IoT: pwning the things

ethergroup

Disclaimer:

El contenido de esta charla tiene como propósito compartir información con fines educativos. Los nombres y marcas pertenecen a sus respectivos dueños.

Ni Ethergroup en su calidad de empresa (Cyber Security E-group S de R.L. de C.V.) ni sus colaboradores, se hacen Responsables de cualquier acto ilícito realizado con la información siguiente.

El conocimiento es libre.

ethergroup

IOT: Internet of Things

¿Qué es IoT?

Es el concepto de la interconexión de objetos cotidianos a internet.

El término fue propuesto por Kevin Ashton en el Auto-ID Center del MIT (Massachusetts Institute of Technology), lugar donde se realizaban investigaciones sobre la identificación por medio de RFID.

¿QUÉ HAY CONECTADO AL INTENET DE LAS COSAS?

ethergroup

Algo de historia

Hackable Cardiac Devices St. Jude

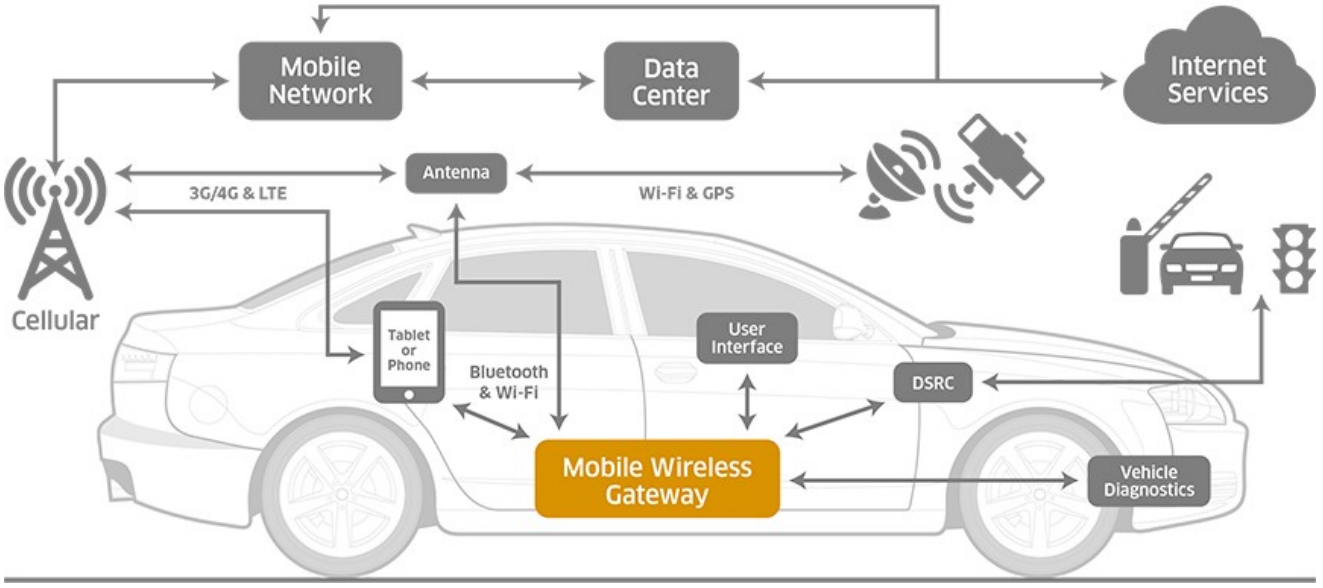
St. Jude Medical

A inicios del año 2017 se detectaron vulnerabilidades en marcapasos implantables. Dichas vulnerabilidades permitían que un atacante accediera a los mismos y pudiese provocar descargas eléctricas en los pacientes o drenar las baterías de los dispositivos

The jeep Hack

The Jeep Hack

La IBM Security Intelligence detectó que realizando un secuestro y modificación del firmware de los vehículos, estos podrían ser controlados. Era posible acelerar, frenar o hasta girar el volante a voluntad.



"Era uno, pero con eso basta"
- IBM Security Intelligence

https://securityintelligence.com/

Ot ≡ toda la industria
y la estadística

ethergroup

OT = TODA LA INDUSTRIA Y LA ESTADÍSTICA

OT: Operational Technology

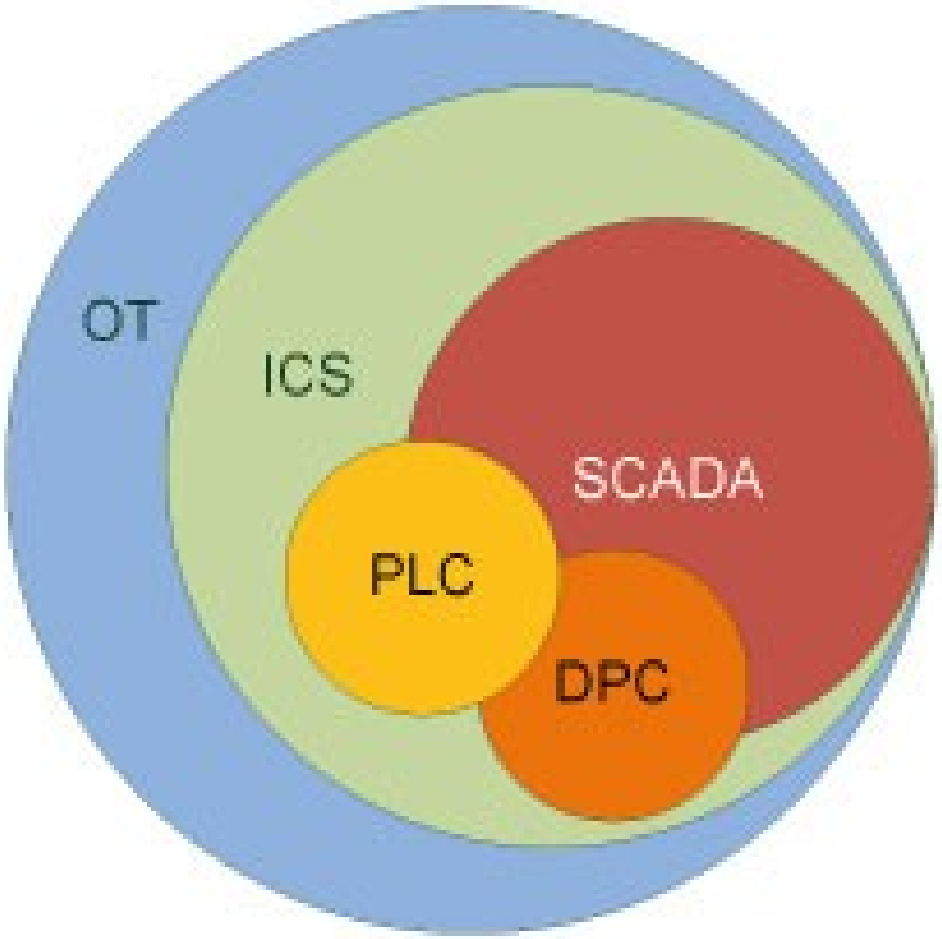
SCADA: Supervisory Control and Data Acquisition

PLC: Programmable Logic Controller

DPC: Discrete Process Control System

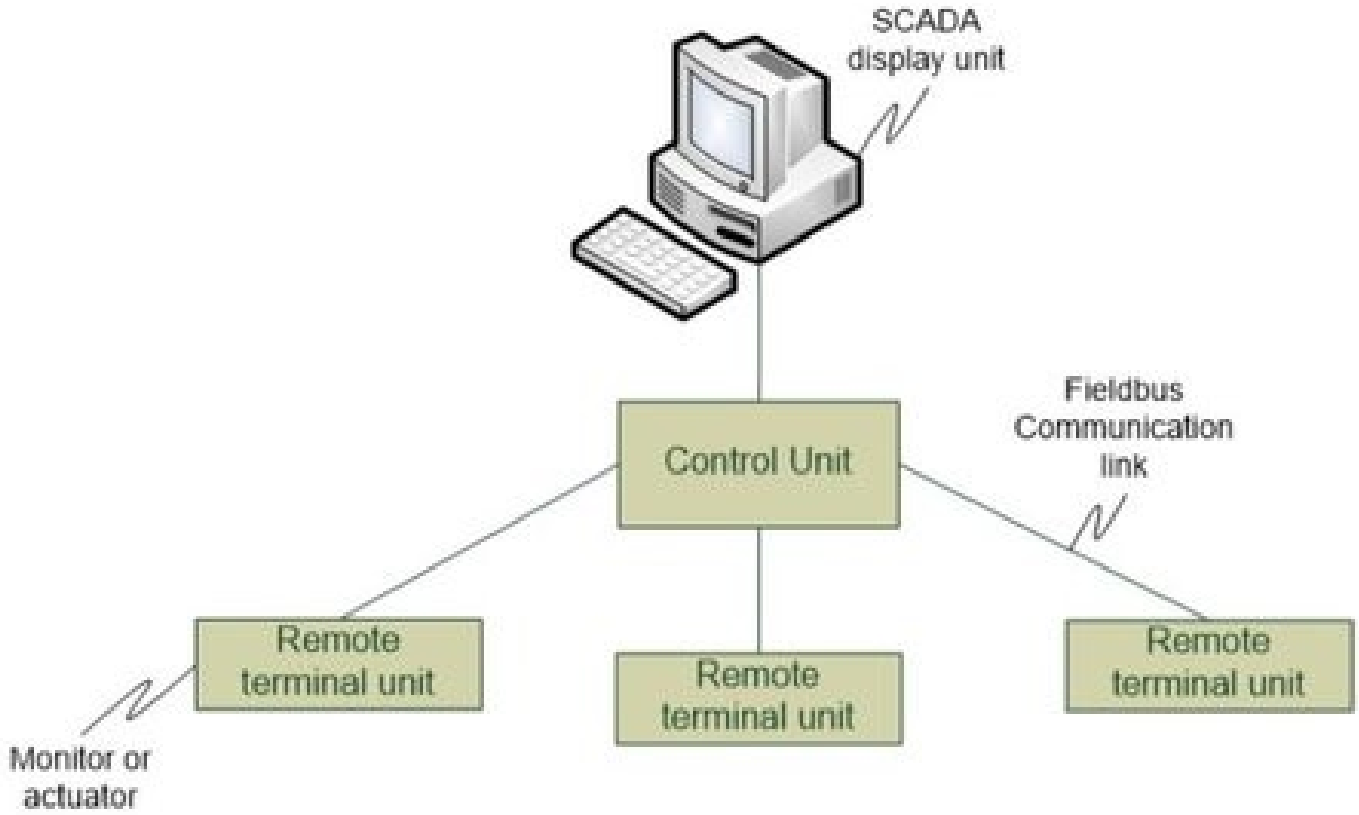
ICS: Industrial Control system

RTU: Remote Terminal Units



https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

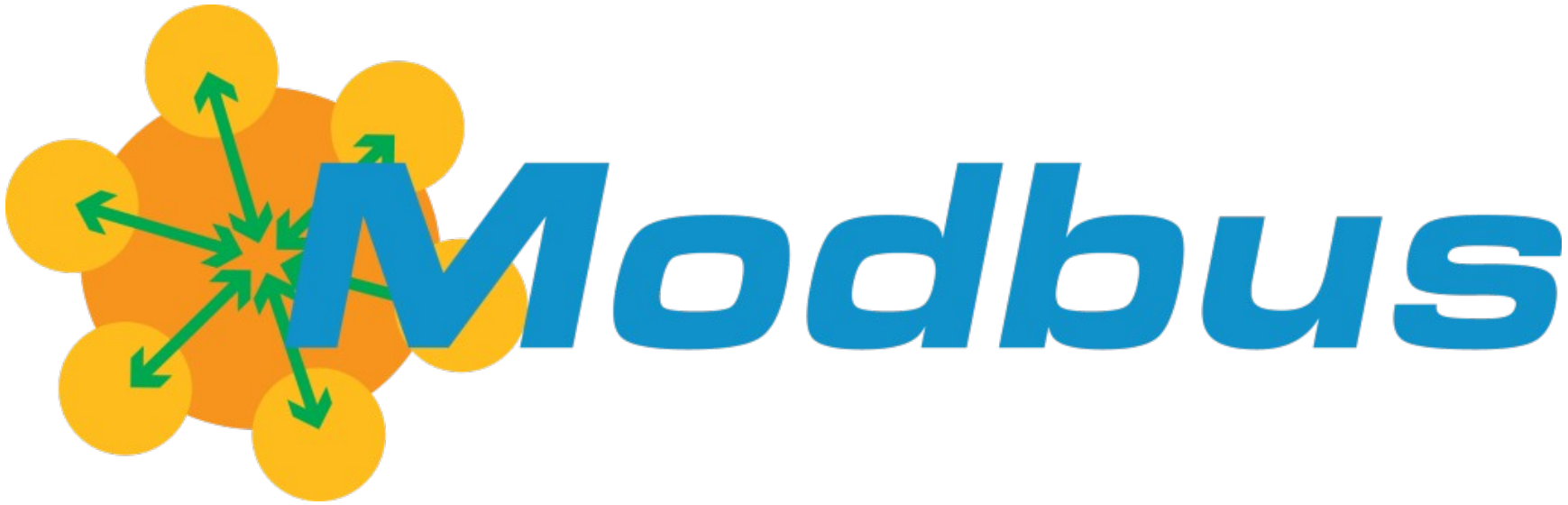
Configuración básica



https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

Protocolo estrella...

ethergroup



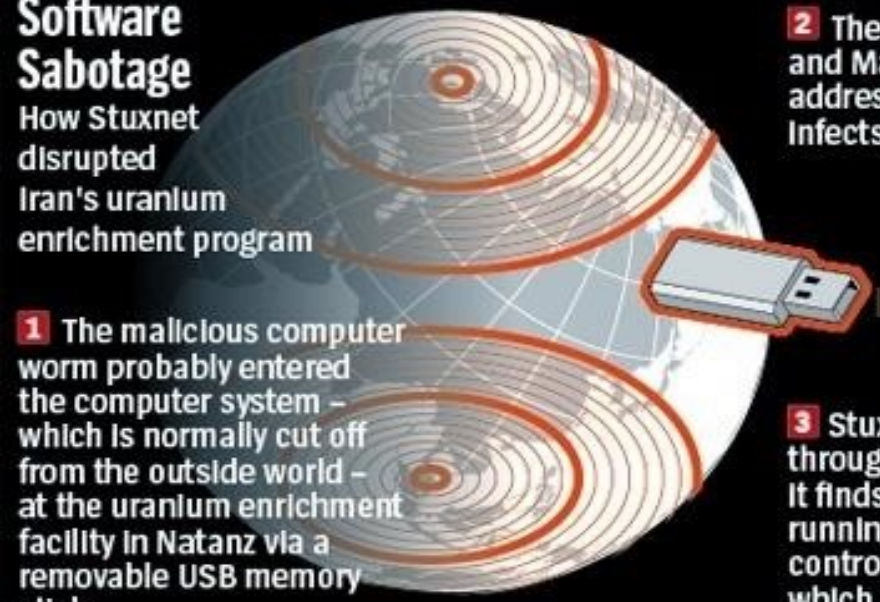
Stuxnet: pwning Nuclear systems

Stuxnet

ethergroup

Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

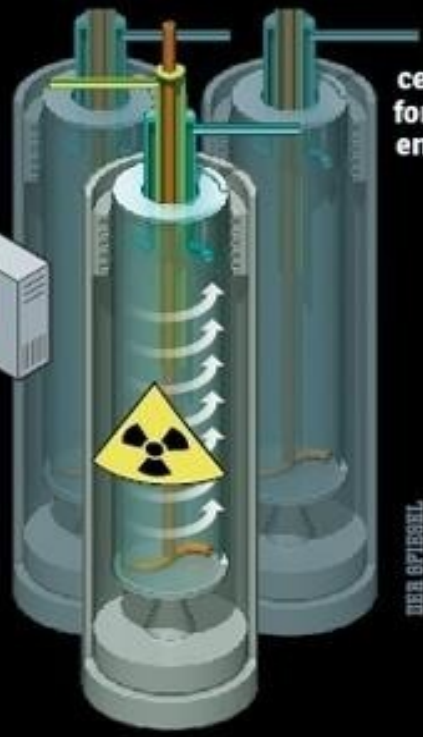


1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

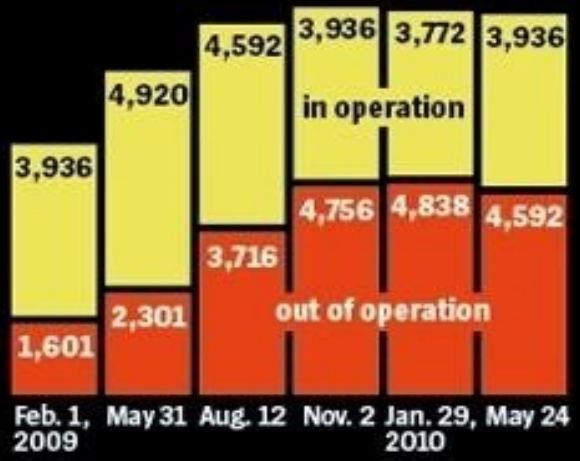
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.



Iranian centrifuges for uranium enrichment

DER SPIEGEL

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.



Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

BOTNET INTERNALS

¿Anna-senpai?

ethergroup

hackforums.net (30/09/2016)

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by **Anna-senpai**.)

Anna-senpai
L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

The Mirai Bontnet (Aka Dyn Attack)

Dyn Attack

Fue un ataque realizado con una Botnet Llamada Mirai (+ 600,000 dispositivos infectados). Esto produjo que existiera un ataque a sitios de mucho renombre como lo son Spotify, Twitter y Github.

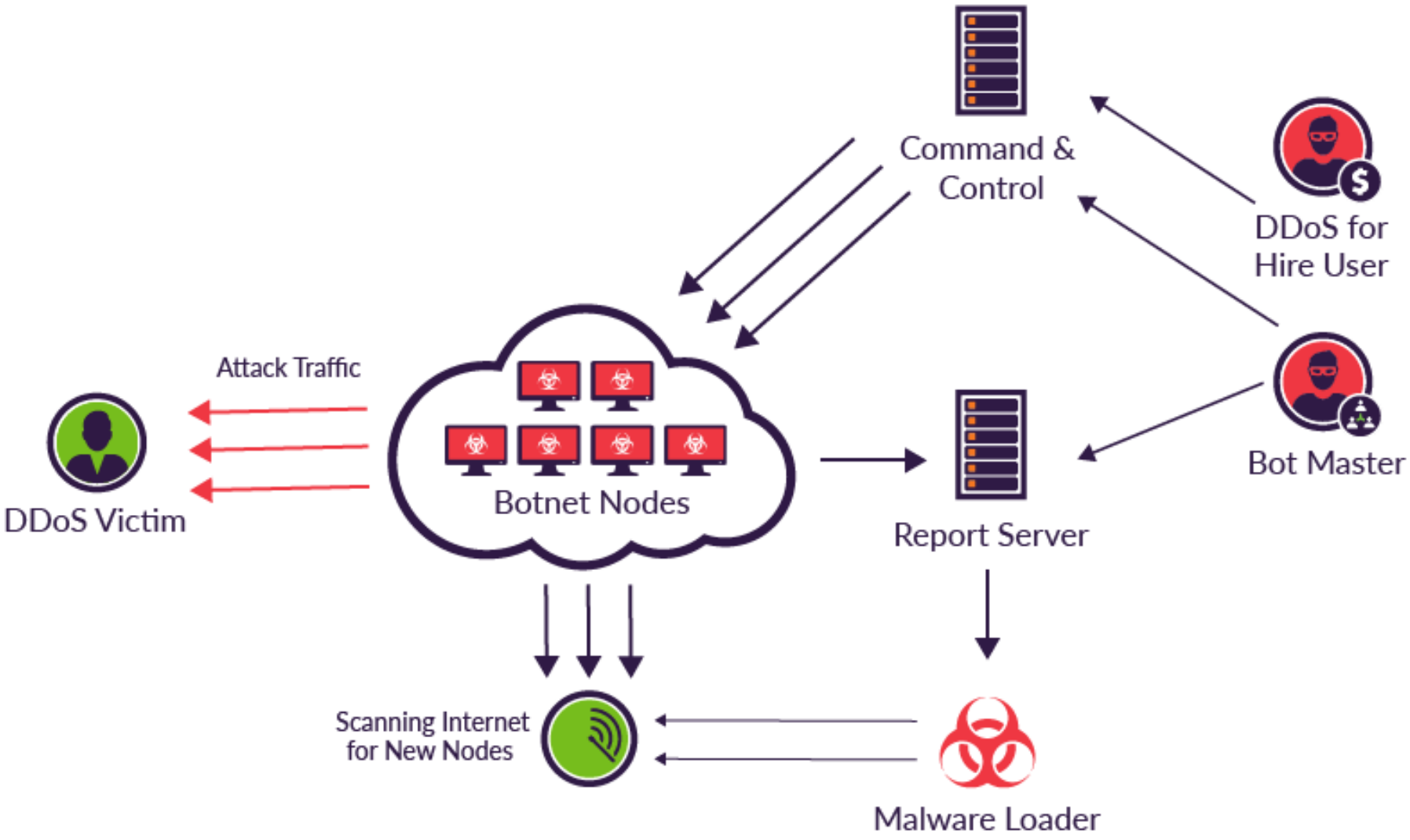
Los dispositivos infectados son en su mayoría sistemas embebidos. El ataque fue producido en un inicio con 600 Gps de transferencia. En el pico más alto llegaron hasta 1 Tbps.

https://kumarde.com/papers/understanding_mirai.pdf

Dyn Attack

ethergroup

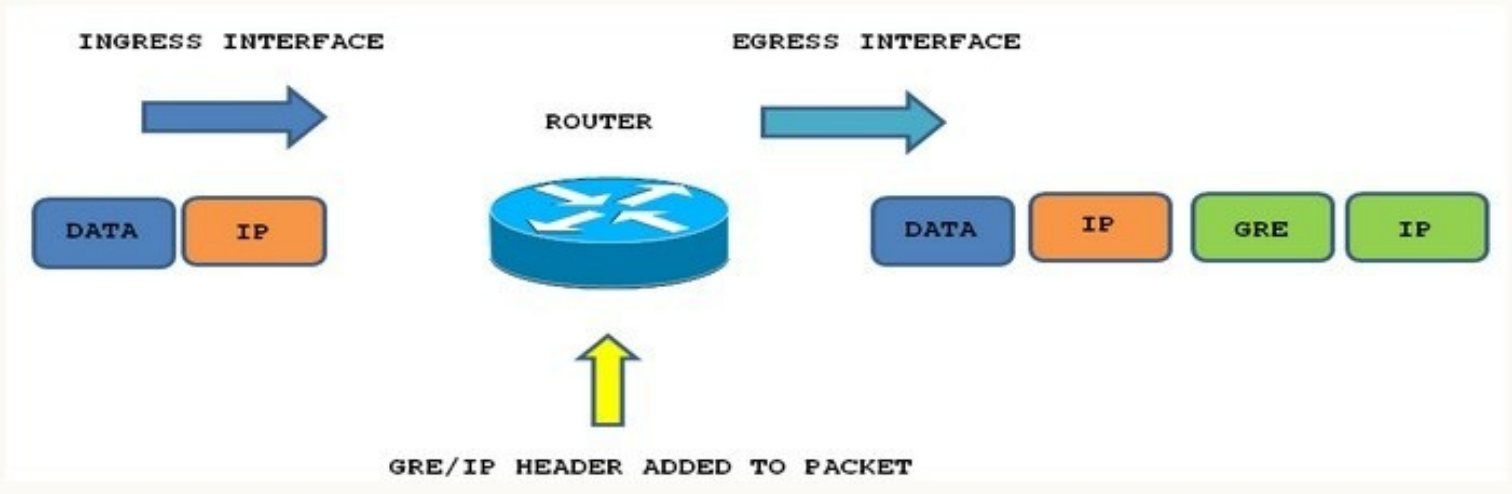
Mirai at a Glance



Dyn Attack

El código fuente (thanks Anna-Senpai) del funcionamiento de la BotNet fue liberado en el sitio hackforums.net

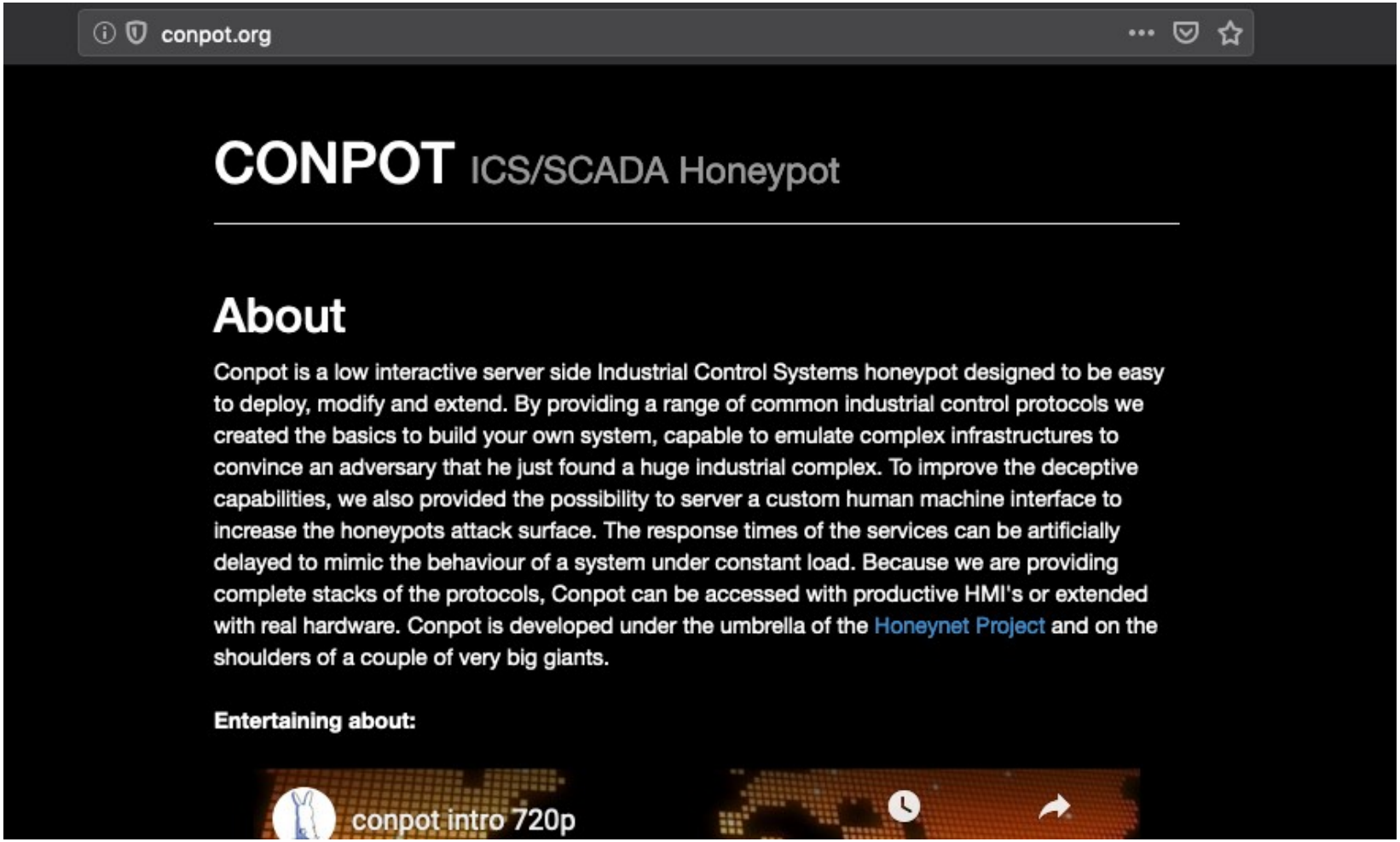
Dicha acción provocó que fueran prolíferas las variantes de esta botnet.
La forma en que funciona Mirai era utilizando tráfico con túneles GRE (Había una parte dedicada a ello)



https://github.com/krh3rtz/Mirai-Source-Code-imported

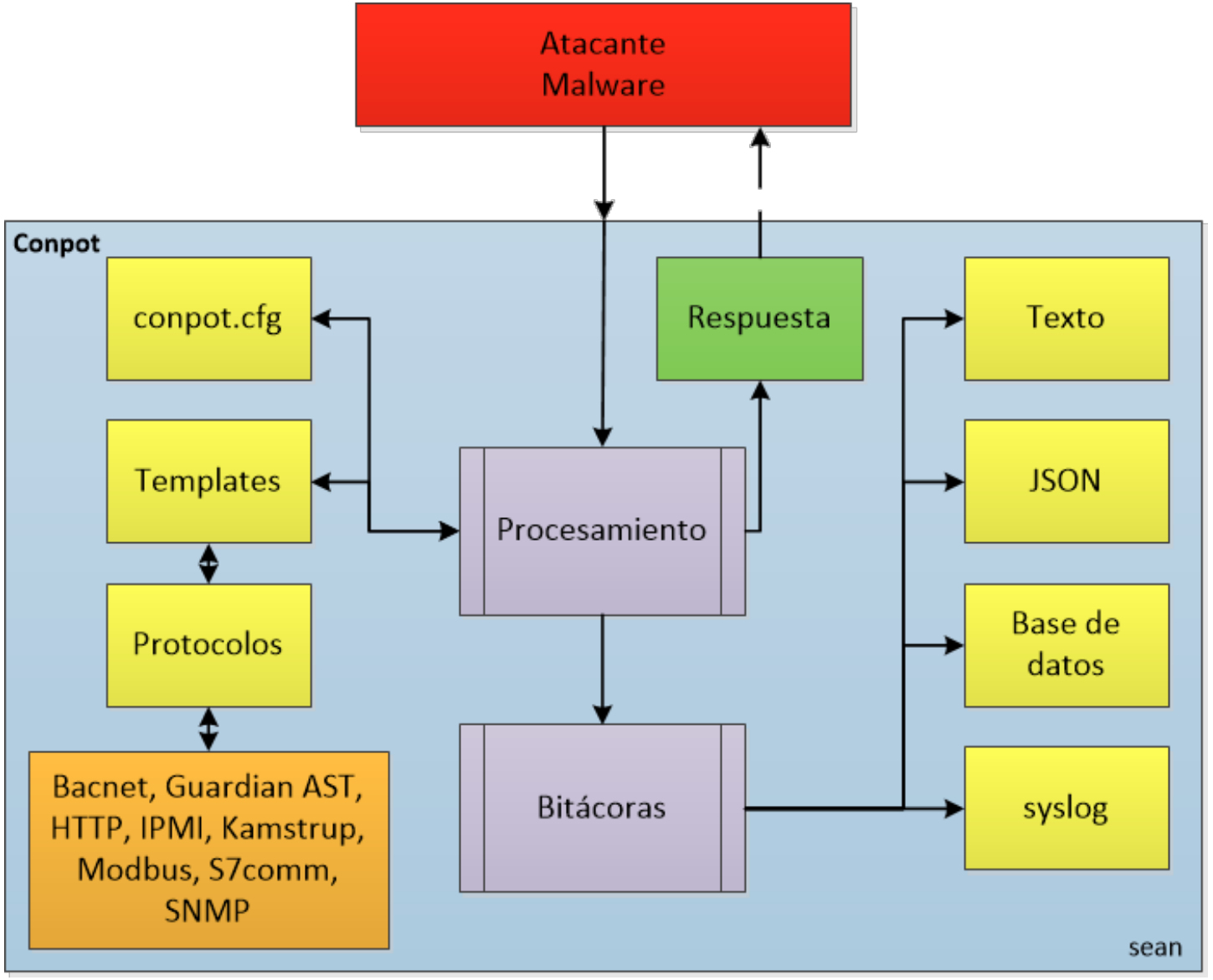
POC (Proof Of Concept): CONPOT

Conpot



https://github.com/mushorg/conpot
https://conpot.readthedocs.io/en/latest/installation/install.html

ICS/SCADA NET



algunos tarros de miel para Practicar:

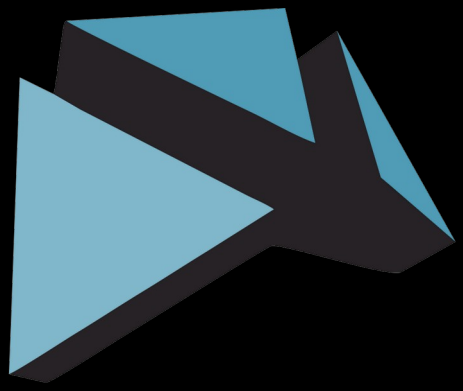
Honeyd

Gaspot

Gridpot

https://github.com/krhertz/
http://krh3rtz.blogspot.com
https://www.youtube.com/user/Cardician526

Imir Torres – CEO @ Ethergroup
Email: imir.torres@ethergroup.mx
Cyber Security E-group S de R.L. de C.V.



ethergroup

HAPPY HACKING