

IoT: PWINING THE THINGS



DISCLAIMER:

EL CONTENIDO DE ESTA CHARLA TIENE COMO PROPÓSITO COMPARTIR INFORMACIÓN CON FINES EDUCATIVOS. LOS NOMBRES Y MARCAS PERTENECEN A SUS RESPECTIVOS DUEÑOS.

NI ETHER GROUP EN SU CALIDAD DE EMPRESA NI SUS TRABAJADORES, SE HACEN RESPONSABLES DE CUALQUIER ACTO ILÍCITO REALIZADO CON LA INFORMACIÓN SIGUIENTE.

EL CONOCIMIENTO ES LIBRE.

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 INTERNET DE LAS COSAS?



ALGO DE HISTORIA

HACKABLE CARDIAC DEVICES ST. JUDE

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

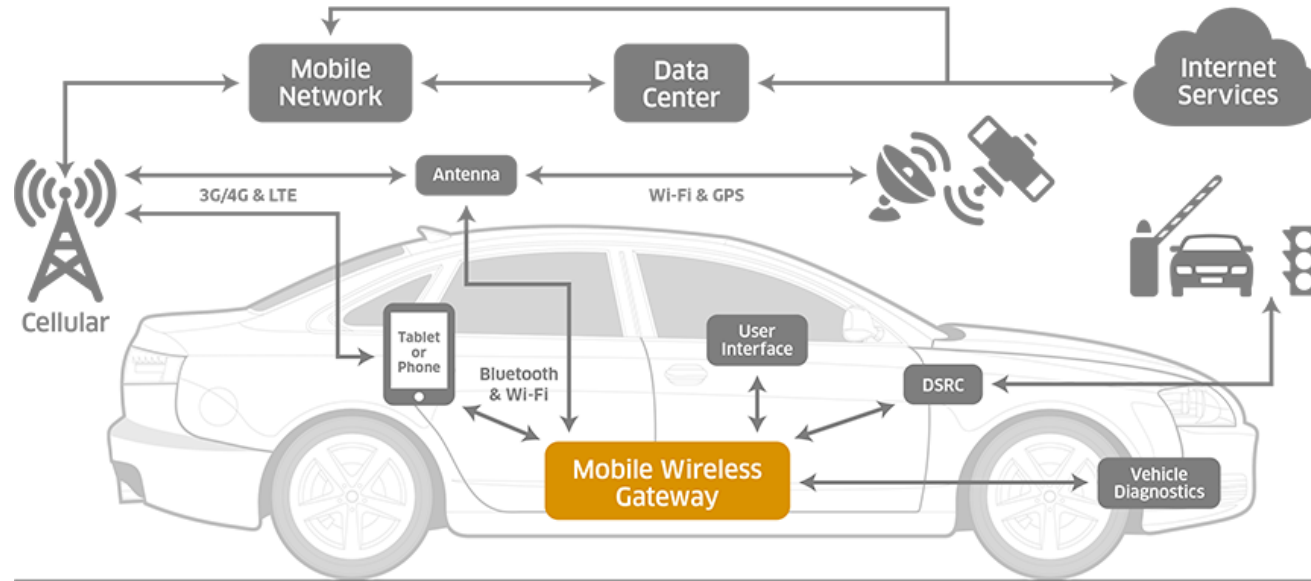


THE JEEP HACK

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***

STUXNET: PWINING NUCLEAR SYSTEMS

STUXNET

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.



BOTNET INTERNALS

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.

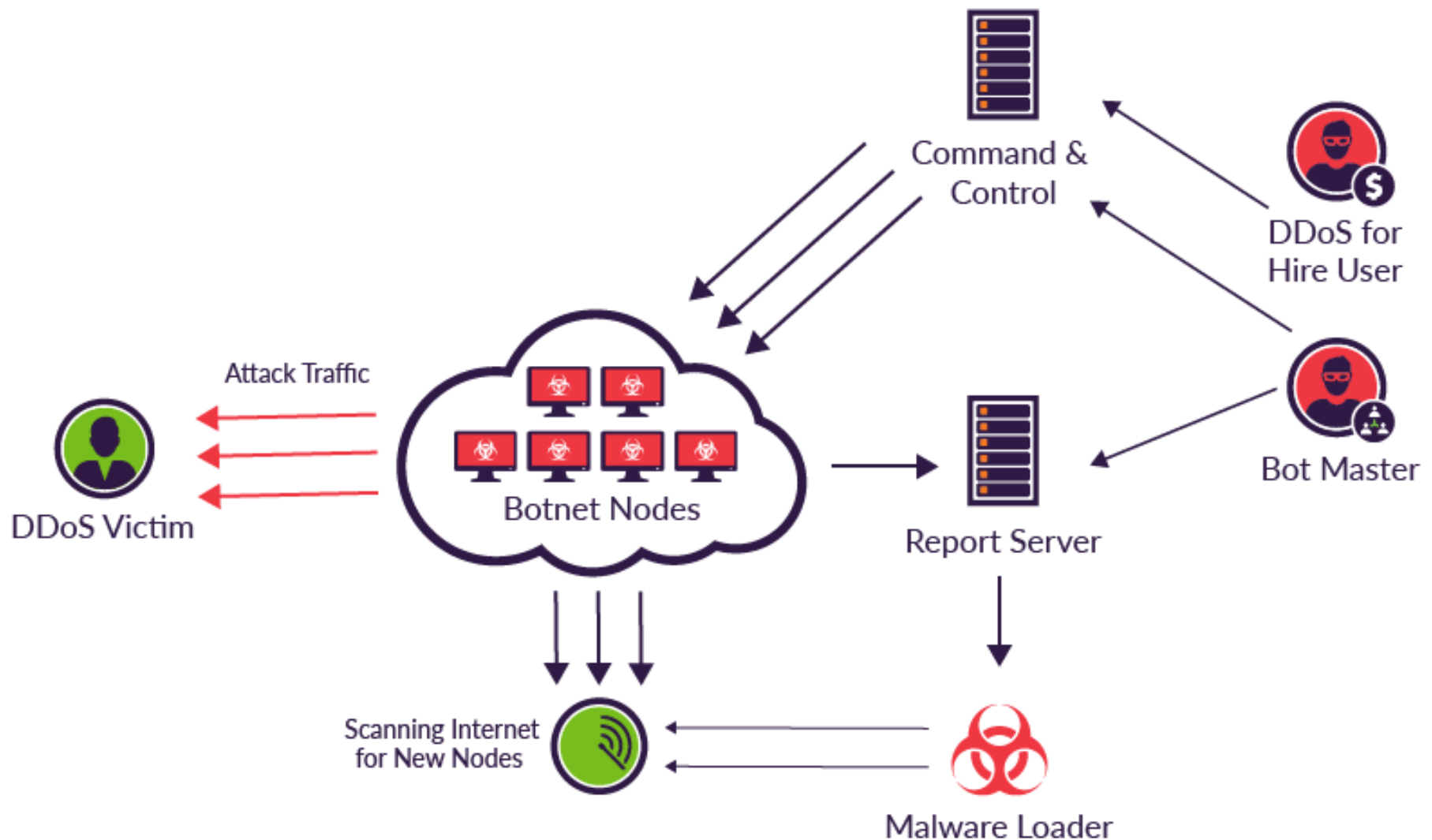
Los dispositivos infectados son en su mayoría sistemas embebidos. El ataque fue producido en un inicio con 600 Gps de transferencia. En el pico más alto llegaron hasta 1 Tbps.



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

DYN ATTACK

Mirai at a Glance

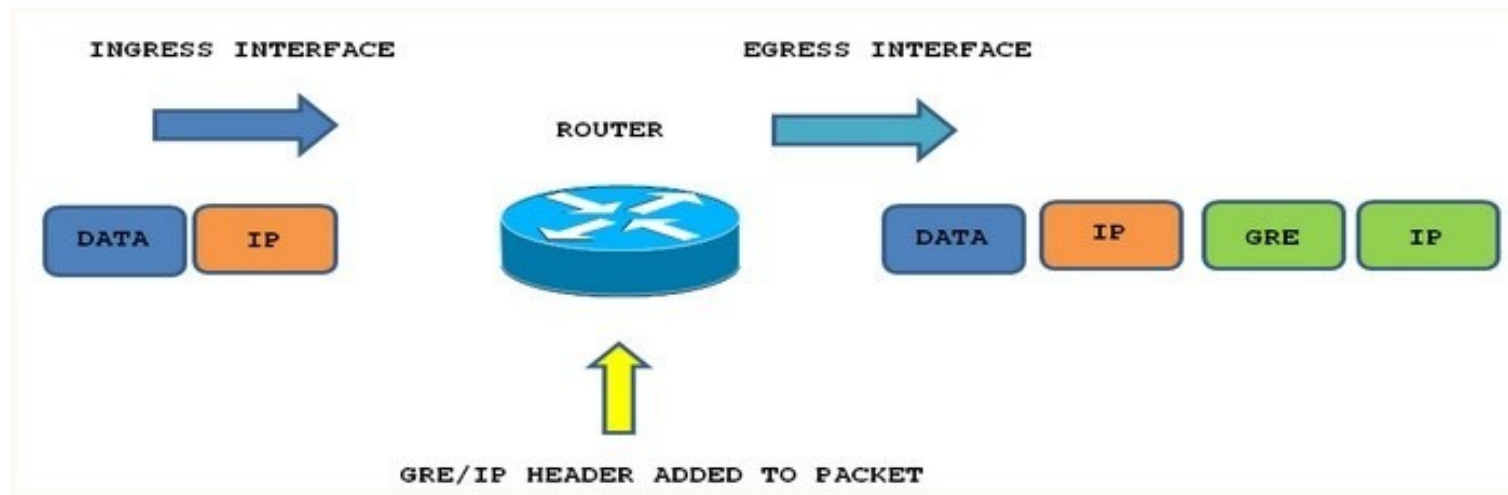


DYN ATTACK



El código fuente 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/jgamblin/Mirai-Source-Code>

POC (PROOF OF CONCEPT)



- * SSH-BOT
- * GLOCAL
- * ZMAP
- * SHODAN, CENSYS

GRACIAS A...



Centro de Innovación Acelerada AC



GULAG

LAGUNA 4.0

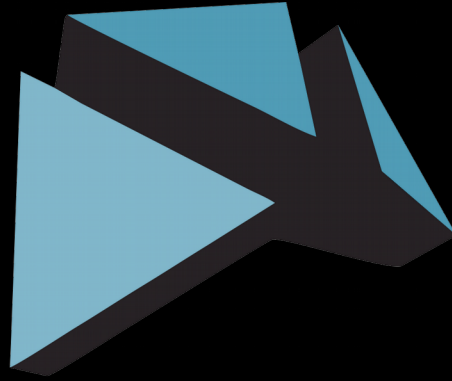


ALGO ESTÁ POR LLEGAR...



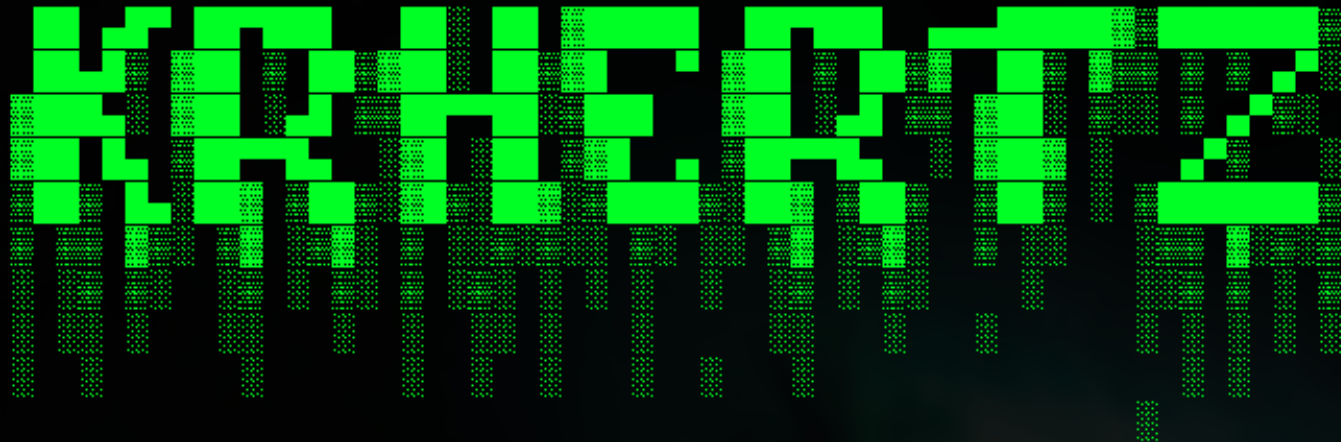
HACKOLYMPICS





ethergroup

HAPPY HACKING



<https://github.com/krhertz/>

<http://krh3rtz.blogspot.com.mx>

<https://www.youtube.com/user/Cardician526>

Imir Torres – CSO (Chief Security Officer) Ether Group

Email: ing.imir.torres@gmail.com