Telefónica Tech

Aristeo: el Dios industrial de las abejas OT para ciberseguridad

Inteligencia predictiva de amenazas en entornos OT

MWC 2023

MAKING THINGS HAPPEN

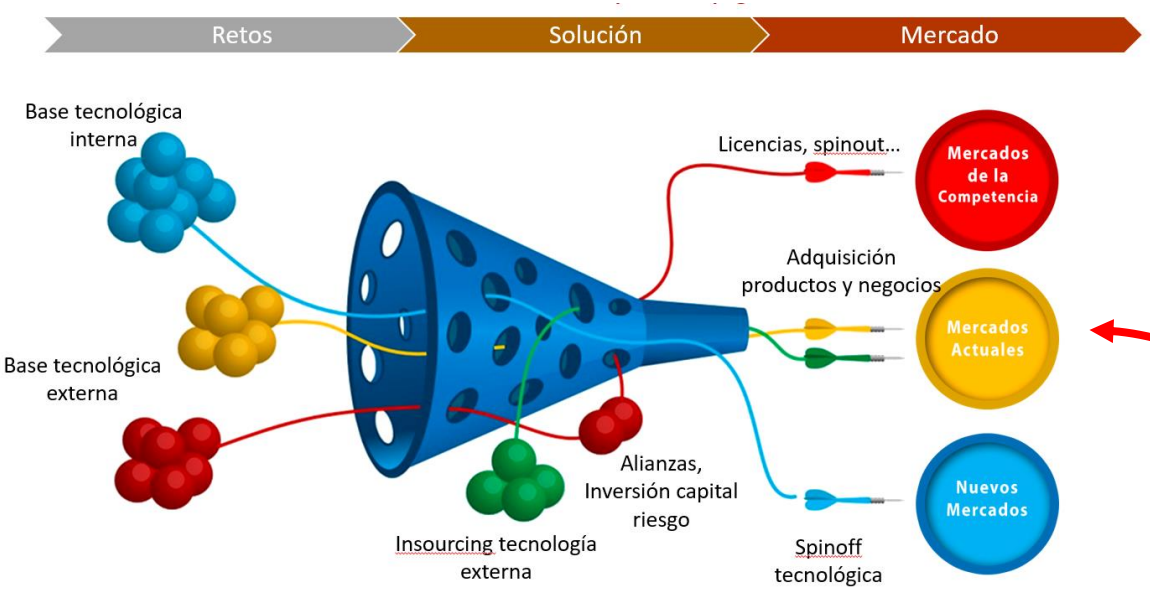
¿Quién soy?

joseantonio.cascallanaarroyo@telefonica.com
https://www.linkedin.com/in/josecascallana/

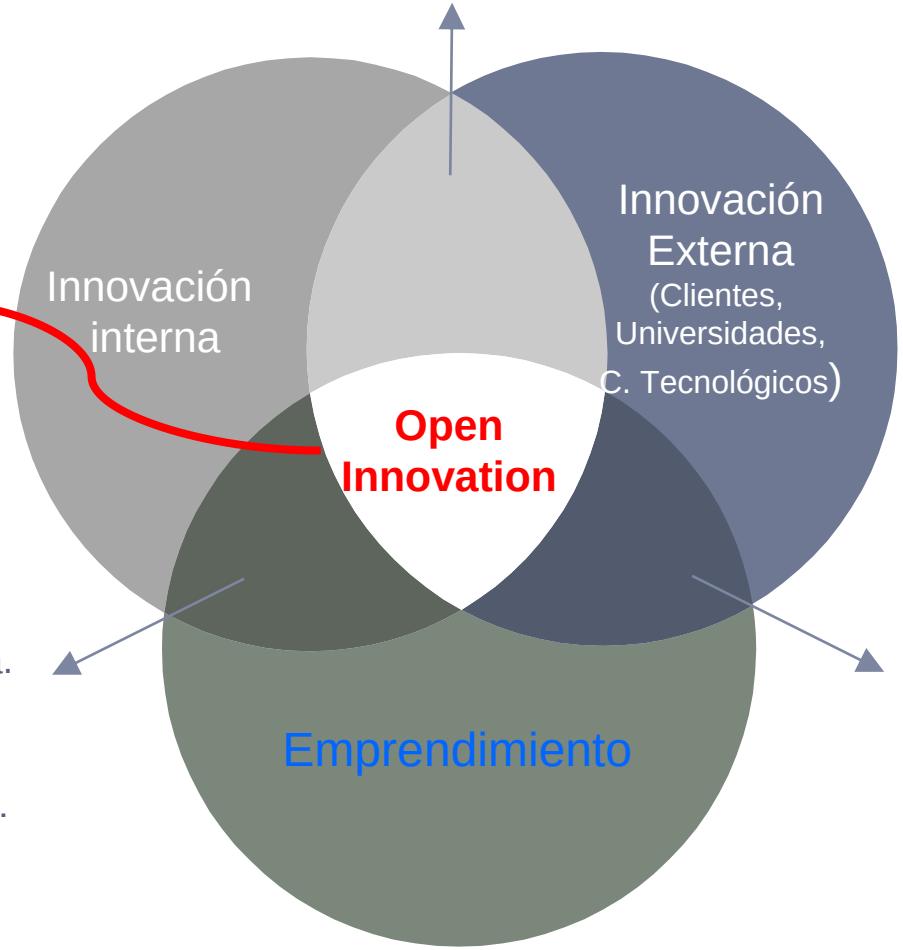
Nuestra visión de la Innovación

Telefónica TECH Cyber & Cloud

¿Cómo innovamos?
Innovación Interna, Externa & Emprendimiento



- Co-innovación hacia nuevos productos / servicios…



- Incorporación a portfolio Telefónica.
- Integración / mejora productos actuales.
- Inversión / adquisición tecnología…

- Obtener conocimiento
- Comercialización
- Licencias
- SpinOut

Nuestra visión de la INNOVACIÓN: proceso de convertir una idea o invención en un bien o servicio que **crea valor agregado, por el que los clientes están dispuestos a pagar y permite obtener mayor rentabilidad.**

La importancia de la ciberseguridad industrial

Telefónica TECH Cyber & Cloud

¿Qué es la ciberseguridad en entornos industriales?

Ciberseguridad Industrial es el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías

Gartner

STAMFORD, Conn., July 21, 2021

Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans

Organizations Can Reduce Risk by Implementing a Security Control Framework

By 2025, cyber attackers will have weaponized operational technology (OT) environments to successfully harm or kill humans, according to Gartner, Inc.

Attacks on OT – hardware and software that monitors or controls equipment, assets and processes – have become more common. They have also evolved from immediate process disruption such as shutting down a plant, to compromising the integrity of industrial environments with intent to create physical harm. Other recent events like the Colonial Pipeline ransomware attack have highlighted the need to have properly segmented networks for IT and OT.

"In operational environments, security and risk management leaders should be more concerned about real world hazards to humans and the environment, rather than information theft," said Wam Voster, senior research director at Gartner. "Inquiries with Gartner clients reveal that organizations in asset-intensive industries like manufacturing, resources and utilities struggle to define appropriate control frameworks."

According to Gartner, security incidents in OT and other cyber-physical systems (CPS) have three main motivations: actual harm, commercial vandalism (reduced output) and reputational vandalism (making a manufacturer untrusted or unreliable).

Gartner predicts that the financial impact of CPS attacks resulting in fatal casualties will reach over $50 billion by 2023. Even without taking the value of human life into account, the costs for organizations in terms of compensation, litigation, insurance, regulatory fines and reputation loss will be significant. Gartner also predicts that most CEOs will be personally liable for such incidents.

https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

¿Qué es la ciberseguridad en entornos industriales?

https://actualidad.rt.com/actualidad/203175-hackers-infiltran-planta-depuradora-agua

'Hackean' una planta potabilizadora y cambian la composición química del agua

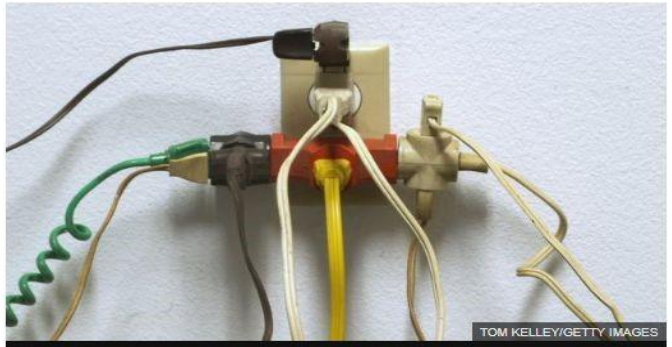
Publicado: 27 mar 2016 17:23 GMT | Última actualización: 27 mar 2016 17:25 GMT

Si bien no se informó en qué país se produjo el 'hackeo', el envenenados en un ataque de características similares.

grupo de hackers rusos al que acusan de atacar redes eléctricas en Estados Unidos

Redacción
BBC News Mundo

28 julio 2018 — Compartir



Los hackers pueden haber sido responsables de varios apagones, dice el Departamento de Seguridad de Estados Unidos.

Un grupo de hackers rusos tuvo acceso remoto a las salas de control de varios proveedores de energía de Estados Unidos, según el Departamento de Seguridad Nacional estadounidense.

muyseguridad.net/2016/04/27/planta-nuclear-malware/

INICIO | ACTUALIDAD | AMENAZAS | CIBERCRIMEN | HACKING | SOLUCIONES | TRUCOS | PRIVACIDAD

AMENAZAS

Una planta nuclear de Alemania cierra tras descubrirse malware

por Arantxa Asían 27 de abril, 2016

G+1 +11 Recomendar esto en Google — Twittea — Me gusta 126

ATAQUE A TWITTER Y OTRAS COMPAÑÍAS ›

Varios ciberataques masivos inutilizan las webs de grandes compañías

Son los más graves de la última década. Los primeros indicios descartan a un país extranjero

220

UILLÉN | JOAN FAUS | ROSA JIMÉNEZ CANO

Washington / San Francisco - 22 OCT 2016 - 14:01 ART

ela el nombre de la planta ni el país donde

Ciberataque paraliza temporalmente a importantes diarios de Estados Unidos

Redacción
BBC News Mundo

30 diciembre 2018 — Compartir

La planta de impresión del principal diario de Los Ángeles, LA Times, fue uno de los blancos del ataque el viernes.

Varios de los principales diarios de Estados Unidos sufrieron interrupciones de impresión y distribución el sábado, tras un ciberataque, informan los medios del país.

El ataque atrasó la distribución de los periódicos *The Los Angeles Times*, *Chicago Tribune*, *Baltimore Sun* y otros que **pertenecen a la empresa mediática Tribune Publishing**.

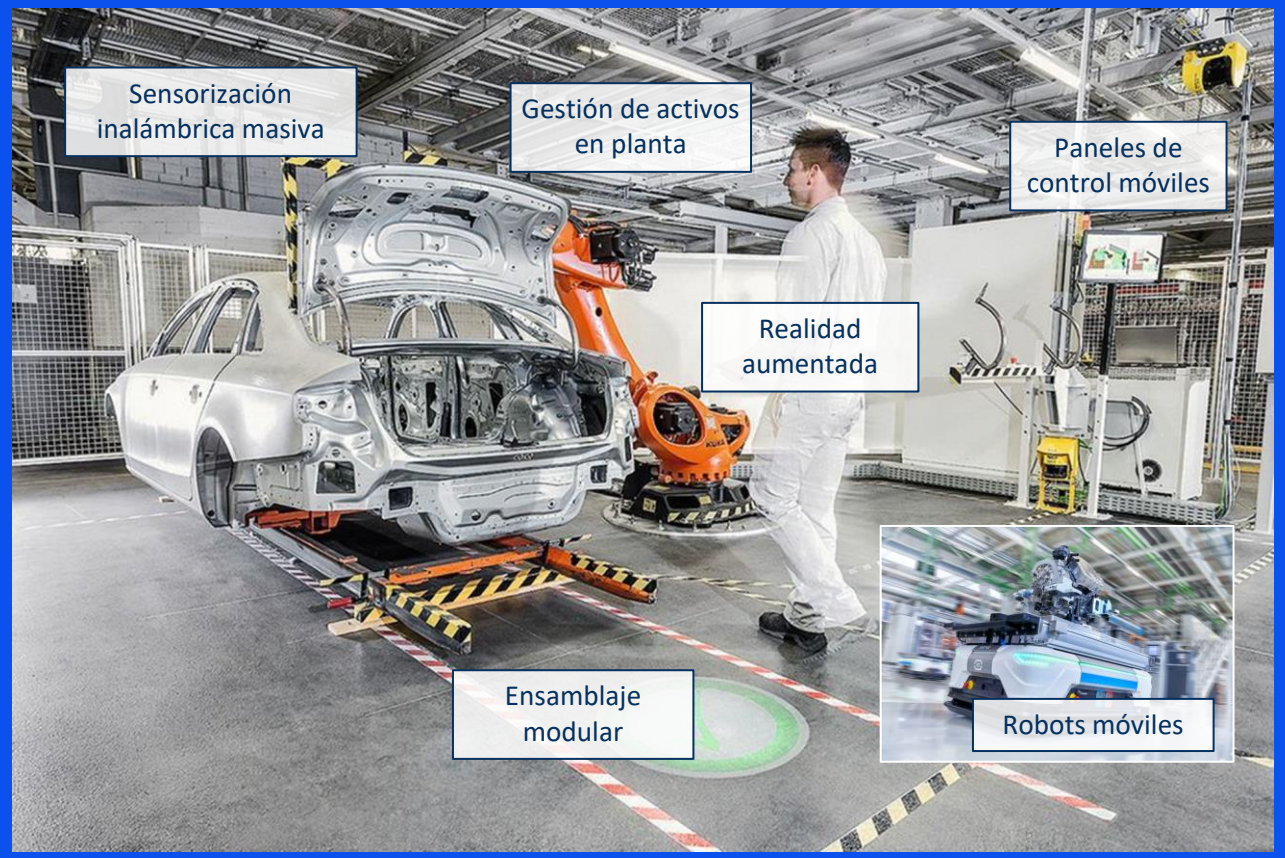
La compañía dijo haber detectado el programa maligno el viernes, que atacó a los diarios que comparten la misma planta de impresión.

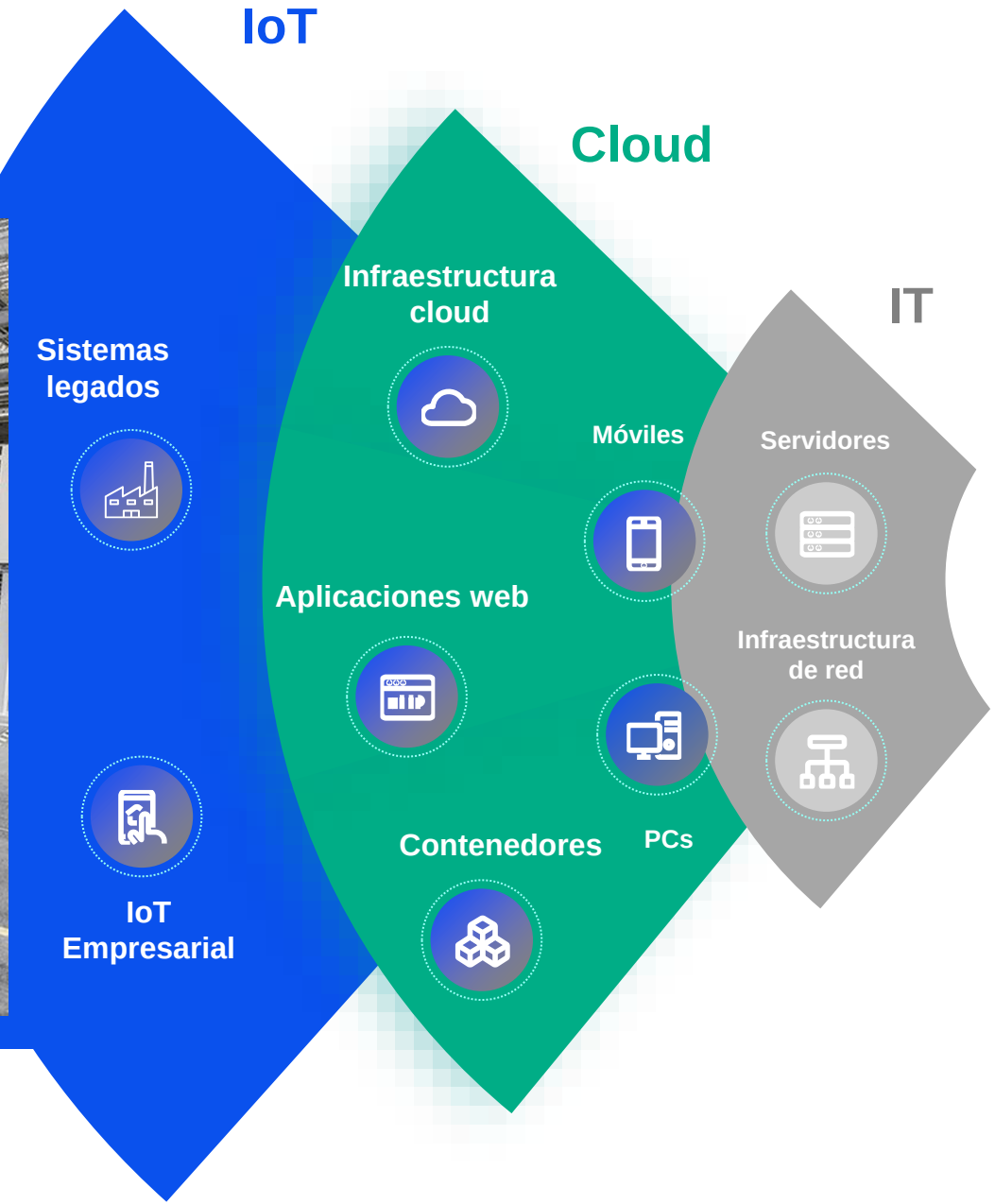
Ya en 1983…
“¿Podría suceder algo así en el mundo real?”.

Con esta pregunta efectuada a su equipo asesor el expresidente de Estados Unidos Ronald Reagan expresó toda su preocupación y desconcierto luego de ver la película War Games (1983).

Extraño juego, el único movimiento para ganar es no jugar.

El **Internet de las Cosas** es una nueva ola en el proceso de transformación digital de especial relevancia para la ciberseguridad en la **Industria** por el significativo aumento de su **superficie de exposición**





Resumen de los incidentes históricos más relevantes que afectan a las infraestructuras industriales

2010 …

- Stuxnet interrumpe el programa nuclear iraní

2013

- Compuertas de la presa de Nueva York comprometidas

2014

- Bombas de infusión de medicamentos hospitalarios hackeadas
- Semáforo de la ciudad hackeado

2015

- Horno siderúrgico alemán destruido

- Transmisión del coche y frenos controlados

- La red eléctrica de Ucrania se desconecta

2017

- Producción global de una gran farmacéutica cerrada por ransomware (1000M pérdida)

- Cierre global de la compañía naviera por ransomware (250M pérdida)

2018

- Trisis/Triton: Malware diseñado para comprometer el safety

2019

- Cierre de productor global de aluminio por ransomware
- Partes de ASCO paradas por ransomware

2020

- Ataque de ransomware Ekans en varios sectores
- SolarWinds Orion

2021

- Intento de envenenamiento del suministro de agua

- Cierre del oleoducto por ransomware

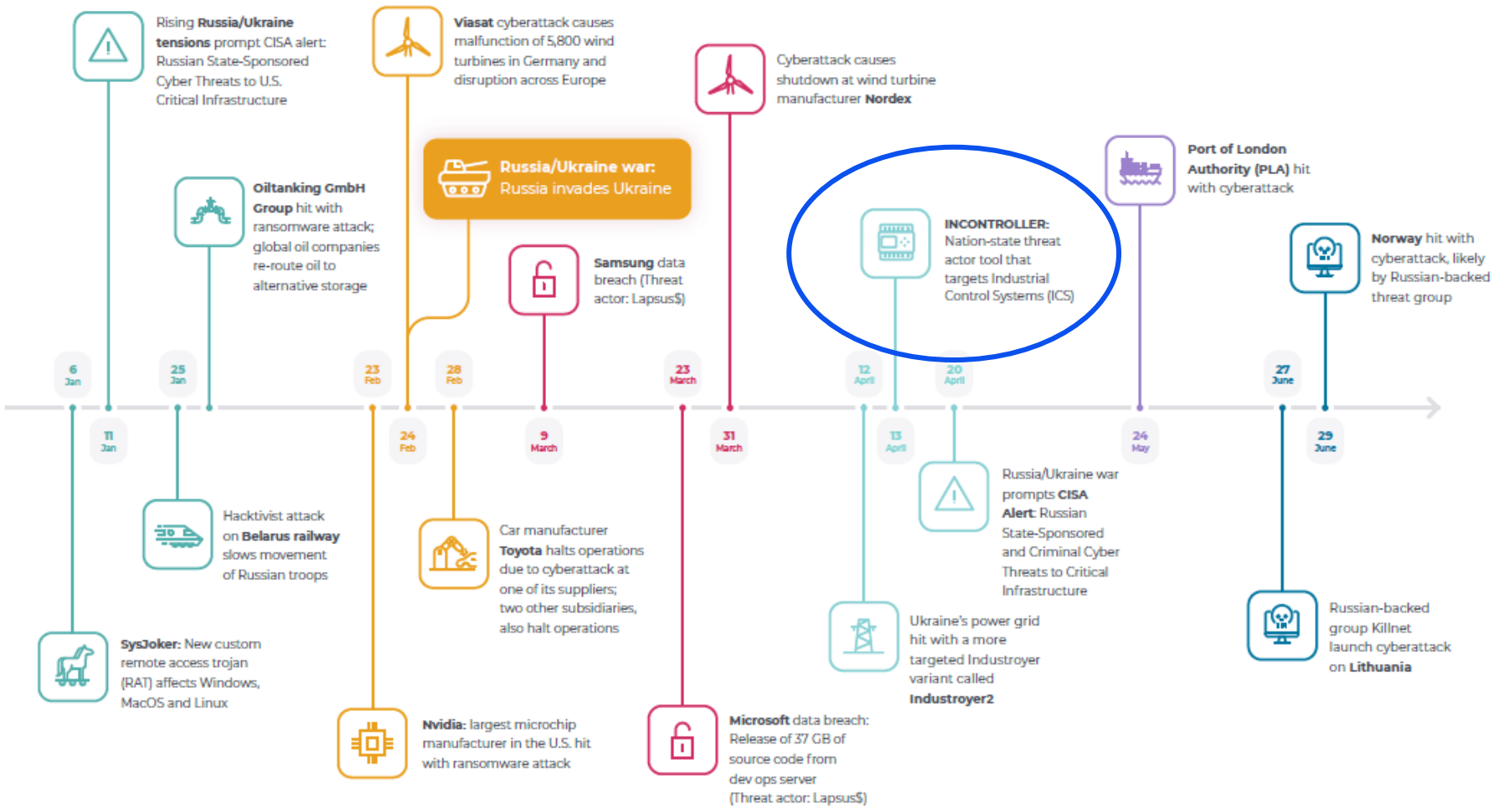
Source: Original Fortinet slide completed with recent incidents

Pero no hace falta recurrir a la historia, tenemos otros mucho más recientes

Timeline of Notable Cyber Events in the First Half of 2022

This timeline highlights several significant cyber events between January and June 2022 that have helped shape the current threat landscape.

Since **Russia** invaded Ukraine in February 2022, we have seen activity from several types of threat actors, including hacktivists, state-backed APTs and cyber criminals. We also saw robust use of **wiper malware**, and an Industroyer variant, dubbed **Industroyer2**, was developed to misuse the IEC-104 protocol, which is commonly used in industrial environments.



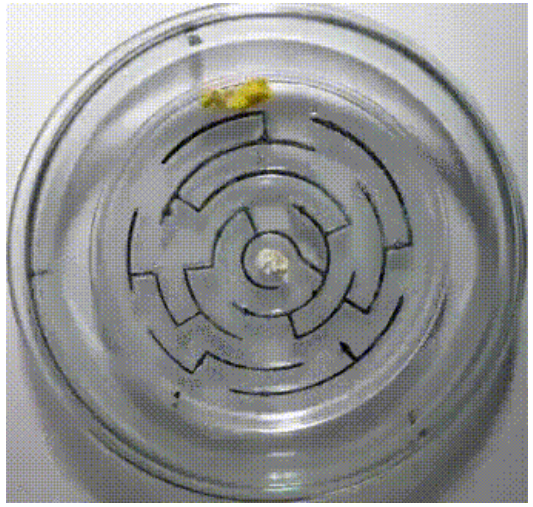
Source: 2022 H1 Nozomi OT/IoT Cybersecurity Report

Necesidad de mercado: Innovación ciberseguridad OT

Nace Aristeo

Telefónica Tech

Definición y diseño: ¿Qué es Aristeo?

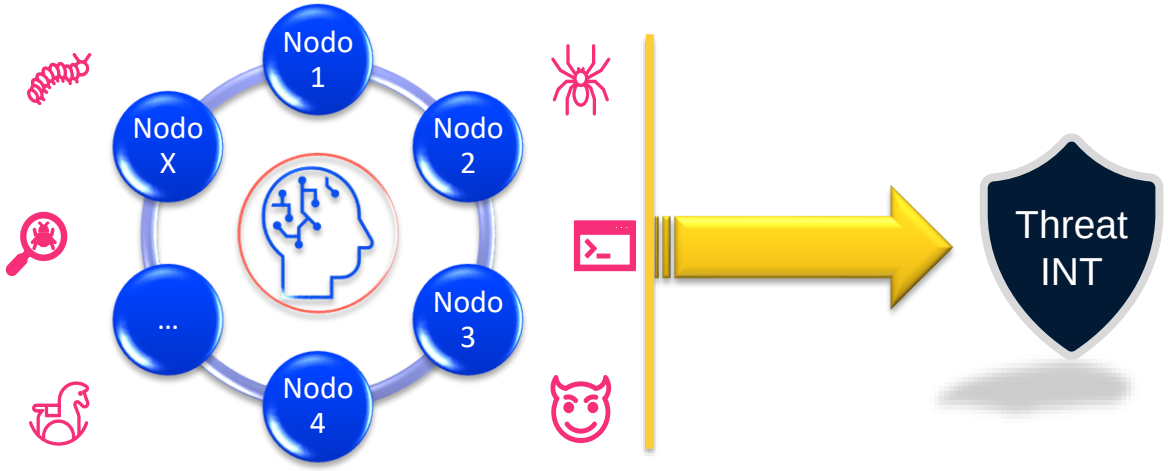


Meta: Establecer una red de señuelos industriales **reales** para el análisis predictivo de amenazas OT.

Espíritu: Evitar elementos superfluos. Ser un entorno real es su mayor valor.

Características fundamentales: Flexibilidad y adaptabilidad

- Entornos adaptables al cliente y sus necesidades
  - Sectorizable
  - Configurable como la infraestructura y procesos del cliente
- No ocupa espacio en las instalaciones del cliente



Definición y diseño: ¿Qué es Aristeo? Inteligencia predictiva.

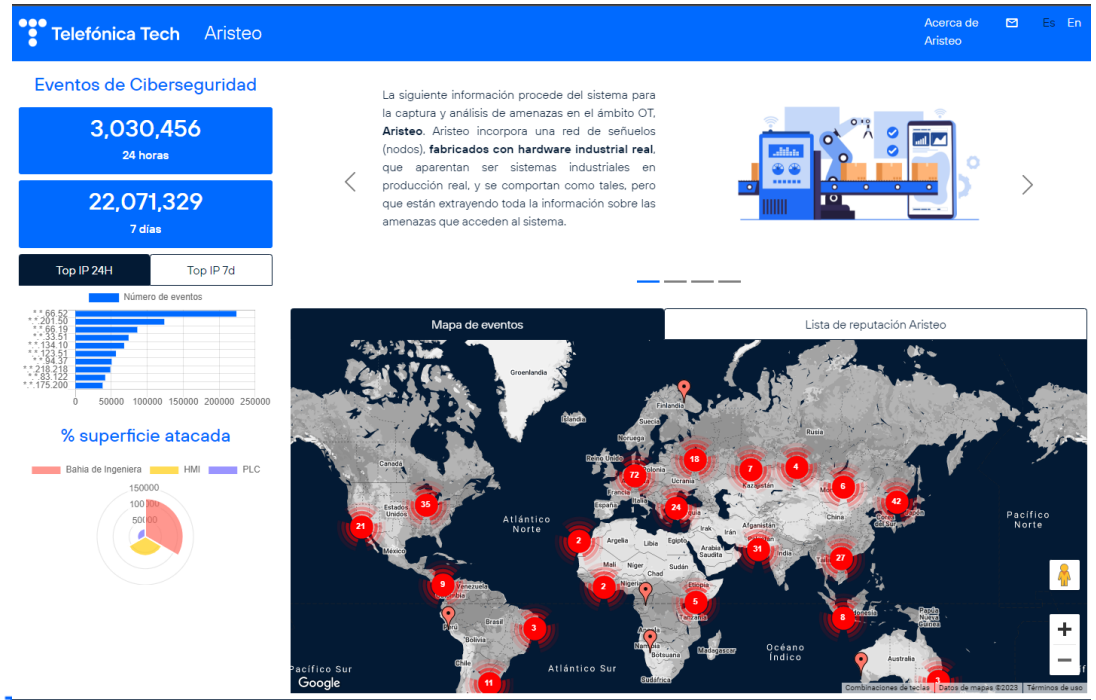
Threat X

Dynamic Use Cases

PLANTA INDUSTRIAL PARA EL PROCESAMIENTO DE AGUAS

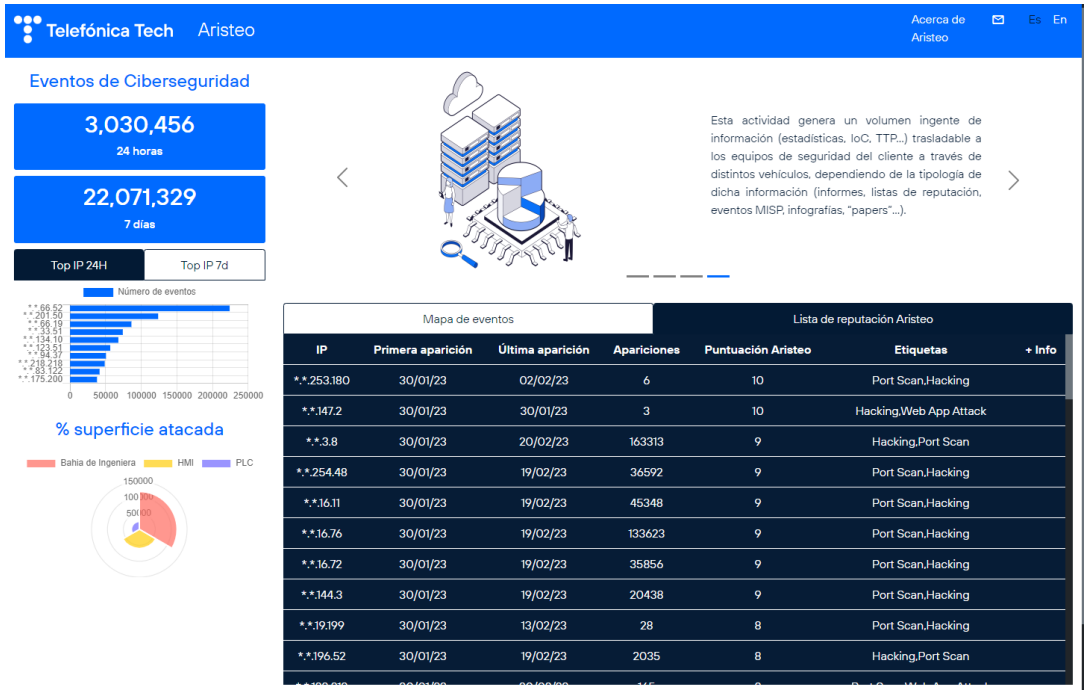
Nodo 1

El Nodo 1 tiene un HMI y varios PLC de distintos fabricantes. Además, tiene sensores y actuadores que se comportan de la misma forma en la que lo harían en una planta de tratamiento de aguas normal y corriente.



Nodo 1: planta industrial para el procesamiento de aguas

El Nodo 1 tiene un HMI y varios PLC de distintos fabricantes. Además, tiene sensores y actuadores que se comportan de la misma forma en la que lo harían en una planta de tratamiento de aguas normal y corriente.



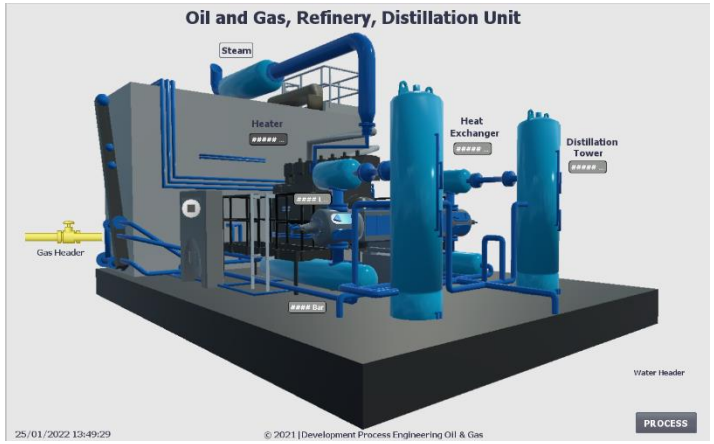
IP	Primera aparición	Última aparición	Apariciones	Puntuación Aristeo	Etiquetas	+ Info
..253.180	30/01/23	02/02/23	6	10	Port Scan,Hacking	
..147.2	30/01/23	30/01/23	3	10	Hacking,Web App Attack	
..3.8	30/01/23	20/02/23	163313	9	Hacking,Port Scan	
..254.48	30/01/23	19/02/23	36592	9	Port Scan,Hacking	
..16.11	30/01/23	19/02/23	45348	9	Port Scan,Hacking	
..16.76	30/01/23	19/02/23	133623	9	Port Scan,Hacking	
..16.72	30/01/23	19/02/23	35856	9	Port Scan,Hacking	
..144.3	30/01/23	19/02/23	20438	9	Port Scan,Hacking	
..19.199	30/01/23	13/02/23	28	8	Port Scan,Hacking	
..196.52	30/01/23	19/02/23	2035	8	Hacking,Port Scan	

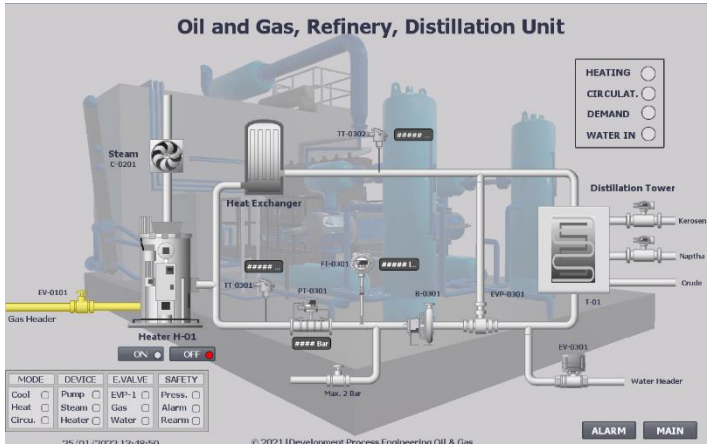
Nodo 2: Planta Industrial de oil & gas, unidad de destilación

Proceso de lazo cerrado implementado con lógica de funcionamiento real.

Más de 16 etapas diferentes para que sea indistinguible de un proceso real. Pérdidas y cargas de agua, extracción de producto, temperaturas graduales…

Entorno operable, con efecto en presiones, flujos, temperaturas…



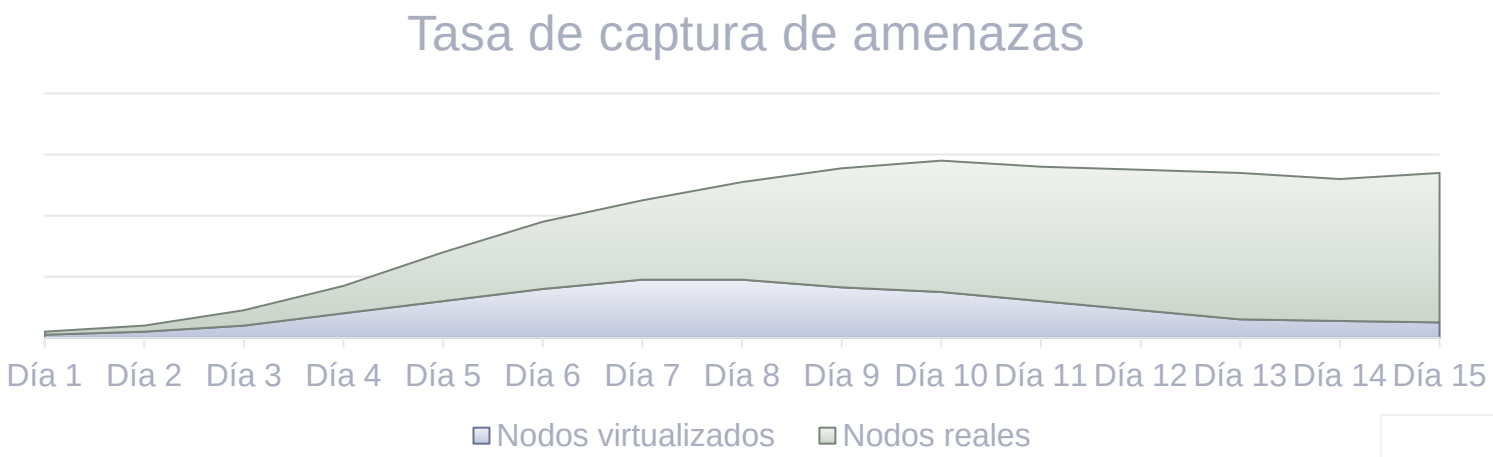


Nodo 2: Planta Industrial de oil & gas, unidad de destilación

Proceso de lazo cerrado implementado con lógica de funcionamiento real.

Más de 16 etapas diferentes para que sea indistinguible de un proceso real. Pérdidas y cargas de agua, extracción de producto, temperaturas graduales…

Entorno operable, con efecto en presiones, flujos, temperaturas…

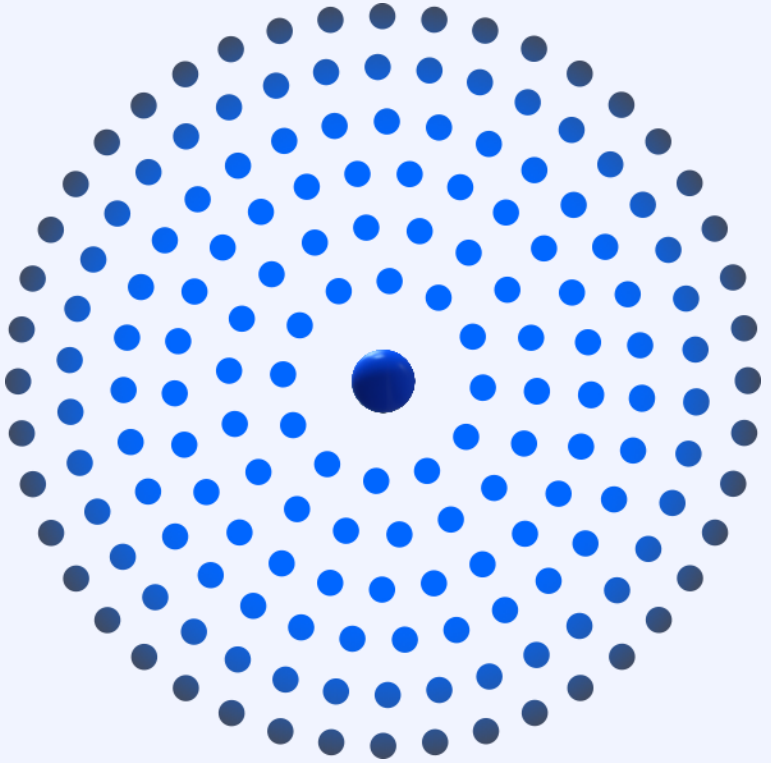


Más de 700 millones de eventos registrados en 2022

Más información:
https://aristeo.elevenlabs.tech/

Outputs de la tecnología

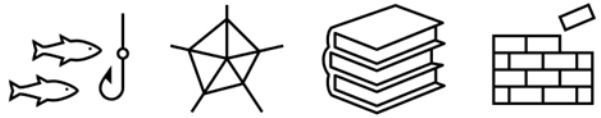
Distintos sabores



Outputs de la tecnología: análisis y observación para la protección

Entornos de Deception OT/ IT&OT

Feed de inteligencia



Análisis Ecosistema actual de amenazas

Entorno de test Red/Blue Team

Amenaza X

Alerta temprana

Outputs de la tecnología: análisis y observación para la protección

Una navaja ~~suiza~~ española

Análisis del ecosistema mundial de amenazas

- Análisis de amenazas detectadas
- Investigaciones sobre amenazas externas a la red
- Análisis predictivo sobre el ecosistema de amenazas

Investigación sobre amenazas

- Análisis de amenazas relevantes
- Alerta temprana
  - Investigación sobre APT
  - Investigación sobre 0-day
  - Detección de campañas

Aristeo Lab

- Entornos para RED/BLUE TEAM
- Pruebas sobre dispositivos nuevos / antiguos

Entornos de deception OT

- Bastionado y despliegue de migas de pan para capturar ataques dirigidos o de nivel avanzado
- Integración con sistemas de Deception IT

Feed de Threat Intelligence

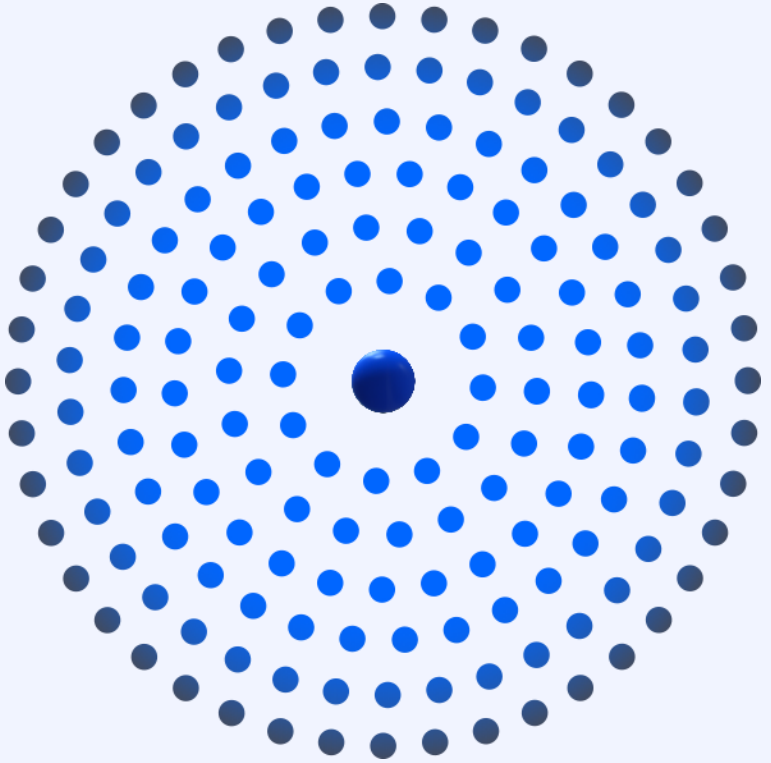
- Integración con la TIP del SOC en TCCT
- Integración con otros sistemas de clientes (SIEM, IDS)

Generador de casos de uso actualizados

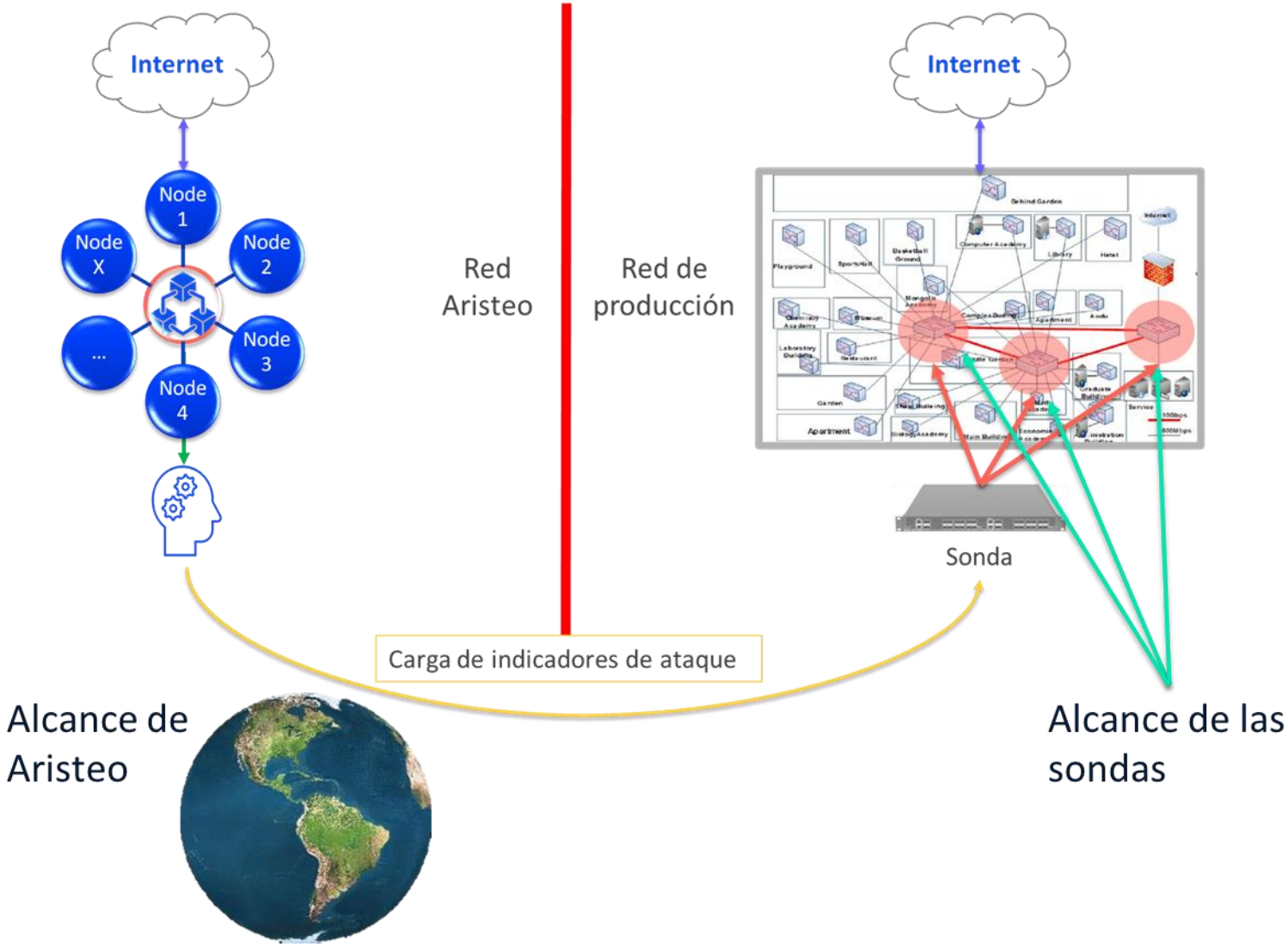
- Casos de uso para amenazas OT detectadas en la red
- El equipo de IR sabe qué hacer frente a amenazas “frescas” cuando se las encuentran en la red del cliente

¿Qué nos diferencia de la competencia?

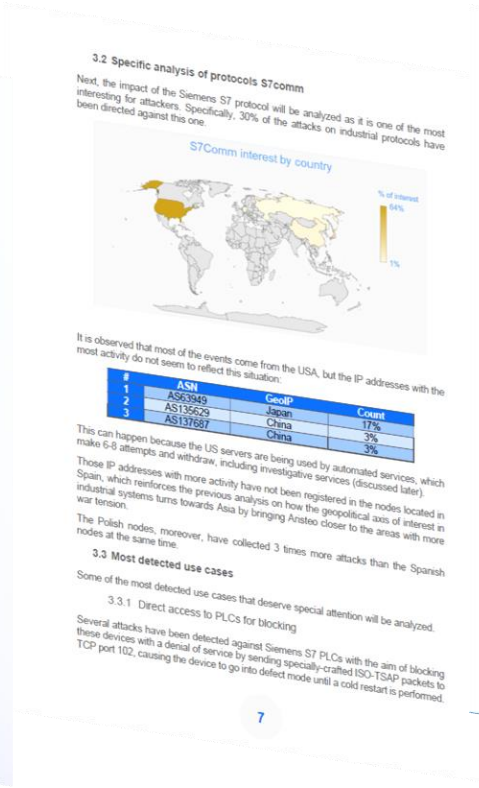
Caso de éxito reciente



¿Qué diferencia Aristeo de la competencia?:
Logra detectar al enemigo antes de que sea demasiado tarde



Caso de éxito: informe inteligencia sobre amenazas OT para cliente infraestructuras críticas de Centro Europa


3.2 Specific analysis of protocols S7comm

Next, the impact of the Siemens S7 protocol will be analyzed as it is one of the most interesting for attackers. Specifically, 30% of the attacks on industrial protocols have been directed against this one.

S7Comm interest by country

It is observed that most of the events come from the USA, but the IP addresses with the most activity do not seem to reflect this situation:

#	ASN	GeoIP	Count
1	AS63949	Japan	17%
2	AS135629	China	3%
3	AS137687	China	3%

This can happen because the US servers are being used by automated services, which make 6-8 attempts and withdraw, including investigative services (discussed later).

Those IP addresses with more activity have not been registered in the nodes located in Spain, which reinforces the previous analysis on how the geopolitical axis of interest in industrial systems turns towards Asia by bringing Aristeo closer to the areas with more war tension.

The Polish nodes, moreover, have collected 3 times more attacks than the Spanish nodes at the same time.

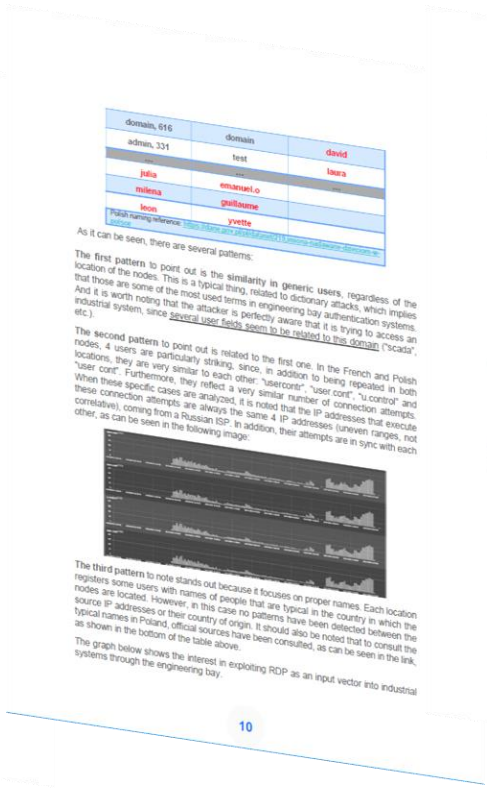
3.3 Most detected use cases

Some of the most detected use cases that deserve special attention will be analyzed.

3.3.1. Direct access to PLCs for blocking

Several attacks have been detected against Siemens S7 PLCs with the aim of blocking these devices with a denial of service by sending specially-crafted ISO-TSAP packets to TCP port 102, causing the device to go into defect mode until a cold restart is performed.

7


domain, 616	domain	david
admin, 331	test	laura
julia	emanuel.o	
milena	guillaume	
leon	yvette	

Polish naming reference:

As it can be seen, there are several patterns:

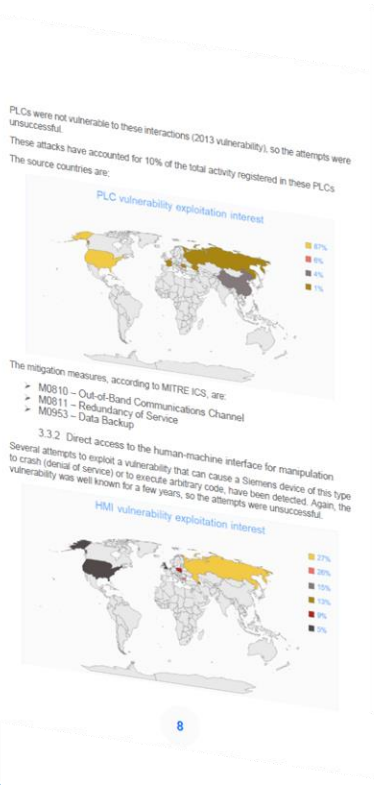
The first pattern to point out is the **similarity in generic users**, regardless of the location of the nodes. This is a typical thing, related to dictionary attacks, which implies that those are some of the most used terms in engineering bay authentication systems. And it is worth noting that the attacker is perfectly aware that it is trying to access an industrial system, since several user fields seem to be related to this domain ("scada", etc.).

The second pattern to point out is related to the first one. In the French and Polish nodes, 4 users are particularly striking, since, in addition to being repeated in both locations, they are very similar to each other: "usercont" - "user.cont", "u.control" and "user cont". Furthermore, they reflect a very similar number of connection attempts. When these specific cases are analyzed, it is noted that the IP addresses that execute these connection attempts are always the same 4 IP addresses (uneven ranges, not correlative), coming from a Russian ISP. In addition, their attempts are in sync with each other, as can be seen in the following image:

The third pattern to note stands out because it focuses on proper names. Each location registers some users with names of people that are typical in the country in which the nodes are located. However, in this case no patterns have been detected between the source IP addresses or their country of origin. It should also be noted that to consult the typical names in Poland, official sources have been consulted, as can be seen in the link, as shown in the bottom of the table above.

The graph below shows the interest in exploiting RDP as an input vector into industrial systems through the engineering bay.

10


PLCs were not vulnerable to these interactions (2013 vulnerability), so the attempts were unsuccessful.

These attacks have accounted for 10% of the total activity registered in these PLCs

The source countries are:

PLC vulnerability exploitation interest

The mitigation measures, according to MITRE ICS, are:

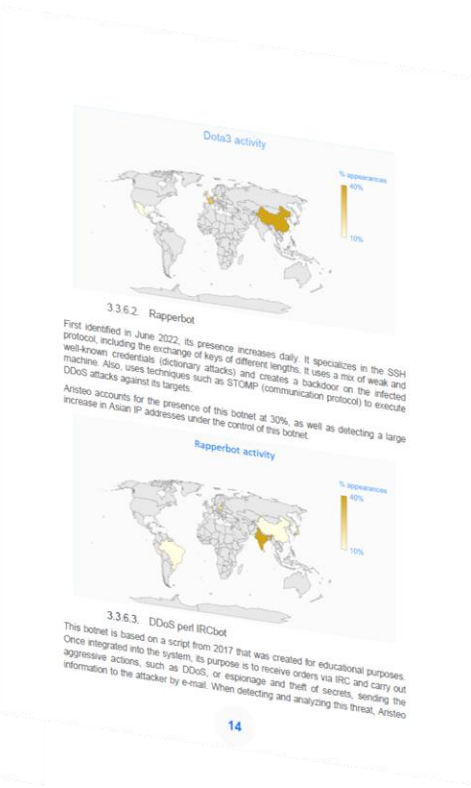
- M0810 – Out-of-Band Communications Channel
- M0811 – Redundancy of Service
- M0953 – Data Backup

3.3.2. Direct access to the human-machine interface for manipulation

Several attempts to exploit a vulnerability that can cause a Siemens device of this type to crash (denial of service) or to execute arbitrary code, have been detected. Again, the vulnerability was well known for a few years, so the attempts were unsuccessful.

HMI vulnerability exploitation interest

8


Dota3 activity

3.3.6.2. Rapperbot

First identified in June 2022, its presence increases daily. It specializes in the SSH protocol, including the exchange of keys of different lengths. It uses a mix of weak and well-known credentials (dictionary attacks) and creates a backdoor on the infected machine. Also, uses techniques such as STOMP (communication protocol) to execute DDoS attacks against its targets.

Aristeo accounts for the presence of this botnet at 30%, as well as detecting a large increase in Asian IP addresses under the control of this botnet.

Rapperbot activity

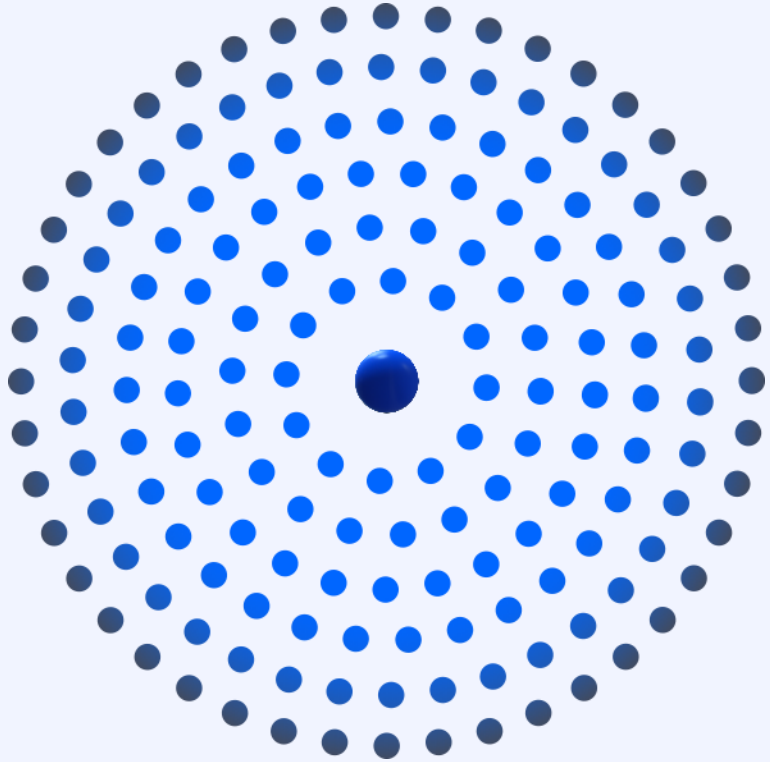
3.3.6.3. DDoS perl IRCbot

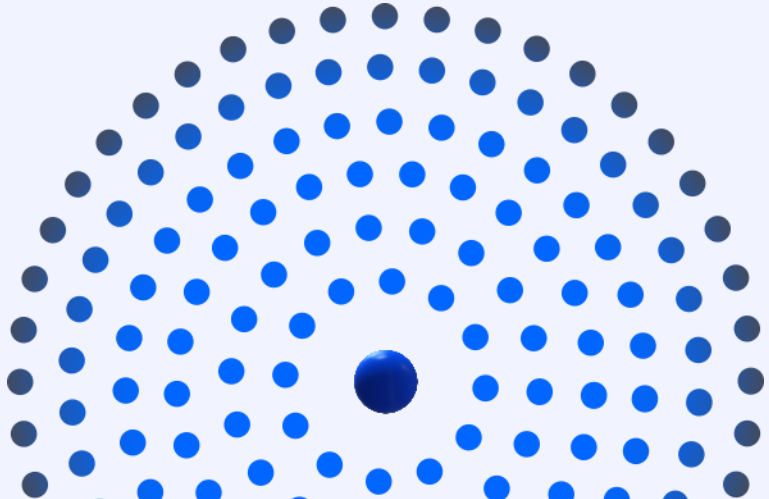
This botnet is based on a script from 2017 that was created for educational purposes. Once integrated into the system, its purpose is to receive orders via IRC and carry out aggressive actions, such as DDoS, or espionage and theft of secrets, sending the information to the attacker by e-mail. When detecting and analyzing this threat, Aristeo

14

MWC 2023

MAKING THINGS HAPPEN





Telefónica Tech

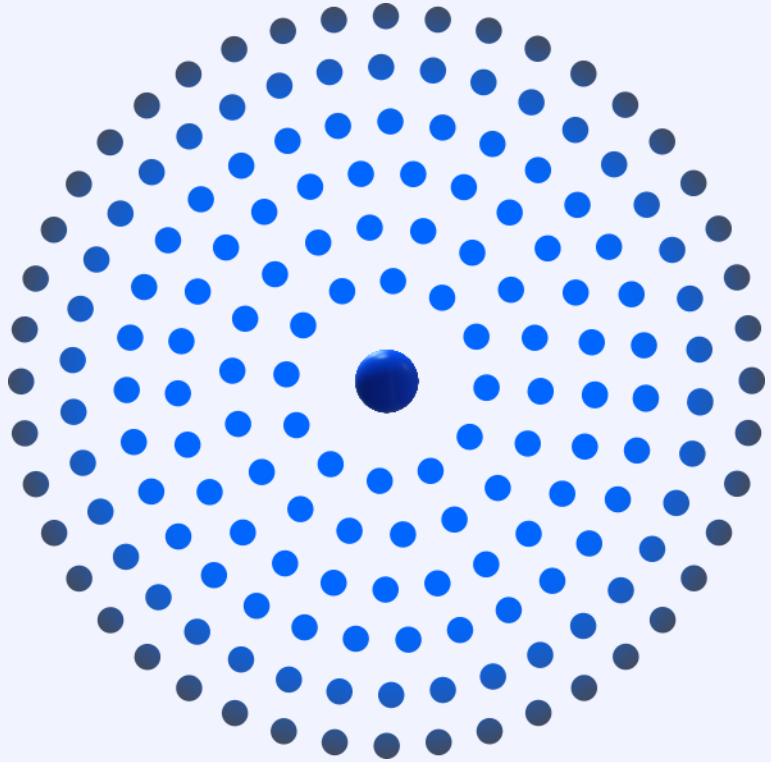
Aristeo

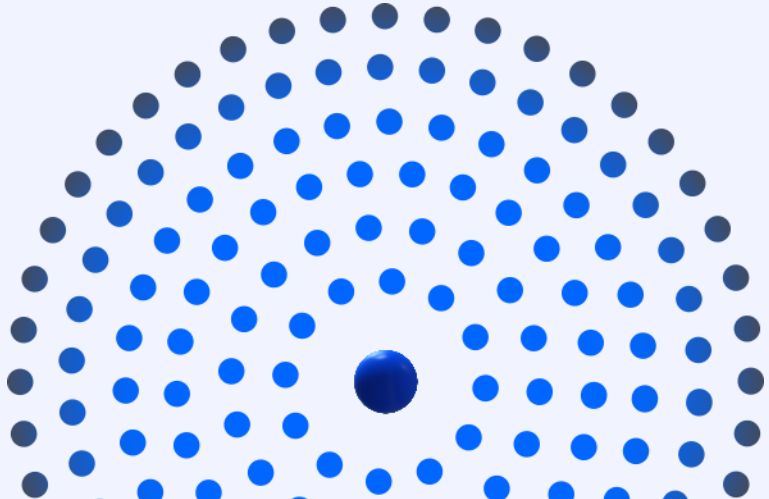
Red OT de captura y análisis predictivo de amenazas

Tecnología 100% desarrollada por Innovación Telefónica TECH Cyber & Cloud desde León, para hacer un mundo más seguro.

GRACIAS!!!

joseantonio.cascallanaarroyo@telefonica.com
https://www.linkedin.com/in/josecascallana/
https://aristeo.elevenlabs.tech/
https://telefonicatech.com/





Telefónica Tech