



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**

Projeto AMPARO

Fortalecimento da capacidade regional
de atendimento a incidentes de segurança na
América Latina e o Caribe



Incidentes na 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

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



Ameaças na Internet

- O tipo de ameaças encontradas na Internet está mudando de foco
- Antes...
 - ◆ Predominância de virus e worms (Slammer, CodeRed)
- Agora...
 - ◆ Vírus, worms, cavalos de Tróia e outros “personagens”, mas operando como ferramentas para obter lucros
 - ◆ Tem se gerado uma “economia subterrânea”



A “Insegurança” do Software

- Quais são os fatores que possibilitam tudo isso?
 - ◆ Em primeiro lugar, a própria natureza humana
 - ◆ Os usuários de Internet em geral não lhe dão um lugar prioritário à segurança de seus PCs
 - ◆ Sempre há “elementos” procurando obter lucro fácil às custas dos outros
- Mas também...
 - ◆ A própria natureza do software
 - ◆ Fazer software não é fácil, parece mais uma arte que uma ciência
 - ◆ A segurança em um projeto, em geral, é considerada apenas no final do mesmo



Por que aprender com o inimigo?

- Problemas com as táticas tradicionais de defesa
 - Aproximação tradicional à identificação de ameaças baseada em “*identificar o já conhecido*”
 - Sistemas baseados em firmas (Antivírus, IDS/IPS)
 - O desenvolvimento de firmas para sistemas não abertos depende do ciclo de desenvolvimento dos provedores
 - Que sejam denunciados os problemas
 - Que sejam desenvolvidas e distribuídas as firmas
 - Estamos protegidos do “*já conhecido*”, mas...
Que acontece com o desconhecido?



Por que aprender com o inimigo? (2)

- Mudanza de foco dos atacantes: *atacar diretamente às aplicações*
 - ◆ É onde tem mais para ganhar
 - ◆ Além de ou apoiando-se no vírus/ worm/ cavalo de Tróia “massivo” tradicional
- No ciclo de aprender-responder-prevenir, passar a ficar um passo adiante



Ferramentas para consegui-lo

- Técnicas de tipo forense
 - ◆ Análise de artefatos
 - ◆ Artefatos: arquivos (executáveis, textuais) achados em computadores que têm sido comprometidos
- Técnicas de tipo “ativo”
 - ◆ As técnicas ativas, em geral, oferecem um alvo que parece interessante mas que está cuidadosamente monitorado
 - ◆ Exemplos
 - ◆ Honeypots
 - ◆ Spampots
 - ◆ Darknets



Um exemplo.... Spampots

- Ideia similar à do honeypot, mas aplicada ao problema do spam (correio eletrônico não solicitado.)
- Características desejadas:
 - ◆ Emular os serviços procurados pelos *spammers*:
 - ◆ SMTP “open relay”
 - ◆ Proxies abertos
 - Armazenar todo o correio eletrônico que passa por ele
 - Tentar “enganar” os spammers o mais possível
 - Procurar superar as provas de verificação que eles realizam
 - Simples de instalar, manter, operar. Robusto.



Spampots (2)

- Classificação do tráfego de correio:
 - ◆ Todo o tráfego de correio que passa através do spampot é correio não solicitado
 - ◆ De forma nenhuma tráfego legítimo circula por ele
 - ◆ De esta forma a própria natureza do spampot resolve um dos problemas mais difíceis que apresenta a luta contra o Spam
 - ◆ CERT.br tem sido suporte fundamental no desenvolvimento desse sensor, e é um exemplo claro de colaboração entre centros de resposta



Projeto AMPARO

Fortalecimento da capacidade regional de atendimento de incidentes de segurança na América Latina e o Caribe



Objetivos gerais

- Aumentar a capacidade regional de prevenir a ocorrência de incidentes de segurança informática
- Responder pronta e efetivamente, provendo às organizações dos diferentes países de uma capacidade de proteção pró-ativa
- Dotá-las de maior capacidade de resposta perante os ataques informáticos de alto impacto



Objetivos específicos

- Desenvolver atividades de pesquisa aplicada que apoiem os processos e prioridades regionais
- Promover a criação de CSIRTs a nível de organizações do setor público e privado dos diferentes países da região
- Construir uma plataforma regional de capacitação de especialistas em segurança informática
- Contribuir na análise de possíveis modelos e possibilidades para a construção de um CSIRT Regional



O que é um CSIRT?

- Um conjunto de técnicos treinados para resolver incidentes de segurança informática massivos
- Devem ter conhecimentos atualizados de segurança e redes, e principalmente contatos com a comunidade que detecta e responde a incidentes
- Devem conseguir determinado nível de legitimidade na sua comunidade como para que as organizações ou pessoas afetadas possam confiar-lhes informação confidencial no pior momento!
- Em seu acionar parecem com uma equipe de bombeiros de alta especialização



Estratégias de desenvolvimento do Projeto AMPARO

- Pesquisa Regional. Promover a criação de uma plataforma de cooperação e coordenação em pesquisa
- Criação de capacidades regionais. Desenhar um programa regional de capacitação em criação e administração de CSIRTs, incluindo o desenvolvimento de materiais e guias metodológicas para os instrutores.
- Formação de formadores. Propiciar a formação de um grupo de profissionais da região que possam atuar como instrutores



Estratégias de desenvolvimento do Projeto AMPARO

- Capacitação em escala. Desenvolver um conjunto de cursos-oficinas na região atendida por LACNIC com base no programa de capacitação desenhado.
- Contribuir ao estudo sobre as possibilidades de criação de um CSIRT Regional. Identificar boas práticas e propor possíveis modelos para a criação de uma organização de segurança de segundo nível.



Componentes do Projeto

- **Plataforma regional de pesquisa em cibersegurança.**
Será promovida a conformação de uma rede de especialistas em segurança e pesquisadores centrada na troca e desenvolvimento de conhecimento acerca dos problemas atuais e emergentes de cibersegurança e suas formas de prevenção e controle.
- **Elaboração de materiais de capacitação de uso público**
Serão desenvolvidos materiais para o treinamento, os mesmos serão de uso público e de livre disponibilidade, contemplando devidamente os aspectos relativos à propriedade intelectual e referências.



Componentes do Projeto

- **Formação de formadores.**
O projeto implica a formação de especialistas com habilidades adequadas para capacitar novos grupos de profissionais nos países da região.
- **Realização das primeiras edições de capacitação.**
Serão oferecidas as primeiras edições de capacitação, com o objetivo de difundir os conteúdos e ajustá-los às necessidades do projeto.
- **Identificação de líderes e financiamento para a explicitação de boas práticas na região.**



Resultados esperados

- Uma agenda regional de prioridades de pesquisa em segurança informática disponível
- Materiais para a capacitação de especialistas em criação e operação de CSIRT disponíveis
- Oficinas regionais realizadas
- Oficinas para instrutores realizadas
- Especialistas capacitados em criação e operação de CSIRTs
- Especialistas capacitados em metodologias e ferramentas de segurança informática



Resultados esperados

- ◆ Instrutores regionais em criação e operação de CSIRTs capacitados
- ◆ Projetos de pesquisa acerca das problemáticas de segurança executados
- ◆ Publicação com a identificação e sistematização de Best-Practices difundida
- ◆ Análise de possíveis modelos, necessidades financeiras e impactos da implantação de uma organização de segundo nível de alcance regional



Visão participativa

- Projeto orientado a satisfazer as necessidades dos especialistas em segurança
- Gerar espaços de colaboração e confiança
- Gerar conhecimento experimentado e atualizado
- Apoiar ao técnico... sob ataque!!!
- Aberto a sugestões



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**

Muito obrigado