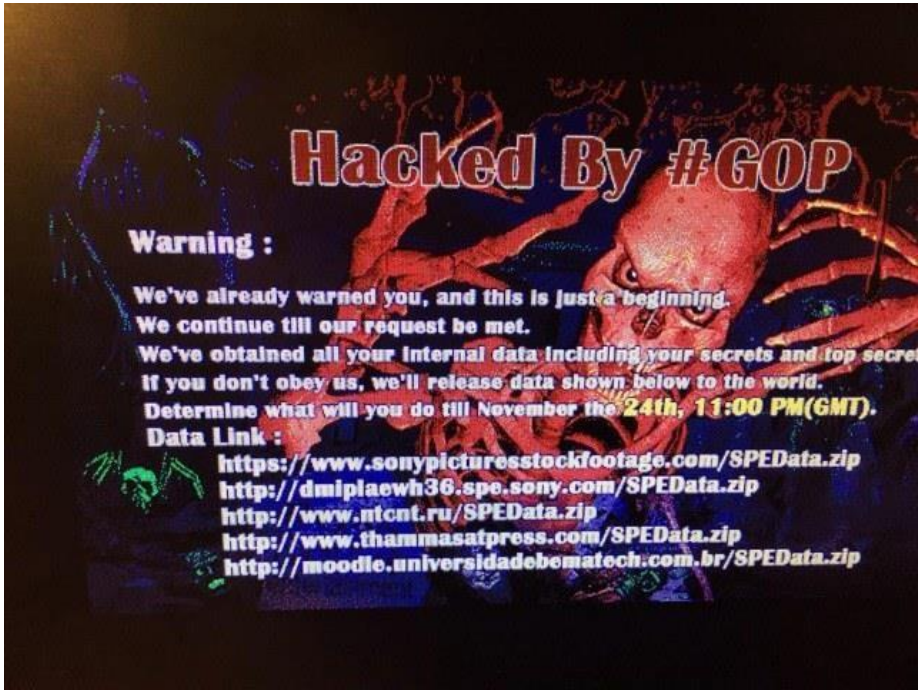
¿Son reales las amenazas?



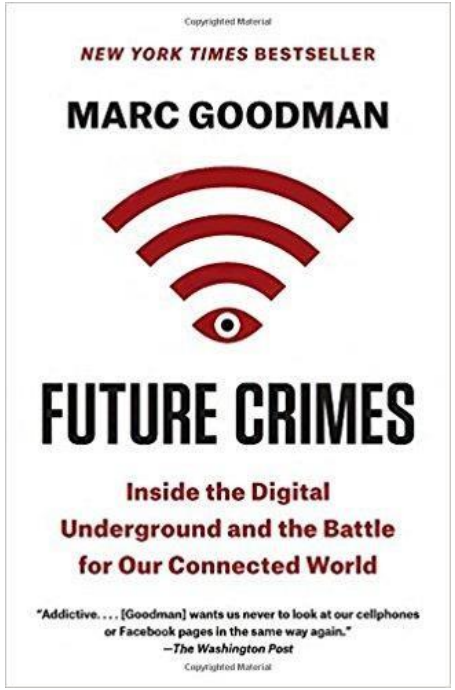
BRIEF CONTENTS

¿Son reales las amenazas?

¿Son reales las amenazas?



¿Son reales las amenazas?



CONTENTS

¿Son reales las amenazas?

¿Son reales las amenazas?

¿Son reales las amenazas?

¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

¿Qué es seguridad de la información?

- Según el diccionario:
  - *Seguridad*: Calidad de Seguro
  - *Seguro*: Exento de todo peligro o riesgo.
- Tres vértices:
  - Psicológico: Estado o situación de la persona y su estado o actitud.
  - Real: El sistema, la tecnología y el marco legal.
  - Filosófico: Conjunto de principios establecidos para ordenar la seguridad.
- Seguridad: *Conjunto de principios aplicado a un adecuado sistema de protección, unidos a una actitud de obrar en forma lógica y razonable para generar una sensación o estado de tranquilidad real"*

¿Qué es seguridad de la información?

El propietario de la información necesita preservar la ...	• Confidencialidad • Propiedad • Integridad • Autenticidad • Disponibilidad • Utilidad	... de la información de hechos accidentales o intencionales por parte de personas o fuerzas que puedan causar ...	• destrucción o copia • interferencia con el uso • uso de datos falsos • modificación o reemplazo • tergiversación o repudio • abuso o inutilización • encontrar o tomar • revelar u observar • poner en peligro
... por la aplicación de protecciones y prácticas ...	• evitar y disuadir • prevención y detección • mitigar e investigación • transferencia • sanciones y recompensas • recuperación y corrección • educación	... que son seleccionadas cuidadosamente para obtener ...	• evitar negligencia • una sociedad ordenada y protegida • cumplimiento de leyes y regulaciones • conducta ética • comercio exitoso • privacidad

GUERRA DE INFORMACIÓN

Guerra de Información

- El gran descubrimiento que facilitó el surgimiento de la era de la información es que se puede representar todo lo que hay en el mundo en secuencias de unos y ceros. (Richard Szafransky)
- La información es la materia prima para la toma de decisiones
- *Warfare*: conjunto de acciones letales y no letales llevadas a cabo con el fin de someter la voluntad de un adversario o enemigo.
- Las tecnologías informáticas y de comunicaciones han llevado el conflicto a una nueva dimensión: el ciberespacio.
- *Information warfare*: la preparación y el uso de armas físicas y/o lógicas para inutilizar o destruir la información y los sistemas de información con el fin de degradar o inutilizar las funciones que dependen de la información y los sistemas de información

Guerra de Información

- Los problemas afectan indiscriminadamente todos los aspectos de la vida:
  - Seguridad Nacional
  - Mundo económico
  - Privacidad Personal
- Hay cuatro elementos principales:
  - Recursos de información
  - Participantes
  - Operaciones defensivas
  - Operaciones ofensivas.

- Recursos de información: se clasifican por función en:
  - contenedores
  - transportadores
  - sensores
  - grabadores
  - procesadores

Guerra de Información

- **Infraestructura de Información:** Es el conjunto de los recursos de información, incluidos los sistemas de comunicaciones, que soportan una industria, una institución o una población.
- **Espacio de información:** Conjunto de todos los recursos de información disponibles.
- **Valor de los recursos:**
  - *de intercambio:* se determina por el valor que tiene en el mercado, y es cuantificable
  - *operacional:* se determina por los beneficios que se pueden obtener al usar el recurso. Puede no ser cuantificable

  El valor de los recursos puede ser diferente para cada una de las partes

Guerra de Información

	Independ.	Guerra Civil	WWII	Golfo Pérsico	Futuro
Orientación	Telescopio	Telégrafo	Radio/ cables	Cuasi tiempo real	Tiempo real
Observación	Semanas	Días	Horas	Minutos	Continuo
Decisión	Meses	Semana	Días	Horas	Inmediata
Acción	Estación	Un mes	Una semana	Un día	Una hora o menos

Tiempo y Comando

LAS ORGANIZACIONES Y LA SEGURIDAD DE LA INFORMACIÓN

Estadísticas 2022

- Casi mil millones de correos electrónicos fueron expuestos en un solo año, afectando a 1 de cada 5 usuarios de internet.
- Las filtraciones de datos costaron a las empresas una media de 4,35 millones de dólares en 2022.
- Alrededor de 236,1 millones de ataques de ransomware se produjeron en todo el mundo en el primer semestre de 2022.
- 1 de cada 2 internautas estadounidenses sufrió una violación de sus cuentas en 2021.
- El 39% de las empresas británicas declararon haber sufrido un ciberataque en 2022.

Estadísticas 2022

- Alrededor de 1 de cada 10 organizaciones estadounidenses no tiene seguro contra ciberataques.
- 53,35 millones de ciudadanos estadounidenses se vieron afectados por la ciberdelincuencia en el primer semestre de 2022.
- La ciberdelincuencia costó a las empresas británicas una media de 4200 libras en 2022.
- En 2020, los ataques de malware aumentaron un 358% en comparación con 2019.
- La ciberamenaza más común a la que se enfrentan empresas y particulares es el phishing.

Cibercrimen en Colombia

- En 2022 las denuncias crecieron un 26%: una denuncia cada 8 minutos
- Delitos más comunes:

Delito	Denuncias	Crecimiento con respecto a 2021
Hurto por medios informáticos	25.413	34%
Acceso abusivo a sistema informático	13,318	62%
Violación de datos personales	12,775	3%
Suplantación de sitios web	12,775	4%

Cibercrimen en Colombia

- La intercepción de datos informáticos creció de 1.331 a 1.927
- Estos delitos están asociados con espionaje industrial y afectaciones a la información confidencial
- Los sectores más afectados fueron industria, gobierno y salud. Representan el 67% de los casos
- Las pequeñas y medianas industrias son las más afectadas por los ciberdelitos
- Se estima que solo el 7% de las PYMEs que sufren un ciberataque en el primer año de trabajo, subsisten
- Es llamativo el incremento en el número de casos de fuga de datos en entidades del gobierno en 2022

Referencias

- Videos: https://www.pbs.org/wgbh/nova/video/cyberwar-threat/
- Estadísticas mundiales: https://aag-it.com/the-latest-cyber-crime-statistics/
- Estadísticas Colombia: https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/
- Parker, D. B. (1998). Fighting Computer Crime: A New Framework for Protecting Information. Wiley. http://www.amazon.com/dp/0471163783
- Campen, A., Dearth, D., & Goodden, R. (1996). Cyberwar: Security, Strategy, and Conflict in the Information Age. http://scholar.google.com/scholar?q=alan+d.+campen&btnG=&hl=en&as_sdt=0%2C5#1
- Campen, A., & Dearth, D. (1998). Cyberwar 2.0: Myths, mysteries and reality. http://dl.acm.org/citation.cfm?id=551792
- Campen, A., & Dearth, D. (2000). Cyberwar 3.0: Human factors in information operations and future conflict. http://www.ncjrs.gov/App/abstractdb/AbstractDBDetails.aspx?id=191421
- National Academy of Engineering. (2019). Privacy and Security in the 21st Century. In S. Olson (Ed.), Privacy and Security in the 21st Century. https://doi.org/10.17226/25575
- ENISA, ENISA Threat Landscape 2022, November 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

@iucolmayor