Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para América Latina y Caribe
Registro de Endereços da Internet para América Latina e Caribe

PROYECTO *AMPARO*

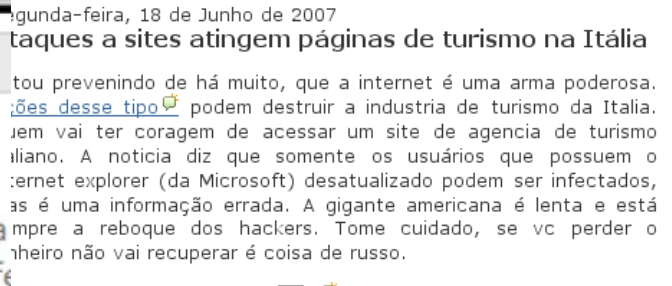
Fortalecimiento de la capacidad regional de atención de incidentes de seguridad en América Latina y el Caribe

Eduardo Carozo
LACNIC

Agenda

- Incidentes recientes en Internet
- Botnets
- DDoS
- Phishing
- ¿Por qué aprender del enemigo?
- Herramientas para lograrlo
- Algunos resultados obtenidos localmente
- Proyecto AMPARO

Incidentes recientes en Internet



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**
    - Se ha creado una "economía subterránea"

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
- Pero además…
  - **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

Malware

- Taxonomía del *malware*
  - **Medios de propagación**
    - Virus
    - Gusanos
    - Troyanos
  - **“Funcionalidad”**
    - Adware
    - Dialers
    - Backdoors
    - Proxies
    - Rootkits
    - Control Remoto

¿Cómo llegan a sus víctimas?

- Vecto
  - Pro
    - "v
  - Mec
    - "b
  - Troy
    - C
      re

SecurityFocus™ About

Home | Bugtraq | Vulnerabilities | Mailing Lists | Jobs | Tools | Beta Programs | Search:

News
Infocus
- Foundations
- Microsoft
- Unix
- IDS
- Incidents
- Virus
- Pen-Test
- Firewalls

Columnists
Mailing Lists
- Newsletters
- Bugtraq
- Focus on IDS
- Focus on Linux
- Focus on Microsoft
- Forensics
- Pen-test
- Security Basics
- Vuln Dev

PRINT EMAIL

Apple patches iPhone SMS vulnerability

Published: 2009-08-04

Consumer technology firm Apple issued a patch on Friday to fix a critical iPhone flaw that could have allowed attackers to execute code just by sending a specially-crafted text message.

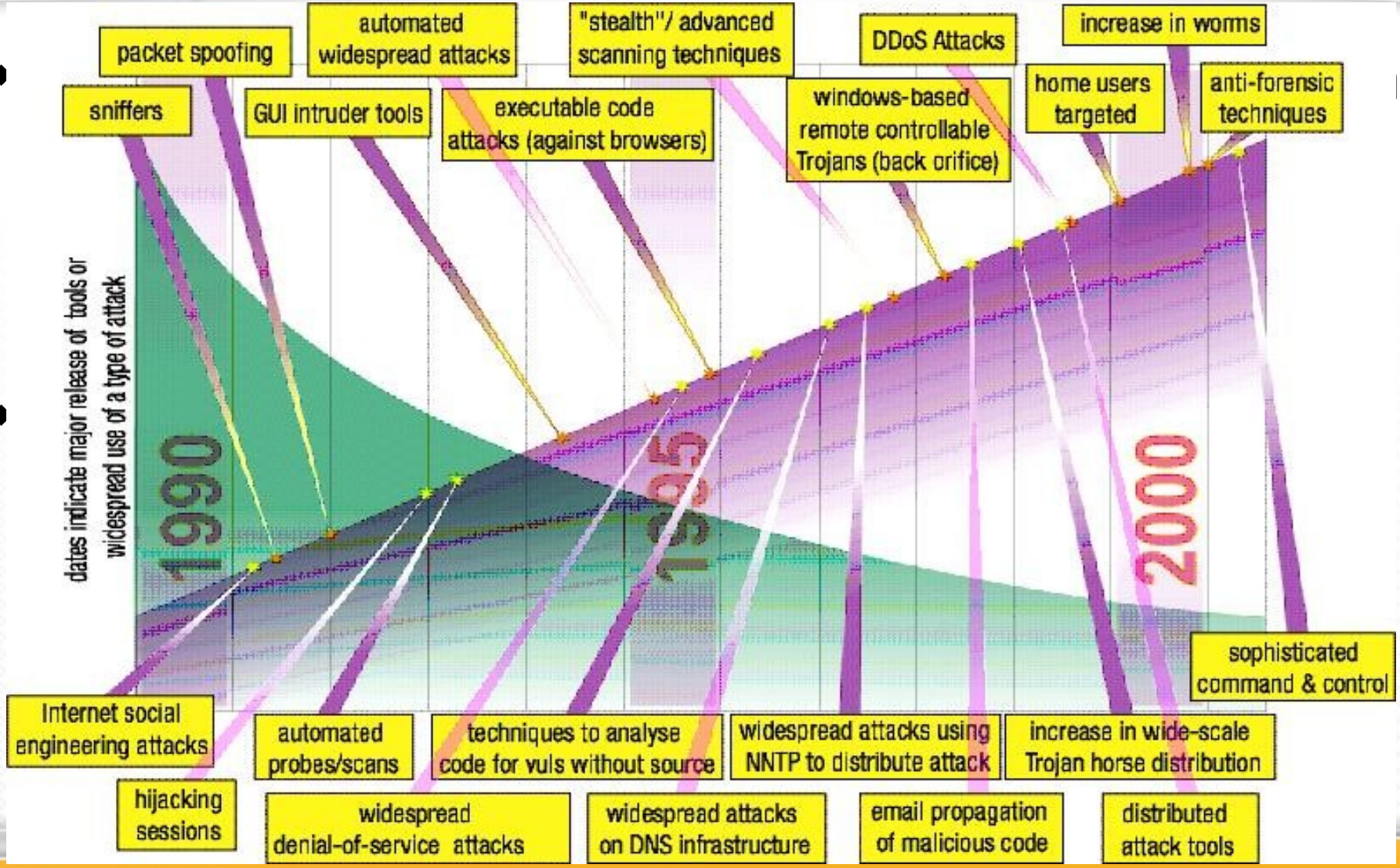
Charlie Miller, a consultant with Independent Security Evaluators, and Collin Mulliner, a PhD student at the Technical University of Berlin, presented the details of the vulnerability at the Black Hat Security Conference in Las Vegas last week. The memory-overflow issue could allow a minor crash or remote exploitation by sending a malicious text message to the iPhone over the short message service (SMS) available on all phones.

"Receiving a maliciously crafted SMS message may lead to an unexpected service interruption or arbitrary code execution," Apple stated in its advisory. "This update addresses the issue through improved error handling."

¿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, salas de chat, etc.
- Tercera etapa
  - **Obtención de ganancias económicas**
    - Phishing, DDoS

Integración



Botnets

- Una "*botnet*" está formada por un conjunto de sistemas comprometidos y bajo el control de un operador central
  - "*robot*" + "*network*"
- En cada sistema comprometido hay instalado alguna forma de *malware* que permite al operador controlarlo

Ciclo de Vida de una Botnet

- *Herding*
  - **Fase de crecimiento de la botnet**
  - **Ciclo de infección y agregado de nuevos bots**
  - **Cada nuevo bot**
    - Un PC es infectado o instala algún tipo de troyano
    - Búsqueda de blancos “cercanos” para propagar el bot
    - El bot levanta un canal de comando y control (C&C)
- **Equilibrio**
  - **La red no crece “activamente” pero si hay una permanente “lucha” entre malwares y se dan dinamicamente bajas y altas en la misma**
- **Utilización**
  - **Ingresa al “mercado underground” para su uso**

Utilización de una Botnet

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

La Economía Subterránea

Las botnets son un item adecuado para ser compradas, vendidas y alquiladas

- **Tienen flexibilidad para hacer diferentes cosas**
- **Se pueden controlar fácilmente**
- **Anonimizan…**

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 ▸ or Other Security Stories ▸

Comments (1) Recommendations: 35 — Recommend this article

May 17, 2007 (IDG News Service) -- A spree of denial-of-service attacks against Web sites in Estonia appears 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 less-trafficked sites run by small schools, said Hillar Aarelaid, chief security officer for Estonia's Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restor service.

"Yes, it's serious problem, but we are up and running," Aarelaid said.

internetnews.com

Regional News: Boston | D.C. | New York | Silicon Valley More Tech News: Newslinx

Business | Developer | Ecommerce | Enterprise | Networking | Security

Storage | Wireless | xSP | Special Reports | Stats | Commentary

you are in:

7 day summary PODCAST

Add the power and flexibility of SlickEdit to Eclipse. The SlickEdit Plug-In provides developers with a powerful set of symbol analysis and navigation tools to save time and maximize control over code.

Developer

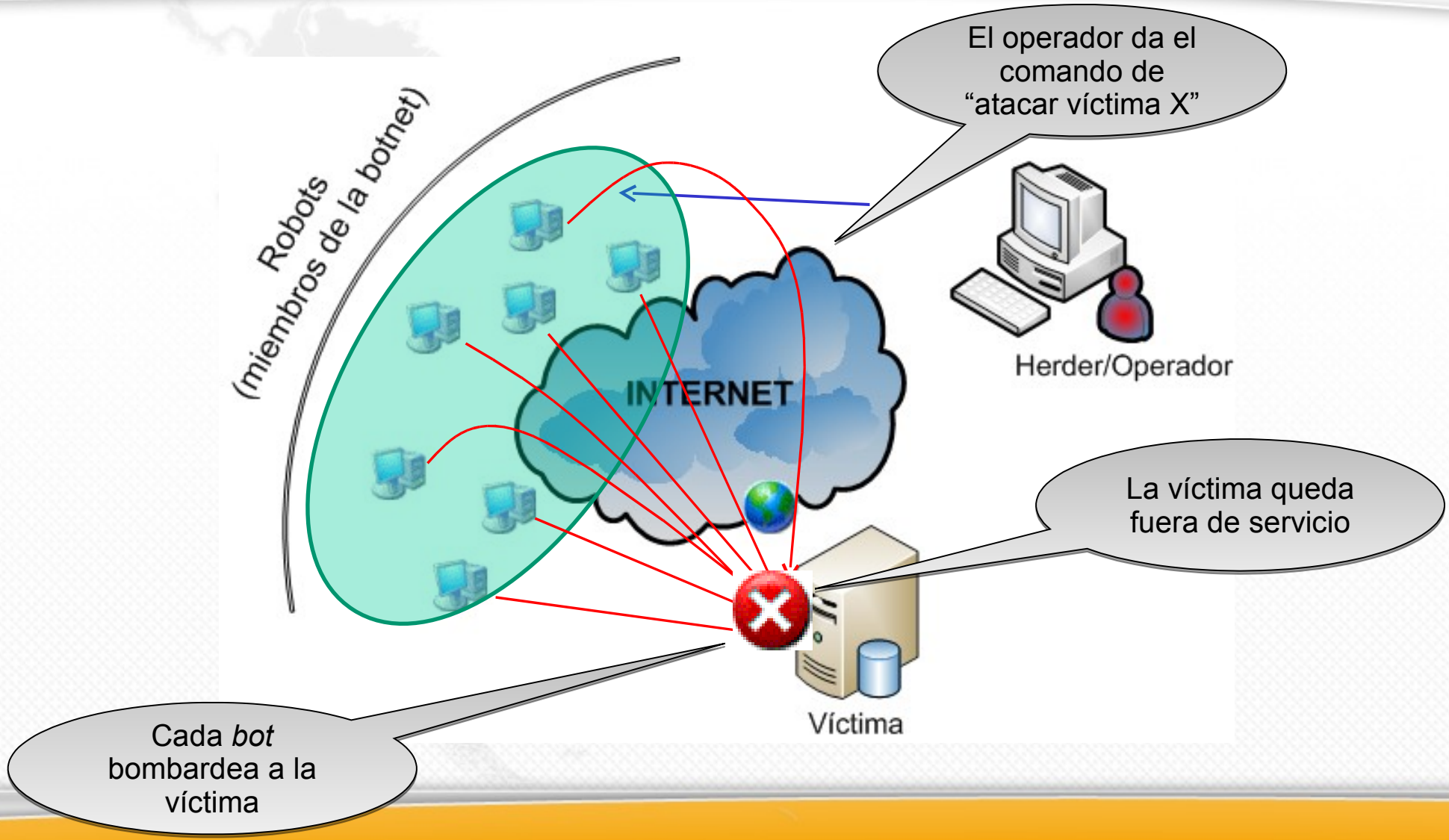
October 23, 2002

Massive DDoS Attack Hit DNS Root Servers

By Ryan Naraine

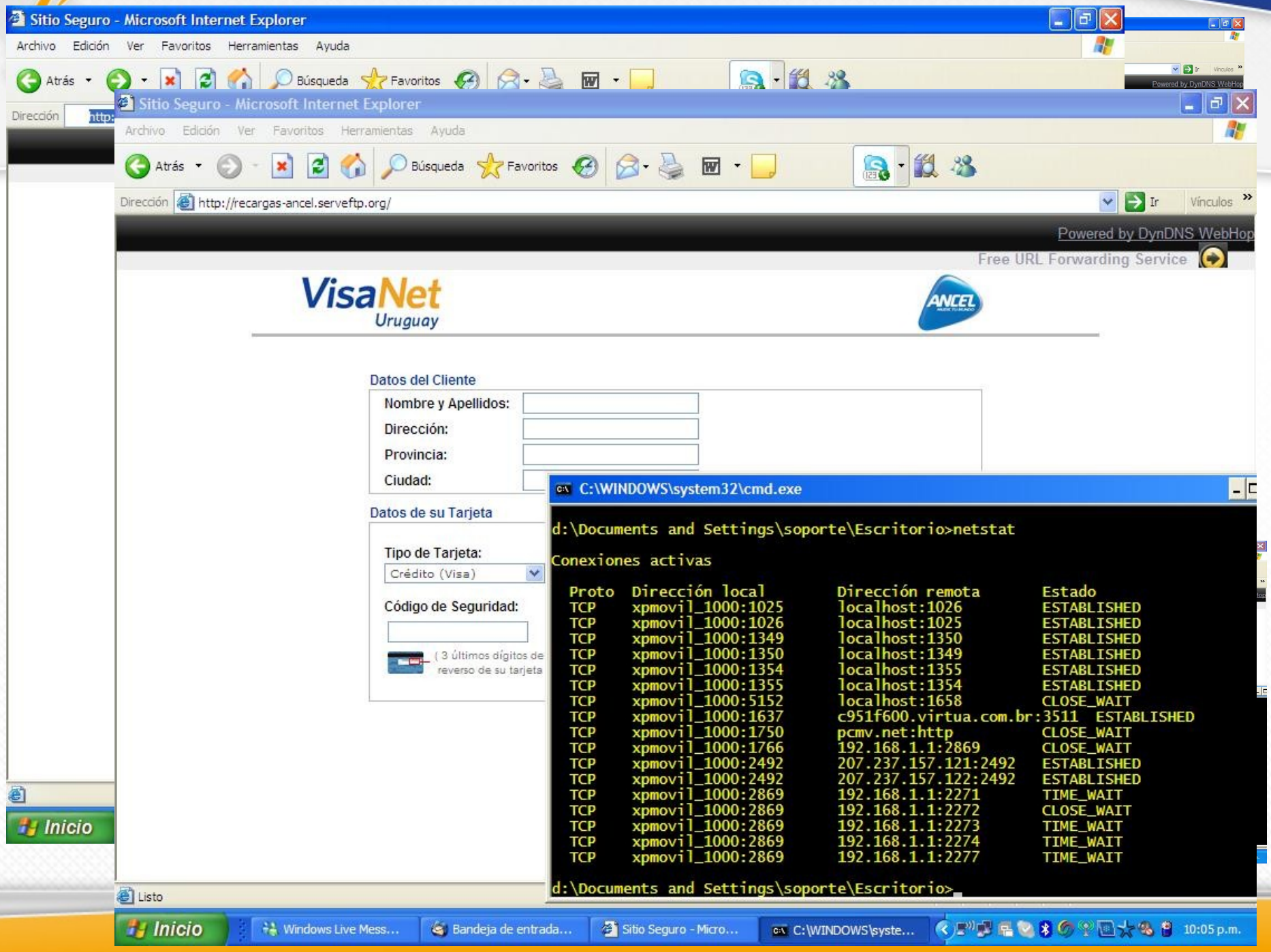
A massive distributed denial-of-service (DDoS) attack (define) of unknown origin briefly interrupted Web traffic on nine of the 13 DNS "root" servers that control the Internet but experts on Wednesday dismissed the overall threat as "minimal."

Botnets para DDoS

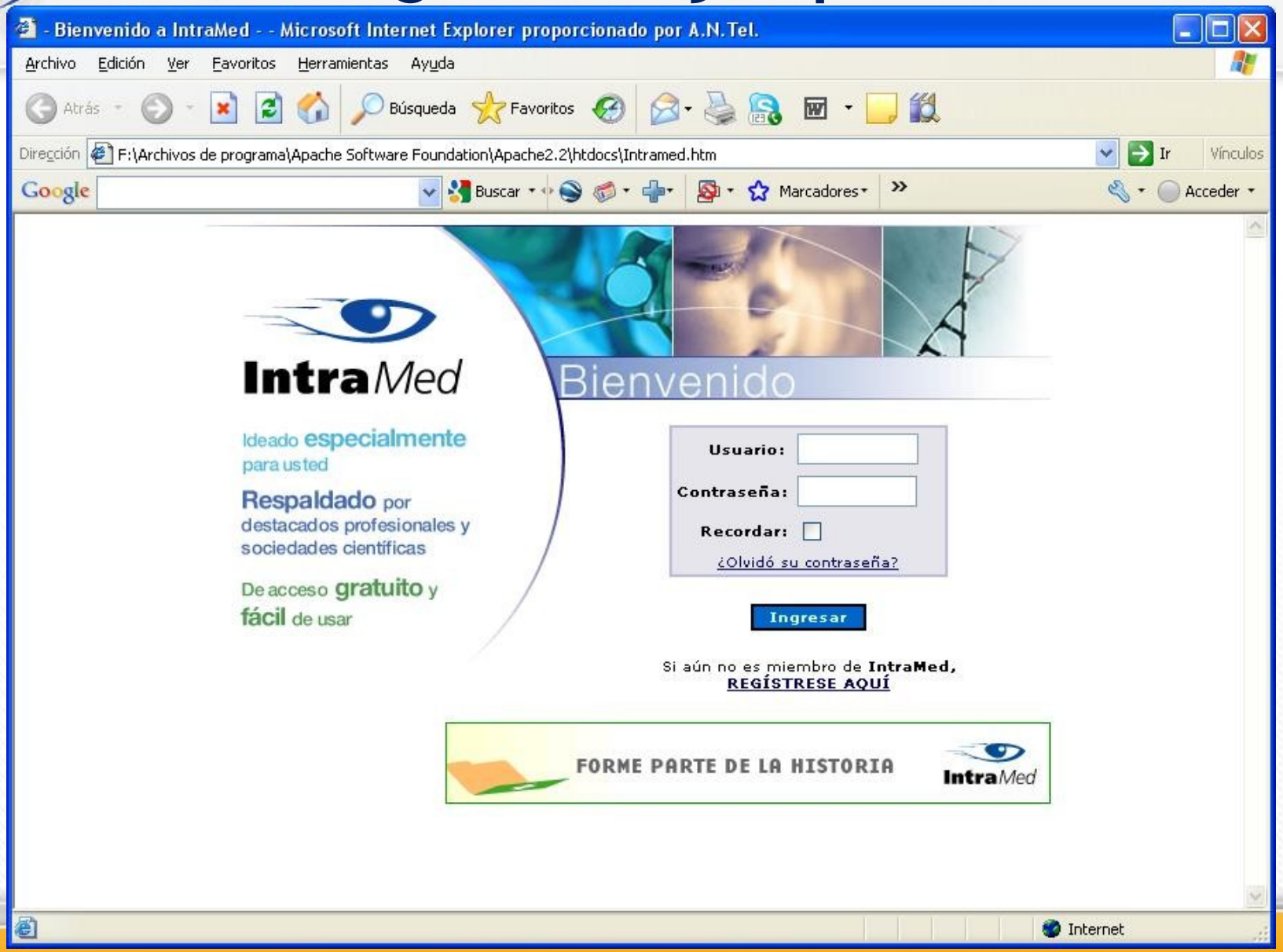


Phishing, secuencia de acciones

- Escaneo de vulnerabilidades de Equipos en Internet
- Captura de un servidor Web, preferentemente con IP fija
- Confección de páginas web dentro de esa URL, en el que se solicitan datos personales, se intenta el ingreso al sitio original, y en caso de acceder se deriva al cliente al mismo
- Creación de una casilla de correo para colectar dichos datos, así como la respuesta afirmativa/negativa de la validez de los datos contra el sitio original
- Creación de mensajes engañosos
- Envío de Spam, preferentemente con una Botnet


Sitio Seguro - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección http://recargas-ancel.serveftp.org/
Ir Vínculos
Powered by DynDNS WebHop
Free URL Forwarding Service
VisaNet Uruguay
ANCEL
Datos del Cliente
Nombre y Apellidos:
Dirección:
Provincia:
Ciudad:
Datos de su Tarjeta
Tipo de Tarjeta:
Crédito (Visa)
Código de Seguridad:
(3 últimos dígitos de reverso de su tarjeta
Listo
Inicio
Windows Live Mess...
Bandeja de entrada...
Sitio Seguro - Micro...
C:\WINDOWS\syste...
10:05 p.m.
C:\WINDOWS\system32\cmd.exe
d:\Documents and Settings\soporte\Escritorio>netstat
Conexiones activas
Proto Dirección local Dirección remota Estado
TCP xpmovil_1000:1025 localhost:1026 ESTABLISHED
TCP xpmovil_1000:1026 localhost:1025 ESTABLISHED
TCP xpmovil_1000:1349 localhost:1350 ESTABLISHED
TCP xpmovil_1000:1350 localhost:1349 ESTABLISHED
TCP xpmovil_1000:1354 localhost:1355 ESTABLISHED
TCP xpmovil_1000:1355 localhost:1354 ESTABLISHED
TCP xpmovil_1000:5152 localhost:1658 CLOSE_WAIT
TCP xpmovil_1000:1637 c951f600.virtua.com.br:3511 ESTABLISHED
TCP xpmovil_1000:1750 pcmv.net:http CLOSE_WAIT
TCP xpmovil_1000:1766 192.168.1.1:2869 CLOSE_WAIT
TCP xpmovil_1000:2492 207.237.157.121:2492 ESTABLISHED
TCP xpmovil_1000:2492 207.237.157.122:2492 ESTABLISHED
TCP xpmovil_1000:2869 192.168.1.1:2271 TIME_WAIT
TCP xpmovil_1000:2869 192.168.1.1:2272 CLOSE_WAIT
TCP xpmovil_1000:2869 192.168.1.1:2273 TIME_WAIT
TCP xpmovil_1000:2869 192.168.1.1:2274 TIME_WAIT
TCP xpmovil_1000:2869 192.168.1.1:2277 TIME_WAIT
d:\Documents and Settings\soporte\Escritorio>

Phishing: otros ejemplos



Phishing: ejemplo de correo

¿Por Qué Aprender del Enemigo?

- **Problemas con las tácticas tradicionales de defensa**
  - **Aproximación tradicional a la identificación de amenazas basada en "*identificar lo ya conocido*"**
    - Sistemas basados en firmas (*signatures*)
      - Antivirus, IDS/IPS
  - **El desarrollo de firmas para sistemas no abiertos depende del ciclo de desarrollo de los proveedores**
    - Que se denuncien los problemas
    - Que se desarrollen y se distribuyan las firmas
  - **Estamos protegidos de lo "*ya conocido*", pero, ¿Qué pasa con lo desconocido?**

¿Por Qué Aprender del Enemigo? (2)

- Cambio de foco de los atacantes: *atacar directamente a las aplicaciones*
  - **Es donde hay mas para ganar**
  - **Además de o apoyándose en el virus/gusano/troyano "masivo" tradicional**
- En ciclo de aprender-responder-prevenir, pasar a estar un paso mas adelante

Herramientas para Lograrlo

- Técnicas de tipo forense
  - **Análisis de artefactos**
    - Artefactos: archivos (ejecutables, textuales) encontrados en computadores que han sido comprometidos
- Técnicas de tipo “activo”
  - **Las técnicas activas se basan en general en ofrecer un blanco que parezca interesante pero que este cuidadosamente monitorizado**
  - **Ejemplos**
    - Honeypots
    - Spampots
    - Darknets

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 monitoreo del mismo.***
- En resumen
  - **Ofrecer un blanco interesante**
  - **Observarlo**
  - **Sacar conclusiones**

Honeypots (2)

- **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.
- **Herramientas disponibles**
  - **Baja interacción**
    - "honeyd" (http://www.honeyd.org)
      - Orientado a emular redes, hosts y enlaces
    - "mwcollect" y "nephentes" (http://mwcollect.org)
      - Orientados a emular vulnerabilidades conocidas y tratar obtener los ejecutables que los atacantes tratan de instalar

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**
  - **Correlacionar eventos y comparar información**

Ejemplo B.I.: “honeyd” (2)

- Servicios para los que existen emulaciones:
  - **SMTP**
  - **POP3**
  - **TELNET**
  - **HTTP**
    - Apache
    - IIS
  - **Open proxies**
    - HTTP / Squid
    - SOCKS v4 /v5

Spampots

- Idea similar a la del honeypot, pero aplicada al problema del spam (correo electrónico no solicitado.)
- Características deseadas:
  - **Emular los servicios buscados por los *spammers:***
    - SMTP “open relay”
    - Proxies abiertos
  - **Almacenar todo el correo electrónico que pasa por él**
  - **Tratar de “engañar” lo mas posible a los spammers**
    - Buscar superar las pruebas de verificación que ellos realizan
  - **Sencillo de instalar, mantener, operar. Robusto.**

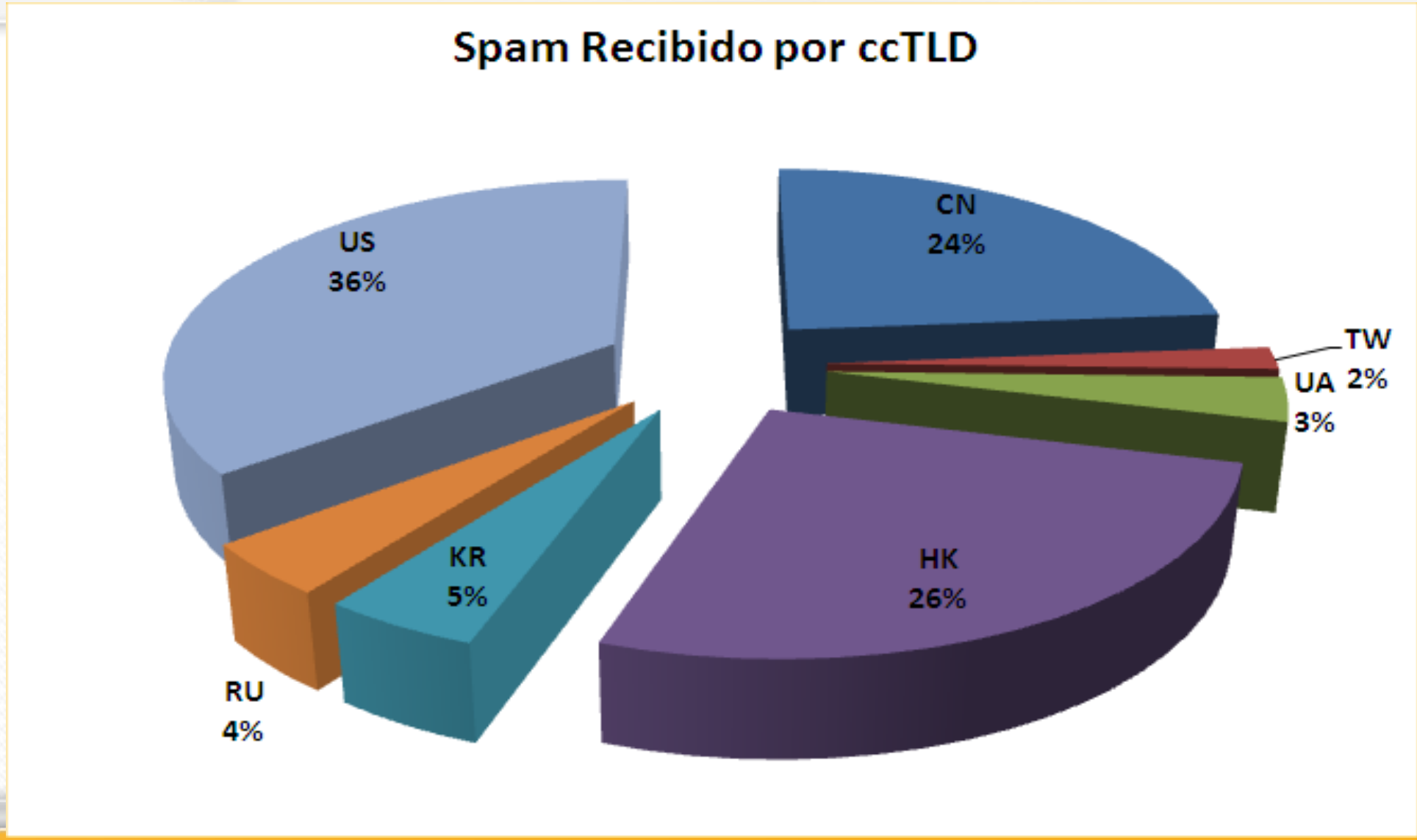
Spampots (2)

- Clasificación del tráfico de correo:
  - **Todo el tráfico de correo que pasa a través del spampot es correo no solicitado**
  - **De ninguna forma tráfico legítimo circula por él**
    - De esta forma la propia naturaleza del spampot resuelve uno de los problemas mas difíciles que presenta la lucha contra el Spam
  - **CERT.br ha sido soporte fundamental en el desarrollo de este sensor, y es un claro ejemplo de colaboración entre centros de respuesta**

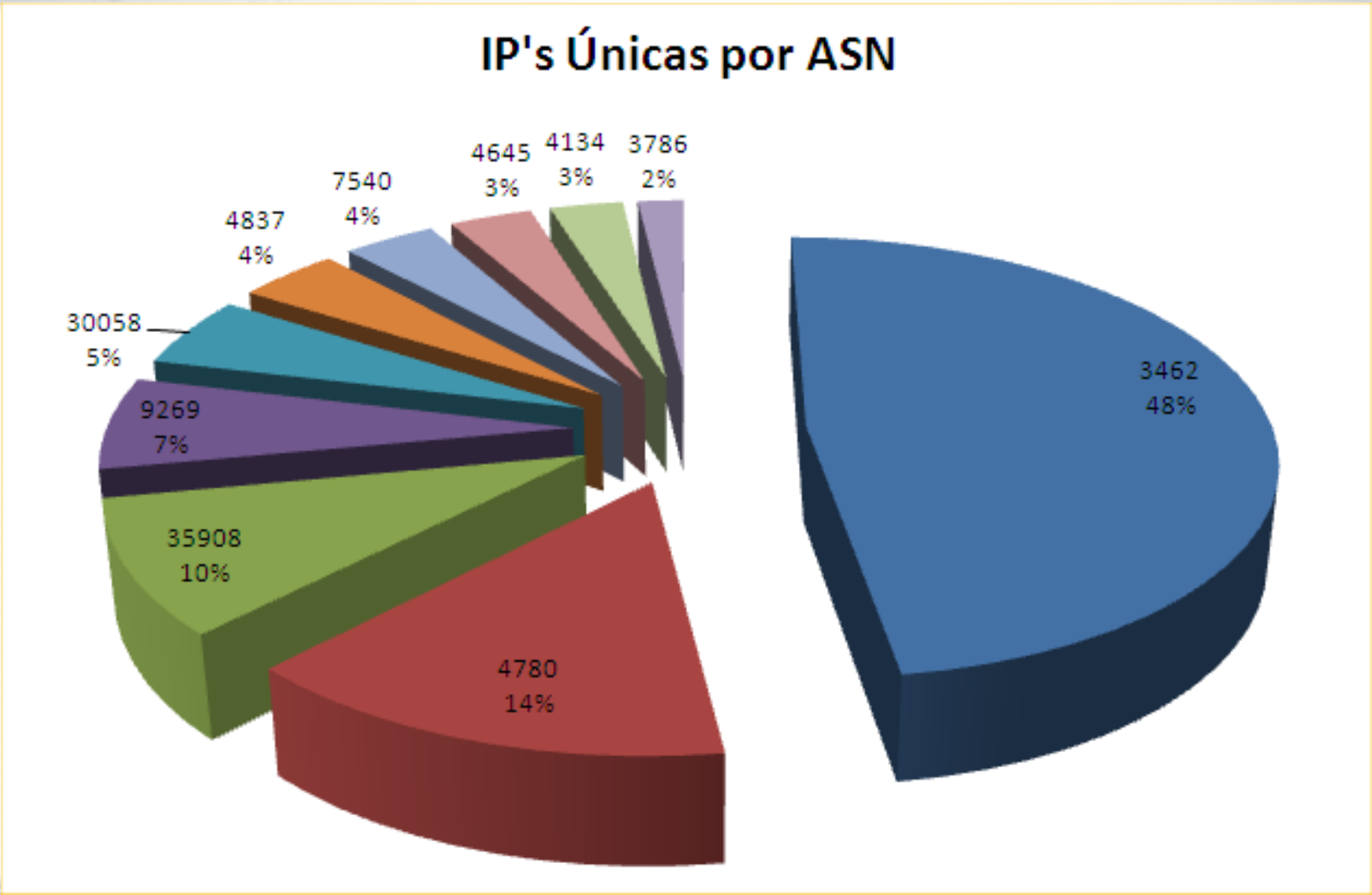
Resultados (1)

- Spampot, en sus primeros diez días de operación en nuestro CSIRT (CSIRT-Antel)
  - **2.362.213 de correos spam individuales**
  - **12.620.655 de destinatarios individuales identificados**
  - **6.2 gigabytes comprimidos de información capturada**
  - **Limitado por el ancho de banda asignado (256 kbps)**
  - **317 direcciones IP diferentes identificadas**

Resultados (2)



Resultados (3)



Darknets (2)

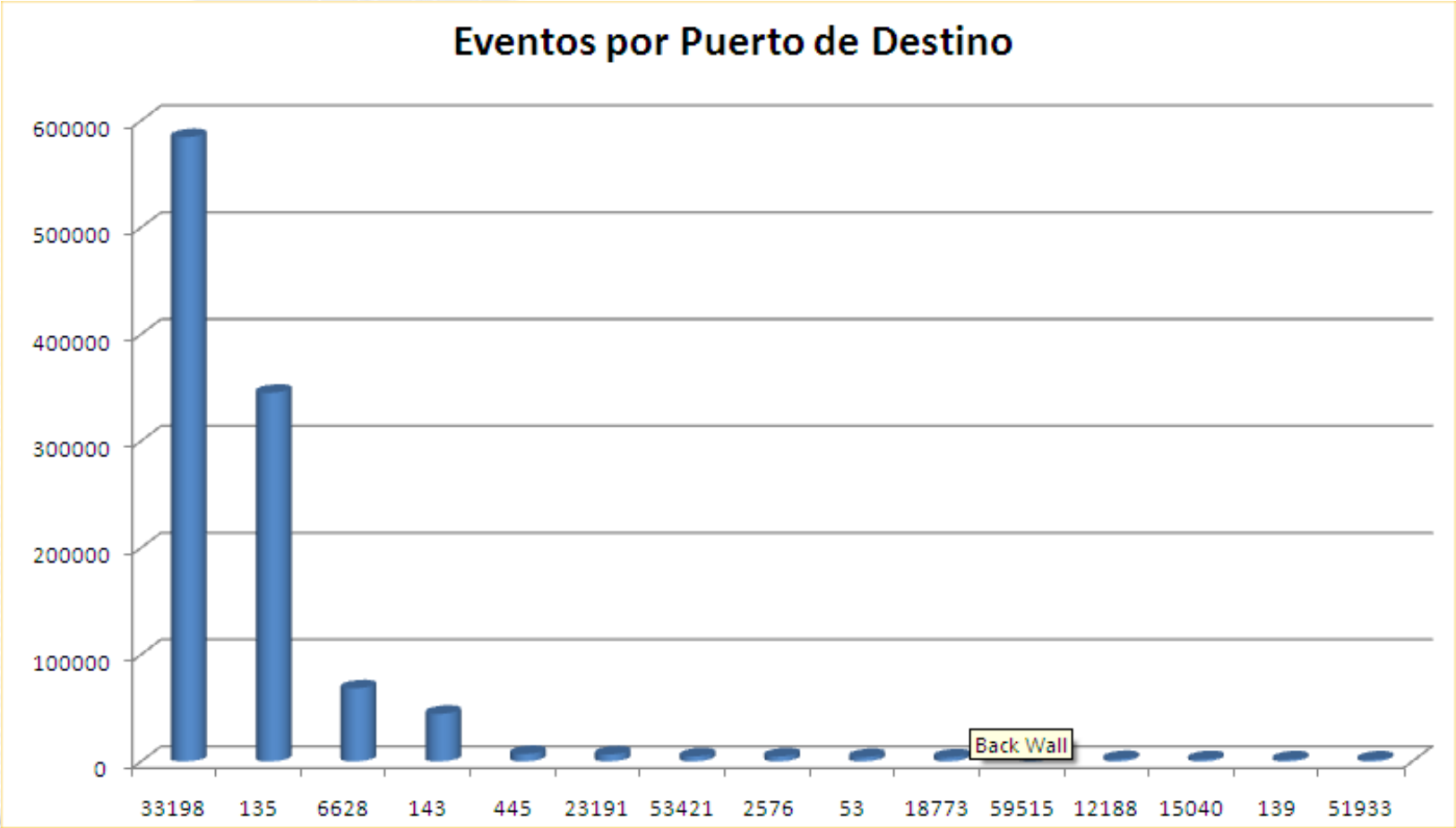
- **Darknet:**
  - **Destinar una pequeña parte del espacio en reserva, distribuido inteligentemente y "escuchar" el tráfico que llega a él**
  - **No responder nada**
    - No ICMP "*unreachables*" o "*TTL exceeded*" por ejemplo
  - **Colectar**
  - **Analizar**

Piloto “Darknet”

- Configuración muy mínima:
  - **Un único sensor**
  - **Una única dirección IP monitorizada**
- Algunos resultados primarios
  - **1.514.007 eventos capturados en 15 días**
    - Cada paquete dirigido a la IP monitorizada cuenta como un evento
  - **Los puertos que son “probados” exhiben una concentración importante**
    - Los 30 mas activos concentran el 72% de todos los eventos
  - **Las direcciones IP de origen en cambio tienen una cola mucho mas pesada**
    - Las 30 mas activas apenas el 8.9% de todos los eventos

Resultados (4)

- Darknet



PROYECTO AMPARO

Fortalecimiento de la capacidad regional de atención de incidentes de seguridad en América Latina y el Caribe

LACNIC

Objetivo general

Aumentar la capacidad regional de prevenir la ocurrencia de incidentes de seguridad informática y responder pronta y efectivamente, proveyendo a las naciones y organizaciones relevantes de la región de una capacidad de protección proactiva y dotarlas de mayor resiliencia frente a ataques informáticos de alto impacto.

Objetivos específicos

- Desarrollar actividades de investigación aplicada que apoyen los procesos y prioridades regionales;
- Promover la creación de CSIRTs nacionales y a nivel de grandes organizaciones del sector público y privado de los diferentes países de la región;
- Construir una plataforma regional de capacitación de expertos en Seguridad Informática;
- Contribuir a la constitución de un CSIRT Regional, que potencie las iniciativas de la región, proveyendo una red de confianza para el intercambio de información, frente a la ocurrencia de incidentes.

Que es un CSIRT?

- Un conjunto de técnicos entrenados para resolver incidentes de seguridad informática masivos
- Deben disponer de conocimientos actualizados de seguridad y redes, y sobre todo contactos con la comunidad que detecta y responde a incidentes
- Deben lograr un nivel de legitimidad tal en su comunidad, como para que las organizaciones o personas afectadas confíen a dicho Team información confidencial en el peor momento!
- Son en su accionar muy similares a un equipo de bomberos de alta especialización

Estrategias de desarrollo del Proyecto AMPARO

- Investigación Regional. Promover la creación de una plataforma de cooperación y coordinación en investigación
- Creación de capacidades regionales. Diseñar un programa regional de capacitación en creación y gestión de CSIRTs, incluyendo el desarrollo de materiales y guías metodológicas para los instructores.
- Formación de formadores. Propiciar la formación de un grupo de profesionales de la región que puedan actuar como instructores

Estrategias de desarrollo del Proyecto AMPARO

- Capacitación a escala. Desarrollar un conjunto de cursos-talleres en la región atendida por LACNIC en base al programa de capacitación diseñado
- Bases para la formación de un CSIRT Regional. Identificar buenas prácticas y proponer un modelo para la creación de una organización de seguridad de segundo nivel.

Componentes del Proyecto

- **Plataforma regional de investigación en ciberseguridad**.
- Se promoverá la conformación de una red de expertos en seguridad e investigadores centrada en el intercambio y desarrollo de conocimiento sobre los problemas actuales y emergentes de ciberseguridad y sus formas de prevención y control
- **Elaboración de materiales de capacitación de uso público**
- Se desarrollarán materiales para el entrenamiento, los mismos serán de uso público y de libre disponibilidad, contemplando debidamente los aspectos relativos a la propiedad intelectual y referencias.

Componentes del Proyecto

- **Formación de formadores**.
- El proyecto implica la formación de expertos con las habilidades adecuadas para capacitar a nuevos grupos de profesionales en los países de la región.
- **Realización de las primeras ediciones de capacitación**
- Se brindarán las primeras ediciones de capacitación, con el objetivo de difundir los contenidos y ajustarlos a las necesidades del proyecto.
- **Identificación de líderes y financiamiento para la explicitación de buenas prácticas en la región**

Componentes del Proyecto

- **Análisis de la formación de un CSIRT de segundo nivel**
- Se realizará un análisis que incluirá aspectos de pertinencia, aceptabilidad, financiamiento, etc.

Resultados esperados

- Una agenda regional de prioridades de investigación en Seguridad Informática disponible
- Materiales para la capacitación de expertos en creación y operación de CSIRT disponibles
- Talleres regionales realizados
- Talleres para instructores realizados
- 120 expertos capacitados en creación y operación de CSIRTs
- Expertos capacitados en metodologías y herramientas de seguridad informática

Resultados esperados

- Instructores regionales en Creación y Operación de CSIRTs capacitados
- Proyectos de investigación sobre problemáticas de seguridad ejecutados
- Publicación con la identificación y sistematización de Best-Practices difundida
- Análisis sobre posibles modelos, necesidades financieras e impactos de la implantación de una organización de segundo nivel de alcance regional

Visión participativa

- Proyecto orientado a satisfacer las necesidades de los especialistas de seguridad
- Generar espacios de colaboración y confianza
- Generar conocimiento experto y actualizado.
- Apoyar al técnico… bajo ataque!!!
- Abierto a sugerencias

Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para América Latina y Caribe
Registro de Endereços da Internet para América Latina e Caribe

Por dudas, consultas o sugerencias:

ecarozo@gmail.com

Skype: eduardo.carozo