

Amenazas en Internet

- El tipo de amenazas que encontramos en Internet está cambiando de foco
- Antes...
 - Prevalencia de virus y gusanos
 - *Slammer, CodeRed*
- Ahora...
 - Virus, gusanos, troyanos y otros "personajes" pero operando como herramientas para obtener ganancias

La "Inseguridad" del Software

- ¿Qué factores hacen posible todo esto?
 - La propia naturaleza humana en primer lugar
 - Los usuarios de Internet en general no le dan un lugar prioritario a la seguridad de sus PCs
 - Siempre hay "elementos" buscando obtener ganancias fáciles a cuesta de otros
 - La propia naturaleza del software
 - Hacer software no es fácil, se parece mucho más a un arte que a una ciencia
 - La seguridad en un proyecto es algo que en general se considera sólo al final del mismo, o veces luego!, en general motivado por un incidente de seguridad

¿Para Qué Tomarse Este Trabajo?

- Primera etapa
 - Demostrar conocimiento, obtener prestigio personal en ciertos ámbitos
- Segunda etapa
 - Diseminación de información
 - "a ciegas", en general enviando trozos de documentos a direcciones de correo electrónico
- Tercera etapa
 - Obtención de ganancias económicas
 - *Phishing, DDoS*

ANTEL

Botnets

- Una "botnet" está formada por un conjunto de sistemas comprometidos (*zombies* o *herd*) y bajo el control de un operador central (*bot herder* o *bot master*)
 - "robot" + "network"
- En cada sistema comprometido hay instalado alguna forma de *malware* que permite al operador controlarlo
- Se compran, se venden, se alquilan "customizadas"
 - news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf

ANTEL

Utilización de una Botnet

- Envío de correo electrónico no solicitado (*spam*)
- Ataques de DDoS
- Phishing
- Instalación de *adware*
- Sniffing de tráfico
- Keylogging
 - Guardar las "teclas" pulsadas por el usuario y enviar esa información al "bot herder"
- Fraude del clic
 - Generación de clicks fraudulentos a herramientas de promoción en Internet (Google, Yahoo)

ANTEL

DDoS

- DDoS: *Distributed Denial of Service* o "ataques de denegación de servicio distribuidos"
 - Nombre por el cual se conocen a ataques que provienen de una nube "difusa" de direcciones IP con destino a un blanco único
 - Generación de suficiente tráfico como para saturar enlaces WAN y servidores

Estonia recovers from massive DDoS attack
Denial-of-service onslaught may have Russian origins

Jeremy Kirk, *Today's Top Stories* - [in Other Security Stories](#)

Comments (0) | [Recommendations \(0\)](#) | [Recommend this article](#)

May 12, 2007 (DDoS News Service) - A spate of denial of service attacks against Web sites in Estonia appears to be subsiding as the government calls for greater response mechanisms to cyber attacks within the European Union.

The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and local media sites using email, website, and Web-based cloud security office for Estonia's Computer Emergency Response Team (CERT). But most of the off-the-grid sites have been able to reach CERT.

"It's not a serious problem but we are up and running," Aar-Saß said.

Developer
 October 11, 2006
 Multiple DDoS Attack Hit 1000 Web Servers
 by Ryan Soper
 A massive distributed denial of service (DDoS) attack (DDoS) of unknown origin today overwhelmed Web traffic on one of the 11 DDoS "hot" servers that NetworkWatch Internet Ltd reports on Wednesday. Downfall the world's largest...

ANTEL

Botnets para DDoS

- Lanzamiento de un DDoS utilizando una *botnet*

El diagrama ilustra el proceso de un ataque DDoS. Un operador (Hacker/Operador) envía un comando "atacar víctima X" a una botnet (miembros de la botnet) que se encuentra en la Internet. Cada bot dentro de la botnet bombardea a la víctima, lo que resulta en que la víctima quede fuera de servicio.

ANTEL

Honeypots

- En términos muy generales:
 - *Un honeypot es un recurso de red cuyo valor mismo es el de ser atacado o vulnerado. Los beneficios se obtienen mediante mantener un cuidadoso monitorizado del mismo.*
- En resumen
 - Ofrecer un blanco interesante
 - Observarlo
 - Sacar conclusiones

ANTEL

Honeypots

- Taxonomía:
 - Baja interacción
 - Interacción limitada, servicios y topologías emuladas
 - Sencillos de utilizar y mantener. Bajo riesgo.
 - Alta interacción
 - Interacción con sistemas reales (S.O.'s, hardware)
 - Más complejos de mantener. Algún riesgo.

Honeynets

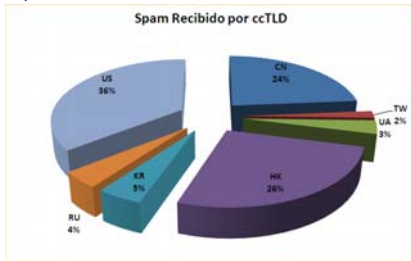
- Un *honeypot* individual tiene visibilidad limitada sobre un rango (usualmente pequeño) de direcciones IP
- Honeynets
 - Instalar *honeypots* de la forma mas distribuida posible
 - Colectar información de los mismos
 - Realizar correlación de eventos y comparar información

Spampots

- Idea similar a la de la honeynet pero aplicada al problema del spam (correo electrónico no solitado)
- Todo el tráfico que pasa por él, es spam

Resultados

- Spampot



Resultados

- Spampot



Proyectos de Colaboración

- Las iniciativas presentadas han surgido en un entorno de inserción internacional
 - Membresía FIRST
 - Colaboración con CERT.br
- A futuro
 - AusCERT
 - Otros



Vinculación institucional del CSIRT

- El nacimiento del CSIRT ANTEL se favoreció por la existencia de un Sistema de Gestión de Seguridad de la Información.
- Marco normativo.
 - Políticas de Seguridad de la Información.
 - Procedimientos de Gestión de Incidentes.
- Medio ambiente favorable.
 - Propensión a la investigación en la organización.
 - Cercanía con el ambiente académico.
 - Aidez de los involucrados en los temas de seguridad.

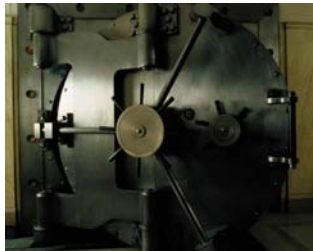
Ejemplos de Incidentes de Seguridad

- Pérdida de integridad de documentos en el Banco Central de Uruguay
- Pérdida de datos de estudiantes en Instituto Universitario en Uruguay
- Extorsión para evitar difusión de bases de datos de tarjetas de crédito internacionales (American Express y otras...)
- Ataques de Denegación de Servicio a ISP
- Basados en Ingeniería social
 - Phishing, a diversas entidades bancarias en y desde Uruguay.
 - SCAM (Nigeria - "Four - One - Nine")

Seguridad de la Información

Definición

- Integridad
- Confidencialidad
- Disponibilidad



Seguridad de la Información

Medidas de seguridad

- Lógicas (*Seguridad lógica*)
- Físicas (*Seguridad física*)
- Ambiental (*Seguridad ambiental*)



ANTEL

Riesgos e impactos

Amenazas



Inherentes:

- Soporte TI
- RRHH
- Entorno
- Medio ambiente

ANTEL

Riesgos e impactos

Amenazas



Inherentes:

- Soporte TI
- RRHH
- Entorno
- Medio ambiente

Origen de la debilidad



Tecnológico

- Recursos Humanos
- Prácticas operativas

Ataque / Falla

- [Hacking](#)
- IP spoofing
- [Virus](#)
- Enmascaramiento
- Spamming
- Caballo de Troya
- Fallas del equipamiento
- Falla de las telecomunicaciones
- Piratería de software

ANTEL

Riesgos e impactos

Amenazas



Inherentes:

- Soporte TI
- RRHH
- Entorno
- Medio ambiente

Origen de la debilidad



Recursos Humanos

- Tecnológico
- Prácticas operativas

Ataque / Falla

- Falta de capacitación
- Errores
- Fraudes
- Negligencia

ANTEL

Riesgos e impactos

Amenazas	Origen de la debilidad	Ataque / Falla
 <p>Inherentes:</p> <ul style="list-style-type: none"> • Soporte TI • RRHH • Entorno • Medio ambiente 	 <p>Tecnológico</p> <p>Recursos Humanos</p> <p>Prácticas operativas</p>	<ul style="list-style-type: none"> • Caballo de Troya • Ingeniería social • Ataques contra la privacidad de los datos • Fraude operativo • Piratería de software

ANTEL

Capítulos de la Política de Seguridad

1. Política de Seguridad
2. Organización de la Seguridad de la Información
3. Gestión de Activos
4. Seguridad de Recursos Humanos
5. Seguridad Física y del Ambiente
6. Gestión de Comunicaciones y Operaciones
7. Control de Acceso
8. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
9. Gestión de Incidentes de la Seguridad de la Información
10. Gestión de la Continuidad del Negocio
11. Cumplimiento

ANTEL

Contribución al Gobierno Electrónico

- AGESIC
 - Constitución del Comité de Seguridad Informática
 - Constitución e implementación del CERTuy
- Promoción y desarrollo de recursos humanos a nivel nacional
- Prevención y protección de las infraestructuras críticas nacionales
- Inserción y respuesta internacional del Uruguay al combate del *cyber-delito*

¡Muchas gracias por su atención!

Eduardo.Carozo@csirt-antel.com.uy
Leonardo.Vidal@csirt-antel.com.uy

ANTEL

www.antel.com.uy
