Tratamento de Incidentes

Paula Tavares e Rogerio Bastos
Ponto de Presença da RNP na Bahia

{paulatavares,rogeriobastos}@pop-ba.rnp.br

POP-BA

Introdução

- Segundo a ITIL, um **Incidente** é qualquer evento que não faz parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção do serviço ou uma redução da sua qualidade;

- Um **Incidente de Segurança** pode ser definido como qualquer evento relacionado à segurança de sistemas de computação levando a perda de um ou mais princípios básicos da segurança: **Confidencialidade**, **Integridade** e **Disponibilidade;**

Exemplos de Incidentes de Segurança

- Tentativas de ganhar acesso não autorizado a sistemas ou dados;
- Ataques de negação de serviço;
- Uso ou acesso não autorizado a um sistema;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso;

Exemplos de Incidentes de Segurança

- Envio de spam, phishing/scam ou correntes da felicidade e de correntes para ganhar dinheiro rápido;
- Cópia e distribuição não autorizada de material protegido por direitos autorais;
- Utilização da Internet para fazer difamação, calúnia e ameaças;
- Ataques a outros computadores;
- Comprometimento de computadores ou redes;

Motivação para o Tratamento

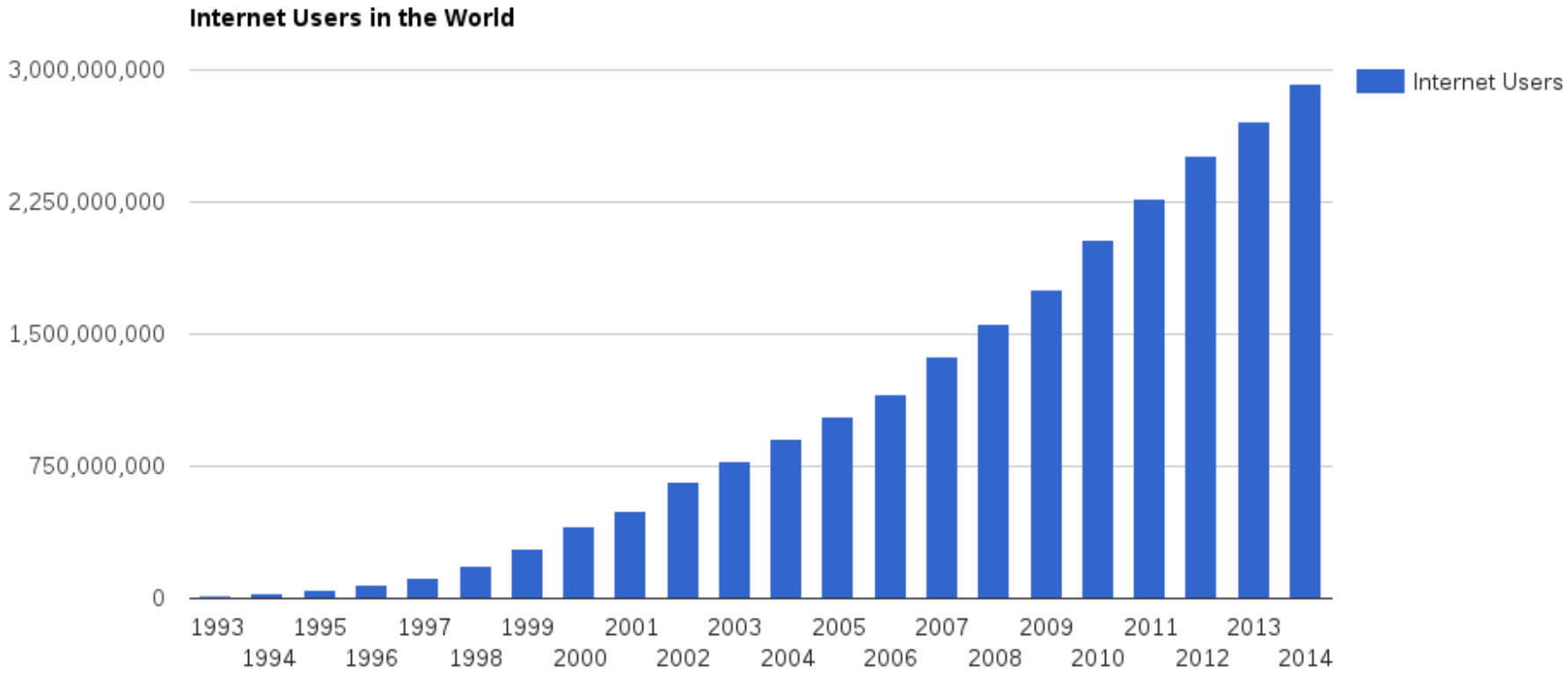
- A resposta adequada aos incidentes deve ser parte integrante da diretiva de segurança geral e da estratégia de atenuação dos riscos;
- O processo de resposta a incidentes de segurança tem fundamental importância para diminuir os danos causados por ataques;
- Prevenir é melhor do que remediar, mas é impossível impedir todos os incidentes de segurança;

Objetivos do Tratamento

- Resposta a incidentes de segurança é uma metodologia organizada para gerir consequências de uma violação de segurança da informação;

- O principal objetivo do processo de resposta a incidentes de segurança é minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível;

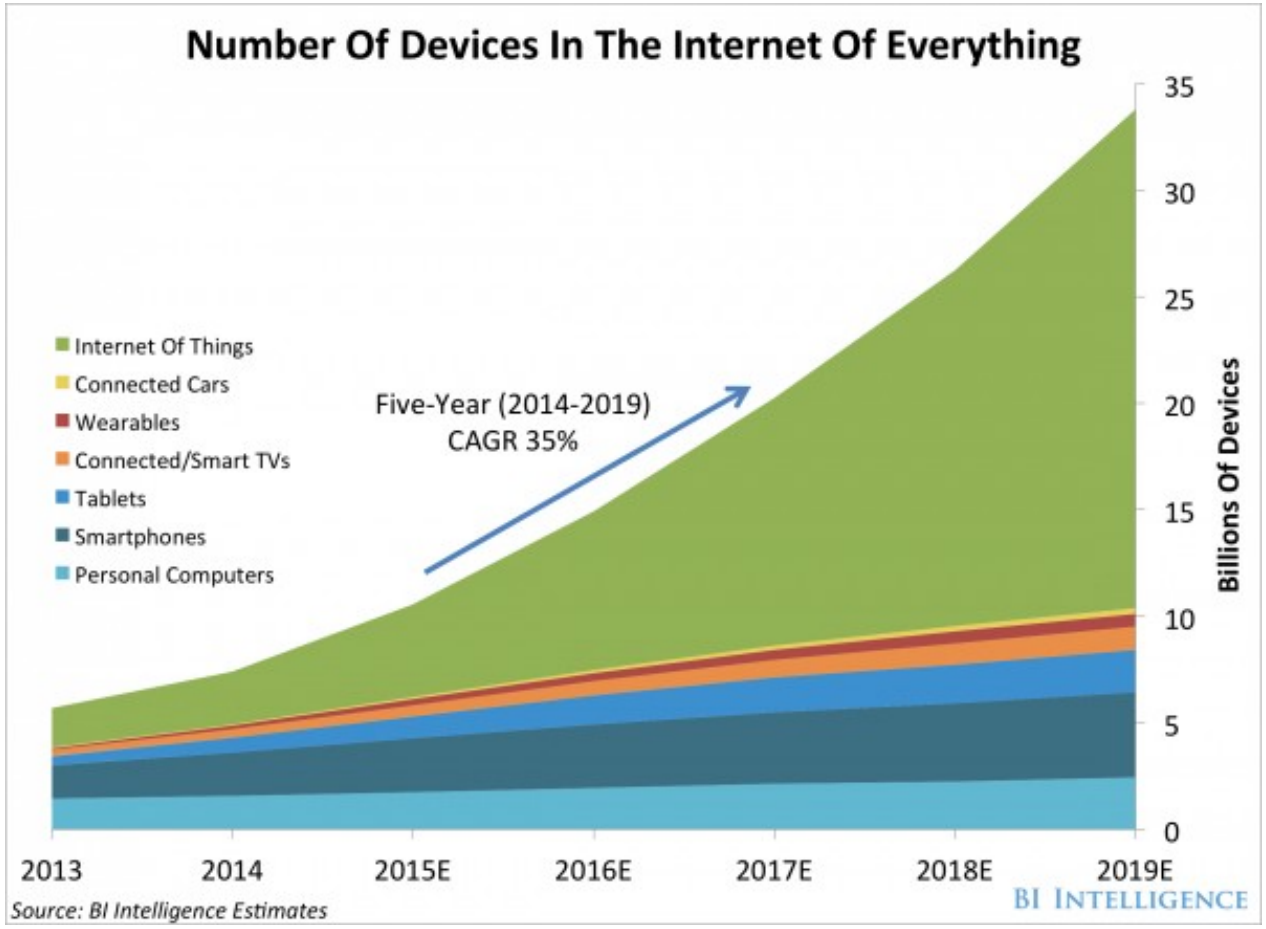
Estatísticas



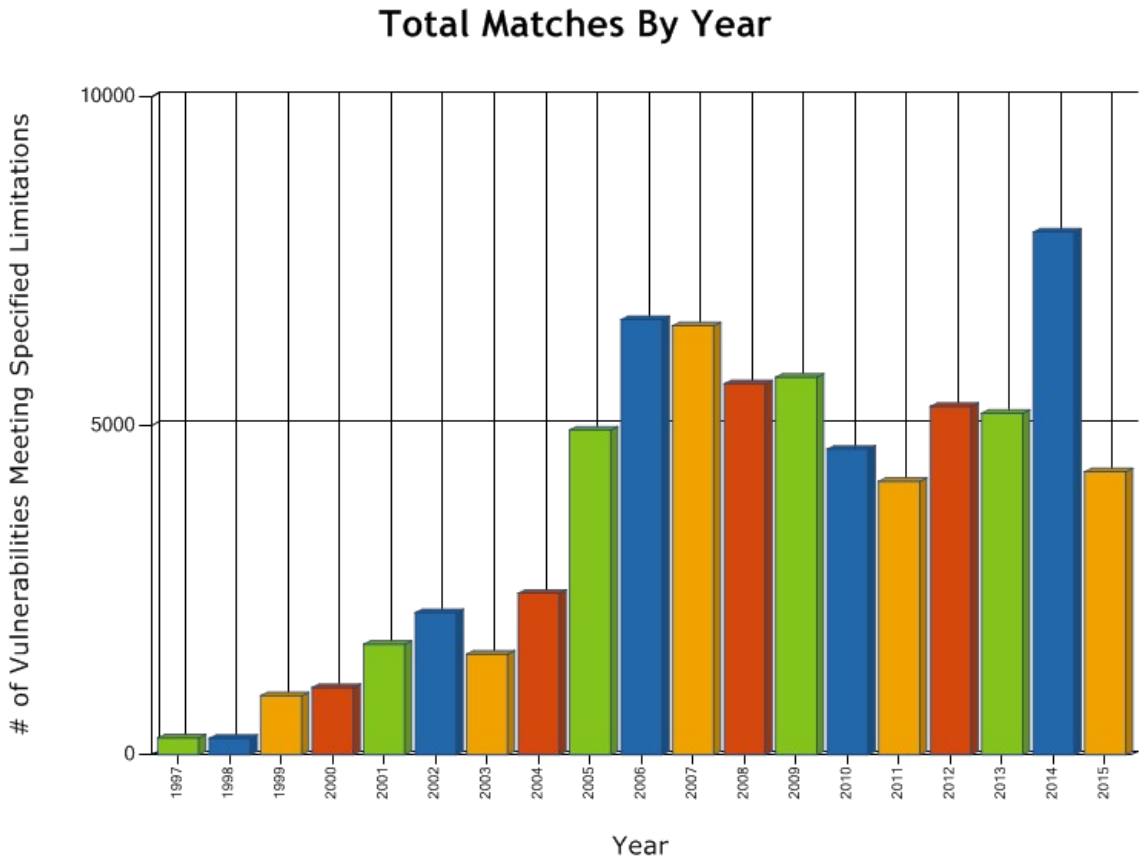
internet live stats

POP-BA

Estatísticas

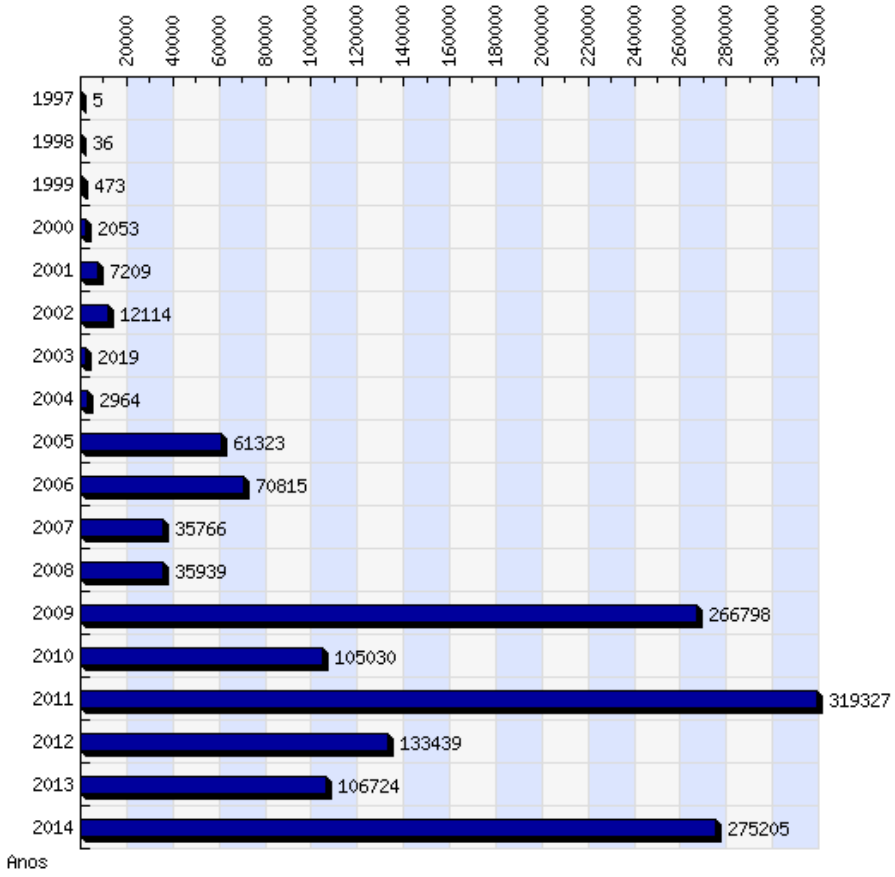


Estatísticas



National Vulnerability Database (NVD) from U.S. government

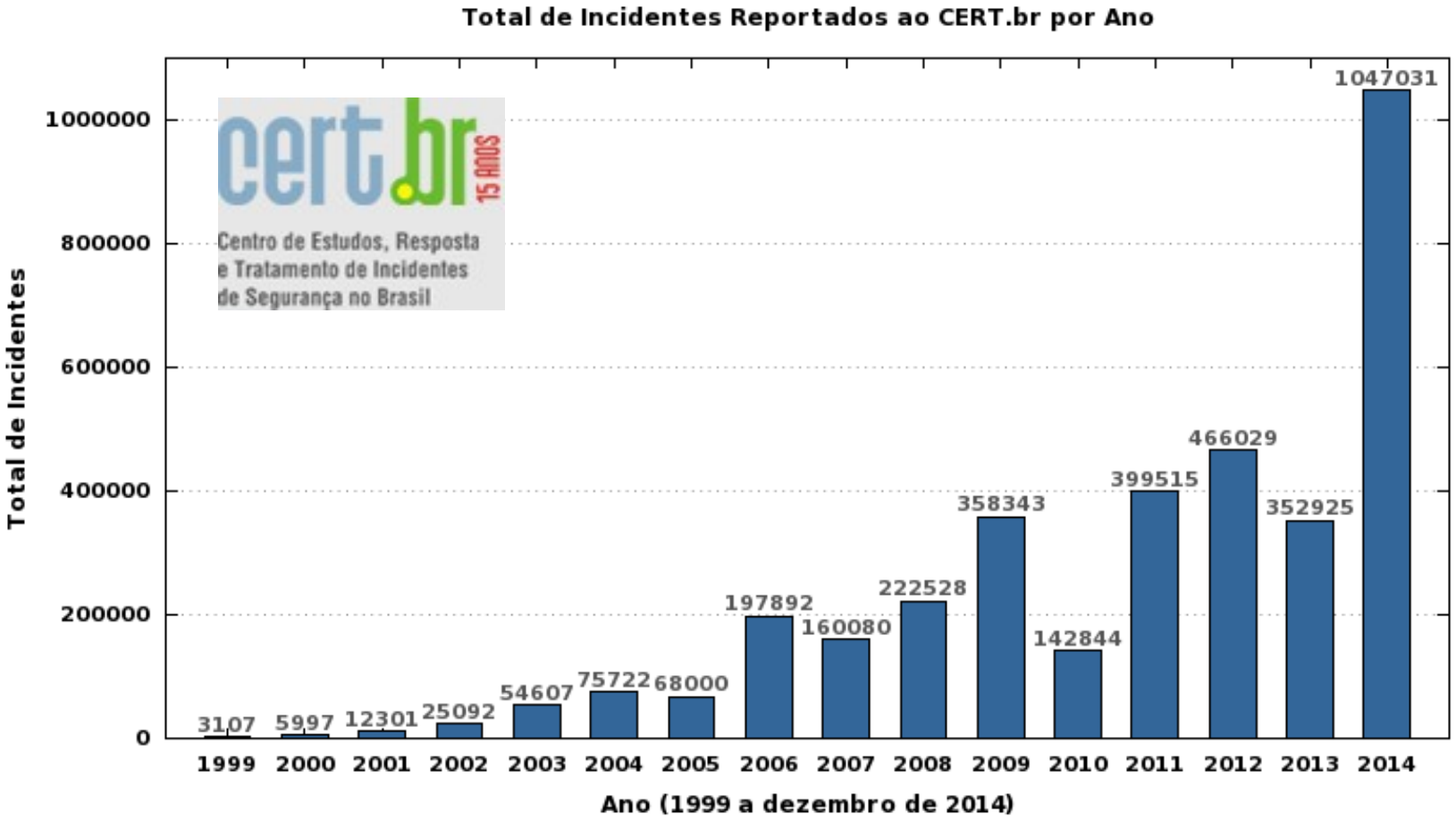
Estatísticas



CAIS Centro de Atendimento a Incidentes de Segurança

POP-BA

Estatísticas



Processo de Tratamento de Incidentes

- **Identificação** - detectar ou identificar de fato a existência de um incidente de segurança
- **Coordenação** - identificar os danos causados pelo incidente em questão
- **Mitigação** - isolar o problema e restabelecer o sistema
- **Investigação** - coletar e analisar as evidências do incidente de segurança
- **Educação** - avaliar o processo de tratamento de incidentes e verificar a eficácia das soluções implementadas

Incidentes

- Ataque de Força Bruta
- Envio de Spams
- Website Defacement
- DoS e DDoS

Ataque de Força Bruta - Definição

- Ataque que busca descobrir credenciais de acesso a um sistema através de tentativas.
  - Ataque de dicionário: utilização das principais senhas utilizadas
  - Ataque de força bruta: tentativa exaustiva

Ataque de Força Bruta - Implicações

- Permite o acesso ao serviço ou aplicação com os privilégios da conta comprometida
  - Exemplos:
    - E-mail: utilizar conta do usuário para envio de SPAM
    - SSH: utilizar recursos do servidor para hospedar arquivos maliciosos, atacar outros hosts na internet, etc

Ataque de Força Bruta - Detecção

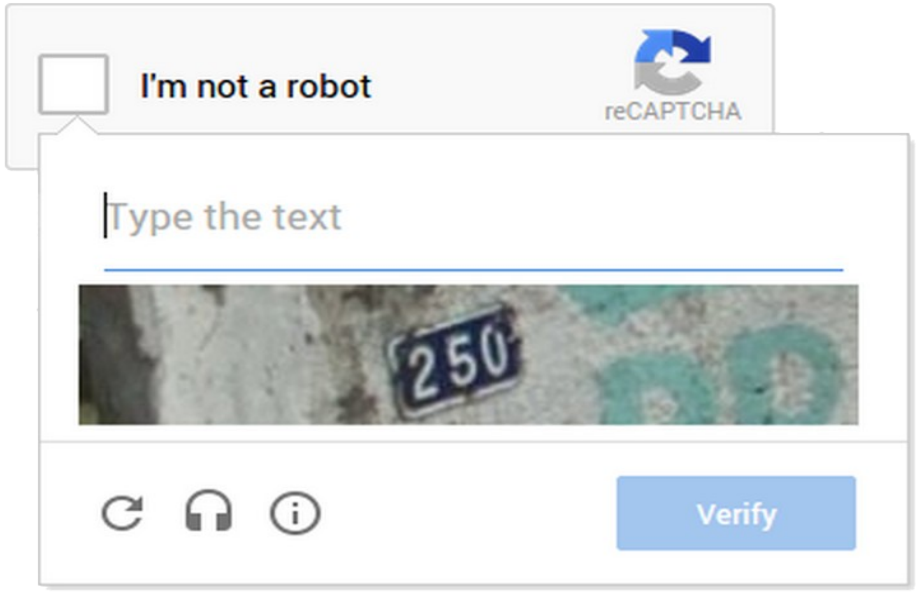
- Registro de log das tentativas de autenticação
- Monitoramento das tentativas sem sucesso
- Avaliação dos intervalos entre as tentativas de autenticação

Ataque de Força Bruta – Prevenir / Mitigar

- Utilização de politica de senhas seguras
  - Possuir no mínimo 8 (oito) caracteres
  - Utilizar pelo menos três tipos de caracteres: letras maiúsculas, minúsculas, números, caracteres especiais
  - Evitar utilizar palavras encontradas em dicionários ou dados associados ao usuário, tais como: nome, data de nascimento, placa de carro
  - Evitar utilizar sequências ou padrões de caracteres como: aaabbb, qwerty, 123321, 123456, abc123

Ataque de Força Bruta – Prevenir / Mitigar

- Solução em nível de aplicação :
  - CAPTCHA
  - Autenticação de dois fatores
  - Alterar o login / senha padrão



Ataque de Força Bruta – Prevenir / Mitigar

- Solução em nível de servidor:
  - Fail2Ban - http://www.fail2ban.org
  - SSHGuard - http://www.sshguard.net
  - Denyhost - http://denyhosts.sourceforge.net

Envio de Spams - Definição

- Quando seu servidor de e-mail passa a enviar spams para outros servidores

Envio de Spams - Implicações

- O servidor pode ser adicionado às *blacklists* e as mensagens de todos os usuários poderão ser rejeitadas ou classificadas como spam por outros servidores de e-mail.

Envio de Spams - Detecção

- Monitoramento do volume e dos destinos das mensagens enviadas
  - Pflogsumm - http://jimsun.linxnet.com/postfix_contrib.html
- Monitoramento das DNS-based Blackhole List (DNSBL)
- Verificar erro das mensagens rejeitadas por outros servidores

Envio de Spams – Prevenir / Mitigar

- Desabilitar ou restringir o uso de relay no servidor de e-mail
- Exigir autenticação para envio de mensagem
- Faça auditoria dos formulários de envio de mensagens nas aplicações web
- Implementar quota de envio de mensagens

Website Defacement - Definição

- Ataque no qual uma ou mais páginas de um site tem a aparência modificada.
- É comum a instalação de malwares para infectar os visitantes do site.

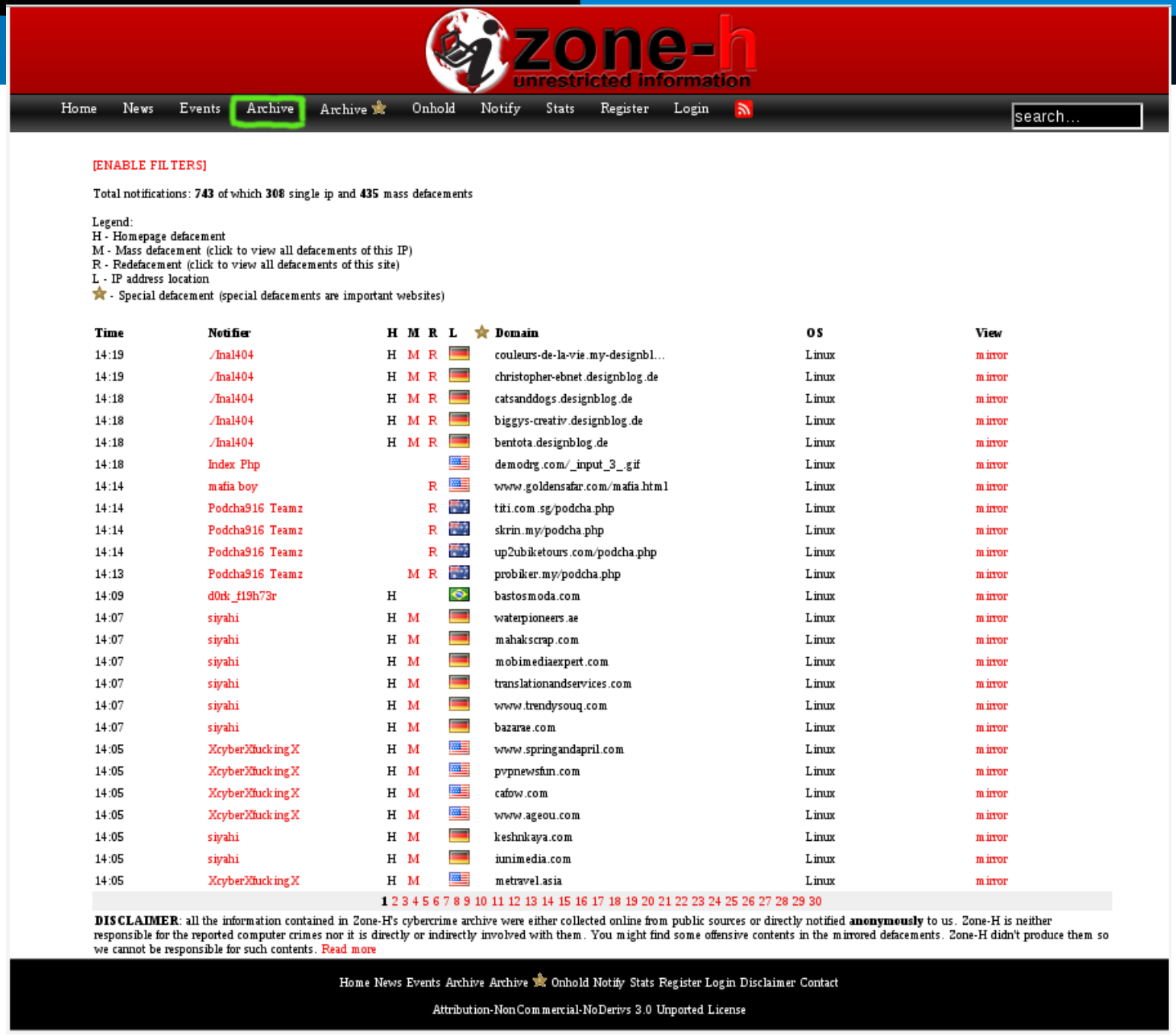
Website Defacement - Implicações

- Indisponibilidade do site
- Comprometimento da imagem da Instituição
- Disseminação de arquivos maliciosos

Website Defacement - Detecção

- Host Intrusion Detection System (HIDS)
  - Monitoramento da integridade dos arquivos
- Monitorar Logs
- Monitorar sites de divulgação de ataques
  - Site zone-h – www.zone-h.com/archive

Website Defacement - Detecção



zone-h
unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login search...

[ENABLE FILTERS]

Total notifications: **743** of which **308** single ip and **435** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Time	Notifier	H	M	R	L	★	Domain	OS	View
14:19	/Inal404	H	M	R			couleurs-de-la-vie.my-designbl...	Linux	mirror
14:19	/Inal404	H	M	R			christopher-ebnet.designblog.de	Linux	mirror
14:18	/Inal404	H	M	R			catsanddogs.designblog.de	Linux	mirror
14:18	/Inal404	H	M	R			biggys-creativ.designblog.de	Linux	mirror
14:18	/Inal404	H	M	R			bentota.designblog.de	Linux	mirror
14:18	Index Php						demodrg.com/_input_3_.gif	Linux	mirror
14:14	mafia boy			R			www.goldensafar.com/mafia.html	Linux	mirror
14:14	Podcha916 Teamz			R			titi.com.sg/podcha.php	Linux	mirror
14:14	Podcha916 Teamz			R			skrin.my/podcha.php	Linux	mirror
14:14	Podcha916 Teamz			R			up2ubiketours.com/podcha.php	Linux	mirror
14:13	Podcha916 Teamz		M	R			probiker.my/podcha.php	Linux	mirror
14:09	d0rk_f19h73r	H					bastosmoda.com	Linux	mirror
14:07	siyahi	H	M				waterpioneers.ae	Linux	mirror
14:07	siyahi	H	M				mahakscrap.com	Linux	mirror
14:07	siyahi	H	M				mobimediaexpert.com	Linux	mirror
14:07	siyahi	H	M				translationandservices.com	Linux	mirror
14:07	siyahi	H	M				www.trendysouq.com	Linux	mirror
14:07	siyahi	H	M				bazarae.com	Linux	mirror
14:05	XcyberXfuckingX	H	M				www.springandapril.com	Linux	mirror
14:05	XcyberXfuckingX	H	M				pvpnewsfun.com	Linux	mirror
14:05	XcyberXfuckingX	H	M				cafow.com	Linux	mirror
14:05	XcyberXfuckingX	H	M				www.ageou.com	Linux	mirror
14:05	siyahi	H	M				keshnkaya.com	Linux	mirror
14:05	siyahi	H	M				iunimedia.com	Linux	mirror
14:05	XcyberXfuckingX	H	M				metravel.asia	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more

Home News Events Archive Archive Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

Website Defacement – Prevenir / Mitigar

- Manter o servidor e a aplicação web atualizados
- Utilizar aplicações e plugins confiáveis
- Web Application Firewall (WAF)
  - ModSecurity - http://www.modsecurity.org
  - IronBee - http://www.ironbee.com

Website Defacement – Prevenir / Mitigar

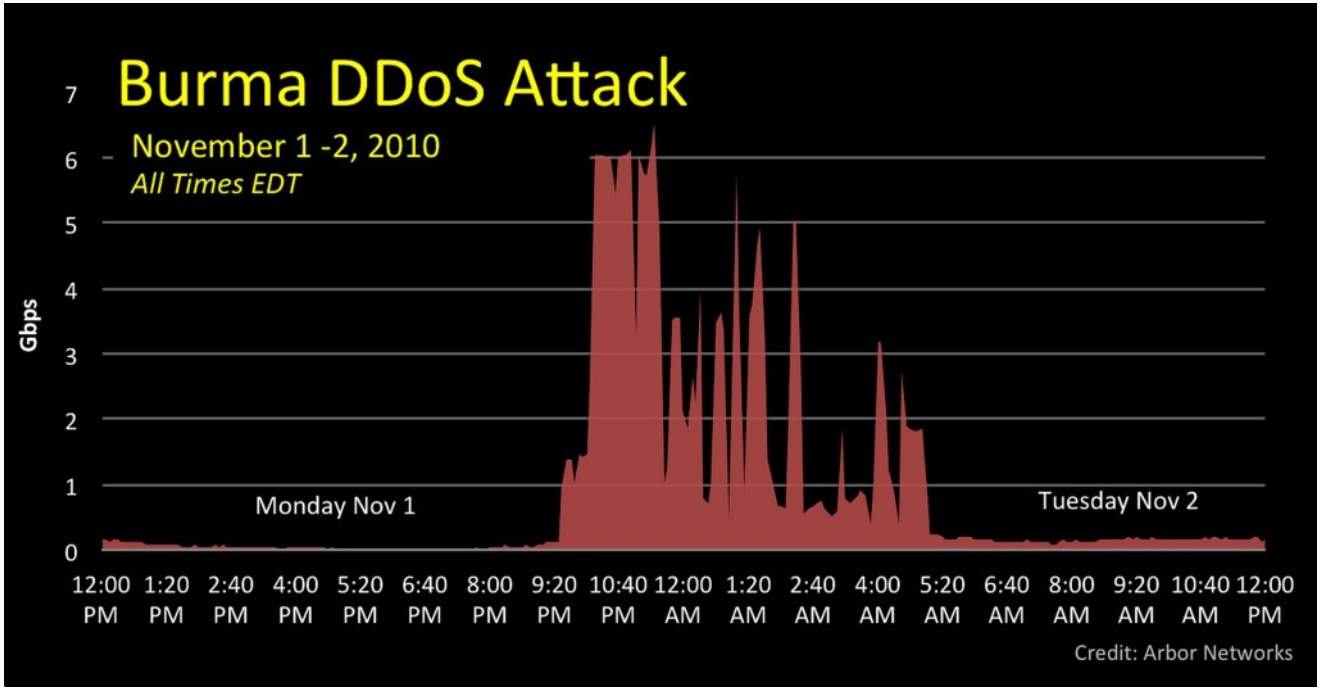
- Realizar testes periódicos em busca de vulnerabilidades
  - Wapiti - http://wapiti.sourceforge.net
  - Sqlmap - http://sqlmap.org
  - Wfuzz - http://www.edge-security.com/wfuzz.php
  - Arachni - http://www.arachni-scanner.com
  - Nikto - https://cirt.net/Nikto2
  - W3af - http://w3af.org
  - ZAP - https://github.com/zaproxy/zaproxy

Website Defacement – Prevenir / Mitigar

- Substitua o site atacado por uma página apresentável
  - Restaurar o backup não resolve o problema
- Investigar se arquivos ou códigos maliciosas foram adicionados ao site
  - Verficiar se constam nos backups recentes
- Identificar e corrigir o mecanismo utilizado para realizar o ataque
- Reestabelecer o serviço num novo servidor

DoS e DDoS - Definição

- DoS: o ataque de negação de serviço tem como objetivo tornar o sistema computacional inacessível através exaustão dos recursos do alvo.
- DDoS: Um ataque utilizando múltiplas máquinas atacando um único alvo leva o nome de ataque de negação de serviços distribuídos.



DoS e DDoS - Tipos

- Ataque baseado em volume tem como objetivo saturar a largura de banda do site
  - UDP floods
  - ICMP floods
  - Ataques de reflexão (DNS, NTP, SNMP)

DoS e DDoS - Tipos

- Ataques de exaustão de protocolo consomem recursos das tabelas de estado de firewall, IPS e servidores
  - TCP SYN floods
  - IP fragmentation
  - Smurf Attack

DoS e DDoS - Tipos

- Ataques na camada de aplicação são compostos por requisições (aparentemente) legítimas como objetivo explorar vulnerabilidades no protocolo ou na aplicação
  - HTTP flood
  - Slowloris
  - Vulnerabilidades

DoS e DDoS - Implicações

- Exaustão dos recursos da rede, aplicação ou serviço
- Indisponibilidade
- Aumento de gastos

DoS e DDoS - Detecção

- Monitoramento dos recursos do servidor
  - CPU, memória RAM, I/O
- Monitoramento da disponibilidade dos serviços
  - Zabbix, Icinga, etc
- Monitoramento do tráfego de rede
  - NetFlow
- Análise do tráfego
  - IPS

DoS e DDoS – Prevenir / Mitigar

- Possuir uma infraestrutura robusta
  - Distribuição geográfica
- Filtrar o trafego malicioso
- Contactar o *upstream*
- Contratar serviços de mitigação

Considerações Finais

- Logs de NAT
  - nfct_snatlog - https://github.com/italovalcy/nfct-snatlog
  - ulogd - https://home.regit.org/2014/02/logging-connection-tracking-event-with-ulogd/
- Os atacantes também usam IPv6
- Os CSIRTs são aliados!

Perguntas?