

Honeypots:

Defendiendo proactivamente a la comunidad.

ANTEL

TELECOMUNICACIONES

TELEFONIA BASICA - TELEFONIA PUBLICA - TELEFONIA CELULAR - DATOS - INTERNET

Natascha Martínez

natascha.martinez@csirt-antel.com.uy

Gonzalo Stillo

gonzalo.stillo@csirt-antel.com.uy

Carlos Martínez

carlos.martinez@csirt-antel.com.uy

- Presentar el proyecto honeypot del CSIRT-ANTEL a la comunidad de seguridad de LACNIC
- Presentar una exitosa aplicación de los datos recolectados con los honeypots desplegados por el CSIRT-ANTEL



- Introducción
- El proyecto HoneyPot del CSIRT- ANTEL
- Implementación en ANTEL
- Aplicaciones practicas
- Conclusiones

¿Quien es ANTEL?

- ANTEL: “La empresa de telecomunicaciones de los uruguayos”
 - Monopolio de la telefonía básica
 - Unidades de Negocio en competencia
 - Datos (ANTELDATA)
 - Celular (ANCEL)
- Operador dominante en el mercado en todas las áreas donde ofrece servicios
- Los clientes de ANTEL no escapan a la realidad de Internet hoy

¿Porque un Honeypot en ANTEL?

- Aumento en cantidad y en ancho de banda de servicios de Internet comercializados
- Como protegerse de los riesgos en Internet no son parte de las prioridades del usuario promedio de Internet
- Resulta relevante que desde los ISP se comiencen a tomar medidas proactivas de defensa

El proyecto Honeypot del CSIRT-ANTEL

- Comienza con la colaboración con el CERT.br en el año 2005
- Apoyo en la creación de honeypots y spampots
- Etapas
 - I. Aprendizaje
 - II. Implementación
 - III. Aplicaciones prácticas
 - Estadísticas
 - Servicio proactivo



(I) Aprendizaje

- Conocimiento mínimo del asunto
 - Sonaba divertido :)
- Que queríamos
 - Sistema con mantenimiento mínimo
 - Análisis “automatizable”.
- Clasificación de Honeypots
 - Baja interactividad
 - Media interactividad
 - Alta interactividad

(II) Implementacion

- Se elijo un honeypot de baja interactividad implementado con *honeyd*.

Características

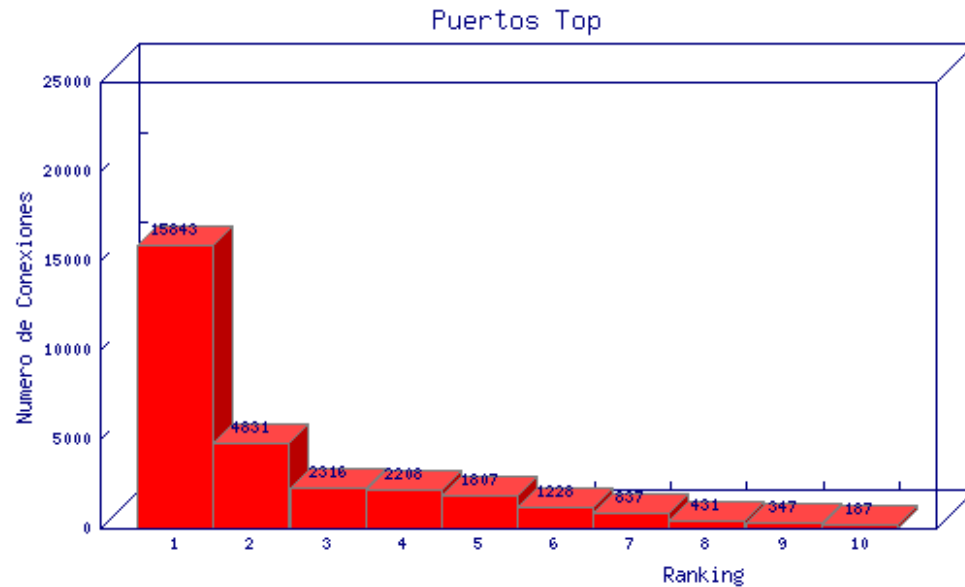
- No son sistemas reales, emula servicios y sistemas
- Fácil de configurar y mantener
- Información obtenida es limitada (IPs de origen, protocolos, puertos atacados)
 - Minimiza la posibilidad de compromiso del sistema operativo real del honeypot
- Hay riesgo de atraer “atacantes” hacia nuestra red

(III) Aplicaciones Practicas

- Dar el difícil paso de la mera recolección de datos a aplicarlos en algo útil para la comunidad del CSIRT-ANTEL
- Mencionaremos
 - Estadísticas
 - Servicio pro-activo de alerta

Aplicaciones - Estadísticas

Top 10 Puertos Accedidos		
Ranking	Puerto	Conexiones
1	1433/tcp	15843
2	135/tcp	4831
3	445/tcp	2316
4	139/tcp	2208
5	22/tcp	1807
6	137/udp	1228
7	8/icmp	837
8	1026/udp	431
9	1027/udp	347
10	5900/tcp	187



<http://www.csirt-antel.com.uy/datos-honey>

Aplicaciones – Reportes IP UY

- Son un resumen de los intentos de conexión a los Honeypots del CSIRT-ANTEL en un determinado día.
- Solo se analizan las conexiones realizadas desde direcciones IP publicas asignadas a ANTEL
- Se busca identificar equipos de servicios comercializados por ANTEL, posiblemente comprometidos

Aplicaciones – Reportes IP UY (2)

- Procedimiento diario:
 - Se busca el reverso en los DNSs de ANTELDATA de las direcciones IP que aparecieron en el honeypot para ver a que tipo de servicio corresponde y se envia reporte por email
 - Desde el momento en que se detecta que es un servicio con IP fija (típicamente un cliente empresarial) el triage abre un ticket de incidente
 - Se hace la consulta a quien tiene el contacto técnico del cliente (en este caso O&M ANTELDATA) y luego se contacta al mismo (vía mail o telefónica) explicandole la situación.

Aplicaciones – Reportes IP UY (3)

REPORTE CSIRT honeyd.log.2008-06-26-07:00

Las siguientes IPs del rango para ANTEL intentaron conectarse con el honeypot

200.40.24.167	= r200-40-24-167-dialup.adsl.anteldata.net.uy.
200.40.73.237	= r200-40-73-237-dialup.adinet.com.uy.
200.40.75.15	= r200-40-75-15-dialup.adinet.com.uy.
200.40.75.166	= r200-40-75-166-dialup.adinet.com.uy.
200.40.66.80	= r200-40-66-80-dialup.adinet.com.uy.

200.40.74.192	= r200-40-74-192-dialup.adinet.com.uy.
200.40.71.248	= r200-40-71-248-dialup.adinet.com.uy.
200.2.47.79	= r200-2-47-79-dialup.adinet.com.uy.
200.40.75.194	= r200-40-75-194-dialup.adinet.com.uy.
200.40.74.199	= r200-40-74-199-dialup.adinet.com.uy.
...	

Aplicaciones – Reportes IP UY (4)

Experiencia novedosa

ANTEL avisa **PROACTIVAMENTE** a sus clientes que algo anda mal en algún elemento de su red.



Aplicaciones – Reportes IP UY(5)

- Buena reacción de los clientes
- Hay varios casos de éxito con clientes empresariales de ANTEL DATA
 - Comprometimientos en servidores web, servidores de mail, etc.
- Al poco tiempo de ser notificados, las IPs generadoras de esos intentos de conexión desaparecen de los registros del honeypot
- En principio se notificaba a TODOS los clientes empresariales que aparecían en el honeypot

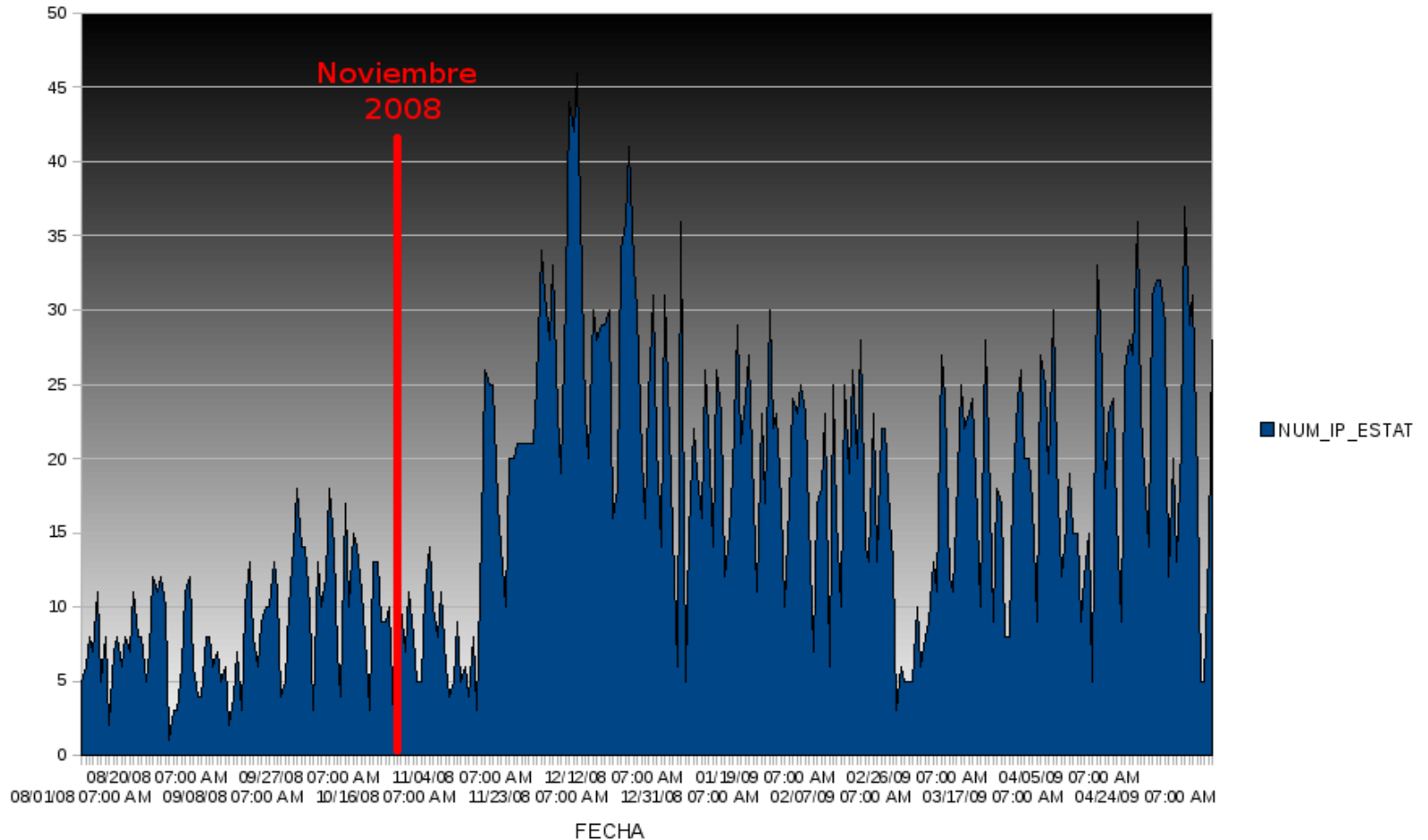
Pero en octubre 2008...

Microsoft Security Bulletin MS08-067:

- Vulnerability in Server Service Could Allow Remote Code Execution (October 23, 2008)
- Critical: Microsoft Windows 2000, Windows XP, Windows Server 2003
- Important: Windows Vista and Windows Server 2008



¿Como afecto el MS08-067 al servicio?



Conclusiones

- Se puede hacer mucho con relativamente poco
- Permite intercambiar datos con otros centros de respuesta a incidentes y corroborar tendencias
- Novel experiencia donde se establece una relación interactiva con el cliente donde en caso de problemas el primer llamado no lo hace el cliente
- Los datos estadísticos son de nuestra realidad
 - Se puede trabajar para prevenir y reaccionar ante problemas de nuestro entorno

- IPv6
 - Mejorar “infraestructura” de análisis
P.ej: Usando bases de datos para almacenamiento
 - Hacer intercambio con otros CSIRTs o CERTs usando IODEF (RFC 3067) y/o IDMEF (RFC 4765)
 - Probar Sebek u otros honeyopots de G.III
<https://projects.honeynet.org/sebek/>
- Etc, etc, etc...

¿PREGUNTAS?



¡Gracias!

¡Gracias por su atención!

