



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



Incidentes en Internet

100 BEST PLACES TO WORK IN IT 2007 **VIEW NOW**

COMPUTERWORLD
Security

JUMP TO

- Home
- News
- E-mail Newsletters
- Tech Dispenser
- + Shark Bait

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](#)

SecurityFocus™

Home | Bugtraq | Vulnerabilities | Mailing Lists | Jobs | Tools | Vista

News
Infocus

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

Focus On: Vista
Columnists

PRINT EMAIL COMMENT

Slammer worm crashed Ohio nuke plant network

Kevin Poulsen, SecurityFocus 2003-08-19

The Slammer worm penetrated a private computer network at the Davis-Besse nuclear power plant in January and disabled a safety system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall, SecurityFocus has learned.

ataques against Web sites in Estonia appears

segunda-feira, 18 de Junho de 2007

ataques a sites atingem páginas de turismo na Itália

Estou prevenindo de há muito, que a internet é uma arma poderosa. Ataques desse tipo podem destruir a industria de turismo da Itália. Quem vai ter coragem de acessar um site de agencia de turismo italiano. A noticia diz que somente os usuários que possuem o internet explorer (da Microsoft) desatualizado podem ser infectados, mas é uma informação errada. A gigante americana é lenta e está sempre a reboque dos hackers. Tome cuidado, se vc perder o seu dinheiro não vai recuperar é coisa de russo.

Postado por Miguel às 18:53



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 costa 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



¿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 (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 más 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



Un ejemplo.... 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



PROYECTO AMPARO

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



Objetivos generales

- Aumentar la capacidad regional de prevenir la ocurrencia de incidentes de seguridad informática
- Responder pronta y efectivamente, proveyendo a las organizaciones de los distintos países de la región de una capacidad de protección proactiva
- Dotarlas de mayor capacidad de respuesta 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 a nivel de 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 al análisis sobre posibles modelos y posibilidades para la constitución de un CSIRT Regional



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
- Contribuir al estudio sobre las posibilidades de creación de un CSIRT Regional. Identificar buenas prácticas y proponer posibles modelos 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**



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
- 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**

Muchas gracias