

Segurança em Redes

Histórico da Internet

- Arpanet
 - Instituições Militares
 - Órgãos do Governo
 - Universidades
- Família de Protocolos TCP/IP
 - Concebida no final da década de 60
 - Funcionalidade era a principal preocupação



"Segurança baseada na confiança mútua"

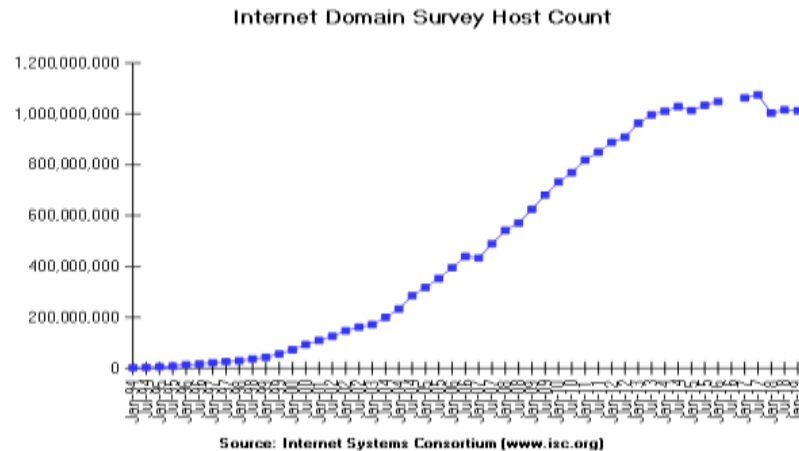
Histórico da Internet

Visão futurista

– Popularização de serviços: Web, E-mail, etc

"Quem esperava a Internet com todo este poder atual?"



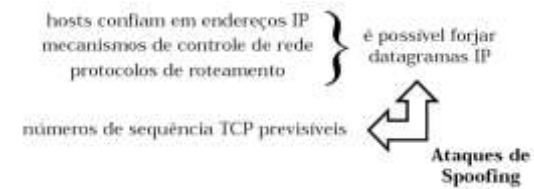


Histórico da Internet

Falhas conceituais do TCP/IP

– Bellovin, 1989

- *Security Problems in the TCP/IP Protocol Suite*



Ausência de criptografia

– Máquinas com baixo poder computacional

– Informações trafegam em claro

- Telnet, FTP, POP, etc

Ataques clássicos



Internet Worm

- Data: 2 de novembro de 1988
- Autor: Robert Morris Jr.
- Internet: 60.000 hosts
- Falhas:
 - Sendmail
 - Finger
 - Rsh
- "Parou cerca de 50% da Internet da época"

Ataques clássicos



Kevin Mitnick

- Preso de fevereiro de 1995 a janeiro de 2000
- 25 acusações federais:
 - fraude no sistema telefônico, roubo de software proprietário (Sun, Motorola, Novell e Nokia)



Obtenção de informação

- Dumpster diving ou Trashing



- Engenharia Social



Scanners

São programas que percorrem as principais portas e serviços do sistema em busca de respostas.

- Exemplo similar seria uma pessoa percorrendo uma rua e indo de porta em porta das casas, verificando se o dono deixou alguma aberta.
- Existem inúmeros tipos de scanners, e eles são de grande ajuda tanto para hackers como para administradores de sistemas.
- Os mais populares são de domínio público (GPL), porém também existem scanners comerciais disponíveis (normalmente para a plataforma Microsoft).
- Para o administrador, conhecer as fraquezas do sistema é algo fundamental, pois cedo ou tarde alguém de fora vai bater à sua porta.

Scanners

Basicamente existem dois tipos de scanners. São eles:

a) PortScanning - Verifica as portas abertas de um sistema. Existem stealth port scanners, que podem não ser detectados, sendo necessárias ferramentas especializadas para sua detecção.

O objetivo de um port scan é detectar as portas de serviços de um sistema, fazendo-as responder cada vez que forem consultadas.

Existem algumas técnicas de portscanning utilizadas. São elas:

TCP CONNECT SCAN, TCP SYN SCAN, UDP SCAN, TCP NULL SCAN, TCP FIN SCAN, TCP XMAS TREE SCAN

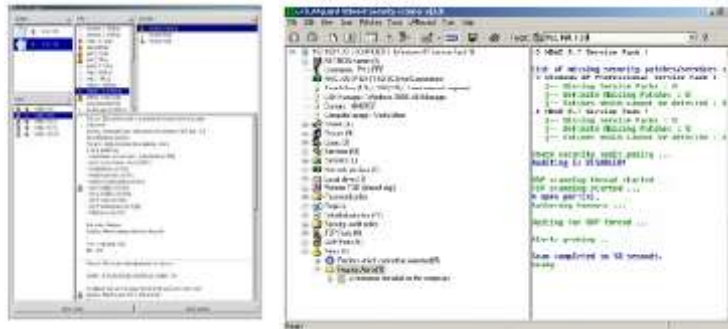
Scanners

b) Scanner de Vulnerabilidade - Utilizado para detecção de vulnerabilidades em softwares executados em um sistema.

- Muito útil para o hacker, já que, através disto, ele pode escolher qual o exploit a ser utilizado para a invasão.
- Muitos crackers desenvolvem scanners private (scanner de uso pessoal não divulgado), e os utilizam para fins não muito éticos.
- A idéia do scanner de vulnerabilidade é, através de uma lista, checar se o sistema está ou não executando um serviço com problemas.

Scanners

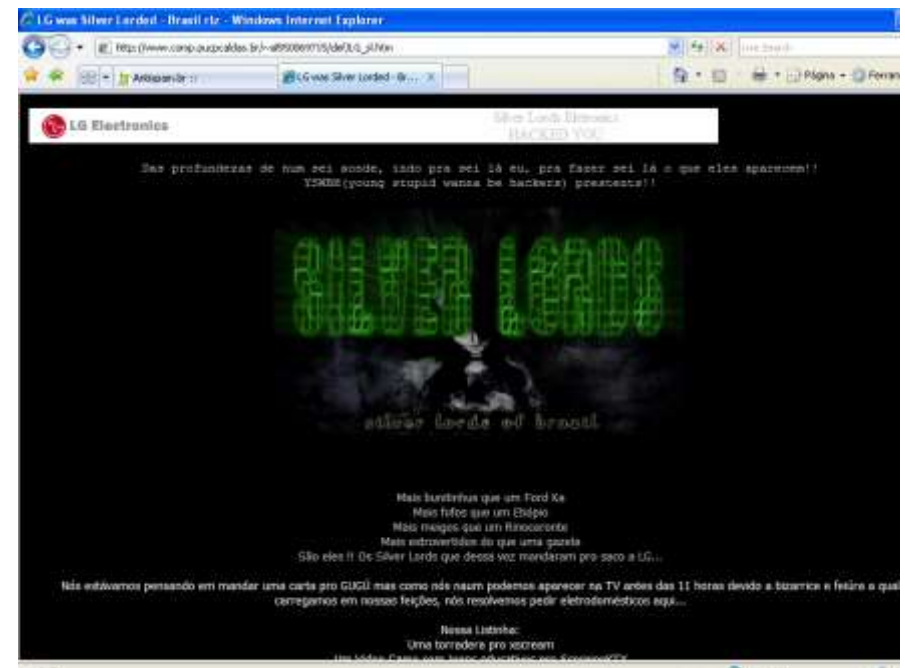
- Scanners de vulnerabilidades
 - Nessus
 - LANGuard



Defacement

*Ato de modificar ou danificar a superfície ou aparência de algum objeto e é empregado comumente na **Segurança da informação** para categorizar os ataques realizados por **crackers** e **script kiddies** para modificar a página de um sítio na Internet.*

Fonte: pt.wikipedia.org/wiki/Defacement
<http://webinhost.com.br/blog/blog-dicas/o-que-se-entende-por-defacement>



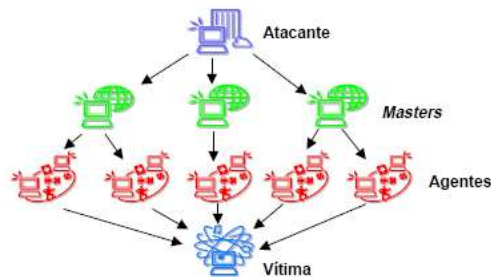
Denial of Service

ATAQUE DE NEGAÇÃO DE SERVIÇO

- Ataques coordenados a grandes sites (Fevereiro de 2000)



- Execução:



Denial of Service

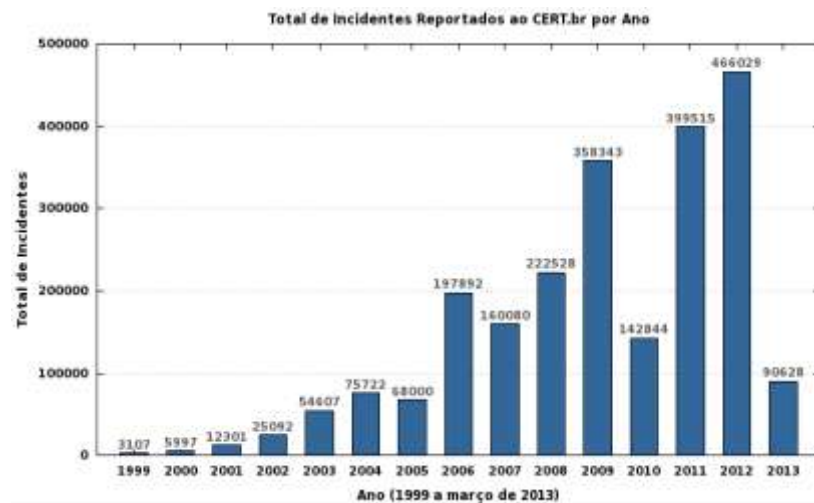
ATAQUE DE NEGAÇÃO DE SERVIÇO

Seria tornar os recursos de um sistema indisponíveis para seus utilizadores.

Alvos típicos são servidores web. O ataque tenta tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

Os ataques são feitos geralmente de duas formas:

- Forçar o sistema vítima a reinicializar ou consumir todos os recursos (memória ou processamento por exemplo) de forma que ele não pode mais fornecer seu serviço.
- Obstruir a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não comunicarem-se adequadamente.



INFORMAÇÕES DE CONTATO DE GRUPOS DE SEGURANÇA BRASILEIROS



Por que o aumento significativo?

- Estamos na Era da Informação
- Rápida adoção da tecnologia por todos
- Explosão da Internet e do comércio eletrônico
- Milhares de vulnerabilidades nas tecnologias
- Falta de maior preocupação com a segurança
- Falta de leis específicas
- Escopo internacional

DESCRIÇÃO DAS CATEGORIAS DE INCIDENTES REPORTADOS AO CERT.BR:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **Dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço;
- **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **Scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles.
- **Fraude**: "qualquer ato enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro".
- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Buffer Overflow

Buffer overflow ou **transbordamento de dados** acontece quando o tamanho de um *buffer* ultrapassa sua capacidade máxima de armazenamento.

Se o programa não foi adequadamente escrito, esse excesso de dados pode acabar sendo armazenado em áreas de memória próximas, corrompendo dados ou travando o programa, ou mesmo ser executado, que é a possibilidade mais perigosa.

Backdoors

- Netbus
- Back Orifice
 - Permitem controlar um host remotamente

*“Se debugar é a arte de
remover bugs, programar é
a arte de inseri-los.”
Donald E. Knuth*

Vírus, Worms e Trojans

- I love you
 - Técnicas avançadas de contágio, via e-mail e compartilhamento
 - Possui um servidor de e-mail próprio
- SirCam
 - *Buffer overflow do Internet Information Service (IIS)*
- CodeRed
 - Checa a data da vítima e gera uma lista aleatória de endereços IP para contágio
 - 1 a 19 de cada mês: fase de infestação
 - 20 a 28 de cada mês: atacar o site da Casa Branca
- Nimda
 - Diferentes meios de disseminação:
 - Bug do IIS, JavaScript, Compartilhamento
 - E-mail, via *Automatic Execution of Embedded MIME Types*
- Klez
 - Desabilita o anti-vírus
 - Não é preciso abrir o e-mail para o contágio
 - Faz o *spoofing de sua origem*
 - Servidor de e-mail próprio
- NetSky
- MyDoom
- Beagle

Conficker: 3º aniversário e mais de 11.000.000 de vítimas

Fonte: <http://www.tecmundo.com.br/>

Wi-Fi (IEEE 802.11b)

Warchalking



www.warchalking.org

VC Warchalking in Silicon Valley		
Symbol	Key	Explanation
+	42C Investment	Back to Church for NASDAQ project sign
WIFI	Dot.com Investment	What's New? What's Working? Call the domain name to a point site
B2B	B2B Investment	Buy the Internet or its Back to Banking
Hardware	Investment	Get the hardware back to Cisco
MP	Supply chain Investment	Merge and acquire. See if we can't be first to another company, particularly in someone else's portfolio
O3	Linux Investment	Hope for recovery in 2003. Otherwise sell it for \$3 cents on the dollar
III	Telco Investment	CEO: CFO behind bars for sales of stocks at 3.5 years with time off for good behavior
WTF	Wireless Investment	What the F???



Wi-Fi (IEEE 802.11b)

Warchalking

O **warchalking** foi inventado nos **USA** há aproximadamente 70 anos, durante a época da depressão, quando pessoas desempregadas que andavam pelas ruas a procura do que fazer sinalizavam locais em que se podiam encontrar serviços gratuitos, tais como uma residência onde um médico não cobrava pela consulta ou um local em que se podia fazer uma refeição segura. Para sinalizar tais locais, eles riscavam sinais com giz, desenhando símbolos que só eles sabiam o que significava.

Atualidade foi uma maneira que muitos usuários de **notebooks** encontraram para identificar um local (**hotspot**) onde haja uma conexão **wifi** (rede sem fio) com sinal aberto ou vazando (sem segurança). Quando localizado, é informado o nome do hotspot, o tipo e a velocidade através de símbolos (warchalking).

Wi-Fi (IEEE 802.11b)

Warchalking



Wi-Fi (IEEE 802.11b)

Warchalking Brasil



Wi-Fi (IEEE 802.11b)

Wardriving



Wi-Fi (IEEE 802.11b)

Wardriving

Trata-se do ato de procurar por redes wireless Wi-Fi se deslocando dentro de um veículo (daí o “driving”). Além do automóvel, o procedimento envolve também, evidentemente, um computador equipado com Wi-Fi, como um notebook ou um PDA para detectar as redes.

Wi-Fi (IEEE 802.11b)

Wardriving



<http://www.wardriving.com/>

CELULARES

• Celulares 2,5G e 3G

- Começam a surgir os primeiros worms



FRAUDES BANCÁRIAS

20/10/2004 - 20h19

PF prende 53 pessoas acusadas de roubar dinheiro pela Internet

SÃO PAULO (Reuters) - A Polícia Federal prendeu 53 pessoas acusadas de roubar dinheiro por meio da Internet nesta quarta-feira. Os golpistas espalhavam e-mails com um vírus, que depois de se instalar nos computadores, repassava para a quadrilha os dados pessoais e senhas bancárias das vítimas.

Os supostos criminosos foram detidos nos Estados do Ceará, Maranhão, Tocantins e Pará, em uma operação chamada pela PF de Cavalo de Tróia II.

Segundo a PF, o prejuízo para os bancos foi de cerca de 80 milhões de reais.

Após recolher as informações das vítimas com o vírus espalhado por spam, o grupo acessava as contas das vítimas e realizava saques e transferências para contas de laranjas, que emprestavam seus cartões e senhas mediante o pagamento de 100 a 500 reais, informou a PF em comunicado. A quadrilha também utilizava uma nova maneira de desviar dinheiro de internautas, que consiste em pagamentos de boletos bancários fraudulentos.

Nesse caso, o infrator utilizava as informações roubadas para pagar boletos que beneficiavam empresas envolvidas em esquemas de lavagem de dinheiro, diretamente ligadas à quadrilha.

(Por Isabel Malzoni)

FRAUDES BANCÁRIAS

Técnicas utilizadas:

- Engenharia Social
- e-mail falso de cadastramento
- site falso idêntico ao do banco



FRAUDES BANCÁRIAS

- Técnicas utilizadas:
 - Keyloggers instalados por worms e trojans













CRIPTOGRAFIA

- SSL (Secure Socket Layer)
 - Segurança no acesso à Web



ANTIVÍRUS

Ver Resultados da Enquete: Qual o Melhor Antivírus?			
Norton		532	18,75%
McAfee VirusScan		151	5,32%
Kaspersky		571	20,12%
NOD32		382	13,46%
Avast!		527	18,57%
AVG		355	12,51%
PC-Cillin		33	1,16%
Panda		91	3,21%
AntiVir		113	3,98%
Outros		83	2,92%



- Firewall pessoal
- Tiny Personal Firewall
- Filtro de pacotes / checagem de integridade

FIREWALL

Product	Pontuação	Proteção
Outpost Firewall Pro 2009	99% / 73	Excellent
Online Armor Personal Firewall	98% / 73	Excellent
Comodo Firewall Pro 3	95% / 73	Excellent
ProSecurity 1.43	93% / 62	Excellent
Privatefirewall 6.0.19.29	90% / 73	Excellent
Online Armor Personal Firewall 2.1	89% / 73	Very good
Kaspersky Internet Security 7.0	85% / 62	Very good
Jetico Personal Firewall 2.0	78% / 73	Good
System Safety Monitor 2.3	77% / 62	Good
PC Tools Firewall Plus 4.0.0.40	74% / 73	Good
Lavasoft Personal Firewall 3.0	70% / 73	Good
ZoneAlarm Pro 7.0.473.000	63% / 73	Poor
Dynamic Security Agent 2.0	62% / 71	Poor
Webroot Desktop Firewall 5.5	60% / 73	Poor
Comodo Firewall Pro 2.4.18.184	55% / 73	Poor
Norton Internet Security 2008	32% / 62	Very poor
Trend Micro Internet Security 2008	27% / 73	None

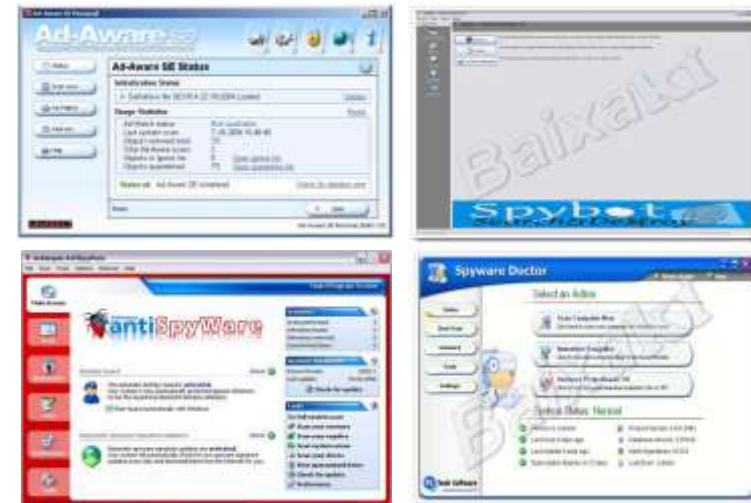
SPYWARES

Consiste num **programa automático de computador**, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o seu conhecimento nem o seu consentimento.

Diferem dos **cavalos de Tróia** por não terem como objetivo que o sistema do usuário seja dominado, seja manipulado, por uma entidade externa, por um **cracker**.

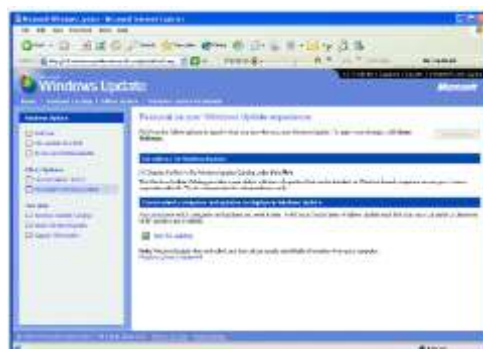
Os spywares podem ser desenvolvidos por firmas comerciais, que desejam monitorar o hábito dos usuários para avaliar seus costumes e vender este dados pela internet.

SPYWARES



ATUALIZAÇÕES

- Windows Update
 - Service Packs
 - Hotfixes
- Linux
 - APT
 - Yum
 - Portage



ALERTAS / INCIDENTES

- CAIS (Centro de Atendimento à Incidentes de Segurança)
 - <http://www.rnp.br/cais>
- NBSO (NIC BR Security Office)
 - <http://www.nbso.nic.br/>
- CERT (Computer Emergency Response Team)
 - <http://www.cert.org>

CÁLCULO DE RISCO

- Componentes do Risco

- **Bens/propriedades**
- **Objetivos da segurança**
 - Confidencialidade da informação
 - Integridade dos dados
 - Integridade do sistema
 - Disponibilidade do sistema ou rede.
- **Ameaças**

(...)

CÁLCULO DE RISCO

- **Motivação:**

- **Motivos financeiros**
- **Motivos políticos**
- **Motivos pessoais/psicológicos**
- **Ataques à vulnerabilidades da corporação**

(…)

CÁLCULO DE RISCO

1º Método: Expectativa de Custo Anual (ECA)

- Expectativa simples para o cálculo do risco.
- Uma vez identificados seus bens, vulnerabilidades e inimigos, pode se então *quantificá-los*.
- Referência: Ozier, Will & etal (eds). “Risk Analysis and Management”. Handbook of information Security Management. CRC Press, 1998.

(…)

CÁLCULO DE RISCO

2º Método: Árvores de Ataque (*Attack Trees*)

- É uma representação visual das possibilidades de ataque contra um determinado alvo.
- Referência: Schneier, Bruce. “Attack Trees: modeling security threats”. Dr. Dobbs' Journal: Dec 1999.

Políticas de Segurança

As decisões que você como administrador toma ou deixa de tomar, relacionadas à segurança, irão determinar quão segura ou insegura é a sua rede, quantas funcionalidades ela irá oferecer, e qual será a facilidade de utilizá-la.

É a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.

Política de Segurança? Por que ter uma?

Seus objetivos devem ser determinados a partir das seguintes determinantes:

Serviços oferecidos versus Segurança fornecida - Cada serviço oferecido para os usuários carrega seus próprios riscos de segurança.

Facilidade de uso versus Segurança - O sistema mais fácil de usar deveria permitir acesso a qualquer usuário e não exigir senha, isto é, não haveria segurança. Solicitar senhas torna o sistema um pouco menos conveniente, mas mais seguro.

(...)

Política de Segurança? Por que ter uma?

Custo da segurança versus o Risco da perda –

Há muitos custos diferentes para segurança:

- **Monetário** (o custo da aquisição de hardware e software como firewalls, e geradores de senha "one-time");
- **Performance** (tempo cifragem e decifragem), e facilidade de uso.

(...)

Política de Segurança? Por que ter uma?

Custo da segurança versus o Risco da perda –

Há também muitos níveis de risco:

- **Perda de privacidade** (a leitura de uma informação por indivíduos não autorizados);
- **Perda de dados** (corrupção ou deleção de informações);
- **Perda de serviços** (ocupar todo o espaço disponível em disco, impossibilidade de acesso à rede).

Cada tipo de custo deve ser contra-balançado ao tipo de perda.

Política de Segurança?

Perfil dos Ataques

- Crime Organizado
 - Aliciando spammers e invasores;
 - Injetando dinheiro na “economia underground”.
- Botnets
 - Usadas para envio de scams, phishing, invasões, esquemas de extorsão
- Redes mal - configuradas sendo abusadas para realização de todas estas atividades - sem o conhecimento dos donos;
- Alvo migrando para usuários finais.

(...)

Política de Segurança?

Perfil dos Atacantes

- Em sua maioria adolescentes
- Pouco ou nenhum conhecimento
 - **Trocam informações no *underground*;**
 - **Moedas de troca:** senhas de administrador/root, novos *exploits*, *contas/senhas de banco*, *números e cartão de crédito*, bots/botnets, etc

Política de Segurança?

Principais Ameaças

- Vulnerabilidades freqüentes;
- Códigos maliciosos explorando essas vulnerabilidades, em curto espaço de tempo;
- Ferramentas automatizadas de ataque;
- Vírus / worms / bots;
- Atacantes + spammers;
- Fraudes / scams / phishing / crime organizado;
- Ataques de força bruta.

Política de Segurança?

Formas de Proteção

- Planejamento do ambiente e da instalação
- Política de segurança
- Política de uso aceitável
- Investir em treinamento
 - Administradores de redes
 - Desenvolvedores
 - Suporte, etc

(...)

Política de Segurança?

Política de Atualização e Correção

- Possuir uma política de atualização de sistemas e aplicação de patches;
 - Sistema operacional (servidores e desktops);
 - Aplicativos;
 - hardware de rede;
- Não aplicar apenas quando estiver sendo explorado;
 - Tarde demais;
- Seguir a política!

Política de Segurança?

Proteção da Rede Interna

Grande risco: propagação de códigos maliciosos de dentro para fora (worms e bots).

- Compartimentalização da rede
- Política de atualização e correção
- Política de conexão de equipamentos na rede interna
 - Terceirizados
 - Notebooks de funcionários, etc