Mejoras de seguridad en la red de la UCM
II Foro de Redes de Campus - Córdoba

Luis Padilla

31 - mayo - 2016

Área de Infraestructura T.I.
Servicios Informáticos UCM

Servicios Informáticos

Situación de partida

- Red docente (PDI y PAS) en red pública creciendo desde principios de los años ‘80.
- Actualmente unos 14.000 equipos.
- Incluye PCs, portátiles, puestos de aulas, servidores, impresoras, cámaras IP, …
- Filosofía “todo **abierto** excepto…”.
- Cerrado de entrada: Netbios, BB.DD., impresión, UPnP, SIP, RPC, syslog, DHCP, SNMP, NTP, DNS, **SMTP** y otros (gusanos y backdoors).
- Cerrado de salida: Netbios, BB.DD., impresión, UPnP, DHCP, SNMP, **SMTP** y otros.

Servicios Informáticos

Situación deseada

- Servidores PDI en DMZ, el resto en VLAN separada y protegida por cortafuegos.
- Filosofía “todo **cerrado** excepto…”.
- Gestión remota mediante VPN corporativa.
- Cerrado de entrada: Todo excepto los servidores registrados por sus puertos de servicio.
- Cerrado de salida: Igual que ahora.
- Problema: Gestión, gestión y ¡gestión!
  - Muchos equipos en uso.
  - Documentación poco fiable de tipo de equipo y persona responsable.

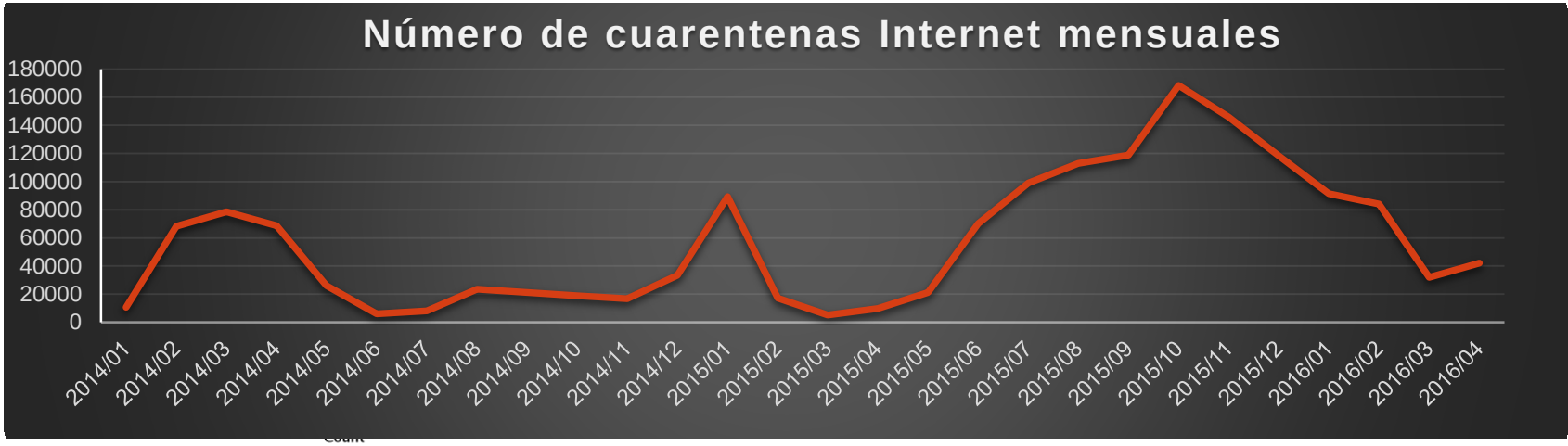
Problemas situación actual

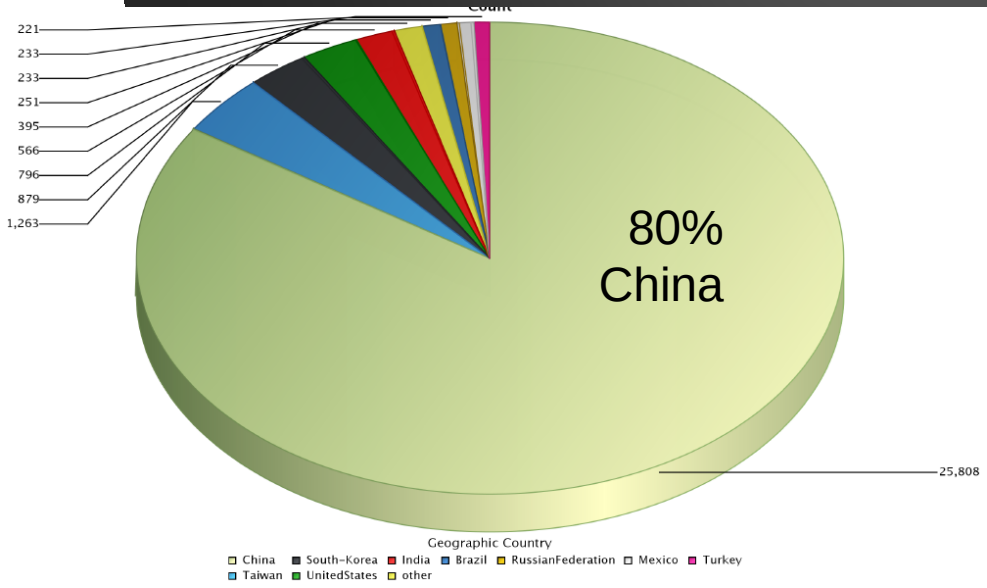
- Ruido que dificulta la detección de incidentes.
- Equipos comprometidos fácilmente.
- Saturación de la lista negra (35.000 objetos).
- Sobrecarga del SIEM (en situaciones extremas).
- Ejemplo incidente impresoras (febrero 2016):
  - Escaneo de servidores FTP con contraseña trivial => las impresoras por defecto tienen FTP sin contraseña.
  - Subida de zip con virus => en impresoras la subida FTP va al spooler.
  - Consecuencia: impresión masiva de hojas con basura => ¡¡¡DoS!!!
  - En un par de semanas se filtran más de 800 impresoras.

Mejoras de seguridad en la red de la UCM

Servicios Informáticos

Estadísticas





Port	Port Use	Q3 '14 Traffic %	Q2 '14 %
23	Telnet	12%	10%
445	Microsoft-DS	8.1%	14%
80	HTTP (WWW)	4.6%	15%
1433	Microsoft SQL Server	2.9%	6.7%
3389	Microsoft Terminal Services	2.6%	4.3%
8080	HTTP Alternate	2.5%	5.5%
22	SSH	1.8%	3.4%
443	HTTPS (SSL)	1.3%	7.7%
3306	MySQL	1.1%	2.1%
8088	Radan HTTP	0.8%	0.5%
Various	Other	62%	–

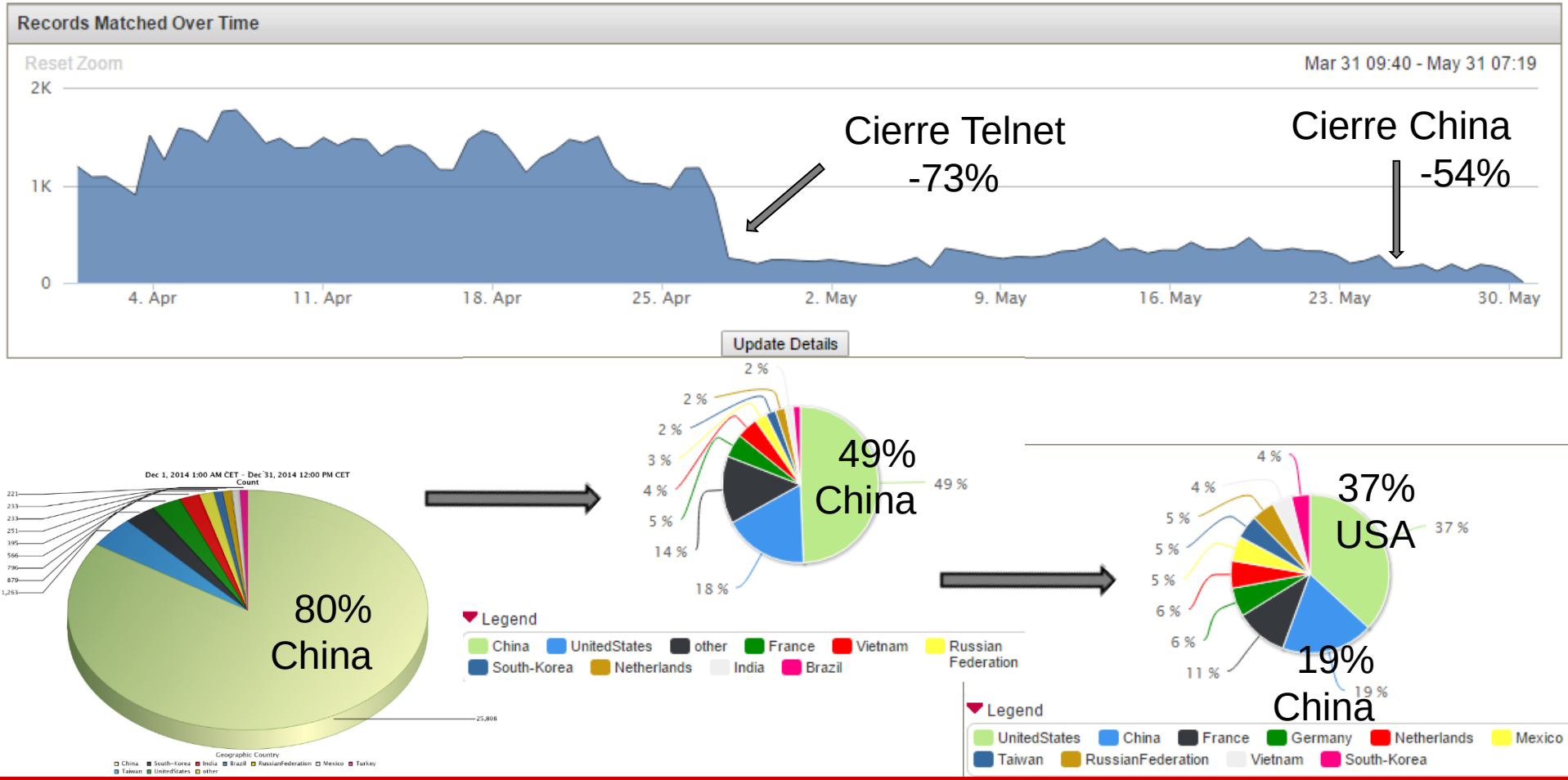
Avances

- **Cierre total de entrada:**
  - A rangos reservados y a subredes sin uso (nov 2014).
  - A subredes de técnicos SS.II. y dispositivos (ene 2015).
- **Cierre progresivo de puertos de entrada:**
  - NTP, SIP, UPnP, …
  - Últimos: **Telnet**, IAMT, IPMI, MongoDB, Elasticsearch API (27 abril 2016).
- **Cierre (parcial) progresivo de dominios con mayor número de ataques:**
  - De momento: China (25 mayo 2016).
  - Se cierra por defecto la entrada hacia la DMZ por puertos distintos a 80 y 443.

Mejoras de seguridad en la red de la UCM

Resultados

Número de cuarentenas de Internet



Futuros pasos en estudio

- Cierre de salida del tráfico DNS:
  - Por protección contra algunos troyanos.
  - Excepción para 8.8.8.8 y algunos otros servidores fiables de uso común.
- Cierre de entrada por fases:
  - 0. Continuar con el cierre de los puertos “cerrables” más atacados y de los dominios más atacantes.
  - 1. Cierre UDP, ICMP y otros.
  - 2. Cierre TCP excepto 22, 80, 443, 3389, otros (por ver).
  - 3. Cierre total de entrada con excepciones a servidores, paso a paso por subredes de clase C.
- ¡No es la panacea pero en seguridad todo ayuda!

Gracias por su atención.

¿Preguntas?

Mejoras de seguridad en la red de la UCM
II Foro de Redes de Campus - Córdoba

Luis Padilla

31 - mayo - 2016

Área de Infraestructura T.I.
Servicios Informáticos UCM