
# GANGS OF INDUSTRY

*Aarón Flecha Menendez*



CyberCamp.es

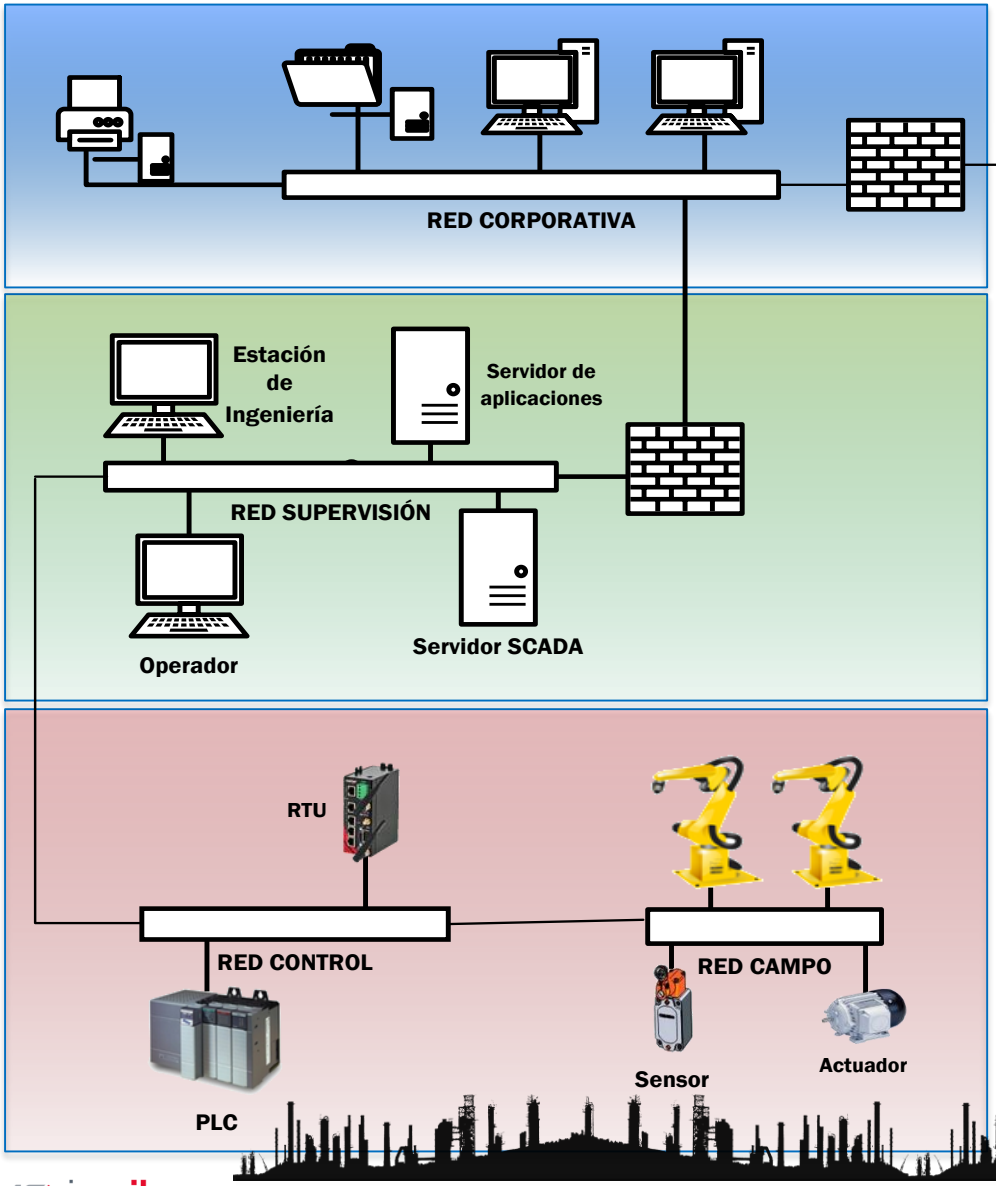
# ¿Quién soy?

- Ingeniero Técnico Informático de Sistemas
- Consultor de seguridad en Sistemas de Control industrial en s21sec
- Estudiante a tiempo parcial

# CONTENIDO

- Entornos industriales
- Ransomware
- Casos Reales
- Desarrollo del ataque
- DEMO
- Conclusiones

# ENTORNOS INDUSTRIALES




DNP3

Modbus

**Sistemas de Control Industrial**

S7

HART

# ENTORNOS INDUSTRIALES

- **Sistema de Control Industrial**

  Conjunto de equipos dispuestos en diferentes niveles (nivel de campo, nivel de control, nivel de supervisión), que están conectados en una misma red y que permiten, mediante acciones en tiempo real, gestionar procesos físicos.





- **Infraestructura crítica**

  Toda aquella infraestructura estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales prestados a la sociedad.

  *Ley 8/2011, de 28 de abril, de Protección de Infraestructuras Críticas*

# ENTORNOS INDUSTRIALES

Energía

Agua

Alimentación

Salud

Transporte

Industria química

Industria nuclear

Tecnologías de la Información y las Comunicaciones (TIC)

Financiero

Instalaciones de investigación

Administración

**Sectores Estratégicos y de carácter crítico en España**

# RANSOMWARE

- **Definición**

Software malicioso cuya misión es restringir el acceso a partes del sistema o archivos alojados en este. Suele venir asociado a un rescate que se pide como moneda de cambio para recuperar los datos. Dependiendo del sistema afectado y de los creadores del ransomware, la cantidad que se pide puede variar.

# RANSOMWARE - TIPOS

## Locker Ransomware
(Bloqueo de dispositivo)

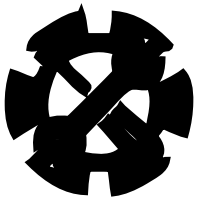

## Crypto Ransomware
(Cifrado de datos)


**Afecta al sector de arranque**

# RANSOMWARE - TI VS TO

## Tecnologías de la Información

- Cifrado permanente de datos y documentos tanto corporativos como personales.
- Cifrado de dispositivos en red (servidores compartidos, ordenadores en red, impresoras en red, etc.).
- Divulgación de información durante los intentos de restauración.



## Tecnologías de la Operación

- Malfuncionamiento de equipos que puede derivar en problemas para los trabajadores de la industria.
- **¡¡¡¡Paradas de producción!!!!!**
- Divulgación de información sobre procesos de carácter importante para la consecución del producto final.

# RANSOMWARE - EJEMPLO

## Industrial Security Advisory - Claims of Ransomware Masquerading as an Allen-Bradley Update

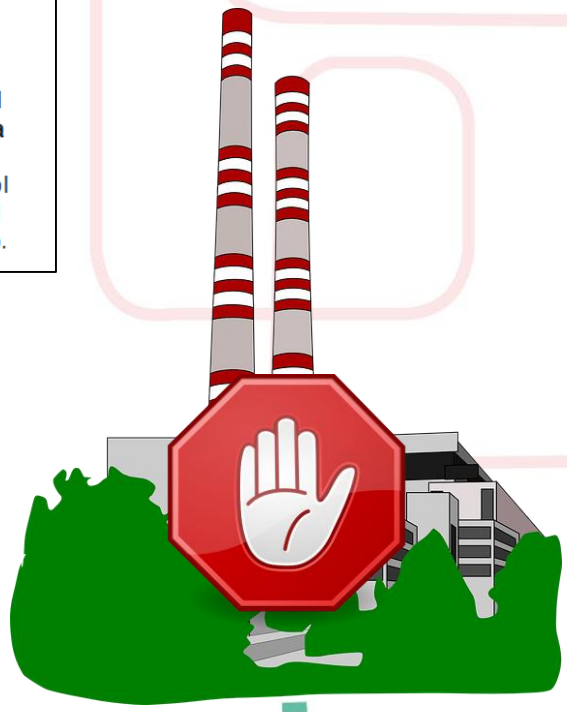
Rockwell Automation released a notice titled "**Industrial Security Advisory - Claims of Ransomware Masquerading as an Allen-Bradley Update".** You are receiving this notification as a Rockwell Automation employee based on the notification profile that you have selected.

Please click on this link to review Knowledgebase ID 799091.

Rockwell Automation has learned about the existence of a malicious file called "Allenbradleyupdate.zip" that is being distributed on the internet. **This file is NOT an official update from Rockwell Automation, and we have been informed that this file contains a type of ransomware malware that, if successfully installed and launched, may compromise the victim's computer.** This advisory is intended to raise awareness to control system owners and operators of reports of the file's existence as a result of reports Rockwell Automation received from the Electricity Information Sharing and Analysis Center ("E-ISAC").

TOP COUNTRIES

| | |
|---|---|
| United States | 2,284 |
| Canada | 365 |
| Spain | 136 |
| Australia | 81 |
| Taiwan, Province of China | 80 |



https://mail.nelson-electric.com/webshare/Documents/Ransomware_Masquerading_as_an_Allen-Bradley_Update.pdf

# CASOS REALES

- Octubre 2015, empresa Sabella (especializada en ingeniería industrial de corrientes marinas)
  - Los atacantes tomaron el control del ordenador de supervisión
  - Familia de ransomware utilizado, Cryptolocker
  - Tardaron 2 semanas en poner de nuevo en marcha la turbina
  - Los atacantes pidieron 4.000$US ≈ 3.738 €

http://france3-regions.francetvinfo.fr/bretagne/finistere/l-hydrolienne-immergee-au-large-d-ouessant-victime-de-pirates-informatiques-954515.html

# CASOS REALES


- Febrero 2016, Hollywood Presbyterian Medical Center
  - Se pagó el rescate de 9000 bitcoins ≈ 6.000.000 €
  - Infección gracias a macros habilitadas en ficheros adjuntos .DOCM (WORD 2007)
  - Provocó trastornos a los pacientes que fueron trasladados

https://threatpost.com/locky-targets-hospitals-in-massive-wave-of-ransomware-attacks/119981/

# CASOS REALES



- Febrero 2016, hospitales alemanes
  - Corte de servicio de servidores
  - El rescate no se pagó
  - Se utilizaron backups para restablecer los sistemas

https://www.helpnetsecurity.com/2016/02/26/crypto-ransomware-hits-german-hospitals/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

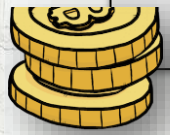
# CASOS REALES

*" You Hacked, ALL Data Encrypted. Contact For Key(cryptom27@yandex.com)ID:681 ,Enter."*

- 26 Noviembre, Metro de San Francisco
  - Más de 2000 ordenadores comprometidos dentro del sistema de transporte público de San Francisco.
  - Se pedía un rescate de 100 Bitcoins ≈ 73.000$ ≈ 65 882€ . Este rescate no fue pagado.
  - 2 días de transporte público gratis.


https://www.sfmta.com/about-sfmta/blog/update-sfmta-ransomware-attack

# DESARROLLO DEL ATAQUE



Explotación

Propagación

Vectores de ataque

Elaboración del ataque

Reconocimiento del terreno

# DESARROLLO DEL ATAQUE

**Reconocimiento del terreno**


- Selección del objetivo
- Búsqueda de información sobre la empresa
  - Direccionamiento (ARIN,APNIC,RIPE,LACNIC,AFRINIC)
  - Organigrama
  - Escaneo de servicios
- Dispositivos y software que utilizan
  - Modelos de dispositivos y fabricantes con los que trabaja
  - Comunicaciones entre los mismos
  - Programas que utilizan
- Empresas con las que trabajan
  - Mantenimientos y soporte que realizan

SHODAN

ZoomEye

NMAP

censys

¿A quién?

# DESARROLLO DEL ATAQUE

**Elaboración del ataque**

**Locker Ransomware**
(Bloqueo de dispositivo)

**Crypto Ransomware**
(Cifrado de datos)


**¿Complejidad del ataque?**

# DESARROLLO DEL ATAQUE

**Vectores de ataque**

*Scan the QR code with your smart-phone or mobile device to access our vast information center on the web.*

**Códigos QR**

**USB**

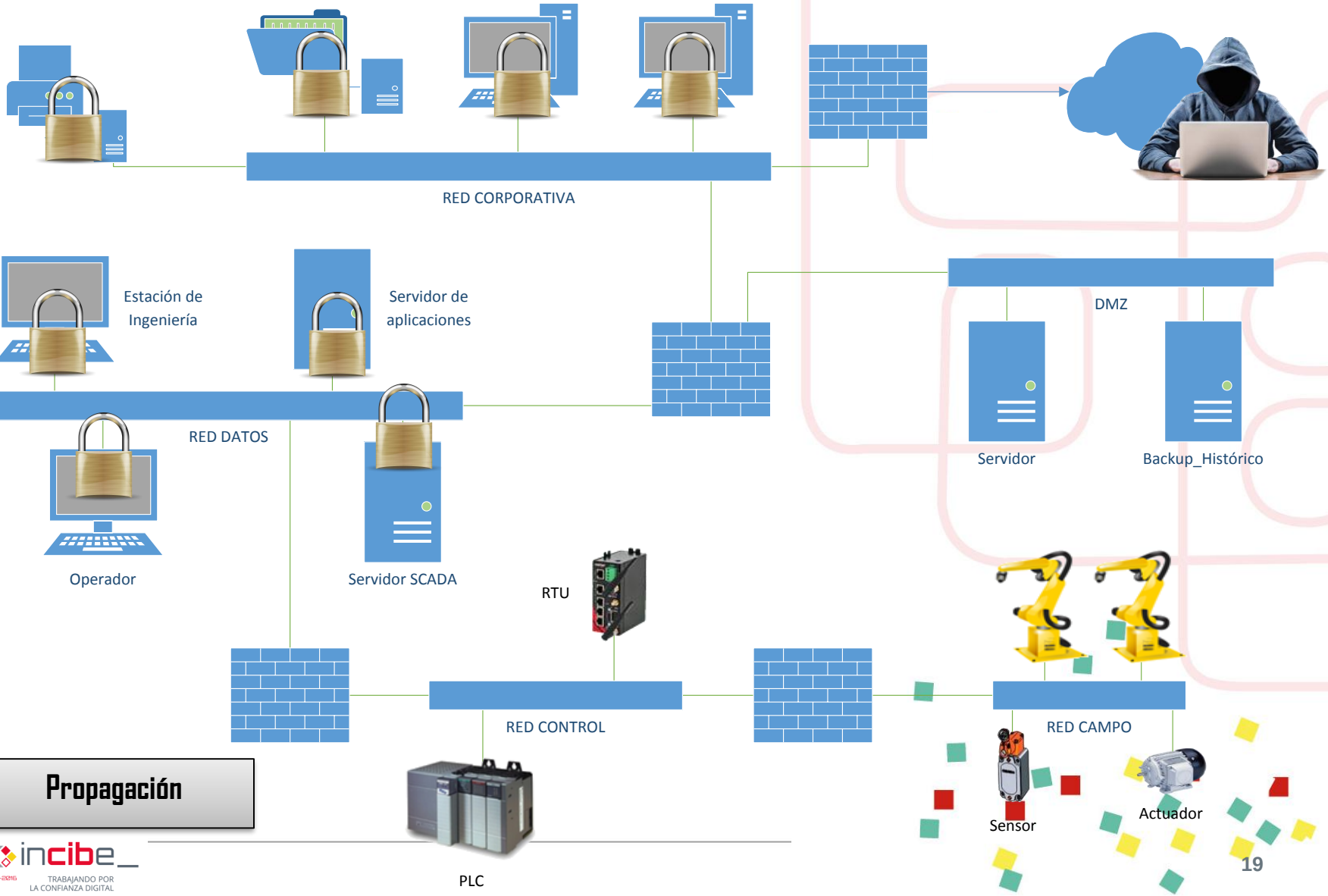
**Ingeniería social**

**Dispositivos móviles**


**Phishing**

¿Cómo voy a infectar a mi víctima?

# DESARROLLO DEL ATAQUE



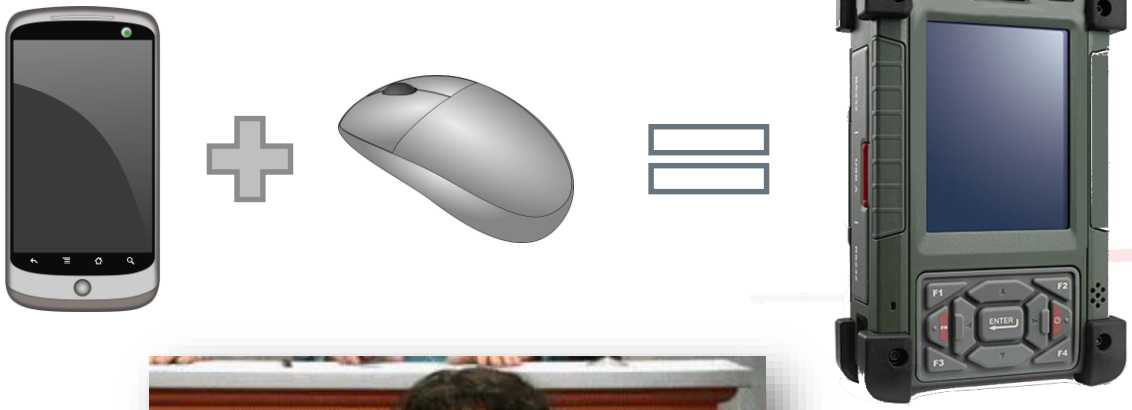

**Propagación**

# DESARROLLO DEL ATAQUE

**Explotación**

- Pérdida de imagen corporativa
- Parada de producción
- Problemas medioambientales o daños en personas
- Pérdidas de dinero

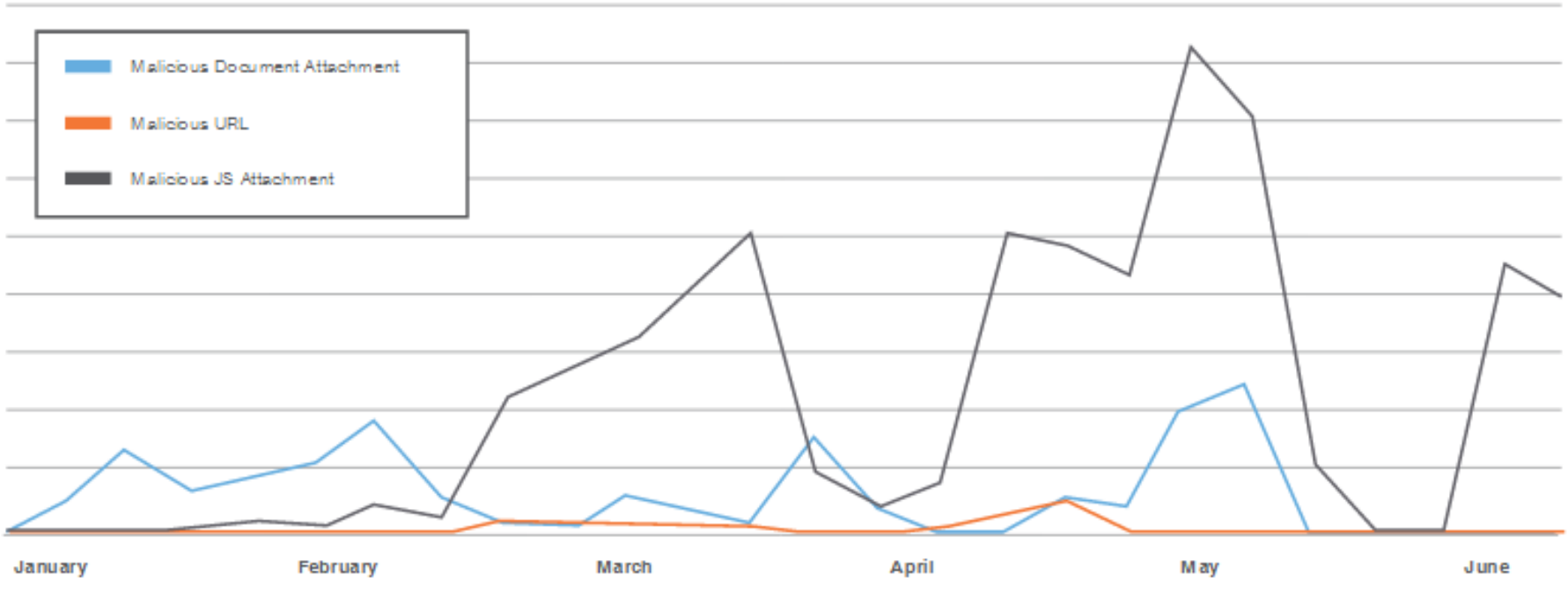
# DEMO




DEMO

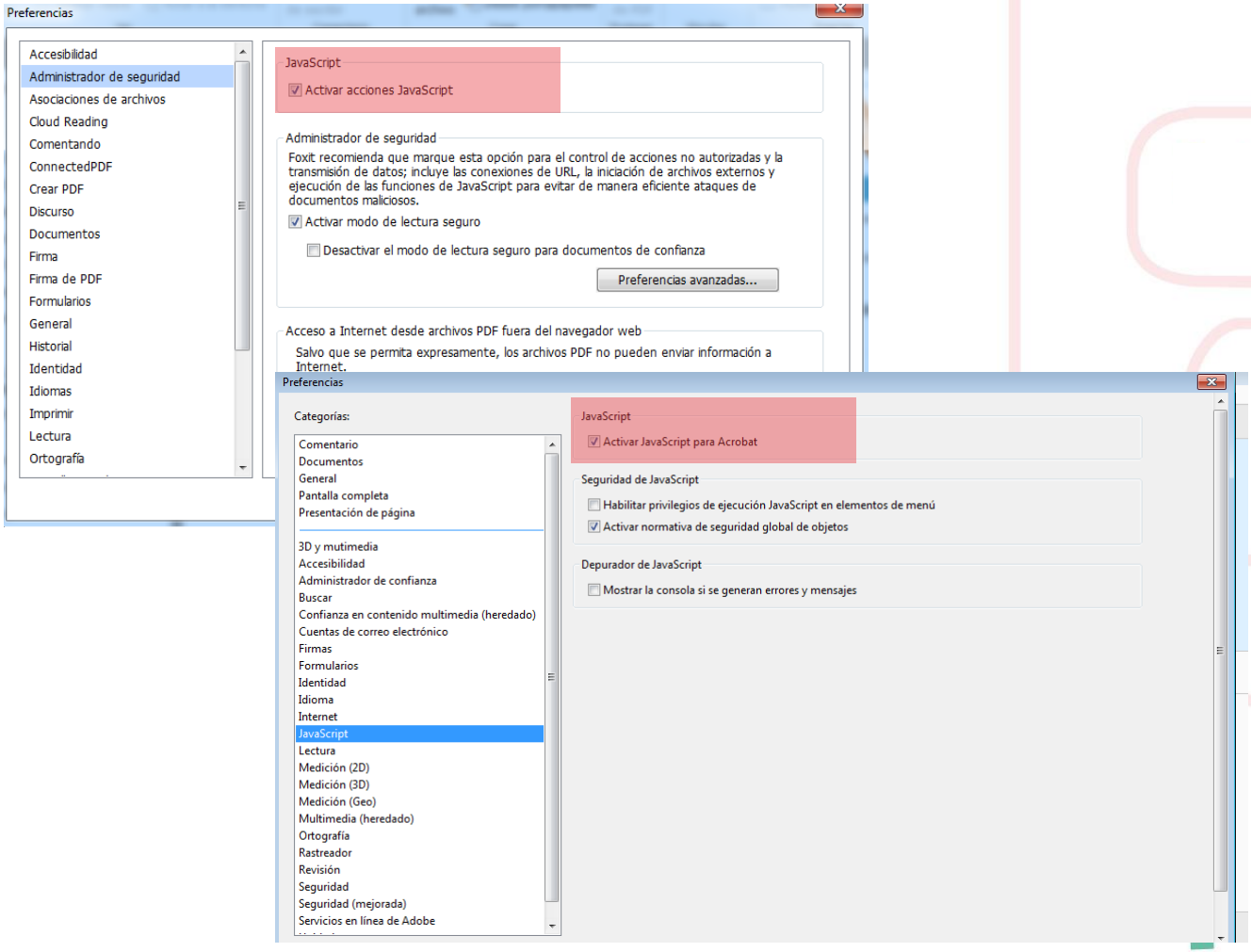
# CONCLUSIONES

## Volumen de mensajes por tipo de ataque




https://www.proofpoint.com/sites/default/files/quarterly_threat_summary_apr-jun_2016.pdf

# CONCLUSIONES

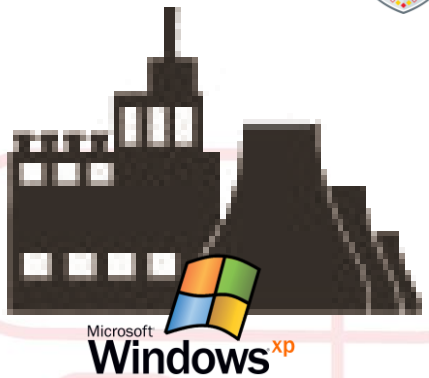


# CONCLUSIONES

- Concienciar a los empleados para que eviten caer en engaños.
- Segmentación de las redes con buenas configuraciones de los dispositivos de seguridad presentes en ellas (cortafuegos, IDS, IPS, etc.).
- No activar las Macros de los documentos sin consultar previamente el propósito de estos dentro del documento.
- Utilizar herramientas antiransomware siempre que sea posible.
- Desactivar JavaScript tanto para lectores de documentos online como en local.
- Reglas de YARA, Indicadores de Compromiso, Listas blancas…

# HERRAMIENTAS UTILIZADAS

- https://github.com/bealerjm/virtuaplant/tree/master/plants/oil-refinery (HMI - Proceso)

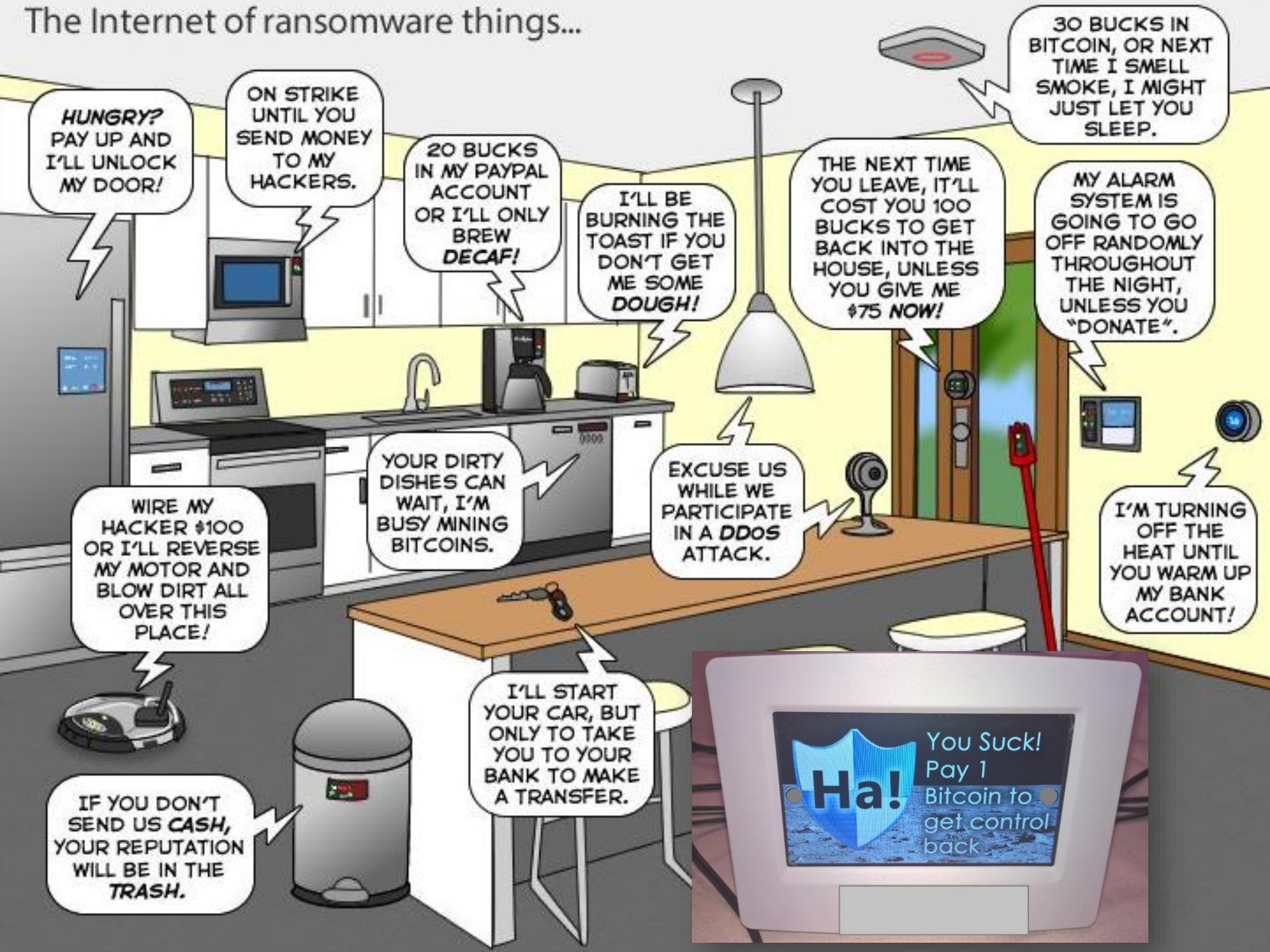



- http://jacekhryniewicz.wixsite.com/website/modbus-simulator-of-tracerco-nucleonic-p (HMI - Local)

- https://github.com/dzzie/pdfstreamdumper

- **Análisis:**
  - https://id-ransomware.malwarehunterteam.com/
  - https://malwr.com/
  - https://sandbox.anlyz.io/
  - https://www.virustotal.com/es/

# The Internet of ransomware things...




# Gracias por su atención

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL