ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

ALE | Where Everything Connects

Seguridad en la red LAN

Experiencias y casos de uso

Jorge Alberto Villa (jorge-alberto.villa@al-enterprise.com)

GHE Verticals Latinamerica

@Reiedan

ACIS Diciembre 2017

Alcatel·Lucent Enterprise

Agenda

PANORAMA MUNDIAL

(in)SEGURIDAD

CÓMO PREPARARSE

CONCLUSIONES

Alcatel·Lucent Enterprise

PANORAMA MUNDIAL

Alcatel·Lucent
Enterprise

El Ciberespacio es una nueva zona de guerra sistemática

Ciberataques como **nueva forma de conseguir fondos** a través de ransomware

El Ciberespacio como una nueva fuente de **"canales de reclutamiento"**

Ciberataques para **acceder a información confidencial y crítica**

Ciberespacio para nuevos tipos de **"canales de comunicación sin control"**

Ciberataques para **control remoto de objetos**

Ciberataques para **controlar personas o influenciar eventos**

Alcatel·Lucent Enterprise

Las agencias de Gobierno bajo ataque

According to research conducted over 18 months:

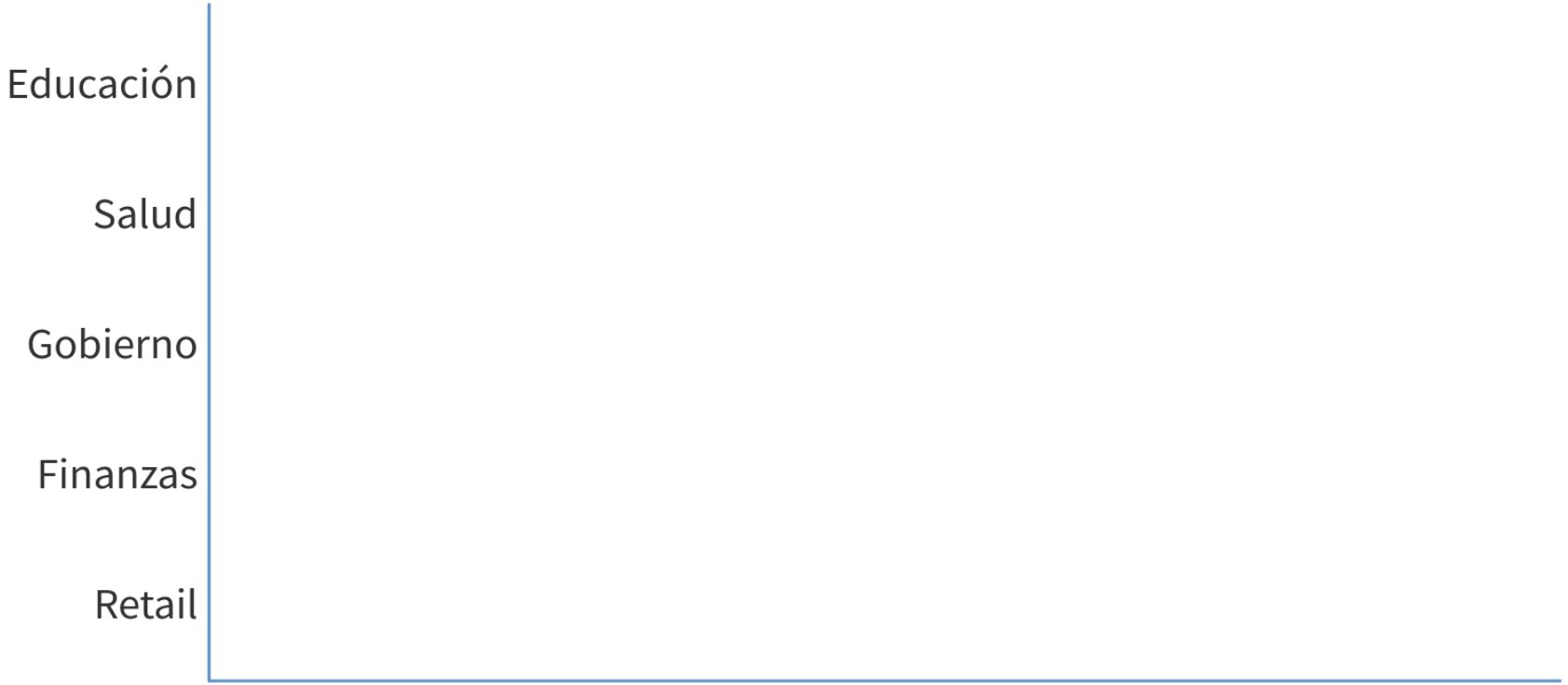
68% of public sector respondents experienced a DDoS attack.

39% experienced theft of data.

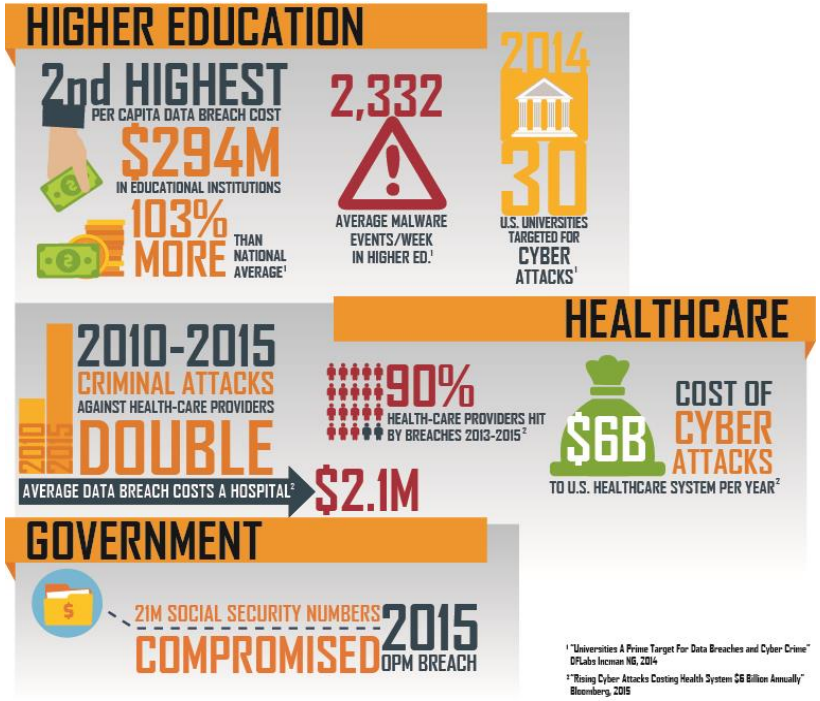
33% were notified of a DDoS attack by a third party.[2]

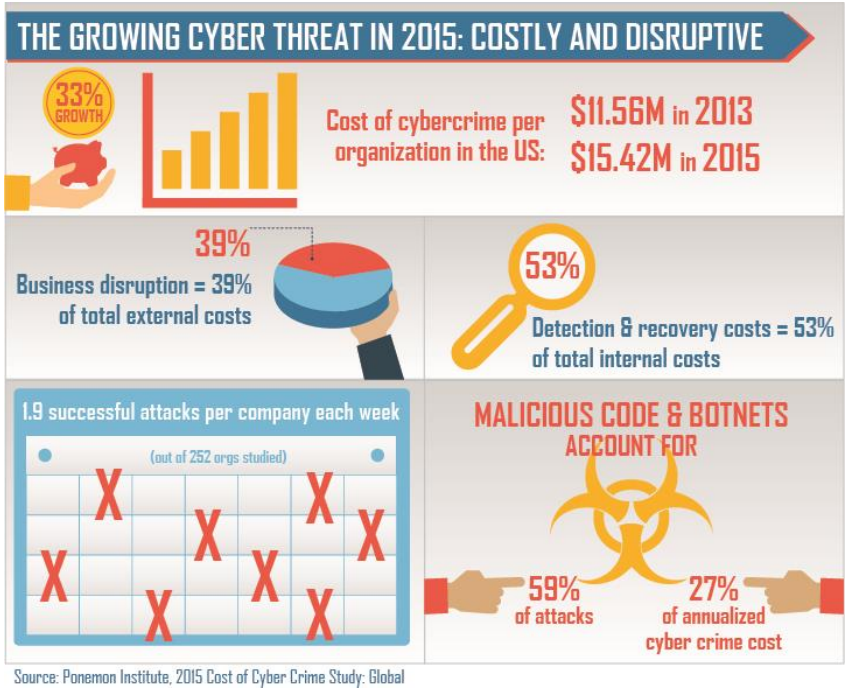
*5 reasons why DDoS attacks are growing, Centers for digital government, 2016

Cuál es el sector más afectado por ciberataques?



La creciente amenaza de ciberseguridad – una tendencia en todo sector





Prevenir un ataque cuesta menos que recuperarse de un ataque

Costo promedio de cibercrimen en 5 años

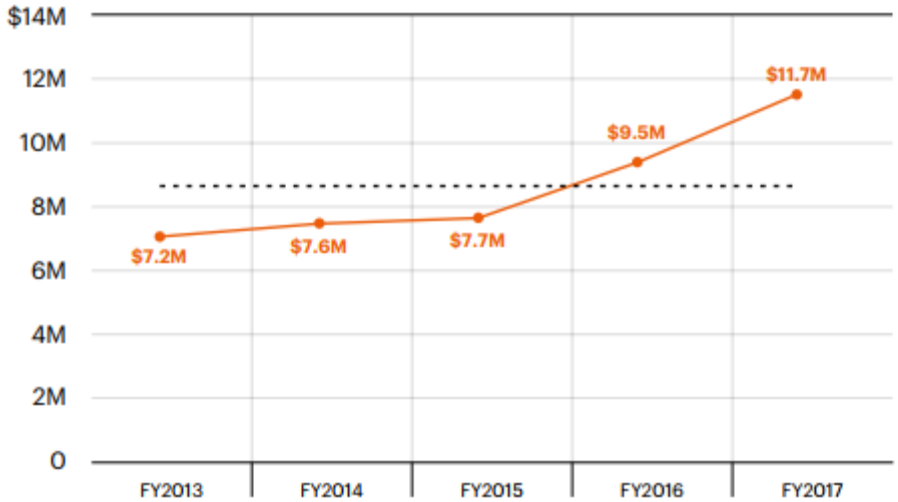


FIGURE 1
The global average cost of cyber crime over five years
US dollars

Legend
Consolidated view
n = 254 separate companies

Total average cost
Five-year average

*Fuente: Accenture 2017 COST OF CYBER CRIME STUDY

Alcatel·Lucent Enterprise

Costo de ataques por sector

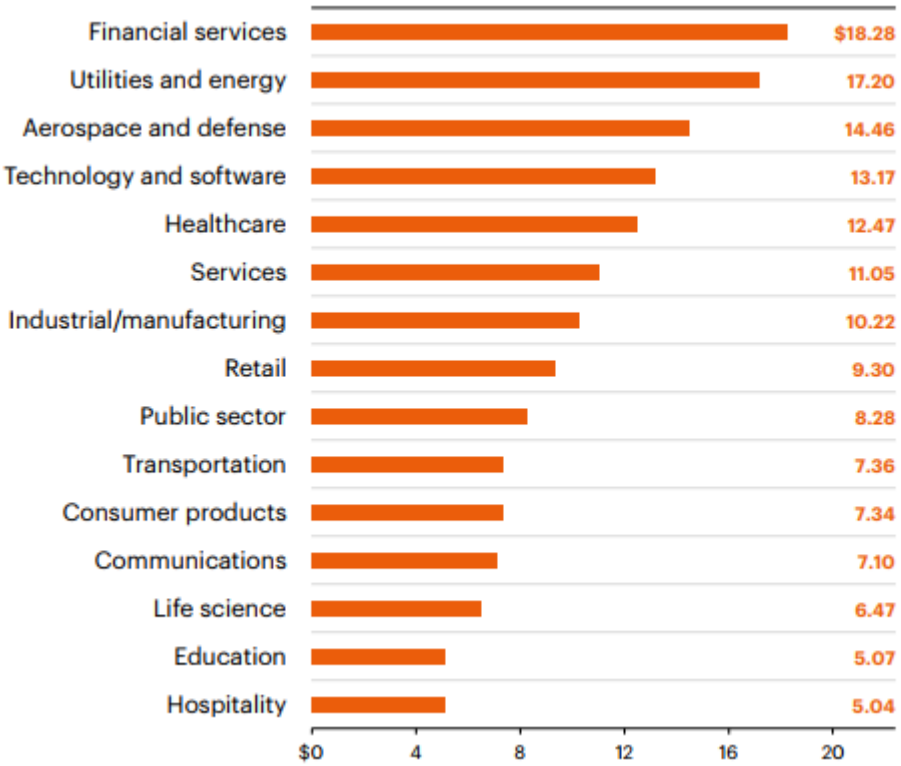


FIGURE 7
Average annualized cost by industry sector
US$ millions

Legend
Consolidated view
n = 254 companies

■ Total annualized cost ($1 million omitted)

*Fuente: Accenture 2017 COST OF CYBER CRIME STUDY

Alcatel·Lucent Enterprise

Tipos comunes de ciberataques

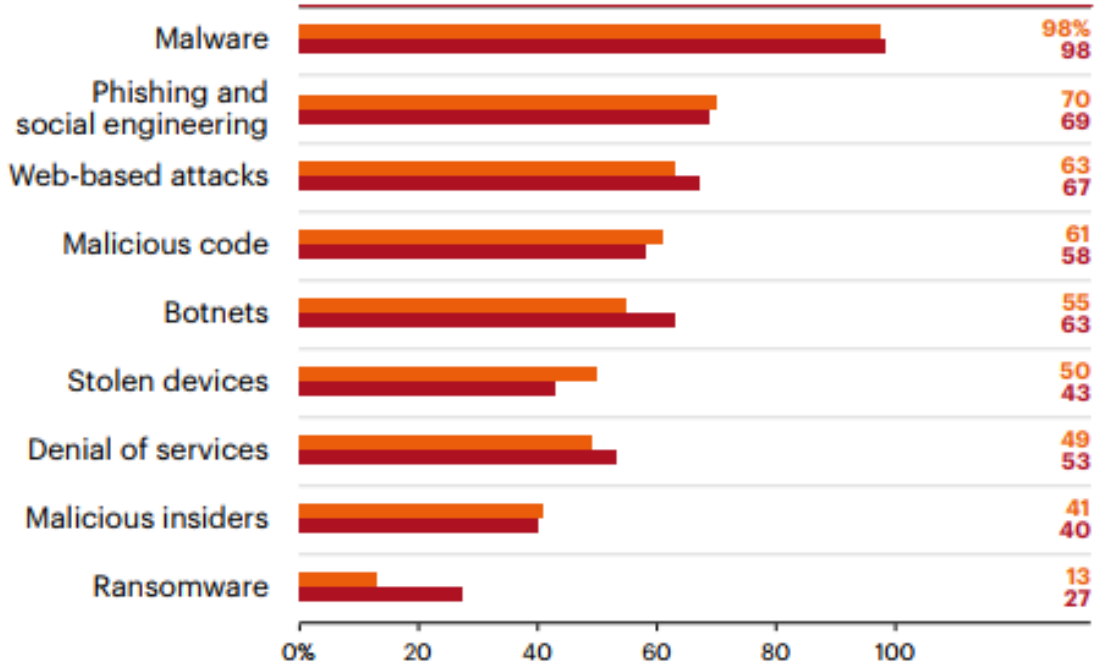


FIGURE 9
Types of cyber attacks experienced by companies

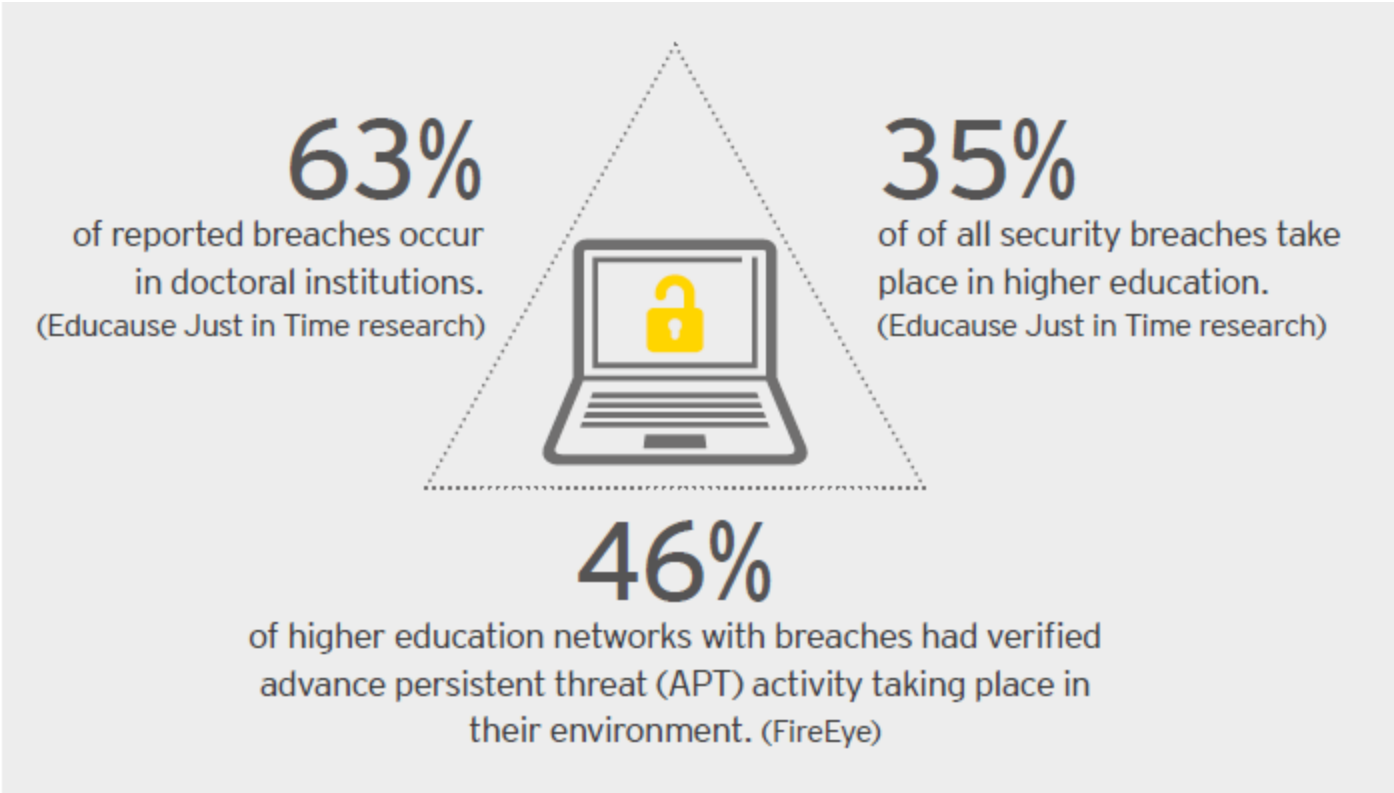
Legend
Consolidated view
n = 254 companies

FY 2016
FY 2017

*Fuente: Accenture 2017 COST OF CYBER CRIME STUDY

Alcatel·Lucent Enterprise

La creciente amenaza de ciberseguridad – una tendencia en Educación



*EY Performance August 2016: Cybersecurity in higher education

Las Universidades son cada vez más interesantes

Busco hacker para modificar notas de Universidad, urgente!

US Ivy League University Harvard announced that it has, for the second time in four months, been the victim of a cyber-breach

Condenaron a estudiante de Los Andes por manipular el sistema de calificaciones

Universidad de Estados Unidos corta internet tras ataque informático

Se sabe que las denuncias han sido interpuestas por universidades de Bogotá, Pasto y Barranquilla.

Si usted ya fue víctima de este ataque, por ningún motivo conecte su equipo a ninguna red. Desconéctelo de la red cableada y de las redes inalámbricas a las que tenga acceso. (Umanizales)

Universidad de Berkeley: 1.600 registros de los empleados y exempleados son robados de los servidores universitarios

La salud es también un objetivo criminal

Networked medical devices pose huge risks to patient safety

Two more hospitals struck by ransomware, in California and Indiana

Hackers will target hospitals like never before in 2017

MedStar attack found to be ransomware, hackers demand Bitcoin

More than half of hospitals hit with ransomware in last 12 months

4,300 records breached at Massachusetts General Hospital in Boston

Ransomware attack on Texas pediatric provider exposes data of 55,000 patients

Kansas hospital hit by ransomware, pays up, then attackers demand second ransom

Otros sectores (Ingeniería Social)

British Airways

Francia

Porsche

RBS Royal Bank of Scotland

Siria

USA

Rusia

China

Caterpillcar

Venezuela

Colombia

(in)SEGURIDAD

Consecuencias

Alcatel·Lucent Enterprise

(in)Seguridad (Motivaciones)

- Robo de información
- Alteración de información (notas, registros, matrículas, situación financiera)
- Cancelación de clases
- Presión por posición política o social
- Prestigio
- Dinero

Anonymous Targets, Threatens Boston Children's Hospital

"By their very nature, these networks have a large number of transient users, making it more difficult to detect and respond to incidents than it would be in a more tightly controlled corporate environment. Requirements to provide easy access for users do not typically allow for rigid access controls and further complicate efforts to monitor network traffic"

* www.scmagazineuk.com

Consecuencias (Efectos)

- DesPrestigio
- Bloqueo de acceso internacional (Blacklisting)
- Usuarios insatisfechos
- Mala percepción de servicio
- Decepción de los profesores y admin
- Recursos insuficientes

Cyber-attack in Japan took down 444 school networks simultaneously

A 15-year-old in Australia is facing 10 years in jail…
he launched the assault as a test.

A Vancouver high school suffered network service degradation…

The student was expelled.

Rutgers Arizona State University and University of Georgia attacks have caused a number of issues resulting in delays during registration and final exams

CALA

- Brasil, México y Colombia son los países de América Latina más afectados por ataques informáticos, que dejaron pérdidas en la región por **184.000** millones de dólares entre agosto de 2015 y agosto de 2016
- En Colombia las pérdidas fueron de **5.700** millones de dólares

  Un aumento en Colombia del **4%** con respecto al año anterior

https://www.elheraldo.co/economia/ciberataques-en-colombia-dejan-perdidas-por-5700-millones-de-dolares-277787

Colombia

- El Instituto Nacional de Investigación y Prevención de Fraude (INIF) en Colombia señala que el nivel de fraude alcanza en la actualidad aproximadamente el 7% del valor de las reclamaciones abarcando todos los ramos: seguros del automóvil y Seguro Obligatorio de Accidentes de Tránsito (SOAT), pólizas de vida, salud, hogar y productos ligados a servicios públicos.
- 350.000 “colados” en el SISBEN (67% más que en 2015)
- Más de $300M en medicamentos al falsificar EHRs en la zona cafetera

*https://www.elheraldo.co/economia/ciberataques-en-colombia-dejan-perdidas-por-5700-millones-de-dolares-277787

**http://www.fasecolda.com/files/7413/9101/0544/parte_i.captulo_15_fraude_en_seguros.pdf

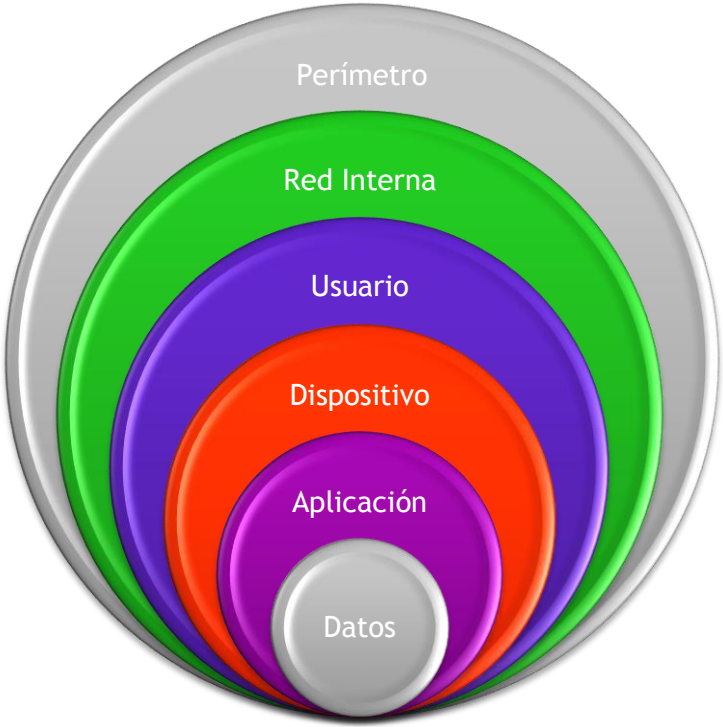
***https://noticias.caracoltv.com/colombia/corrupcion-sin-remedio-dos-exfuncionarios-habrian-robado-300-millones-en-medicamentos

Cómo Prepararse

Diferentes ataques y cómo contenerlos

(Por qué la red LAN)

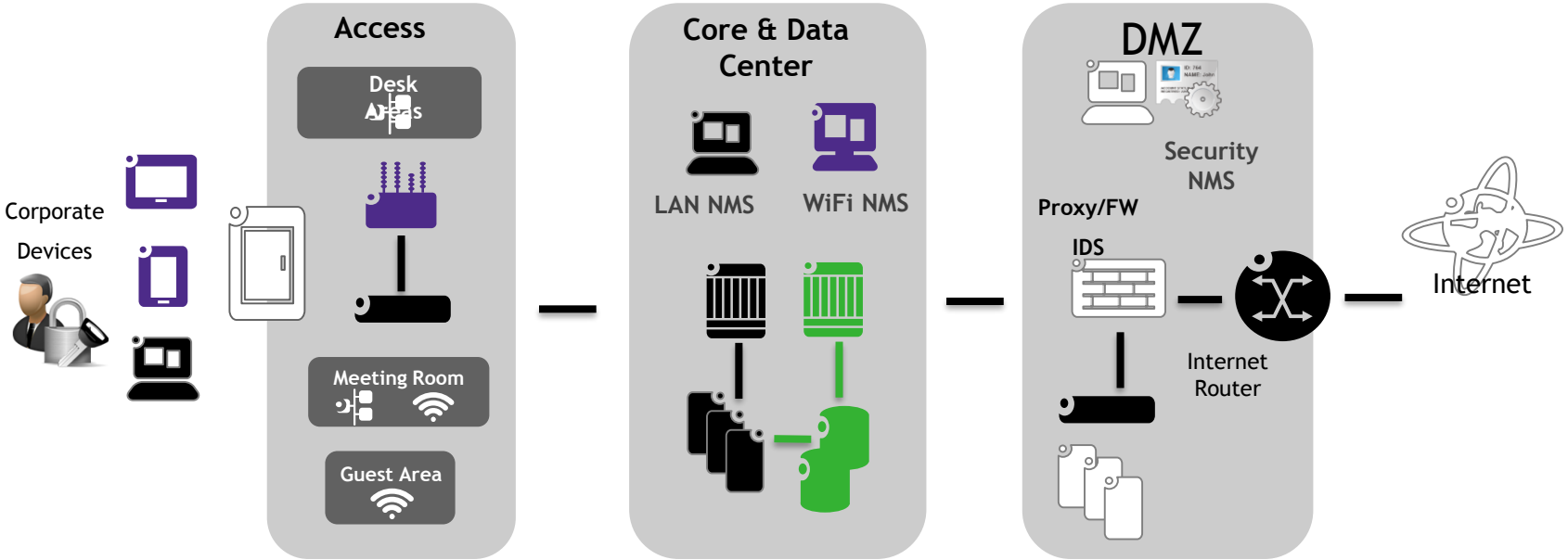
La red tiene un papel muy importante en seguridad



Alcatel·Lucent Enterprise

EL ESTATUS DE LAS REDES EMPRESARIALES HOY

Infraestructura de redes Segura y Robusta

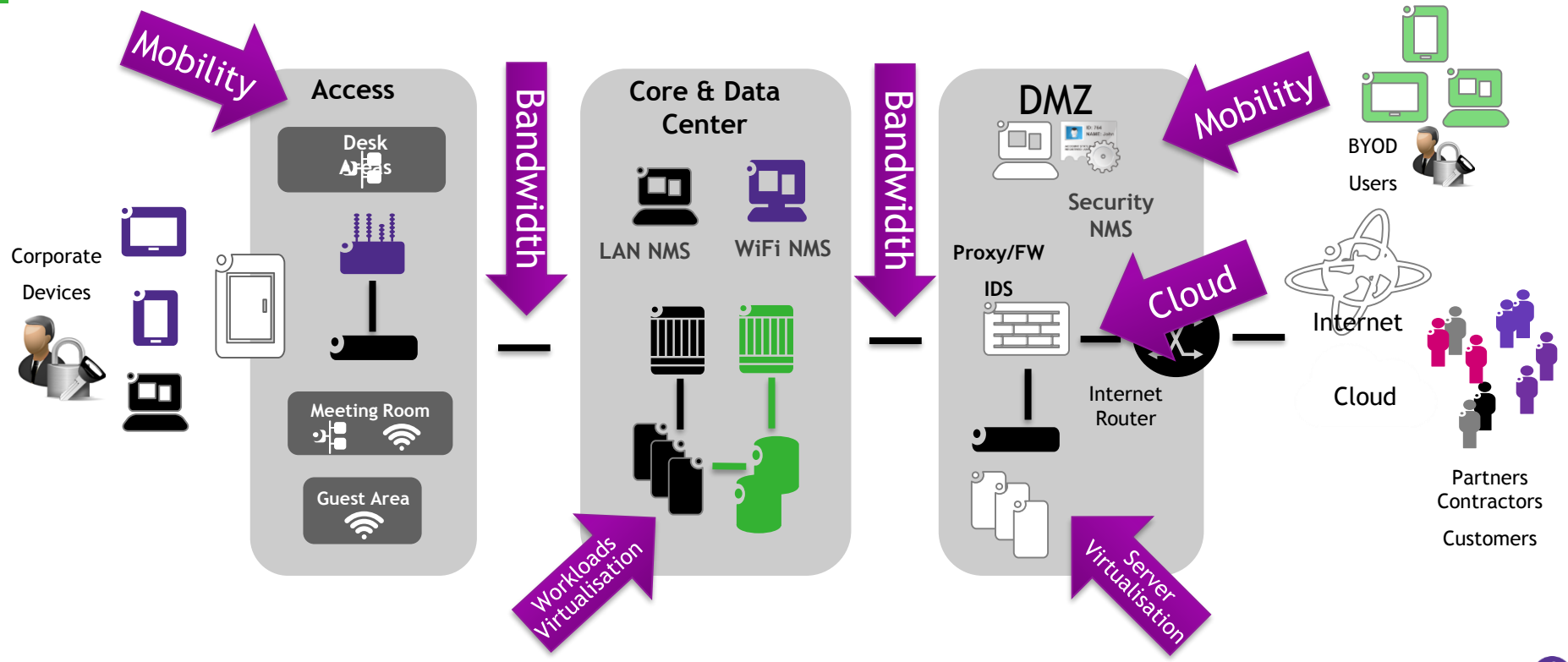


23

Alcatel·Lucent
Enterprise

EL ESTATUS DE LAS REDES EMPRESARIALES HOY

Infraestructura de redes Segura y Robusta



24

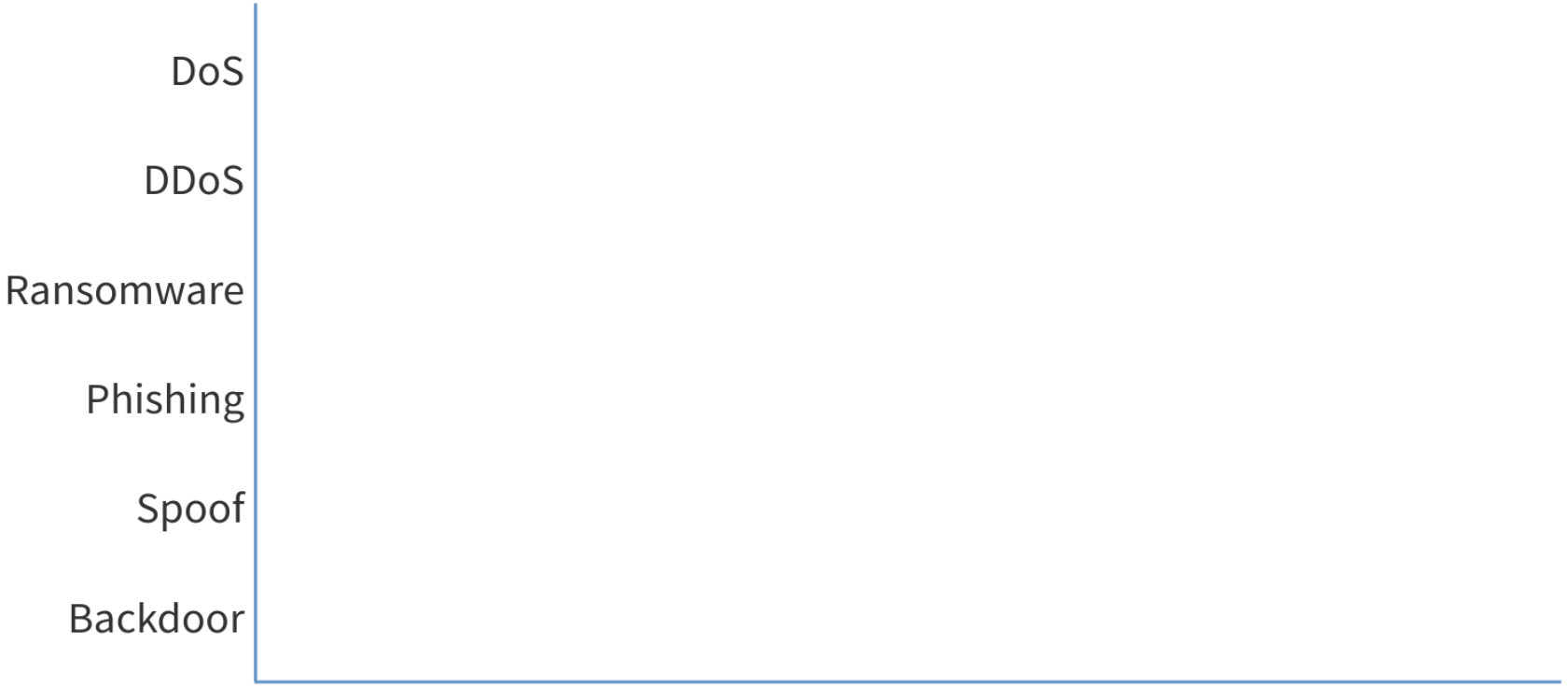
Alcatel·Lucent Enterprise

Tipos de ataques

- Ataques Exógenos
  - DDoS
  - Ransomware
  - Phishing
  - Hacking (Robo de info. Personal)
  - BackDoor exploits
  - DoS a los equipos

- Ataques internos
  (Intencionados ó Inocentes)
  - Phishing
  - DDoS
  - Hacking
  - Spoofing -> IP, MAC
  - DHCP Spoof
  - DNS Spoof
  - MIM
  - Scanners (CAIN)
  - BackDoor exploits

Cuál es el ataque más común?

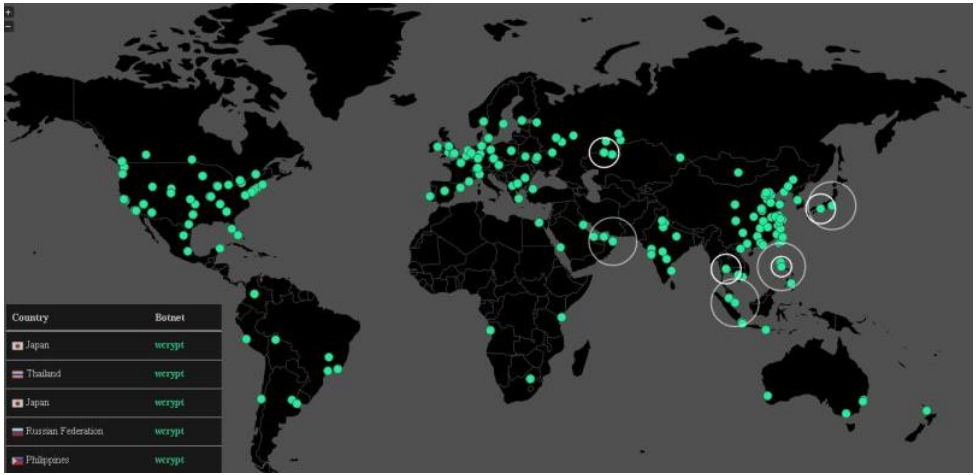


Tipos d

- Ataques E
  - DDoS
  - Ransomv
  - Phishing
  - Hacking
  - BackDoo
  - DoS a lo

CIFRADO DE LA INFORMACIÓN

Los hospitales de Reino Unido han tenido que cancelar todas sus citas tras sufrir un ataque cibernético



- ➢25 Hospitales sin atención
- ➢No hay Teléfonos
- ➢No hay Autorizaciones Médicas
- ➢No hay admisión de pacientes

¿Puede su organización trabajar sin sistemas de información o redes de

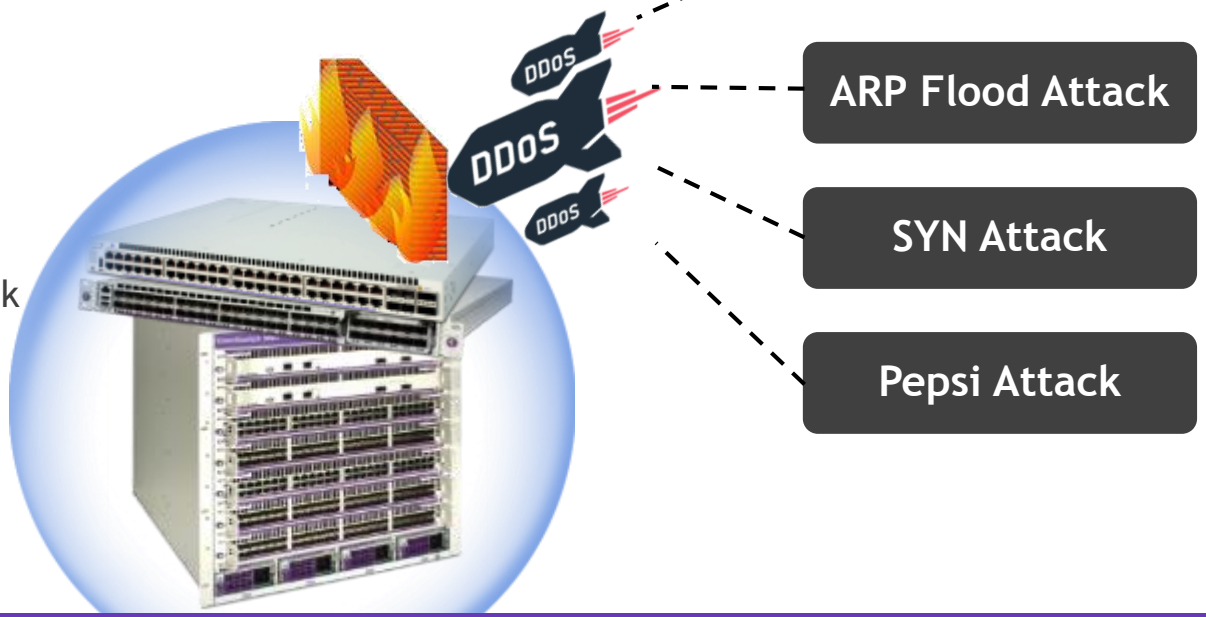
*OK Diario.com

**Intel

Alcatel·Lucent Enterprise

Protección integrada contra ataques de Denegación de Servicio (DoS)

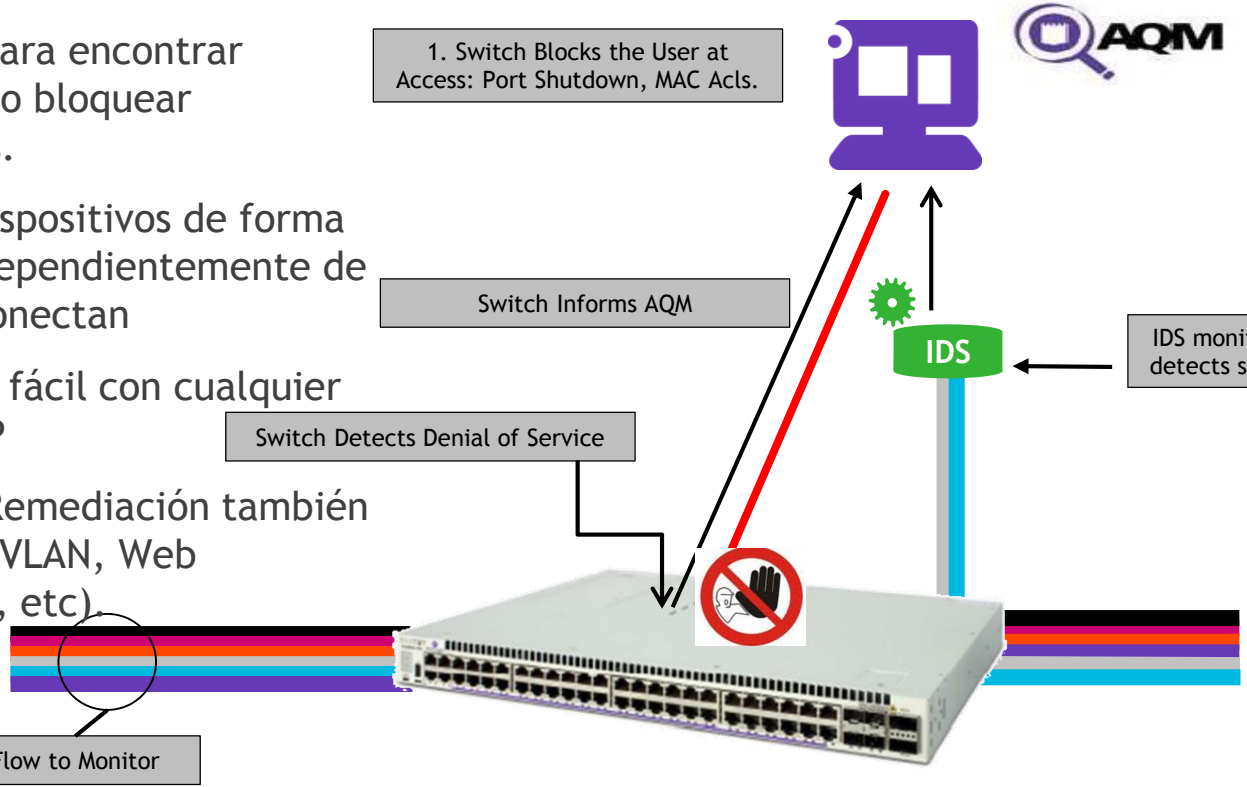
- DOS Attacks (All clases)
  - TTL 0 Floding
  - IGMP Flooding
  - DHCP flooding
  - ARP flooding
  - CAM Oveflow
  - STP Claiming Root role attack
  - DHCP Rogue
  - Attacks on Routing Protocols
  - IPV6 MLD storms



Protegiendo todos los recursos conectados incluyendo dispositivos IoT

NUEVO NIVEL DE SEGURIDAD: HERRAMIENTAS DE AUTOMATIZACIÓN

- Habilidad para encontrar candidatos o bloquear dispositivos.
- Bloquear dispositivos de forma manual independientemente de dónde se conectan
- Integración fácil con cualquier FW/IDS/IDP
- Acción de Remediación también soportada (VLAN, Web redirection, etc).

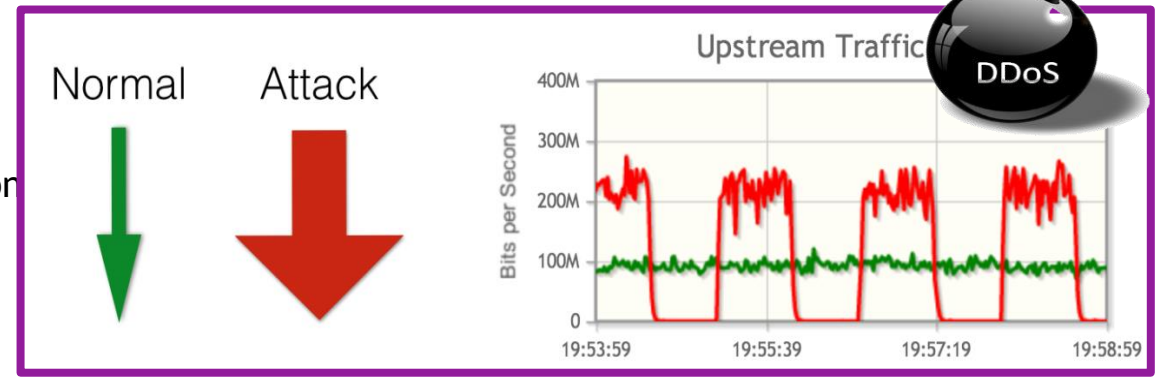


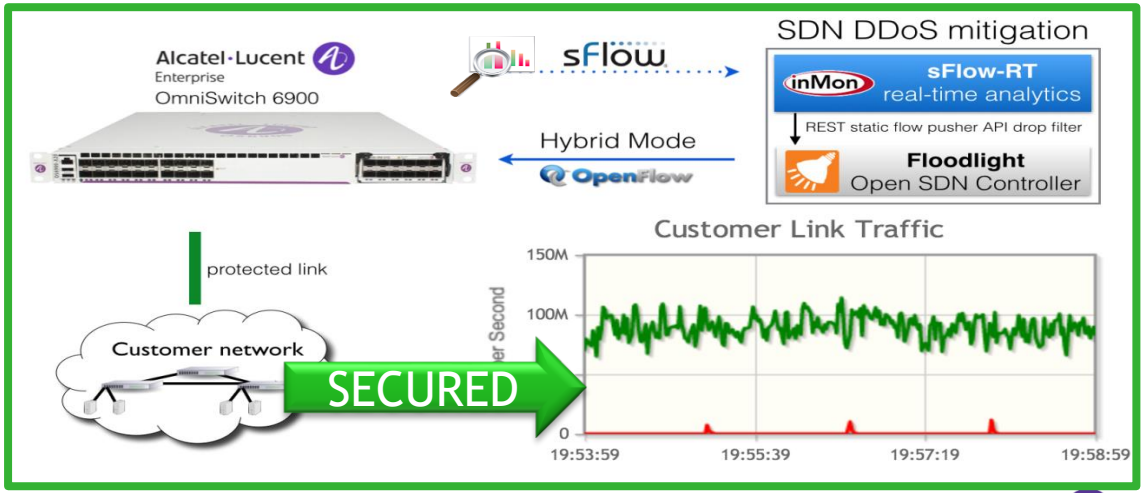
Alcatel·Lucent Enterprise

SDN ANALYTICS
ASEGURAR LA INSTITUCIÓN

Problema:
- Ataques DDoS
- Escalabilidad con puntos de detección distribuidos
- Mecanismos Lentos de respuesta de red
- Reconfiguración Manual de la Red

Beneficios:
- Recolección centralizada con Análisis SDN basado en estándares, en tiempo real
- Respuesta Automática Dinámica Rápida
- Bloqueo de ataques DDoS vía Interfaz Programable ABIERTA





Alcatel·Lucent
Enterprise

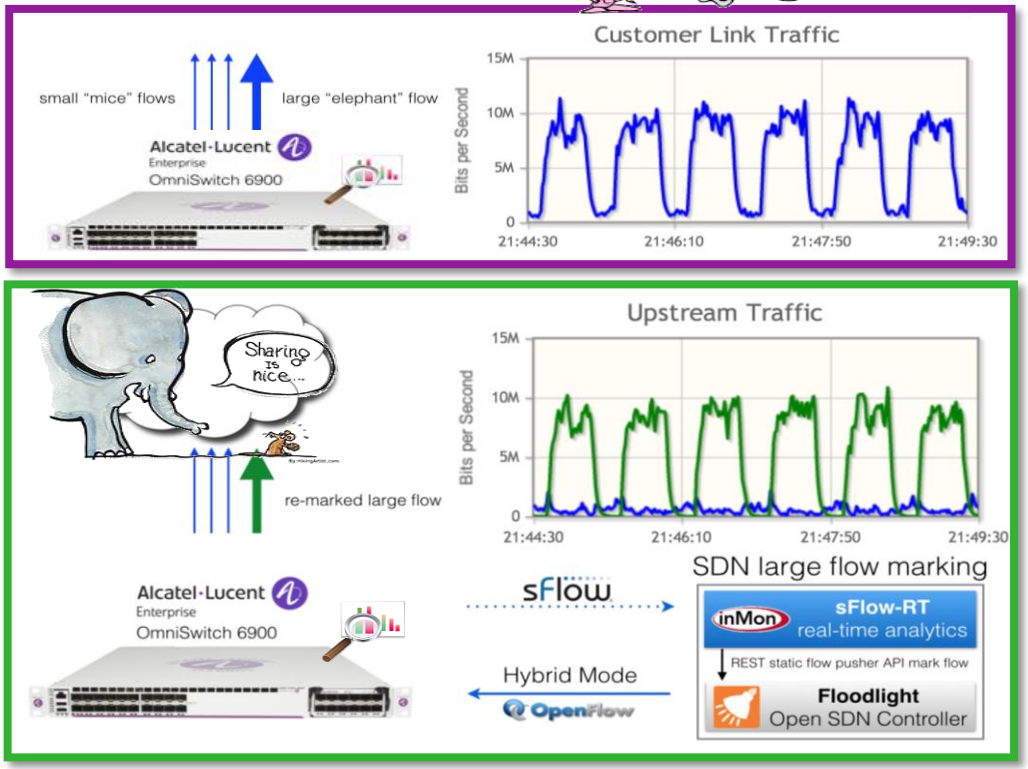
SDN ANALYTICS
INTELLIGENT FABRIC EN LA INSTITUCIÓN

Problema:

- Algunos flujos de gran ancho de banda (Elefantes) causan jitter/latencia a flujos prevalentes con bajo ancho de banda (Ratones)
- Instalar equipo de detección distribuida propietario
- Mecanismos de respuesta intensiva de IT

Beneficios:

- Recolección centralizada con SDN Analytics basado en estándares de tiempo real
- Respuesta Automática Dinámica de Red
- Macar flujos Elefantes vía Interfaces Programables



Alcatel·Lucent
Enterprise

Robo de Información

- Spoof IP
- Spoof MAC
- Spoof DNS
- Spoof DHCP
- Suplantación de identidad

- **Seguridad en el Acceso:**
  - Dynamic ARP Snooping (Inspection)
  - Detección de DHCP Spoofing
  - Learned Port security
  - Private Vlans
  - Rogue Detection
  - STP root guard
  - IPv6 Edge Security
  - Routing Security
  - IP Spoof security
  - LLDP Rogue Detection

Control de Acceso a la Red

Qué?

-> Determine quién está en la red

-> Revise si los usuarios finales cumplen con las definiciones de seguridad

-> Dirija a qué tienen acceso los ususarios en la red

Cómo?

- Autenticación basasda en MAC y 802.1X usando un servidor RADIUS
- Perfiles basados en Roles (ACLs, QoS) por usuario
- Reglas de clasificación en todos los switches para clasificar los usuarios basándose en atributos de puerto y dispositivo (ej.: MAC orígen)
- Portal Cautivo Interno/Externo para autenticación basada en Web o postura
- Integración con *AAA como parte de una solución de acceso unificado y BYOD*

Control de acceso, autenticación, autorización

Debo considerar AAA también para IoT?

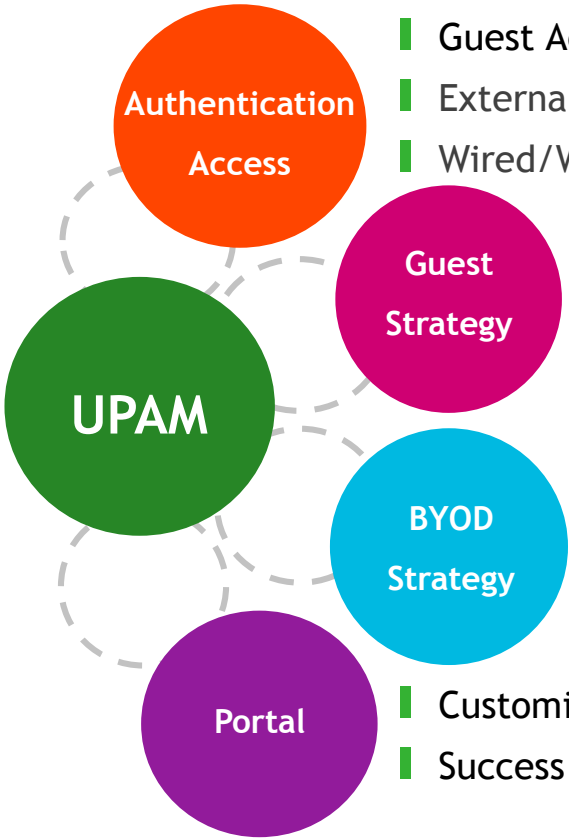
- Qué dispositivos necesito conectar (impresoras, cámaras, cerrojos, puertas, aire acondicionado, etc)?
- Cómo puedo conectar dispositivos en una forma segura?
- Cómo puede la red conectar estos dispositivos sin involucrar a TI?
- Cómo conecto estos dospositivos IoT sin comprometer el desempeño de la red?

A giant botnet made up of hijacked internet-connected things like cameras, lightbulbs, and thermostats has launched the largest DDoS attack ever against a top security blogger. The delivery network has dropped protection for the Krebs on Security blog written by Brian Krebs after an attack delivering 665Gbps of traffic overwhelmed his site. https://goo.gl/rxU2Dc

ALGUNAS SOLUCIONES NECESARIAS EN BYOD

- Direccionamiento IP : Todos los dispositivos que usan una IP (dinámica o estática) deben estar en un “IP store”
- Registro de la cuenta :Los empleados tienen que estar registrados en la “tienda de usuarios”
- Registro de Dispositivos :Los dispositivos tienen que estar registrados en la “tienda de políticas y situaciones”
- Identificación de Dispositivos: Qué clase de dispositivos están conectados a la red y registrados en la “tienda de dispositivos”
- Onboarding :Los dispositivos tienen que estar configurados para poder conectarse y autenticarse
- Autenticación :Los usuarios se autentican a través de sus dispositivos a la red
- Aplicación de Políticas :Las políticas a aplicar dependen del usuario, dispositivo, su situación y la aplicación.

UPAM – Unified Policy Authentication Manager



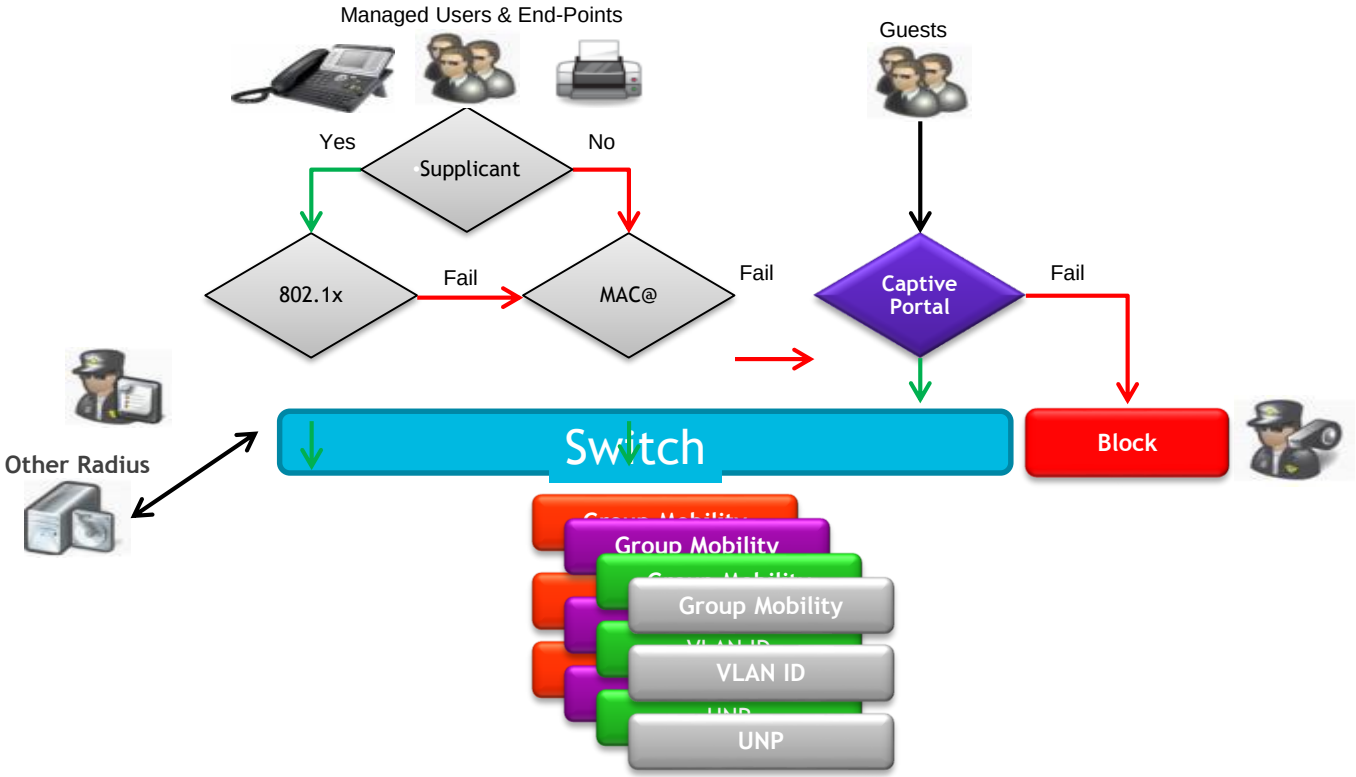
- Guest Access, BYOD, IT Owned
- External Radius, Local DB, AD/LDAP (Role Mapping)
- Wired/Wireless

- Account Creation, Notification (SMS, Email, WEB)
- Self-Registration, Employee Sponsor
- Basic/ Premium Servicing
- Login using Uname/Passwd, Access-Code, Social Account

- Session & Device Control
- Device Fingerprinting (OS, Type, etc.)

- Customizable Pages Guest Access/ BYOD
- Success Redirect URL

SEGURIDAD DE ACCESO EN CADA PUERTO/PUNTO



Alcatel·Lucent Enterprise

OS Exploits

Disable TELNET! Cisco finds 0-Day in CIA Dump affecting over 300 Network Switch Models

SCHOOLMONTANA, SIERRAMONTANA, STUCCOMONTANA: DNT implant for JunOS

SYNful Knock silently changes a router's operating system image

…get access to data in the device's memory, "which could lead to the disclosure of confidential information,"…

HEADWATER: DNT implant for Huawei

Verificación & Validación Independiente

Amenaza potencial en el SW

- Amenazas de Back door
- Malware Embebido
- Vulnerabilidades explotables
- Exposición de información propietaria / clasificada

La solución:

- Aproximación de seguridad proactiva a través de búsqueda y análisis de vulnerabilidades en el software del switch
- Análisis del código para detectar vulnerabilidades y corregir defectos de seguridad

Dirigido a interfaces externas:

- HTTPS Interface
- Login Interface
- NTP Interface
- Command Line Interface
- IP Port Usage
- SNMP Interface

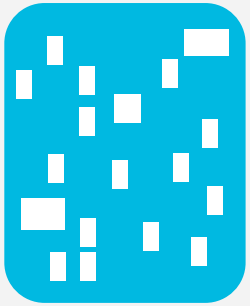
IV&V identifica vulnerabilidades de seguridad en el código fuente
a través del uso de herramietnas automatizadas e inspecciones manuales de código.

41

Object Code Scrambling - Software

Diversificación

Typical network node OS



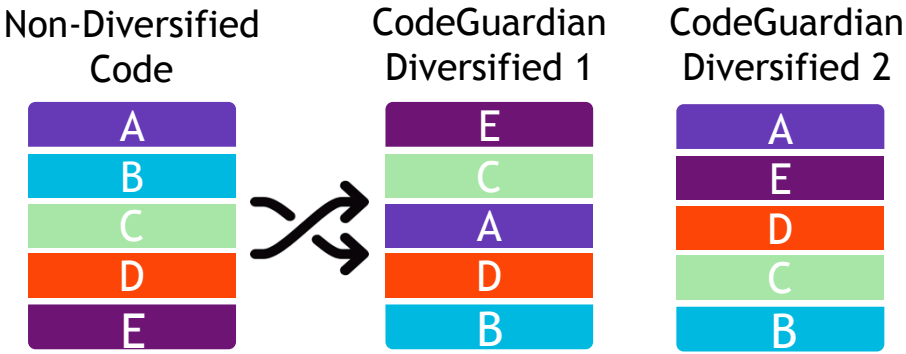
Proprietary code

Open source code

- bootp
- ntp
- Jquery
- libxml2
- net-snmp
- open ssh
- open ssl
- open ldap
- telnet
- traceroute

Most probable entry point for exploitation

Same functionality as the non-diversified code

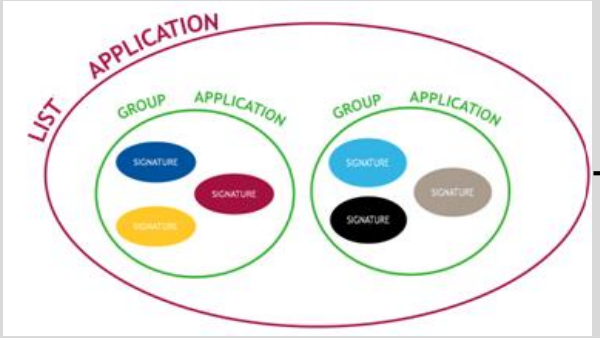


Exploits basados en direcciones son inefectivos debido a la diversificación de software que “mezcla” el mapa de memoria de la imágen binaria del OS

Seguridad de Aplicaciones

- DPI
- Modificación dinámica de parámetros de red

EL FUTURO DE SEGURIDAD DE ACCESO: APP VISIBILITY+ENFORCEMENT




```
-> policy condition c1_fileTxfr dpi app-group file_transfer
-> policy action BW_LIMIT maximum-bandwidth 1mbps
-> policy rule R1 condition c1_fileTxfr action BW_LIMIT
-> qos apply
```

```
-> show dpi app-list
 S/N         Application-List Member Name    Application-List Member Type
-----+-----------------------------------+-----------------------------
 1    Jabber - Initiating CTS                APP
 2    Jabber - proceed in encrypted channel  APP
 3    Jabber - request encrypted channe      APP
 4    Jabber - send instant message          APP
 5    P2P                                    APP-GRP
```

QoS

Each flow is redirected towards the associated QoS policy

QoS

Flow to Monitor

Alcatel·Lucent Enterprise

Contra-ataque (Ejemplos WiFi)

- Desautenticación
  - Se rompe la asociación de un AP o cliente en la interfaz inalámbrica.
- Pozo de Brea (Tarpit)
  - Se atrae a los clientes que intentan asociarse con un AP a un pozo de brea, que puede estar en un mismo canal o en un canal diferente.
- Cableada
  - Se rompe la conexión de un AP o cliente en la interfaz cableada
- Lista Negra
  - Se evita la asociación de un usuario por:
    - Intentos fallidos
    - DoS (Ataque de Denegación de Servicio)
    - MITM (Ataque del Hombre en el Medio)
    - Aplicaciones externas

Conclusiones

Cómo Prepararse

Cómo prepararse

Gobernanza
Visibilidad
Capacitación

Control por puertas
Limitación de BW
Limitación de Puertos
Limitación de Accesos

Automatización
SDN
Cooperación FW-LAN
Contraataque
Perfiles de Red
Virtualización de la red

OS Scrambling
HIC
NAC

Alcatel·Lucent Enterprise

Seguridad de la red

Sólo una aproximación única no puede proporcionar seguridad total

- Falta de Conocimiento de Admins
- Acceso Inválido
- Denegación de Servicio para Gestión
- No seguimiento o registros de actividad
- Error de configuración de la Red
- Integridad de equipos: productos inseguros con “puertas traseras”
- Diseño de equipos IoT: broadcast L2 básico, VLAN fija por direcciones IP

- Contención de tráfico
- Cooperación con Firewall
- AAA para Acceso
- Automatización
- UPAM
- Network Analytics
- OS Scrambling

Una seguridad apropiada requiere una aproximación holística con múltiples capas de defensa

RECOMENDACIONES

- Generar políticas de gobierno de TI que incluyan planes de prevención y reacción
- Aceptar la posibilidad de un ataque.
- Realizar un estudio continuo de vulnerabilidades
- Considerar los ataques externos, pero también la seguridad interna

- Más que una estandarización, los estándares de seguridad aplican a los hábitos de una organización y no tiene que ver con el equipamiento que se instala…

…siempre y cuando los equipos no presenten algún tipo de riesgo de seguridad, claro está.

ALE | Where Everything Connects

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

SEGURIDAD EN LA RED LAN

Experiencias y Casos de Uso

Alcatel·Lucent Enterprise

Alcatel·Lucent
Enterprise