Segurança na Internet2: Considerações atuais e tendências

Liane Tarouco
UFRGS

Sobrevivência da Internet preocupa especialistas

- Painel de especialistas em Davos (Jan/2007)
  - Vinton Cerf
  - John Markoff - escritor especialista em tecnologia
  - Michael Dell - Dell Computadores
  - Hamadoun Toure - secretário-geral da ITU
- "É preciso achar uma solução para garantir a sobrevivência da Internet"
  - Mas não tinham certeza sobre a solução possível
  - **Sistemas operacionais** e **autenticação** - questões importantes para esta solução

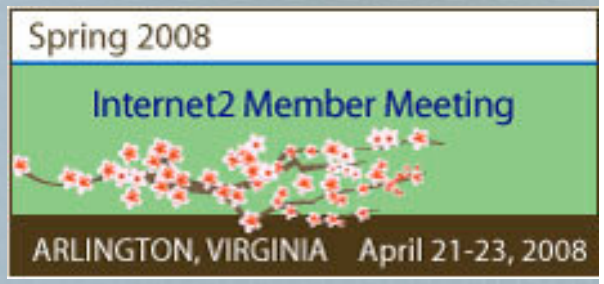
Ciberespaço seguro

- Abordagens de pesquisa
  - Tradicional: problema por problema ou classes de problema
  - Não ortodoxa: combinação multidisciplinar
- Necessidade de dados sobre ataques e medidas de segurança que possam guiar a pesquisa
  - Falta de dados em escala Internet
  - Falta de cenários de teste em escala da Internet
  - Ninguém quer ser o primeiro a expor informação
- Background para pesquisa em rede

Segurança na Internet2

- Rede de alta capacidade
- Uso legítimo deve ser assegurado
- Medidas de segurança não devem impedir o uso que é suposta permitir

Security for advanced networks



- **Security Topics Update -**
  Chris Misra - Univ Massachusetts
  Doug Pearson - REN-ISAC
- **Cyberinfrastructure Architectures, Security and Advanced Applications**
  Joe St Souver - Internet2 & University of Oregon
- **Scaling Security Analysis vs. Next-Gen Botnet Malware-** Nicholas Feamster - Georgia Institute of Technology
- **Extracting Malware Intelligence -** Fengmin Gong - Fireeye

REN-ISAC

- Sediado na Indiana University
- Parte da estratégia para educação superior visando aprimorar segurança de rede através da coleta de informação, análise, disseminação, alertas preliminares e resposta
- Apoia membros na compreensão das ameaças, proteção e mitigação

REN-ISAC

- REN-ISAC recebe, analisa e age sobre informação operacional, ameaças, alertas e ataques reais .
- Informação derivada de instrumentos de rede
- Compartilhamento de informações
- Dados derivados de instrumentos: **netflow**, **router ACL counters**, **darknet monitoring** e sistemas de monitoração operacional de **Global Network Operations Center**

Arquitetura de segurança

- Segurança de Informação é composta de:
  - Políticas
  - Procedimentos
  - Tecnologias e ferramentas
- Como delinear um plano coerente para assegurar que as metas de segurança sejam asseguradas?

Arquitetura de segurança

- “Criar estruturas organizadas, usando ferramentas, técnicas e procedimentos para coesivamente mitigar risco de segurança para a informação, de forma consistente com políticas”

CAMP : Campus Architecture & Midleware Planning

- Bridging Security and Identity Management
  - IAM - identity and access management (IAM) Reduzir exposição de informações de identificação pessoal e outros recursos e serviços importantes
  - Conformidade - log, rastreamento e provisionamento de acesso
  - Escala - reduzir complexidade, que IAM faz correlacionando identidade e acesso em aplicações e sistemas a nível de campus e ensejar a aplicação consistente da política institucional

Workgroup : SALSA

- Security At Line Speed
- http://security.internet2.edu/salsa/
- EDUCAUSE/Internet2 Computer and Network Security Task Force
  - Organizar atividades e criar ferramentas para identificar incidentes de segurança
  - Salsa é um grupo de supervisão integrado por representantes da comunidade de ensino superior
  - Diversos projetos

SALSA - APHIDS

- APHIDS (Advanced Parallel Hypertext Intrusion Detection System)
  - Categorização de itens e estabelecimento de regras
  - Meta: reduzir número de falsos positivos
- Sistema de detecção de intrusão não tradicional
  - Monitora resultados retornados por máquinas de busca

SALSA - RENOIR

- Research and Education Networking Operational Information Repository
  - Projetado visando o conceito de sistema de registro de incidentes lidando com dados de segurança

SALSA - Security Metrics

- Desenvolver ao menos 3 métricas operacionais que possam ser úteis aos técnicos
- Desenvolver ao menos 3 métricas relacionadas com incidentes que possam ser usadas para comunicação de uma instituição para outra
- Desenvolver ao menos 3 métricas que o setor de IT possa usar para demonstrar conformidade com determinações institucionais

SALSA - RADIUS & SAML

- Integrar autenticação em rede e intercâmbio de atributos
- Trabalha em especificações que definem um perfil que inclui mensagens e fluxos inerentes a especificações RADIUS [RFC2865] e SAML
  - Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions)

SALSA - DR

- Disaster recovering
- Explorar e documentar práticas recomendadas para planejamento e recuperação face a desastres
- Vulnerabilidades, armadilhas, potencialidades
- Modelos SLA
- Notificações
- http://security.internet2.edu/dr/

Cenário em transição

- Fornecedores começaram a entregar produtos com segurança “by default”
- Atacantes tornaram-se motivados financeiramente e incrementaram a sua sofisticação operacional

- Busca por ferramentas melhores e mais efetivas

Aspectos a considerar

- Proteger dados sensitivos
- Não apenas os dados das empresas mas os dados dos pesquisadores
- Criptografia nos discos inteiros
- Ferramentas como CU-Spider e outras
- Gerenciamento de identidade
- Malware (virus, worms, spyware, etc.)
- Assinaturas não são suficientes
- Ataques *Distributed denial of service*

Falta pensar

- Impacto de DDoS e SPAM na infraestrutura
- Evolução do gerenciamento das estratégias de firewall para acomodar aplicações avançadas
- Federações - identidade
- Segurança em DNS

DNS

- Monitoração - inspecionar logs para analisar atividade maliciosa
- Software atualizado, apropriado, configuração segura
- Gerência de alterações
- Servidores de nome: alvos de ataques DDoS
- DNSSec Internet2 Pilot

Cyberinfrastructure Architectures

- **Cyberinfrastructure Architectures, Security and Advanced Applications - Joe St Sauver**
- Algumas práticas de segurança e algumas arquiteturas de rede orientadas a segurança atrapalham mais do que ajudam o usuário a realizar seu trabalho
- Como podemos ter uma ciberinsfraestrutura segura e um ambiente online propício às aplicações ao mesmo tempo?

Proteger Ciberinfraestrutura

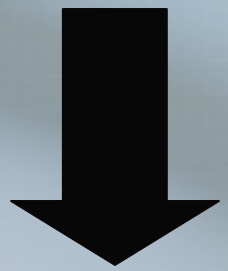
- Ciberinfraestructura
  - armazenamento em larga escala
  - visualização
  - middleware,
  - sistemas operacional e software de aplicação
  - ferramentas de colaboração e
  - até redes!

GENI - Global Environment for Network Innovations

- Projeto visando inovação em rede
- Reprojetar a rede
- Segurança e robustez
- Internet atual tem mecanismos de segurança mas não uma arquitetura de segurança

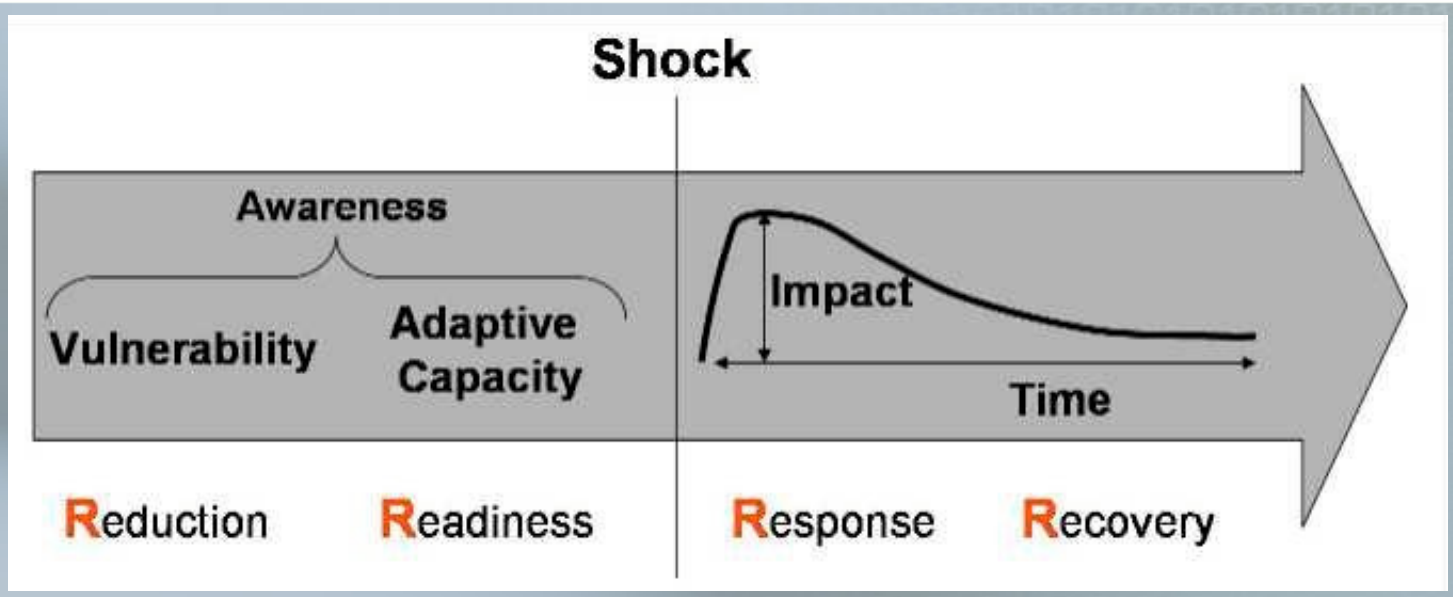
Estratégias

Proteção contra revelação e adulteração não autorizada de dados



Disponibilidade e resistência (resilience) a ataques e falhas

Resilience



- Aspectos críticos da *resilience* organizacional:
  - Vulnerabilidade
  - Capacidade adaptiva
  - Conscientização

Resilience

- A organização deve poder continuar a prover o serviço a despeito da adversidade
  - Reduzir o tamanho e a freqüência das crises (vulnerabilidade)
  - Aprimorar a habilidade e velocidade da organização para gerenciar crises efetivamente (capacidade adaptativa)
  - Conscientização - gerenciamento estratégico de risco como um processo não como um evento

Perfil atual dos problemas

- Maioria dos problemas de segurança atuais não estão na Internet em si mas nos computadores pessoais conectados à Internet
- Meliantes estão mais voltados a vulnerabilidades em aplicações
  - SQL injection attacks
  - XSS (cross site scripting) attacks

A rede não é transparente

- Programadores aprendem que precisam saber conviver com obstáculos :
  - firewalls
  - antivirus gateways
  - traffic shapers
  - proxies
  - outros dispositivos ativos de segurança da rede

Interferência da rede

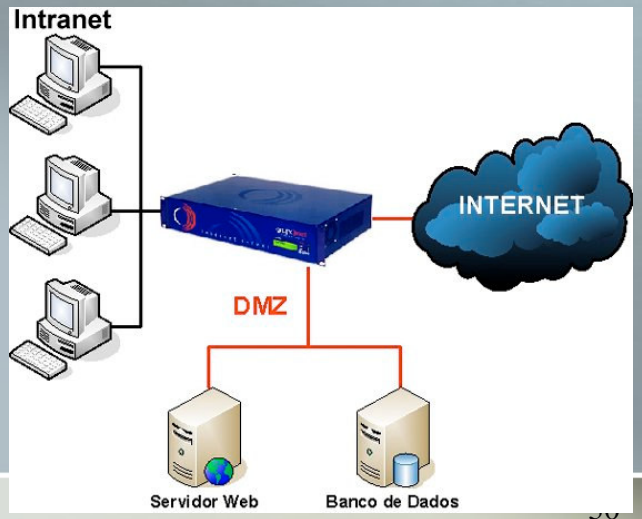
- A rede interfere na transferência ou "não transferência" dos dados
- Tráfego dirigido a host externo pode ser:
  - bloqueado
  - redirecionado

sem aviso ou notificação ao originador

- Problemas enfrentados pelas aplicações
- Ex: grids - Open Grid Forum GFD-I.083 Firewall Issues

Firewall

- Firewall é a base para a segurança mas em função dos problemas causados podem levar a:
  - posicionar servidores na DMZ
  - conectar tais servidores via enlaces físicos ou lógicos dedicados:
    - fibra
    - VPN, VLAN, etc.



Firewall

- Firewall podem introduzir ponto de falha

- Interferir com a operação de aplicações “missão crítica”
- Ocultar a identificação e isolamento de incidentes de segurança se ocorrerem

Firewall são ubíquas

- 2007 E-Crime Watch Survey
  - 97% dos respondentes da pesquisa usam firewall
  - 98% usam antivirus
- Firewall e antivirus são as duas principais tecnologias de segurança usadas
- O que diriam se uma organização não usasse firewall?

Princípios gerais de segurança facilitados pelas firewalls

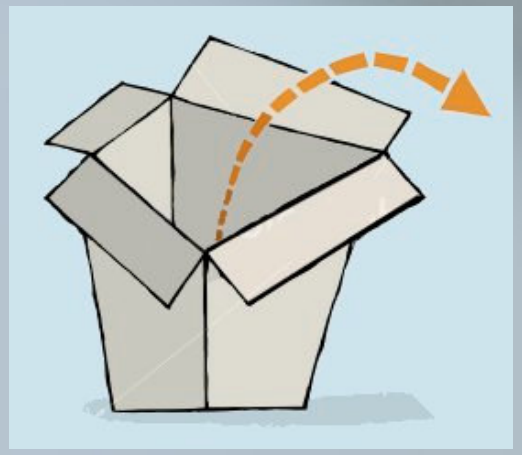
- **Menor privilégio**- conceder a uma pessoa, programa ou computador somente o acesso que necessita para executar sua atividade prevista.
- **Defesa em profundidade** - segurança adicional dos computadores pelo isolamento
- **Separação de tarefas** - monitorar / auditar tráfego da rede

Firewalls são necessárias quando

- **Reinstalação de MS Windows**
  - SANS Survival Time - sistemas sem correções são dominados em 10 minutos
- **Zero Day "Patch Window -** novas disponibilidades descobertas
- **Alguns protocolos podem exigir o uso de firewall**

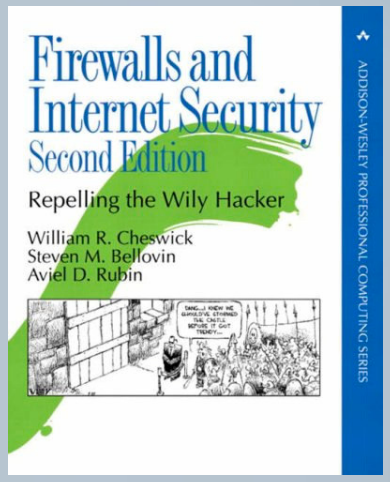
Mas existe vida sem firewall

- Muitos sistemas podem ser tornados seguros na rede, sem uso de firewall
- Mas os sistemas operacionais usuais quando “out ofthe box” estão longe de serem seguros



- I haven't used firewalls in, uh, well, mostly, for ten years or more." and "They still have their use, but I really want my hosts to be secure enough they don't need a firewall."

Bill Cheswick



Skinny dipping

- FreeBSD e Linux
- Muito poucos serviços
  - Single-user hosts
- Serviço perigosos colocados em sandboxes
- Nem todos os computadores são podados
- Implica e abrir mão de serviços
- Exemplo: notebook com Win-XP2
  - Usado basicamente para para apresentações

Skinny dipping

- Poderia ser usado com 50% dos usuários
- Configurações seguras e bloqueadas
- Nada que possa ser clicado,em email ou na web e que possa afetar o ambiente
  - Ex.: ambiente Moodle

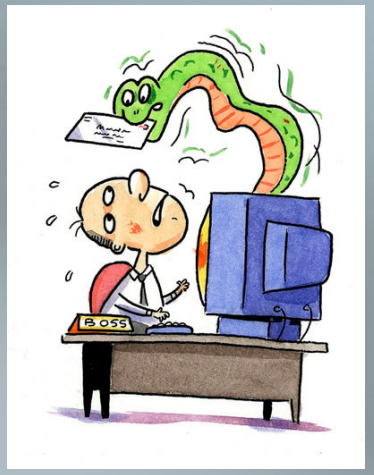
- Nenhum programa portável é executado exceto os assinados
  - Ex.: Sugar

Estratégia de proteção a nível de host

- "All of [the gateway's] protection has, by design, left the internal AT&T machines untested---a sort of crunchy shell around a soft, chewy center."

  Bill Cheswick

- Não é razoável ter expectativa de que usuários compreendam as implicações em termos de segurança da maioria da decisões que precisam tomar

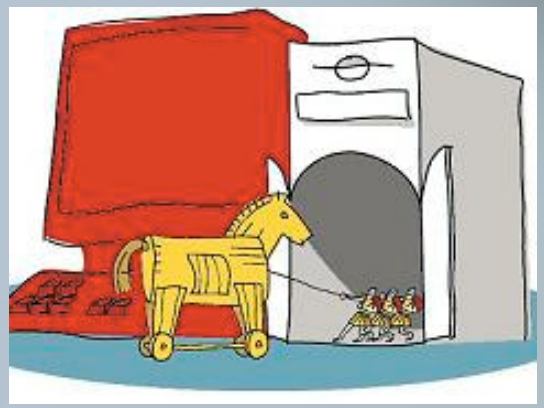


Pensando com os dedos

Usuário “esperto”

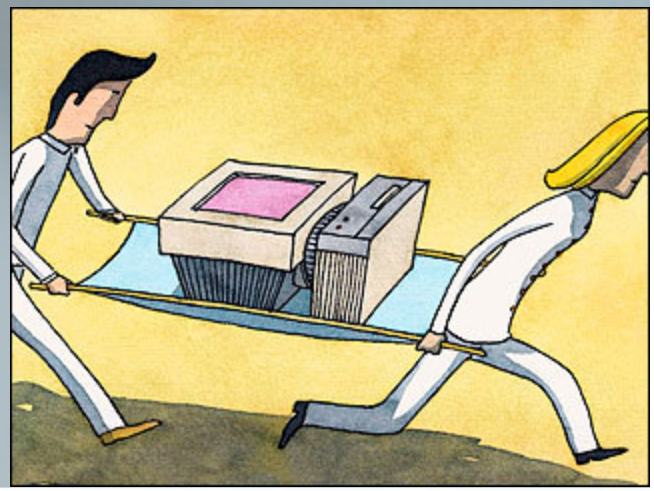
Pirataria oculta malware

- Pesquisas mostram que cerca de 50% dos programas Windows pirateados vieram com programas cavalos de Tróia pré-instalados



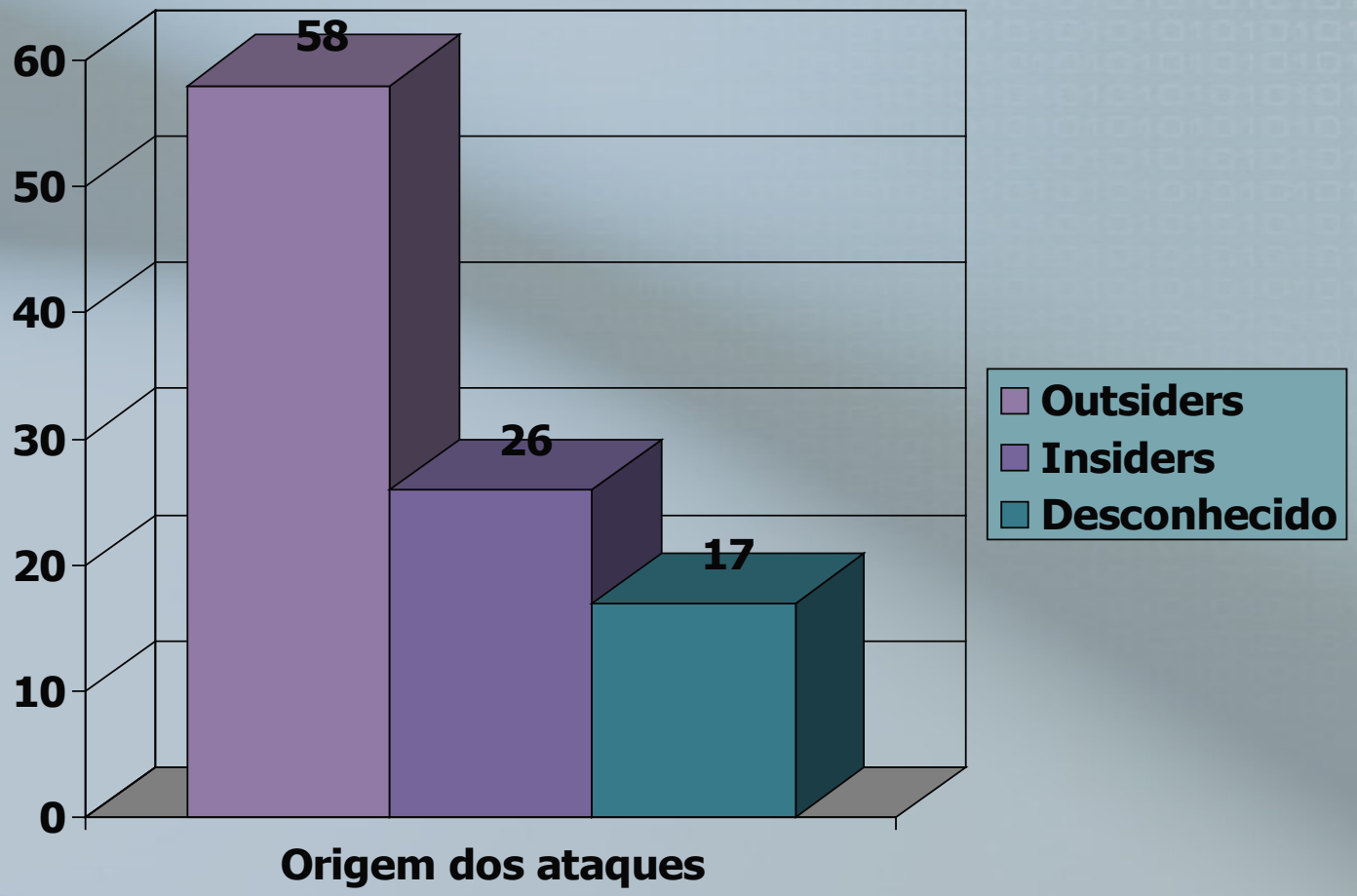
A opinião dos usuários

- Muitos clientes não demandam segurança para o host
  - Não querem pagar pela segurança
  - Usuários leigos tem alta tolerância a infeções



2007 E-Crime Watch Survey

Summary of Security Events

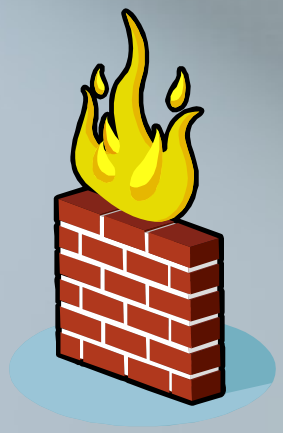


Distributed Denial of Service Attacks

- Tráfego de ataques DDoS constituem 1-3% de todo o tráfego inter-domínio na Internet
  - 1300/ataques DDoS dia
- Firewalls não podem proteger contra DDoS
  - uplink saturado

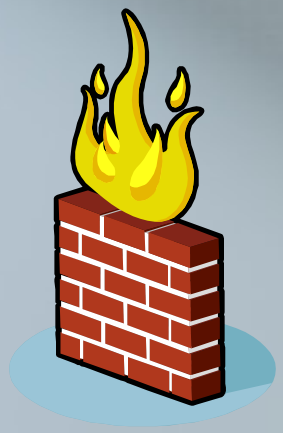
Ameaças tradicionais

- Firewalls tem tradicionalmente como meta mitigar intrusões clássicas
  - "cracking/hacking,”
  - scans automatizados
  - ataques de força bruta



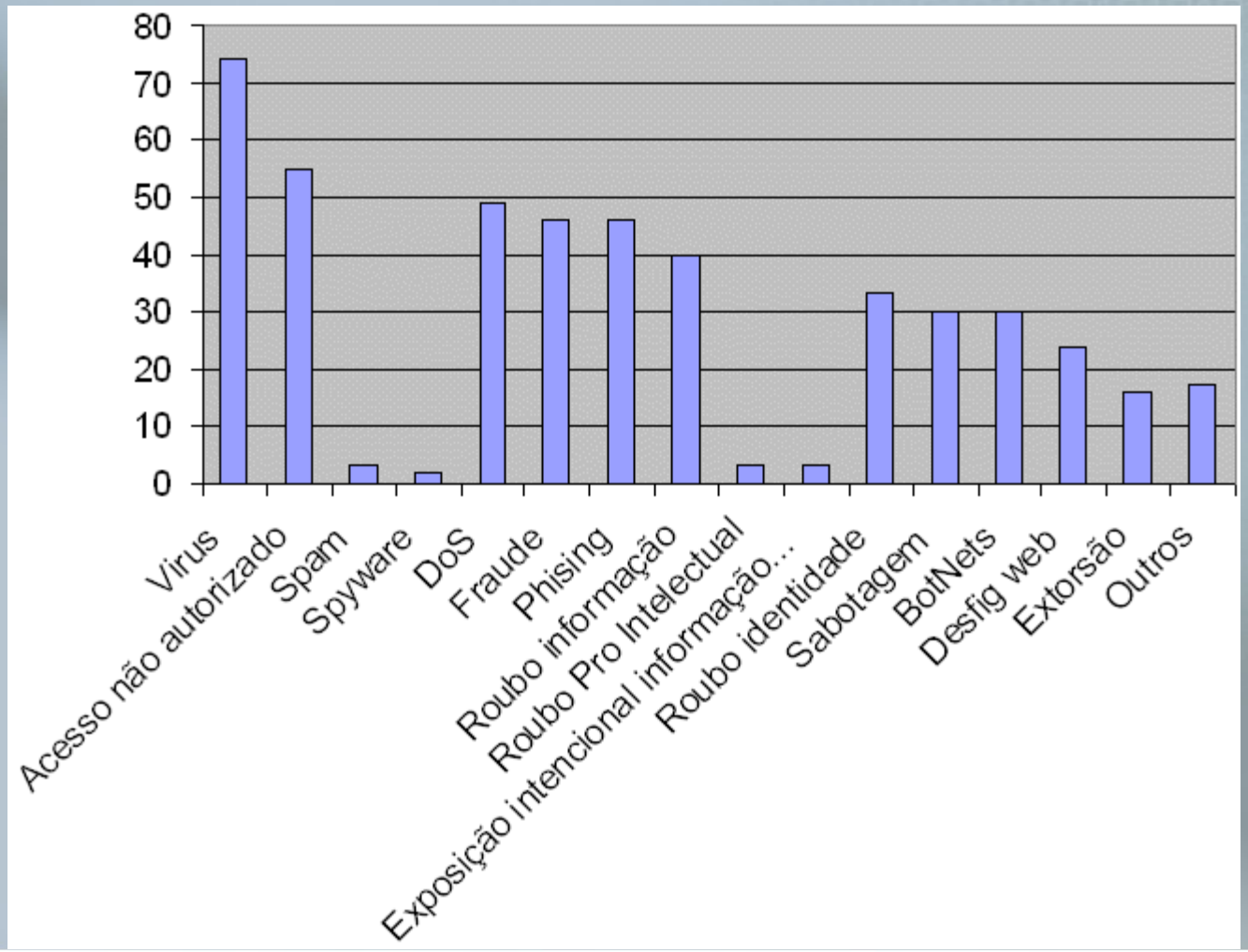
Firewalls podem afetar throughput

- Problema sério em redes de alta velocidade
- Comportamento intermitente em termos de descarte de pacotes pode dificultar diagnóstico de problemas de conectividade

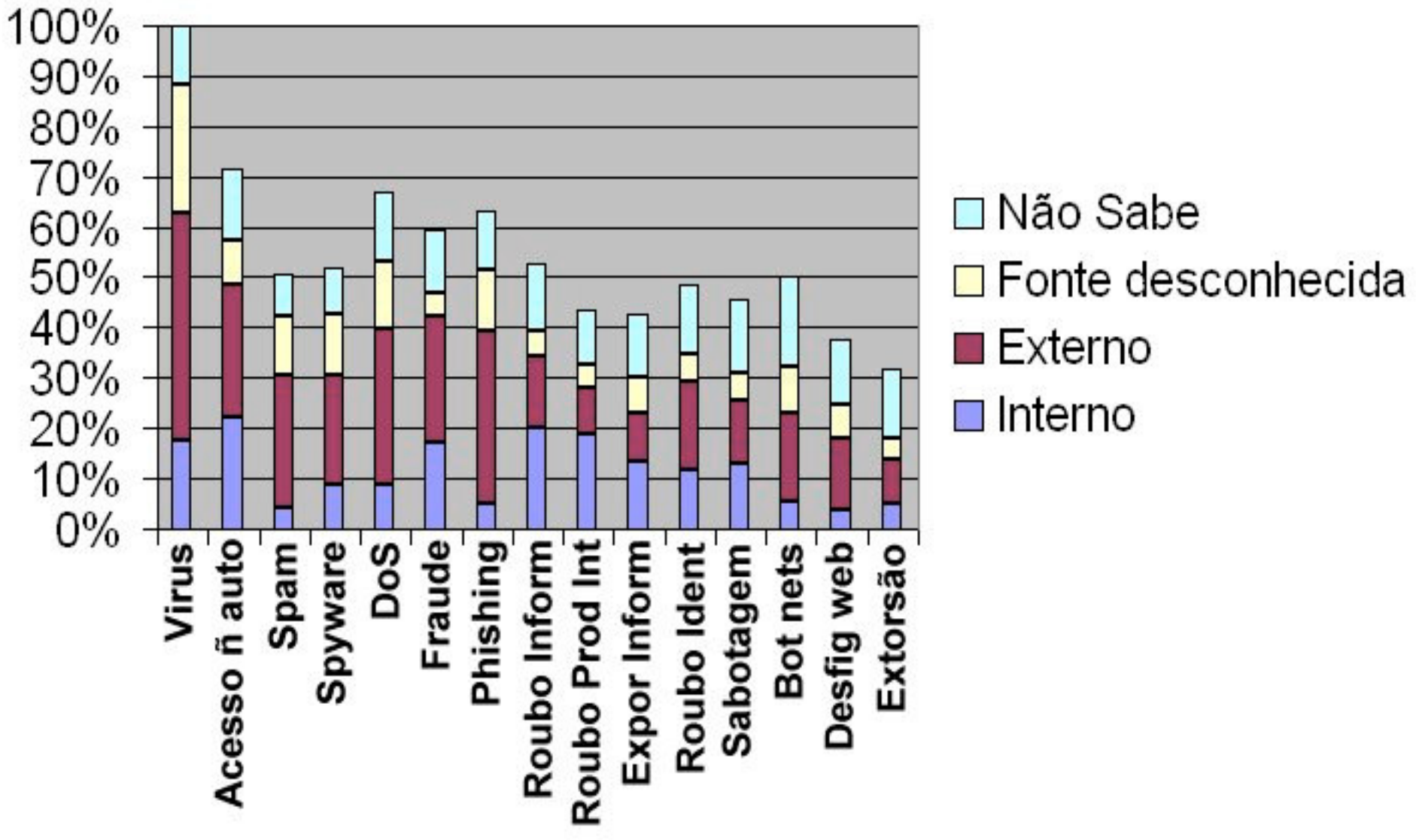


2007 E-Crime Watch Survey

- Crimes cometidos nos últimos 12 meses

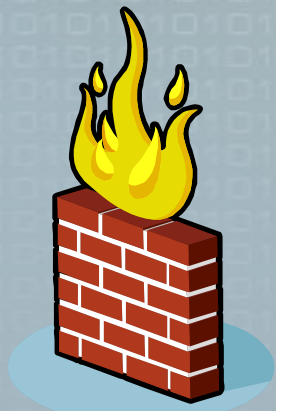


2007 E-Crime Watch Survey



Firewall podem desencorajar experimentação e inovação

- Firewall podem impedir algumas aplicações
  - H.323 (sistema legados)
  - IP v6



http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1338

Description

The default configuration of the AirPort utility in Apple AirPort Extreme creates an IPv6 tunnel but does not enable the "Block incoming IPv6 connections" setting, which might allow remote attackers to bypass intended access restrictions by establishing IPv6 sessions that would have been rejected over IPv4.

Network Usability Officer?

- **Information Security Officer**
- **Chief Information Security Officer**
- **Privacy Officer**

- **Network Usability Officer (NUO)** - alguém dedicado a assegurar que quando agimos para preservar a segurança e proteger nossa privacidade, não destruímos simultânea e inadvertidamente a usabilidade de nossas redes e sistemas computacionais

Mecanismos mais efetivos

- 2007 eCrime Watch Survey

Top 10 Most Effective (Very Effective or Somewhat Effective) Technologies in Use (Base: respondents with technology in use)

2007 Rank	Technology (2007 percentage)	2006 Rank (last year)
1	Statefull Firewalls (82%)	1
2	Access Controls (79%)	Not asked
3	Electronic access controls (78%)	2
4	Application layer firewalls (72%)	6
5	Host-based Anti-virus (70%)	10
6	Password complexity (70%)	3
7	Encryption (69%)	5
8	Heuristics-based SPAM filtering (69%)	7
9	Network-based policy enforcement (68%)	9
10	Network-based Anti-Virus (65%)	4

Mecanismos menos efetivos

- 2007 eCrime Watch Survey

Top 10 Least Effective (Not Very or Not At All Effective) Technologies in Use (Base: respondents with technology in use)

2007 Rank	Technology (2007 percentage)	2006 Rank (last year)
1	Manual Patch Management (26%)	1
2	Surveillance (18%)	2
3	Password Complexity (17%)	8
4	Badging (16%)	6
5	RBL-based SPAM filtering (15%)	13
6	Host-based Anti-SPAM (14%)	15
7	Wireless monitoring (14%)	3
8	Change control/configuration management systems (13%)	5
9	Software development tools & processes (13%)	4
10	One-time passwords (12%)	16

Security policies and procedures

- O que as organizações usam para prevenir ou reduzir eventos de segurança

Account/ password management policies	84%
Acceptable use policy/ Formal "inappropriate use" policy	80%
Internet connection monitoring (external)	59%
Monitor Internet connections	59%
Employee/ contractor background check	57%
Non-disclosure agreement	53%
Conduct regular security audits	51%
New employee security training	43%
Employee Assistance Program	43%
Employee monitoring	42%
Periodic risk assessments	42%
Employees required to review and accept the written inappropriate use policy on any periodic basis	50%
Periodic Security education and awareness programs	38%
Random security audits	36%
Storage & review of e-mail or computer files	36%
Intellectual property agreement	35%

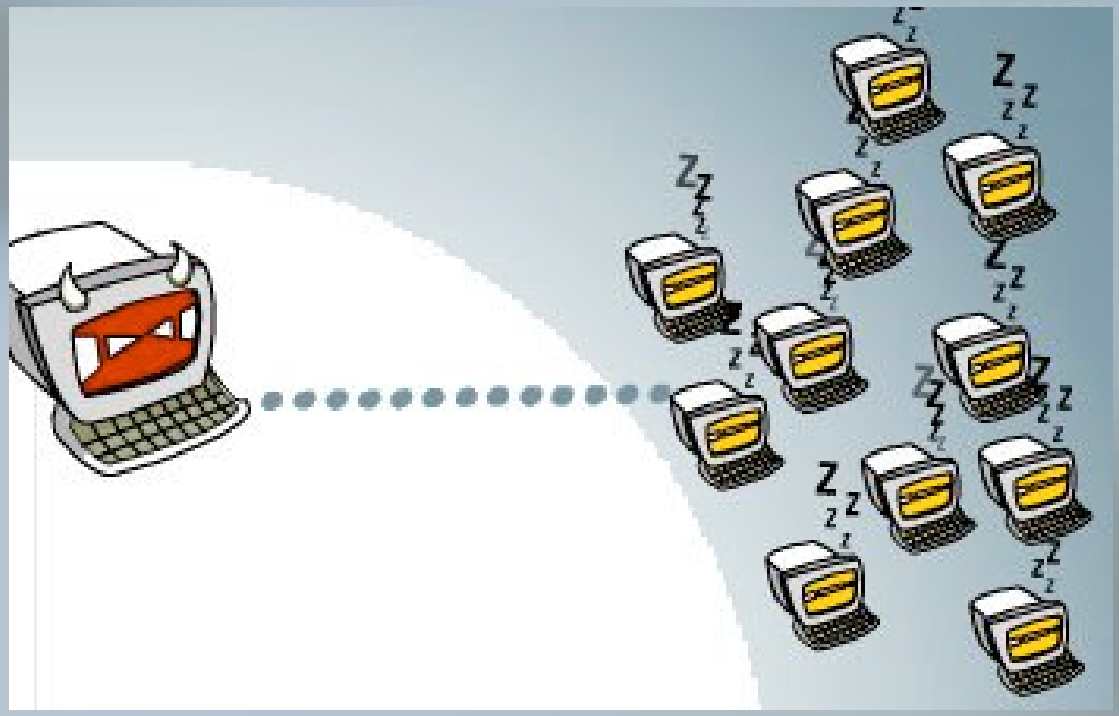
Security policies and procedures

- O que foi efetivo

Security Policy	Deterrence of a potential criminal	Detection of a criminal	Termination of an Employee or Contractor	Prosecution of an Alleged Criminal
Employees required to review and accept the written inappropriate use policy on any periodic basis	58%	6%	35%	10%
Periodic security education & awareness programs	30%	2%	5%	2%
Technically-enforced segregation of duties	30%	4%	9%	2%
Use of “white hat” hackers	30%	13%	5%	5%
Periodic risk assessments	29%	5%	4%	2%
Periodic systems penetration testing	29%	4%	4%	3%
Third-party security audits of PARTNER organizations	29%	7%	7%	4%
Employee/ contractor background check	28%	13%	17%	1%
Government security clearances	28%	10%	13%	-
Monitor Internet connections	28%	11%	24%	3%
New employee security training	28%	4%	5%	1%

Botnets

- Estratégias para conhecer e conter



Notícias recentes

- FBI detecta um milhão de computadores 'zumbis' nos EUA - 14 de junho, 2007
- Hackers 'infectam' páginas de busca na Internet - 29 de novembro, 2007
- Até 25% dos computadores podem estar infectados, dizem especialistas - 26 de janeiro, 2007 - Davos

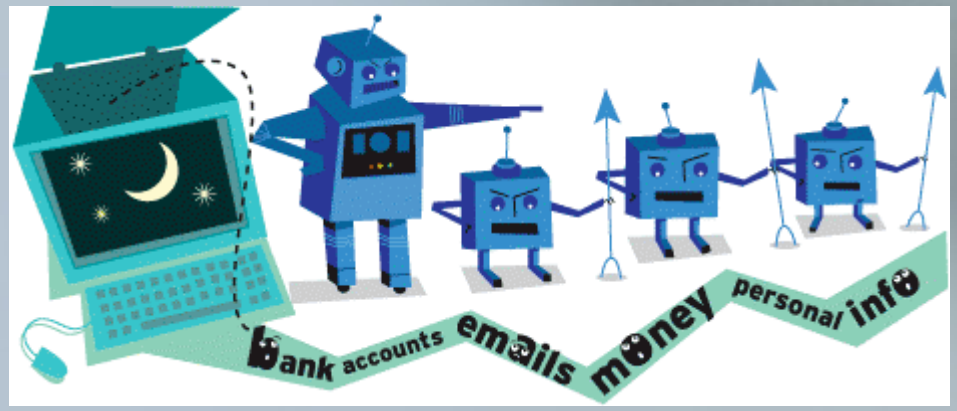
Botnets

- Até 25% dos computadores conectados à internet podem estar sendo usados por criminosos nas chamadas botnets - Vint Cerf
- "(A situação) é tão ruim quanto você possa imaginar, e coloca a internet inteira em risco" - John Markoff

Epidemia generalizada

- Botnets - pandemia
- Dos 600 milhões de computadores na internet atualmente, entre 100 e 150 milhões já fazem parte destas redes botnets

Vinton Cerf- Google



Conseqüências

- Uma única botnet, em um dado momento, usou cerca de 15% da capacidade de busca do Yahoo.

John Markoff

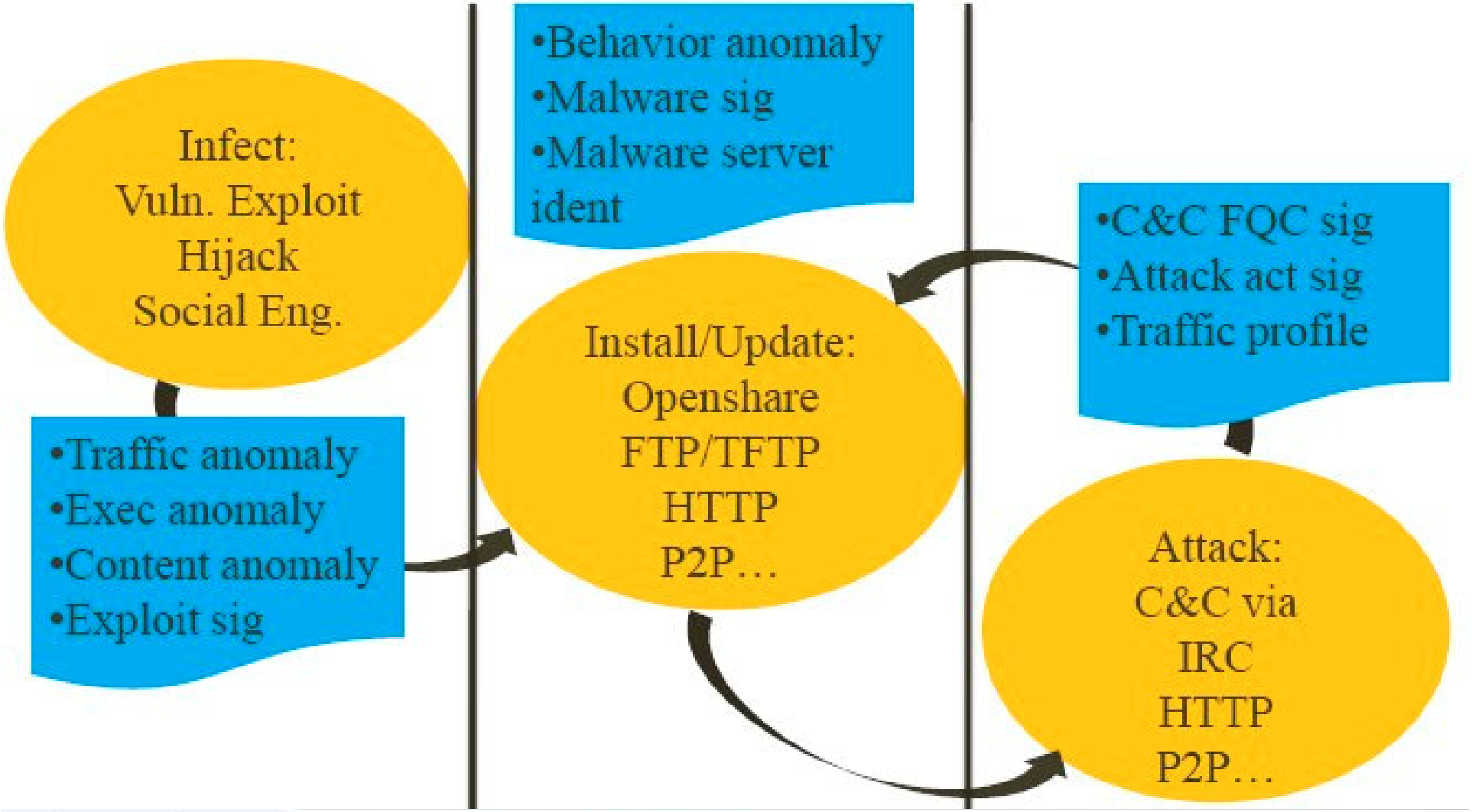
Escreve sobre tecnologia para o jornal

The New York Times

Extracting Malware Intelligence

- **Supporting An Anti-Malware Ecosystem**
- Fengmin Gong - Fireeye
  - Observando o ciclo de vida de uma botnet
  - Melhor estratégia de atacar uma botnet
  - Fator crítico – malware/botnet intelligence

Botnet - Malévolas mas não invisíveis



Conhecendo o inimigo

- Botnets precisam ser construídas,um bot por vez, da infeção à instalação e integração na rede de C&C
- Botnets utilizam computadores em rede mas assim aumenta a área de exposição que oportuniza detecção
- Botnets levam algum tempo para crescer abrindo oportunidade para controle
- Botnet é como uma doença (pandemia) requerendo contramedidas

Tratamento proativo

- Quanto mais madura uma botnet mais severo e disseminado é o dano.
- Medidas proativas devem ser preferidas
- Fator crítico- conhecimento acurado, rápido, disponível e completo sobre malware

Captura

- Detecção de tráfego anormal
  - Captura todo fluxo de tráfego suspeito sondando/explorando vulnerabilidades
  - Heurísticas adaptativas para captura
- Rede Bayesiana para análise da carga útil
  - Captura todas URLs suspeitas entregando conteúdo questionável
  - Acompanhamento “Stateful” dos redirecionamento com ofuscação
  - Cobre exploração clientes web & engenharia social

Máquina virtual

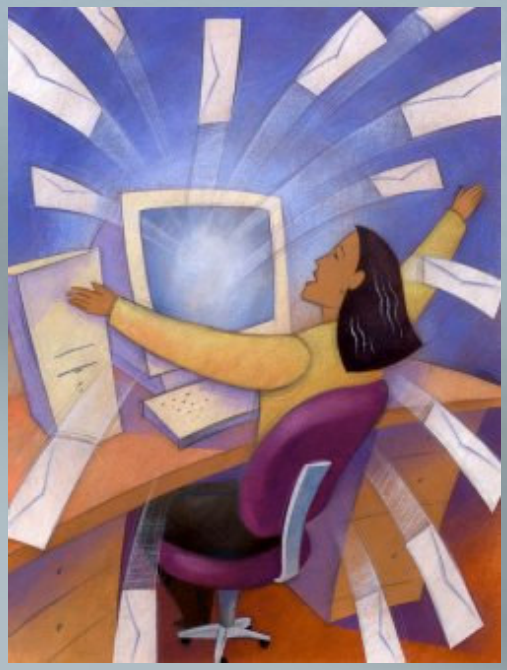
- Mediante o uso de VM obter confirmações
  - Máquinas virtuais vítimas instrumentadas
  - “Replay” adaptativo dos fluxos de tráfego capturados
  - Confirmar assinatura comportamento / efeito com ou sem assinatura

Máquina virtual

- Extrair informações adicionais
  - Extrair assinatura do exploit “0-day”
  - Interceptar todas as comunicações para fora
    - Extrair coordenadas alvo
    - Extrair assinatura de comunicação
  - Capturar imagens do malware
  - Capturar mudanças no Sistema Operacional
  - Prover correlação confiável: infeção-malware-ataque

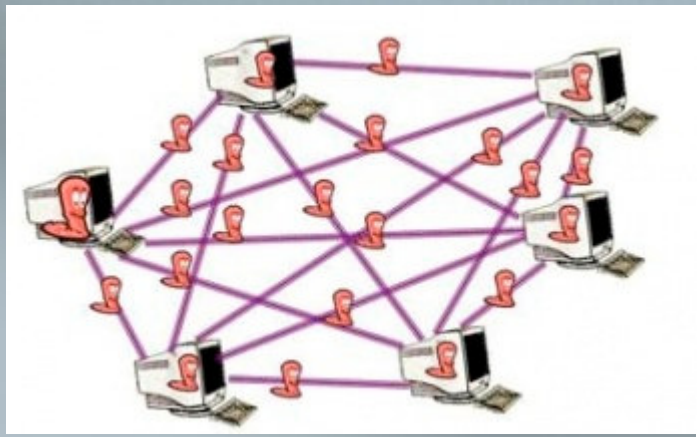
Next-Generation Botnet Malware

- Scaling Security Analysis vs. Next-Gen Botnet Malware Using VM-Based Analysis - Nicolas Feamster - Georgia Institute of Technology
- Redes botnets são usadas para atividades tais como:
  - spam
  - click fraud
  - denial-of-service attacks



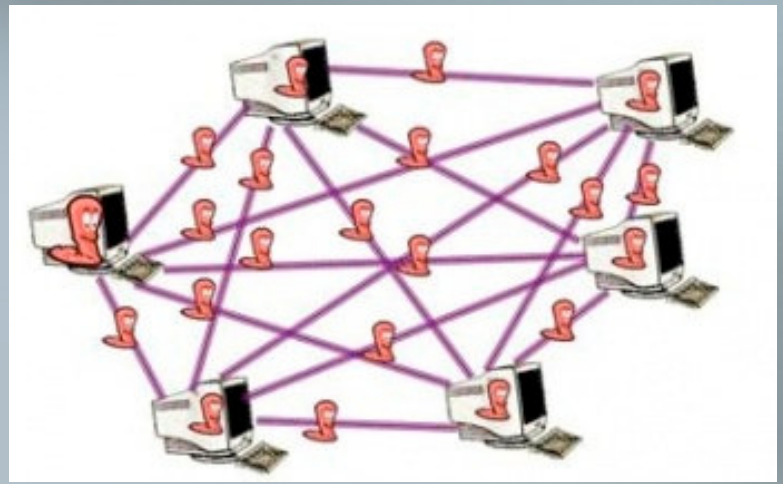
Identificando membros de botnets

- Identificar membros de botnets pode ajudar a demarcar estes ataques mas detectar passivamente a composição dos membros da botnet sem interromper sua operação é difícil.
- Estratégia de monitorar consultas a lista negra para expor composição da botnet.



Contra-inteligência

- Botmaster realizar consultas DNSBL para verificar se seus bots estão listados.
- Usando heurísticas para identificar quais consultas à lista negra DNSBL são feitas por um botmaster é possível compilar uma lista de prováveis bots
- Constatação: Delegação na botnet da incumbência de consultar



Comentários finais

- Quanto mais se aprende mais se descobre o que falta aprender
- Determine que algo pode e deve ser feito e então você achará o caminho para fazê-lo

Cert-RS

Computer Emergency Response Team - Rio Grande do Sul

http://www.cert-rs.tche.br/