# Intrusiones en la red
# (Comprometiendo un servidor)

Hugo Gonzalez
hugo.gonzalez@upslp.edu.mx
@hugo_glez

LI²CIA
Laboratorio de Investigación
e Innovación en Ciberseguridad
e Inteligencia Artificial

CC BY NC SA

# Agenda

- Ejemplos recientes
- Cyber kill chain
- Demo comprometiendo un servidor
- Herramientas para seguridad en la red
- Higiene digital

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# Expositor

- Profesor-investigador en la UPSLP.
- Consultor para RomeoTech.
- Graduado del Instituto Canadiense para la Ciberseguridad.
- Miembro de “The Honeynet Project”.
- Mentor para el GSoC en temas de Android.

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# Intereses de investigación

- Análisis de malware
- Seguridad y análisis forense de red
- Aprendizaje máquina enfocado a seguridad
- Educación y la enseñanza de ciberseguridad
- Explotación y vulnerabilidades

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# Ejemplos recientes

twitter

**Apple**
@Apple

We are giving back to our community. We support Bitcoin and we believe you should too!

All Bitcoin sent to our address below will be sent back to you doubled!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only going on for the next 30 minutes.

4:58 PM · Jul 15, 2020 · Twitter Web App

**658** Retweets and comments **838** Likes

Pinned Tweet

**Elon Musk**
@elonmusk

I'm feeling generous because of Covid-19.

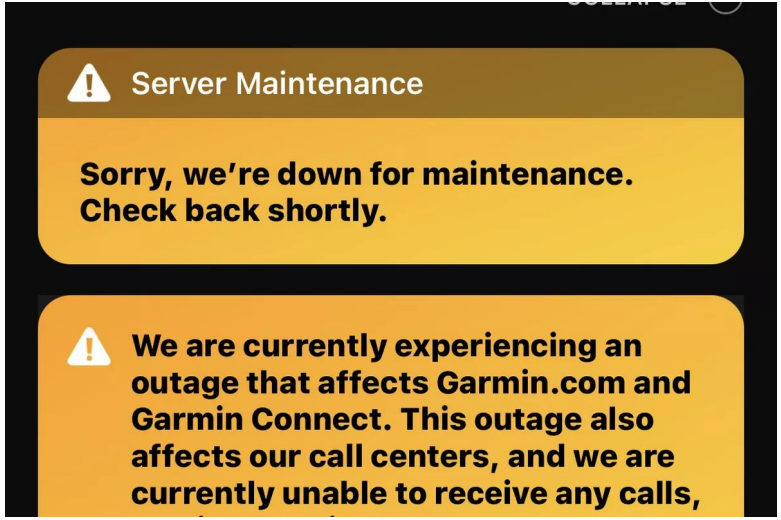
I'll double any BTC payment sent to my BTC address for the next hour. Good luck, and stay safe out there!

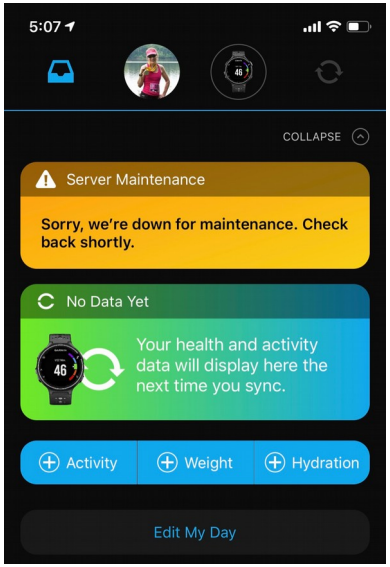
bc1qxy2kgdygjrsq[redacted]

4:17 PM · Jul 15, 2020 · Twitter Web App

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# GARMIN®



LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# FIRST IT WAS INTEL, THEN GARMIN, NOW CANON HAS BEEN HACKED

By David Richards| 10 Aug 2020

SHARE

Ransomware operators Maze told BleepingComputer that they were able to get hold of 10 TB of data and private databases as part of the attack on Canon, no other details were provided, particularly any proof of stolen data, how much the ransom is, and the number of encrypted devices.

Giant Japanese Company Canon has been hacked and some are speculating that it could be bigger than the Intel hack attack.

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

CRUISES

# Carnival Corp. hacked: Cruise passenger and crew information at risk

Associated Press

Published 10:59 a.m. ET Aug. 19, 2020 | **Updated 11:32 a.m. ET Aug. 19, 2020**

The attack was first detected Saturday. The attack accessed an encrypted portion of technology systems for one of the cruise line's brands and certain data files were downloaded, the company said in a filing with the U.S. Securities and Exchange Commission.

Carnival operates Carnival Cruise Line, Princess Cruises, Holland America Line and other lines, but the company didn't say in the filing which cruise line was affected.

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

06 AUG 20

# Hacked Data Broker Accounts Fueled Phony COVID Loans, Unemployment Claims

A group of thieves thought to be responsible for collecting millions in fraudulent small business loans and unemployment insurance benefits from COVID-19 economic relief efforts gathered personal data on people and businesses they were impersonating by leveraging several compromised accounts at a little-known U.S. consumer data broker, KrebsOnSecurity has learned.

CIA
Investigación
en Ciberseguridad
Artificial

# Cyber kill chain

- “Kill chain” tiene su origen en el ejército, como una estratégia de ataque.
- 2011 es adaptada a la seguridad informática
- Varias evoluciones y modelos similares (MITRE ATT&CK framework)

# Las siete fases son:

https://www.idric.com.mx/blog_post/cyber-kill-chain

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# Herramientas

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# Demo

# Herramientas para la seguridad en redes

- Cyber kill chain también puede ser usada para **planear la defensa**.
- Protección perimetral.
- Protección en la red.
- Protección en los equipos.
- Detección de anomalías.
- Monitoreo integral.

- Los diferentes vendedores te ofrecen multiples soluciones.
- También existen soluciones “Open Source” o abiertas que te pueden ayudar a aprender los conceptos básicos.

SNORT®

zeek

logstash

SIEM ?

elasticsearch

kibana

Bacula .org

ClamAV®

WAZUH

t-POt

ALIEN VAULT OSSIM™

OpenVAS

Open Vulnerability Assessment Scanner

LI²CIA

Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# Higiene digital

- El concepto de **higiene digital** podría pensarse como prácticas habituales que permitan mantener nuestro entorno digital lo más **saludable** posible.

https://www.tedic.org/por-que-tener-habitos-de-higiene-en-el-entorno-digital/

# Passwords are like underwear...

Change them often.

Don't share them with friends!

The longer the better.

Be mysterious!

Don't leave yours lying around.

© Office of Policy and Education, University of Michigan, Computer Services, Network Security Team

LI²CIA
Laboratorio de Investigación e Innovación en Ciberseguridad e Inteligencia Artificial

# ¿Preguntas?

LI²CIA
Laboratorio de Investigación
e Innovación en Ciberseguridad
e Inteligencia Artificial