Smart Botnets

Juan Garrido

MVP Enterprise Security

Juan.garrido@nccgroup.trust

Senior Security Consultant

MVP Enterprise Security

https://www.nccgroup.trust

Twitter: @tr1ana

MVP Microsoft® Most Valuable Professional

Hola! Estoy usando {Ponga aquí dispositivo}

La información es poder

- **Durante años hemos convivido con objetos que nos han proporcionado información de valor**
- **En un intento de controlar esa información, nace lo que hoy día llamamos:**
  - Smart City
  - Internet Of Things
  - Connected Cars
  - Etc..

Nuevo modelo para las empresas

Durante años operadores y empresas

- **Han logrado comunicar a personas con personas mediante un sinfín de tecnologías:**
  - Telefonía
  - **S**hort **M**essage **S**ervice
  - Datos
- **Gracias a Internet, lo que antes costaba mucho dinero se volvió barato:**
  - Messenger
  - Skype
  - Whatsapp
  - Telegram
  - Etc..

CCN-CERT
centro criptológico nacional

XI JORNADAS STIC CCN-CERT

Machine to Machine

M2M

- Tecnologías que permiten la comunicación MachineToMachine
- Ésta comunicación puede venir desde redes privadas, redes públicas, o comunicación directa

Dispositivo Embebido

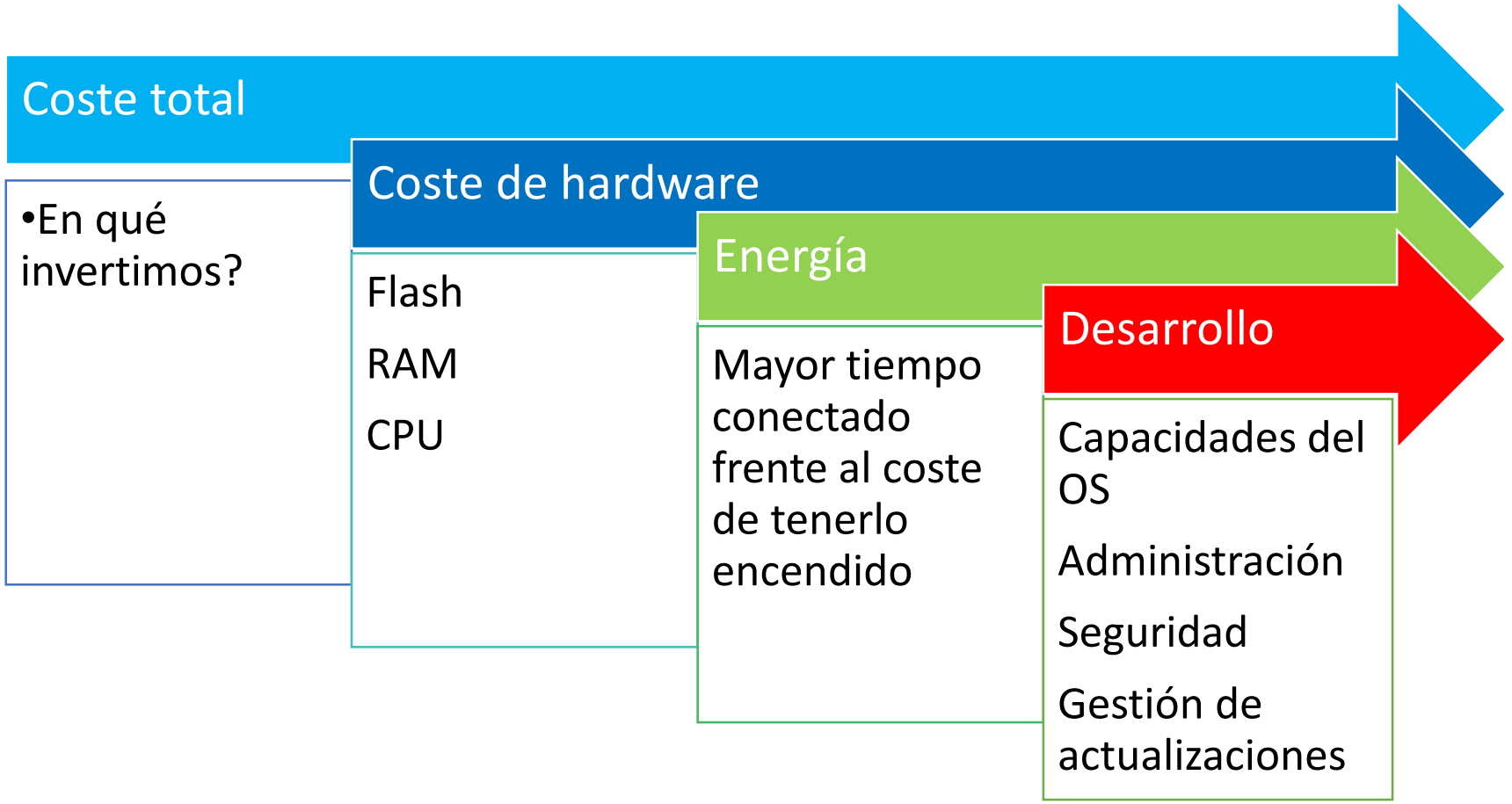
- Combinación de Hardware y Software
- Un porcentaje alto utiliza OS con poca versatilidad
- Utilizan utilidades para enriquecer las opciones del OS (e.g. BusyBox)

Principio de limitación

Diseño acorde con esta clase de dispositivos

- **Dispositivo**
  - Mínima complejidad en Hardware
  - Limitado en memoria/disco
  - Limitado en características del OS
- **Red**
  - Transmisión de datos en paquetes pequeños
  - Disponibilidad. Un dispositivo puede “morirse” en algún punto en un momento determinado y dejar de transmitir para volver a transmitir pasado un tiempo

Coste de distribución



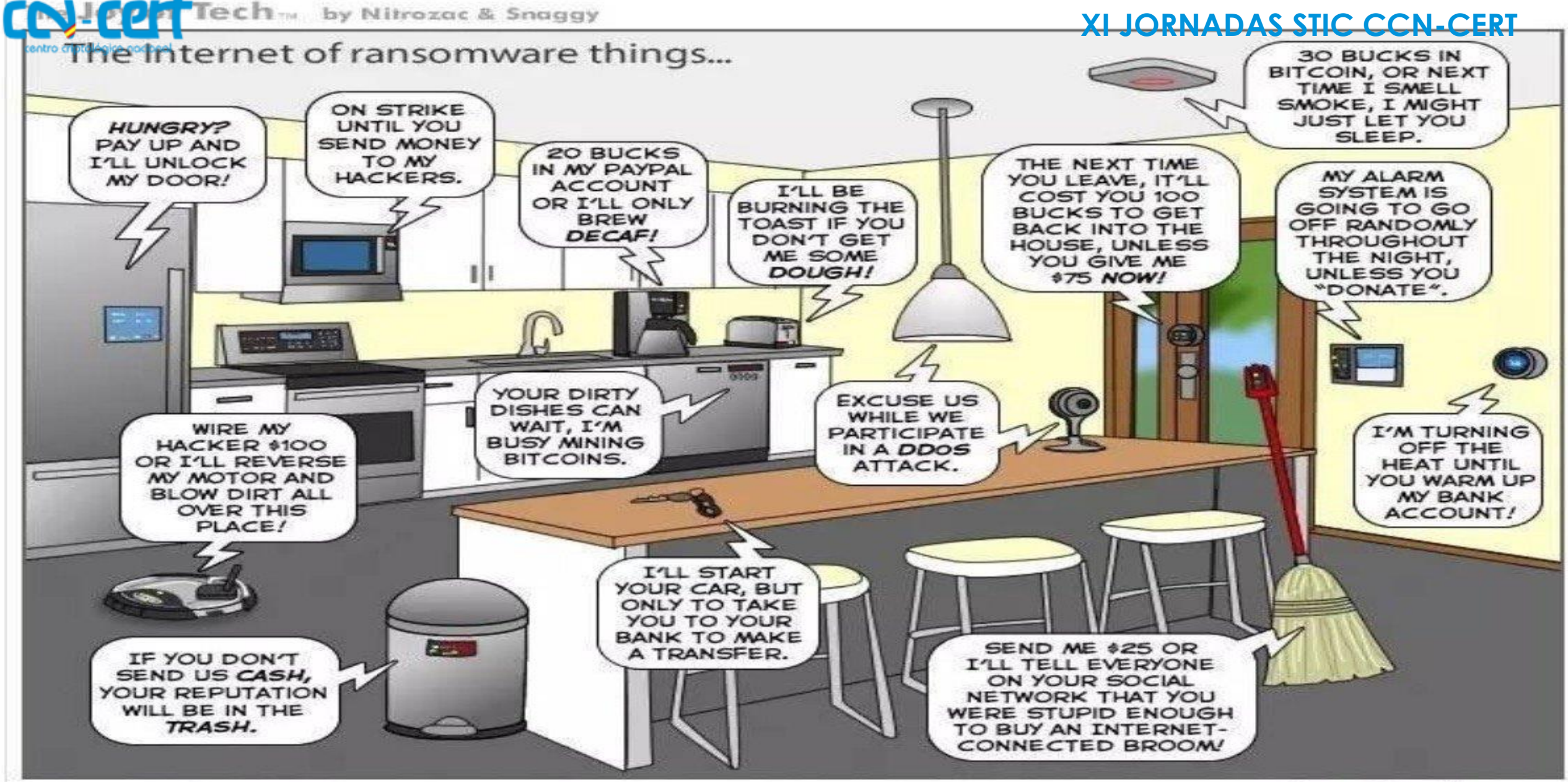
Retos


XML, JSON
Aplicación
Software de calidad
Gestión de parches
HTTP, SIP, XMPP
Sesión
Capa de abstracción
Gestión de eventos
Firewall
UDP
TCP
SCTP
Transporte
Seguro
IPv4,
IPv6
Red
IPv6?
Seguro
Control de errores/congestión
802.15.4
802.11
GSM
LTE
Física
E.164 (Código de país)
Autenticación

Carencias actuales

- **El ecosistema IoT carece de mucho de lo que carecía internet hace 25 años**
  - No existe legislación aparente (Cualquiera puede fabricar lo que sea)
  - Federal Trade Comission (https://www.ftc.gov/)
  - Facua (https://www.facua.org)
- **S-SDLC**
  - Mucho camino por recorrer
  - Gestión de parches? Monitorización? Escalado? Desarrollo seguro?
- **Estándares**
  - Existen muchos. Deberían reutilizarse los existentes o adaptarlos al ecosistema IoT?


Matt Weinberger


Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech
joyoftech.com

Botnets de dispositivos IoT

- Principales dispositivos infectados
  - Cámaras DVR, CCTV
  - Dispositivos de tipo NAS/Printers
  - Routers domésticos
- Propagación
  - Vía Telnet/SSH
- Explotación
  - Vulnerabilidades en código fuente
  - Uso de contraseñas débiles
  - Contraseñas por defecto
- Arquitectura
  - ARM
  - MIPS
  - PowerPC

Mirai Botnet

- Datos generales
  - Malware utilizado para realizar campañas de DDoS
  - Desarrollada en Go y C
- Propósito
  - Localizar y comprometer dispositivos IoT
  - Realizar ataques de DDoS
- Explotación
  - Escaneo masivo a internet en busca de dispositivos
  - Técnicas de fuerza bruta basada en una lista interna de usuario:password

```
uint8_t methods_len = 0;
struct attack_method **methods = NULL;
int attack_ongoing[ATTACK_CONCURRENT_MAX] = {0};

BOOL attack_init(void)
{
    int i;

    add_attack(ATK_VEC_UDP, (ATTACK_FUNC)attack_udp_generic);
    add_attack(ATK_VEC_VSE, (ATTACK_FUNC)attack_udp_vse);
    add_attack(ATK_VEC_DNS, (ATTACK_FUNC)attack_udp_dns);
        add_attack(ATK_VEC_UDP_PLAIN, (ATTACK_FUNC)attack_udp_plain);

    add_attack(ATK_VEC_SYN, (ATTACK_FUNC)attack_tcp_syn);
    add_attack(ATK_VEC_ACK, (ATTACK_FUNC)attack_tcp_ack);
    add_attack(ATK_VEC_STOMP, (ATTACK_FUNC)attack_tcp_stomp);

    add_attack(ATK_VEC_GREIP, (ATTACK_FUNC)attack_gre_ip);
    add_attack(ATK_VEC_GREETH, (ATTACK_FUNC)attack_gre_eth);

    //add_attack(ATK_VEC_PROXY, (ATTACK_FUNC)attack_app_proxy);
    add_attack(ATK_VEC_HTTP, (ATTACK_FUNC)attack_app_http);

    return TRUE;
}
```

Seguridad en IoT

- Estado general de S-SDLC en IOT
  - No está diseñado para ser seguro
  - No está testeado por consultores/hackers
  - La gran mayoría no recibe parches
  - Barato
  - Diseñado para reventar el mercado
- En los próximos años veremos
  - dispositivos IoT van a tener grandes agujeros de seguridad
  - No recibirán ningún tipo de parche

IoT: El despertar de una nueva era

- Experimento
  - Dar nuevos usos a una botnet IoT
  - Concienciar al ciudadano de a pie – sí, ese, tú! - sobre los peligros del IoT
  - ¿Cómo?
    - Tomando como base dispositivos de la botnet Mirai
    - Escaneo masivo a la red mundial
  - Familia elegida
    - Sierra Wireless
    - Análisis de Firmware
  - Uso del dispositivo
    - Coches de policía/Ambulancias
    - Luces de carretera/Tráfico
    - Gasolineras

Recommended Actions

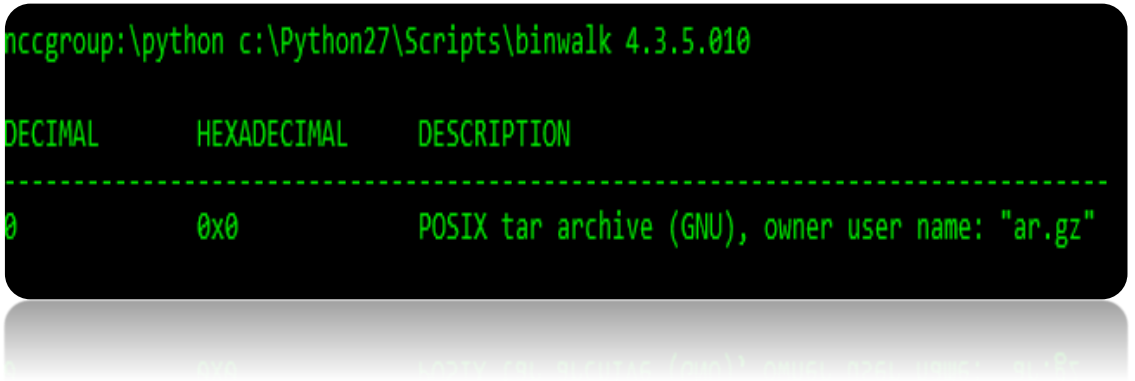
Protecting the gateway

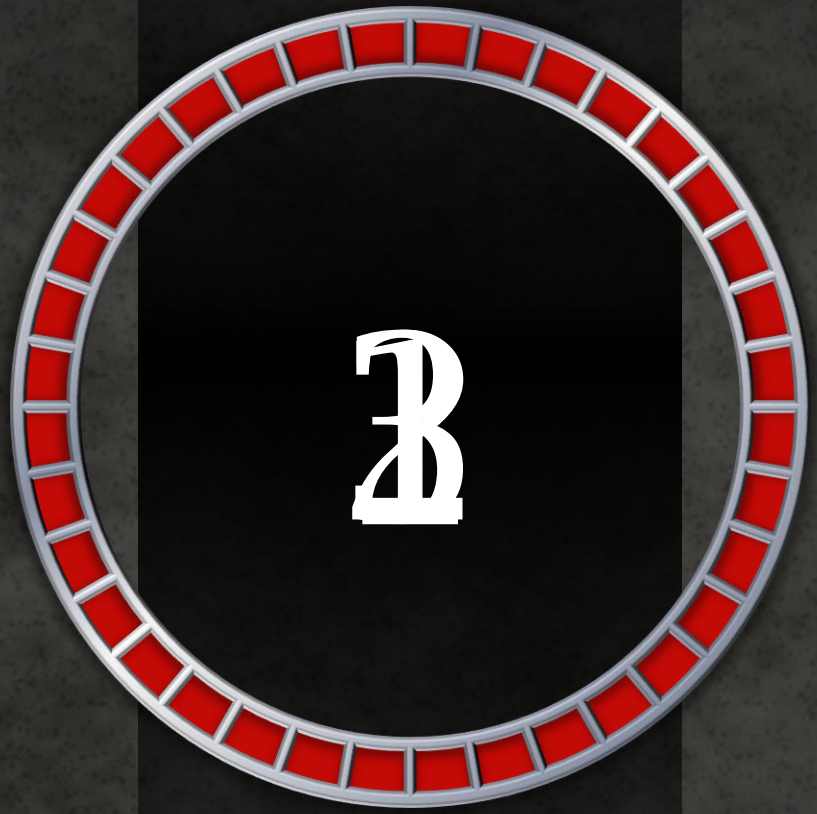
Sierra Wireless strongly recommends that customers with the identified products perform the following steps on each gateway:

1. Reboot the gateway to eliminate any existing Mirai malware; and
2. Immediately change the ACEmanager password to a secure, unique value. The password can be changed by either:
    a. Logging into ACEmanager and navigating to **Admin** > **Change Password**; or
    b. Remotely changing the password using the AirLink Managerment Service (ALMS). Instructions can be found at: https://doc.airvantage.net/alms/reference/monitor/howtos/remotelyChangeACEManagerPassword/

Análisis básico y herramientas

- Herramientas utilizadas
  - Python
  - BinWalk (https://github.com/ReFirmLabs/binwalk)
  - DD (Windows&Linux)
- Análisis de cabeceras
  - python c:\Python27\Scripts\binwalk 4.3.5.010
- Extracción del sistema de ficheros
  - Analizar usuarios passwords
  - Analizar código fuente



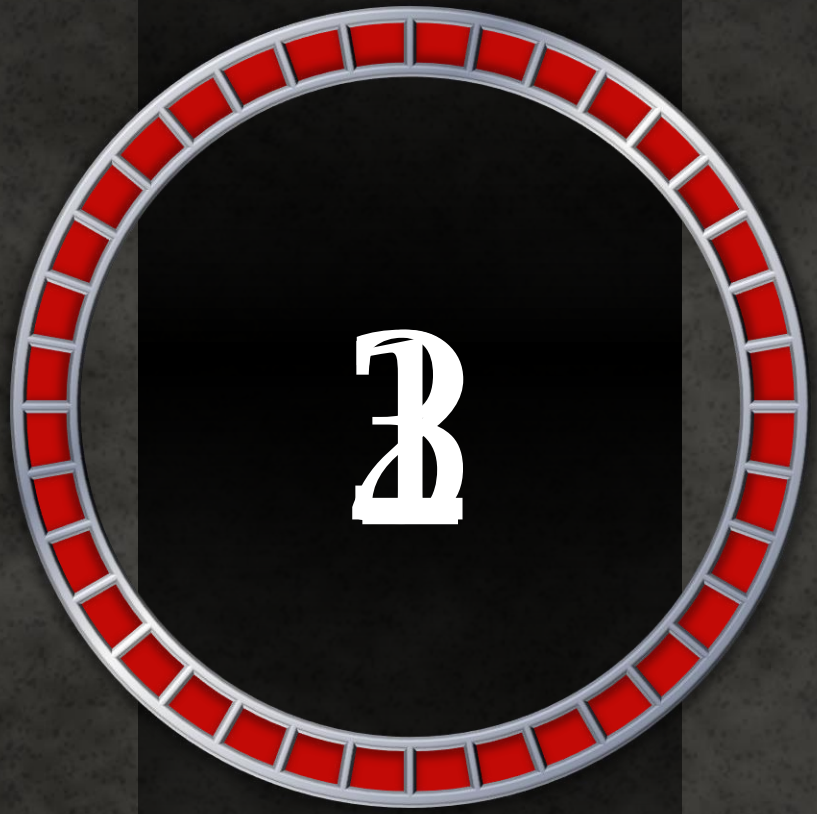


Crack passwords

Fingerprint

```
<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Expires" content="-1"/>
<meta http-equiv="No_storing" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>::: ACEmanager :::</title>
    <link rel="stylesheet" type="text/css" href="brander/ACEmanager.css"/>
    <script type="text/javascript" src="XMLLoader.min.js"/>
    <script type="text/javascript" src="Default.min.js"/>
</head>
```

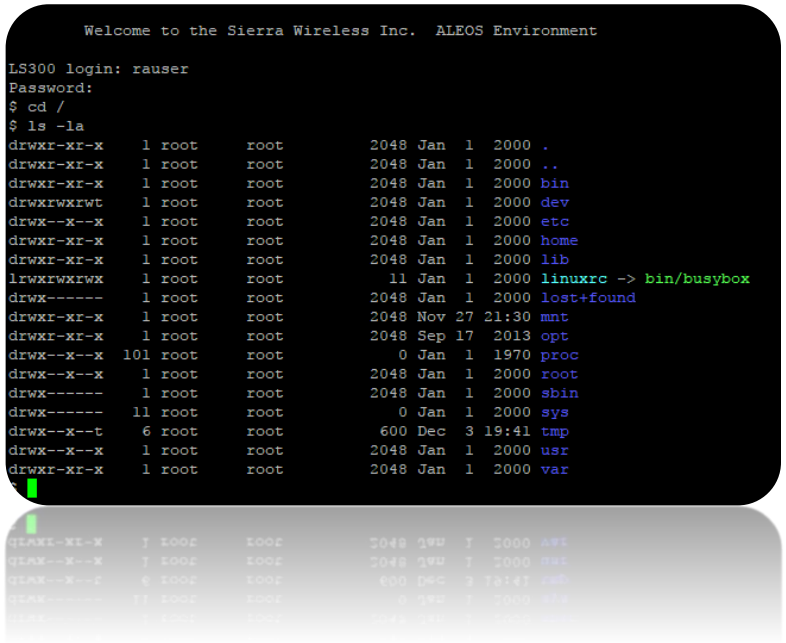
```
31 39 32 2E 31 36 38 2E  15.31...192.168.
31 39 32 2E 31 36 38 2E  15.100..192.168.
31 39 32 2E 31 36 38 2E  17.31...192.168.
31 39 32 2E 31 36 38 2E  17.100..192.168.
39 31 39 31 00 00 00 00  17.150..9191....
30 30 3A 30 30 3A 30 30  US..311.00:00:00
30 00 00 00 44 4F 4F 52  :00:00:00...DOOR
4E 6F 74 20 46 6F 75 6E  SIM.APN Not Foun
30 31 2F 30 31 2F 31 39  d...4...01/01/19
3A 30 30 00 39 34 34 33  70 00:00:00.9443
00 00 00 00 32 32 33 33  ....1024....2233
39 34 39 34 00 00 00 00  5...8F..9494....
6C 65 64 00 31 32 00 00  Not Enabled.12..
32 32 33 33 36 00 00 00  25..E1..22336...
32 32 33 33 38 00 00 00  22337...22338...
31 2C 49 50 2C 00 00 00  0=:0....1,IP,...
4E 6F 74 20 53 74 61 72  22..6...Not Star
32 30 38 2E 38 31 2E 31  ted.....208.81.1
53 69 65 72 72 61 57 69  23.21...SierraWi
37 00 00 00 37 32 30 30  reless..7...7200
```



Shodan/Censys

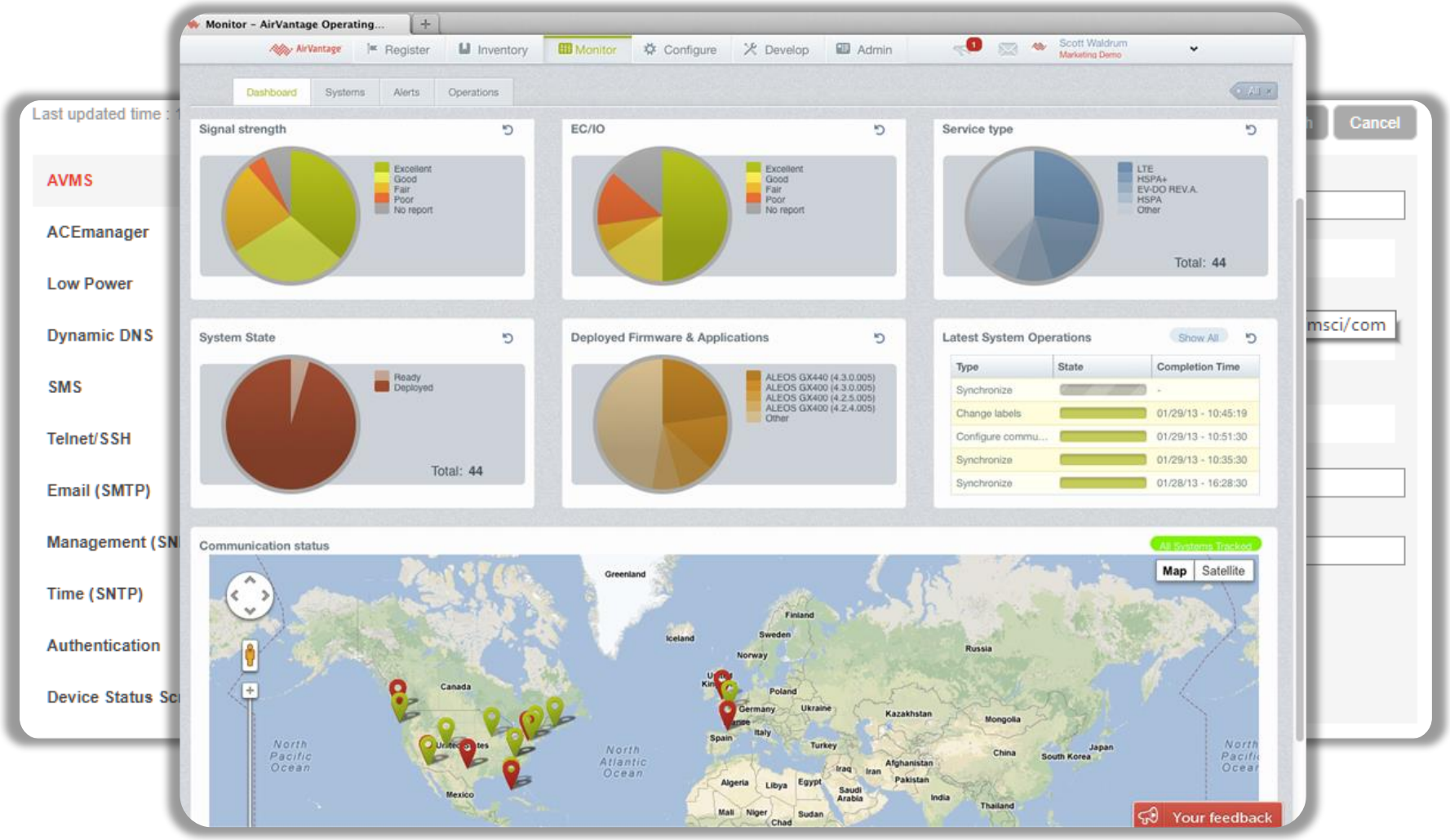
Bind Shell

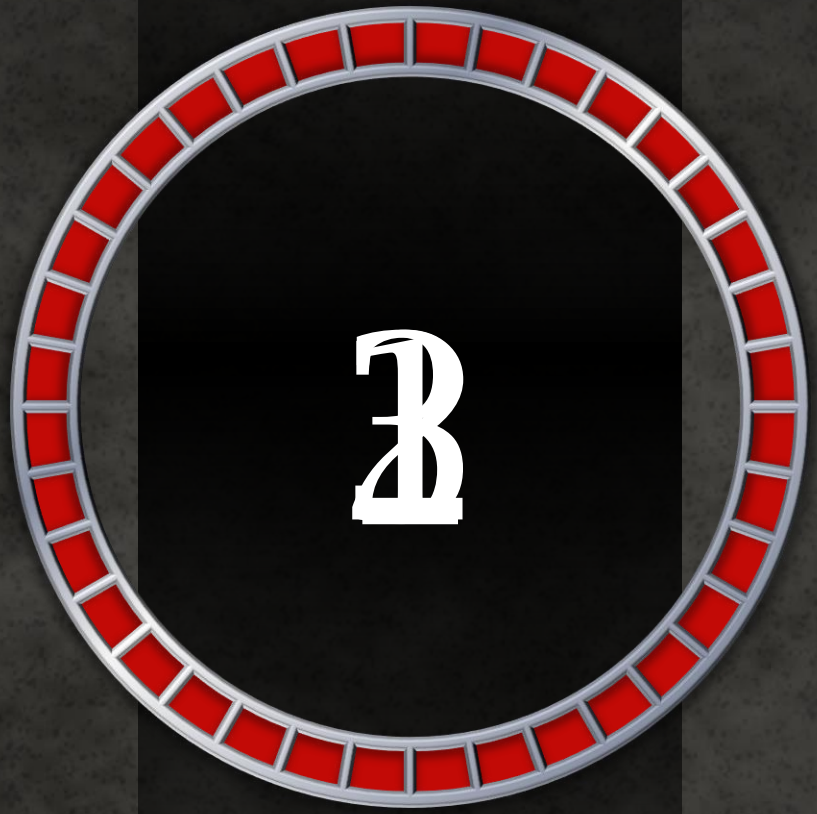
- Por defecto en Web:9191 y Shell:2332
- Firmwares anteriores a 4.4.4 usuario oculto con privilegio /bin/sh
- BusyBox limitado con algunas utilidades (nc, telnet, wget etc..)
- Se puede utilizar para pivotar entre dispositivos
- https://es.slideshare.net/rootedcon/jaime-pealba-y-javier-rodrguez-live-free-or-die-hacking-rootedcon-2012



Command & Control

- Al igual que Mirai, estos dispositivos pueden ser controlados remotamente vía Cloud
- El registro es sencillo requiriendo únicamente:
  - Número de serie del dispositivo
  - URL de conexión
- Por defecto, el pareo del dispositivo con el panel de control es cada 24 horas
- Si se obtiene acceso al panel de control, se pueden configurar estos datos


Monitor - AirVantage Operating...
AirVantage
Register
Inventory
Monitor
Configure
Develop
Admin
Scott Waldrum
Marketing Demo
Dashboard
Systems
Alerts
Operations
Signal strength
Excellent
Good
Fair
Poor
No report
EC/IO
Service type
LTE
HSPA+
EV-DO REV.A.
HSPA
Other
Total: 44
System State
Ready
Deployed
Total: 44
Deployed Firmware & Applications
ALEOS GX440 (4.3.0.005)
ALEOS GX400 (4.3.0.005)
ALEOS GX400 (4.2.5.005)
ALEOS GX400 (4.2.4.005)
Other
Latest System Operations
Show All
Type
State
Completion Time
Synchronize
Change labels
01/29/13 - 10:45:19
Configure commu...
01/29/13 - 10:51:30
Synchronize
01/29/13 - 10:35:30
Synchronize
01/28/13 - 16:28:30
Communication status
Map
Satellite
Greenland
Iceland
Finland
Sweden
Norway
Russia
Canada
Poland
Germany
Ukraine
Kazakhstan
Mongolia
Spain
Italy
Turkey
China
South Korea
Japan
Afghanistan
Iraq
Iran
Pakistan
Algeria
Libya
Egypt
Saudi Arabia
India
Thailand
Mexico
Mali
Niger
Chad
Sudan
North Pacific Ocean
North Atlantic Ocean
Your feedback
Last updated time :
AVMS
ACEmanager
Low Power
Dynamic DNS
SMS
Telnet/SSH
Email (SMTP)
Management (SN
Time (SNTP)
Authentication
Device Status Sc
Cancel
msci/com



AirVantage

Conectividad basada en SIM

- La tecnología IoT se diseña para estar permanentemente conectada
- ¿Qué pasa cuando la conectividad no es posible?
  - Cortes de conexión
  - Ubicaciones remotas
  - Interferencias
  - Baja cobertura de señal
- Muchos de estos dispositivos disponen de conectividad basada en SIM
  - Multi-Operador
  - Servicio continuo de datos sin iteración humana
  - Servicios de datos/voz/SMS
  - Dependiendo de la compañía contratada:
    - Una única SIM para todos los operadores
    - SIM de un operador específico (AT&T, Verizon, Movistar, Vodafone, etc)
    - Plan de datos/voz/SMS personalizados

Conectividad basada en SIM

- La conectividad basada en SIM permite, de manera adicional:
  - Enviar mensajes de control a dispositivos IoT
    - P.Ej: Reinicio, reinicio en modo de fábrica, etc..
  - Recibir información del dispositivo
    - P.Ej: Localización, detección de problemas, consumo, facturación, etc..
- Servicio dirigido a una serie de soluciones de tipo:
  - Máquinas de vending
  - Tiendas ubicadas en sitios con nula conectividad (P.Ej: Un Zara en un desierto)
  - Smart-Cities
  - Servicios financieros
  - Etc..

Envío y recepción de SMS

```
-- Register given client as SMSListener for --
-- incomming sms matching given pattern     --
```

```
-- EMP command for sending new SMS
local function EMPSendSMS(assetid, payload)
    local recepient, message, format = unpack(payload)
    local s, err = messaging.sendSMS(recepient, message, format)
    if not s then
        err = tostring(err)
        log("SMS", "ERROR", "Failed to send SMS from asset (%s), '%s'", tostring(assetid), err)
        return 13, err
    end
    return 0
end
```

```
    patterns[registerid] = {senderp = (senderp ~= "") and senderp or nil, messagep = (messagep ~= "") and messagep or nil}
    log("SMS", "DETAIL", "Asset (%s) registered for SMS [%s|%s] with id %d", tostring(name), tostring(senderp), tostring(messag
    return registerid
end
```

Envío y recepción de SMS

- Dispositivos no están diseñados para discernir cuando se da un mal uso o abuso
- Dispositivos no están diseñados para conocer la identidad del destinatario en una llamada o SMS
  - P.Ej: Voy a hablar con otra máquina? Qué contiene este SMS?
- Todo se realiza mediante comandos AT
  - Dependiendo del dispositivo:
    - Variedad de comandos AT destinados a administración
    - Variedad de comandos AT destinados a envío/recepción de mensajes

Nuevas vías de ataque

- Ataques basados en ingeniería social
  - SMS o llamadas telefónicas de un falso call-center
- Ataques basados al consumo
  - Suscripción a servicios de pago
- Ataques basados en ocultación
  - Realización de llamadas telefónicas/envío de SMS gratuitos con cobertura mundial y de difícil rastreo

LOCUTORIO

"ECONOMICO"

Claro

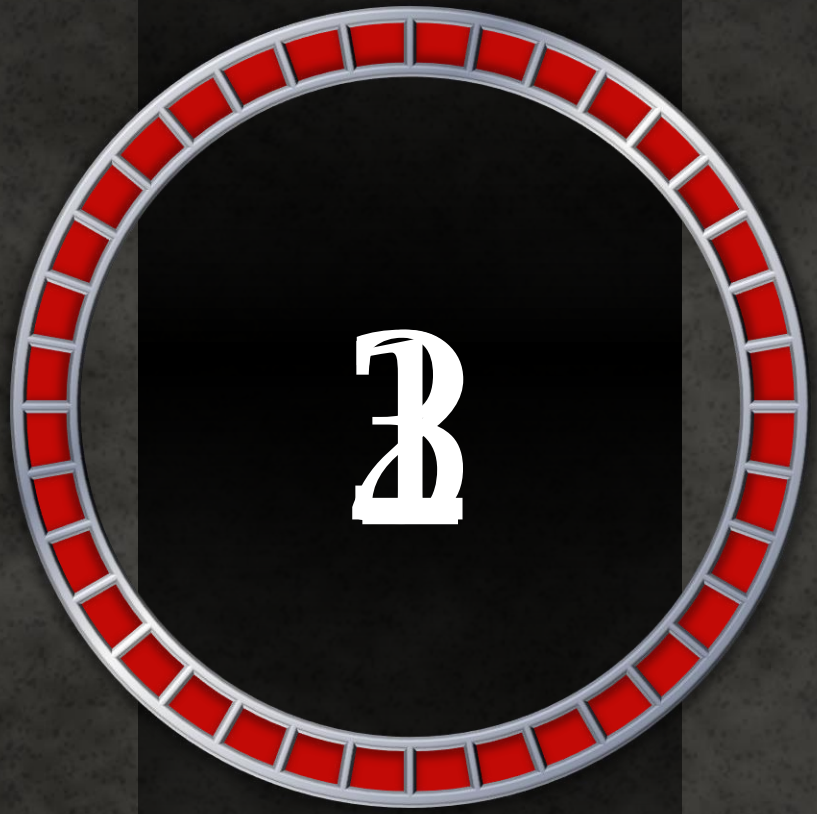
10 CENTIMOS

VENTA DE:

RPM

RECARGA VIRTUAL Y CARGADORES

LOCAL NACIONAL E INTERNACIONAL



Locutorio

Es posible vulnerar el ecosistema de un servicio IoT

Integrar S-SLC en cada una de las soluciones a implementar

Asesórate bien antes de ejecutar una decisión de compra en material IoT