nic.br cgi.br | cert.br

**Web br 2016**

**São Paulo, SP**

14 de outubro de 2016

# Aplicações Web e ataques DDoS: alvo ou origem?

**Miriam von Zuben**
**miriam@cert.br**

cert.br nic.br cgi.br

# Agenda

- **Ataques DDoS**
- **Ataques DDoS a servidores e aplicações Web**
- **Como melhorar o cenário**
- **Referências**

# Ataques DDoS

cert.br nic.br cgi.br

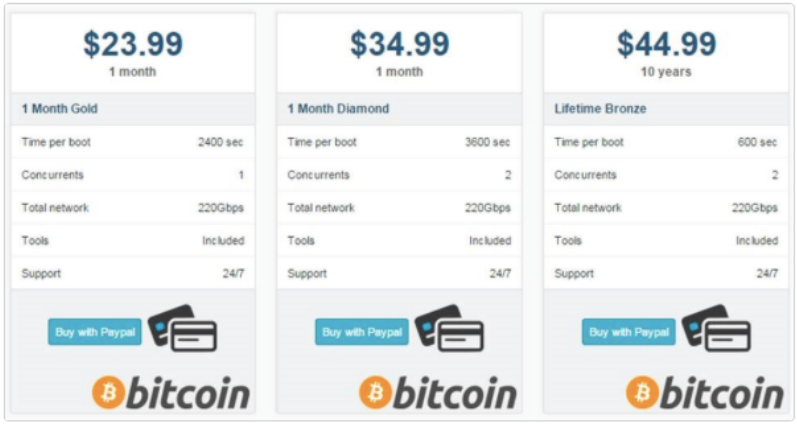
# Ataques DDoS

- **Ataque Distribuído de Negação de Serviço**
  - técnica pela qual um atacante utiliza, de forma **coordenada** e **distribuída**, um **conjunto de equipamentos** para tirar de operação um serviço, um computador ou uma rede conectada à Internet
- **Objetivo:**
  - não é invadir
  - exaurir recursos e causar indisponibilidade ao alvo
    - usuários dos recursos:
      - são diretamente afetados
      - ficam impossibilitados de acessar/realizar as operações desejadas
    - alvo do ataque:
      - não consegue diferenciar os acessos legítimos dos maliciosos
      - fica sobrecarregado ao tentar tratar todas as requisições recebidas
  - distrair equipes de redes e segurança para realizar outros ataques

# Ataques DDoS

- **Simples, fáceis e baratos de serem realizados**
  - *DDoS-as-a-Service* / *DDos-for-hire*
  - *Booters*, *DDoSers*, *Stressers*

| Russian Cybercriminal Underground Service Offerings | | | |
|---|---|---|---|
| **Duração** | **2011** | **2012** | **2013** |
| **1 hora** | **US$4-10** | **US$2-25** | **US$2-60** |
| **24 horas** | **US$30-70** | **US$15-60** | **US$13-200** |




*Example of booter advertised prices and capacities.*

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf
https://www.incapsula.com/ddos/booters-stressers-ddosers.html

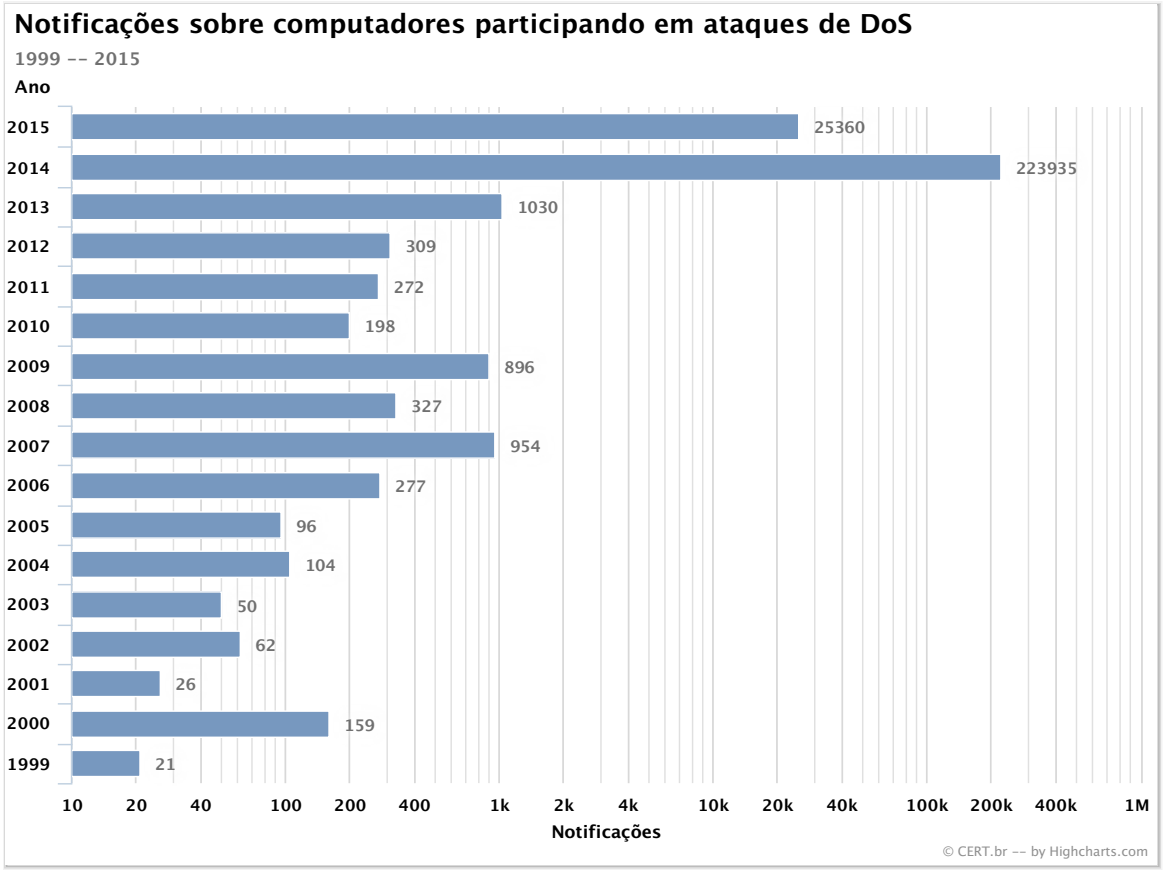
# Tipos de ataques DDoS (1/3)

- **Exaustão de recursos de *hardware***
  - tentam consumir a capacidade de equipamentos e exaurir seus recursos
    - em roteadores:
      - tentam consumir recursos e a capacidade de encaminhamento de pps
    - em *firewalls* e IPSs:
      - tentam consumir a capacidade da tabela de estado de conexões

- **Volumétrico**
  - medidos em Gbps / Tbps
  - tentam exaurir a banda disponível enviando grande volume de tráfego
    - utilizam *botnets,* máquinas com bastante banda, máquinas com pouca banda porém em grande quantidade
    - exploram características de serviços UDP que permitem a amplificação do tráfego (DRDoS)

# Tipos de ataques DDoS Volumétrico – DRDoS (2/3)

- **Serviços UDP permitindo abuso**
  - SNMP, SSDP, DNS recursivo aberto, entre outros



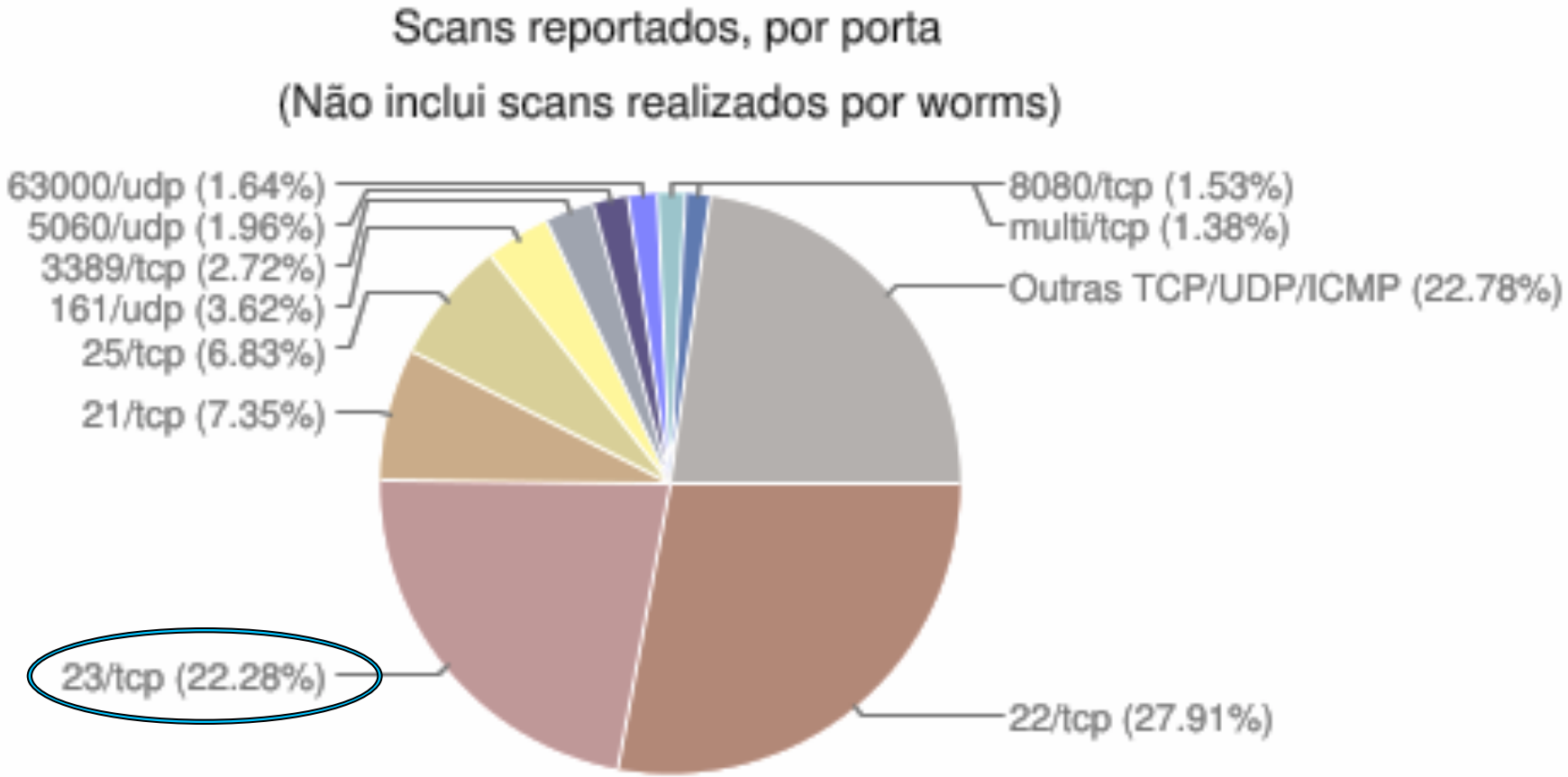
# Tipos de ataques DDoS (3/3)

- **Camada de aplicação**
  - procuram explorar as características específicas de uma aplicação ou serviço (camada 7), de tal maneira a:
    - saturar recursos
    - exceder o máximo de requisições (rps) que um servidor consegue gerenciar
    - fazer consultas complexas aos sistemas que demandem muito processamento
  - costumam ser mais difíceis de ser detectados
    - podem ser confundidos com problemas de implementação da aplicação
    - não precisam de muitas máquinas e nem de muito tráfego para serem realizados

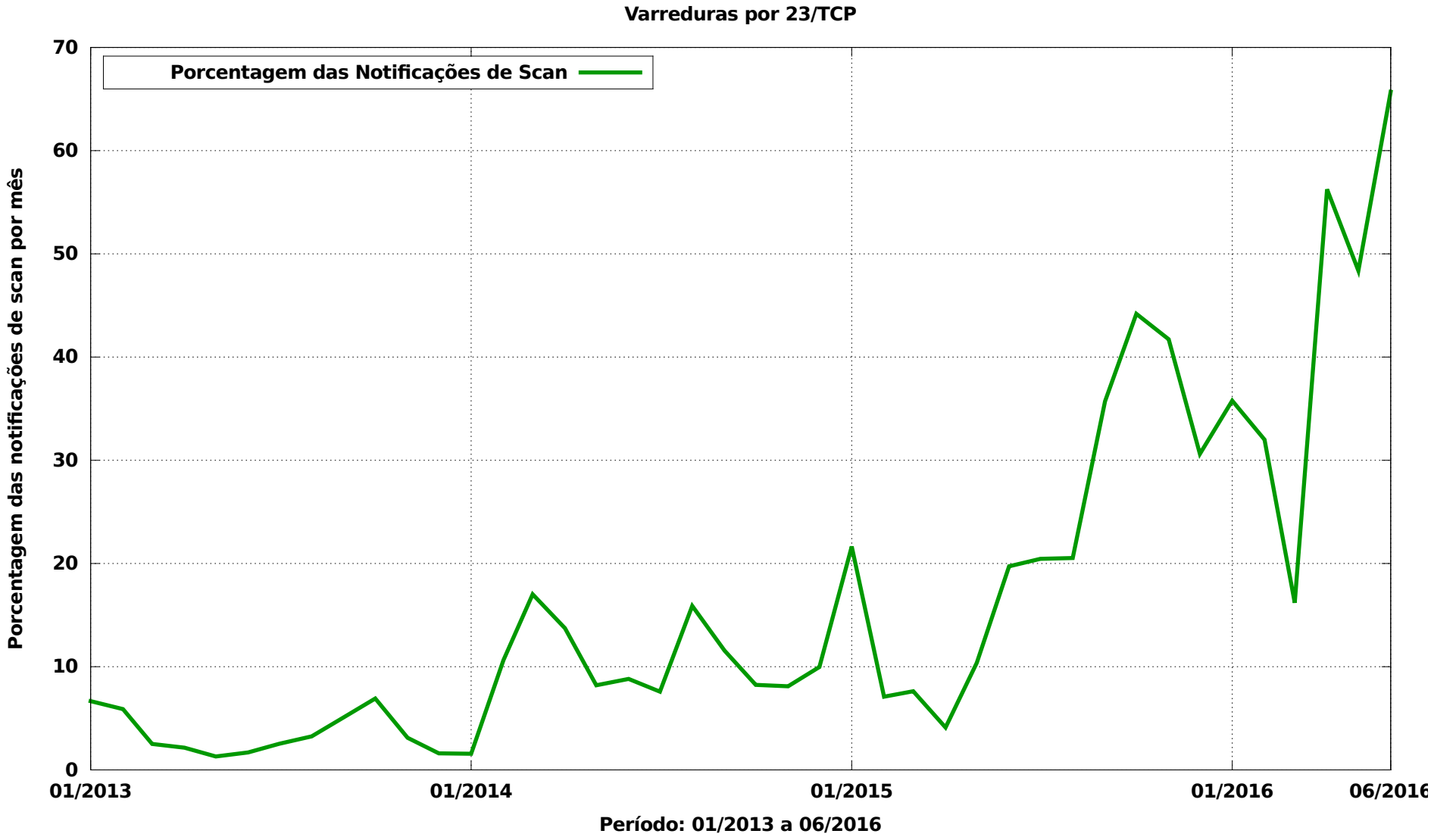
# Ataques usando *botnets*

- **Um dos principais vetores de ataques**
- **Formadas por:**
  - máquinas de usuários comprometidas
  - servidores Web
  - dispositivos IoT
    - CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc
    - *malware* se propaga geralmente via telnet
    - explora senhas fracas ou padrão
    - muitas vezes são “backdoors” dos fabricantes

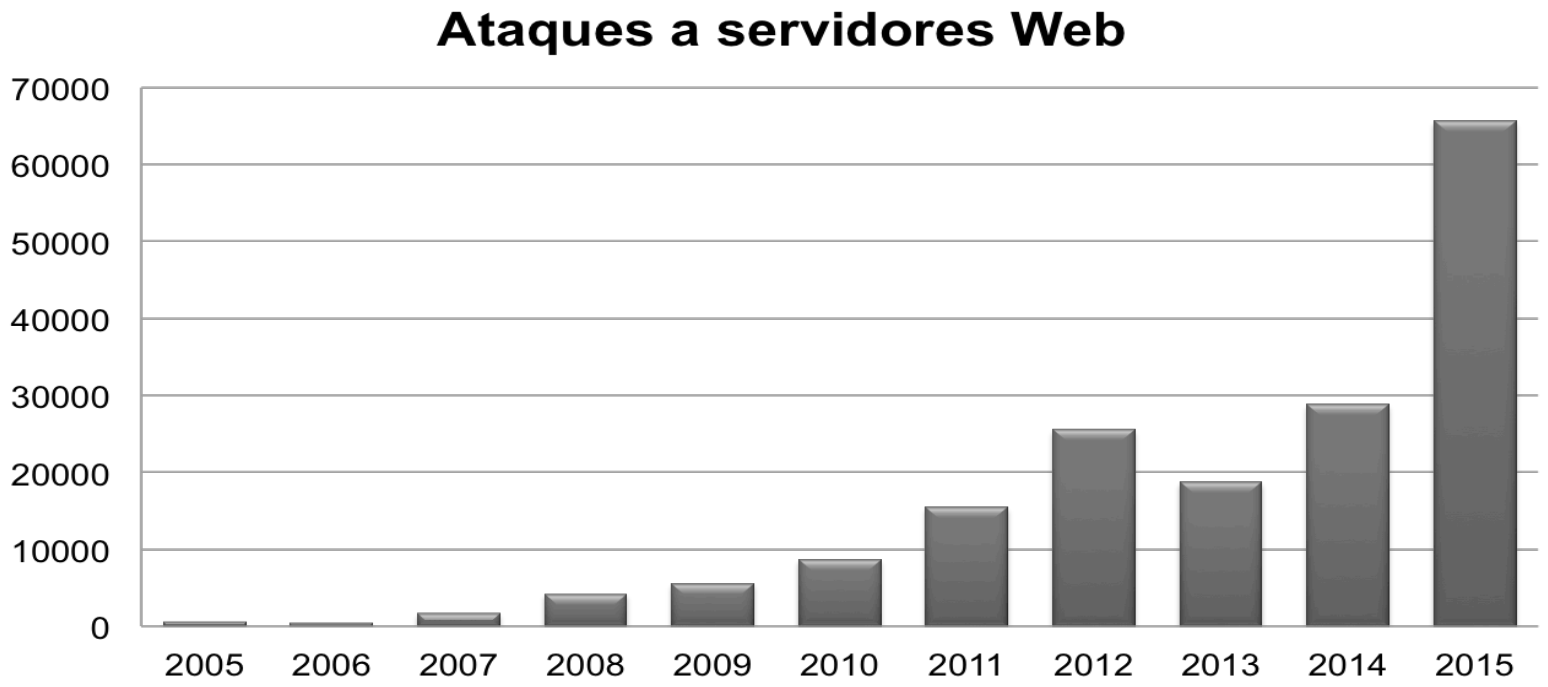
# Notificações ao CERT.br:
# ***Scans* por porta em 2015**



# Notificações ao CERT.br:
# *Scans* por 23/TCP – 2013 a jun/2016



# Estatísticas CERT.br – 2005 a 2015

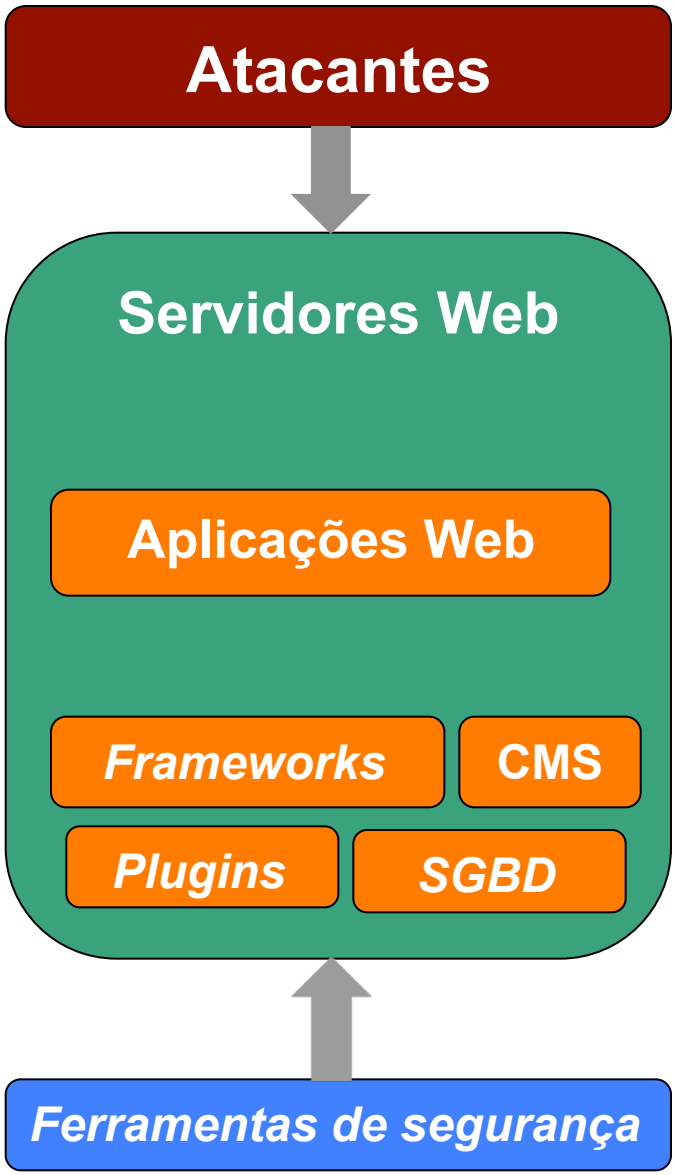



- Aumento de 128% de 2015 em relação a 2014
- Grande quantidade de ataques de força bruta (conta de administração) contra CMS

Ataques visando o comprometimento de servidores Web ou desfigurações de páginas na Internet
http://www.cert.br/stats/incidentes/

# Ataques DDoS a servidores e aplicações Web

cert.br nic.br cgi.br




**Motivação:**
Política, ideológica, econômica
Aplicar e disparar golpes e ataques:
- DDoS, malware e *phishing*
- coleta e repositório de dados

**Ferramentas de ataque:** amplamente disponíveis

Muito visados:
- máquinas bem conectadas
- grande capacidade de processamento

Cada vez mais complexas e com muitas vulnerabilidades
Falta de testes adequados
- testes apenas para casos de uso, não incluem testes de abuso

Pressão econômica para serem lançadas
Precisam estar acessíveis

Instalação e senha padrão
Muitas vulnerabilidades
Necessidade de atualizações constantes
- nem sempre disponíveis

Não conseguem remediar os problemas
*Pen test* de aplicação
- geram efeitos a curto prazo
- não alteram o comportamento

# Ataques Web são reflexo do cenário atual

## Empresas e instituições

Segurança não é parte dos requisitos

- uma das primeiras a ser cortada

Diversas *startups* que cresceram

Dificuldade em:

- entender, lidar com os problemas
  - "Segurança é paranoia, nada vai acontecer"
- avaliar os riscos
  - informações valiosas disponibilizadas
  - imagem da empresa

## Administradores de redes e serviços Web

Precisam correr atrás dos prejuízos

- troca de senhas
- atualizações
- correção de erros
- aplicações legadas

## Desenvolvedores Web

Priorizam a funcionalidade

- em detrimento da segurança
  - aplicações *just in time*
- erros podem trazer prejuízos
  - atuais e futuros

Terceirizam a segurança

- *firewall*, políticas, criptografia
- ultima fase do ciclo de vida do desenvolvimento da aplicação

Sem capacitação para desenvolver com requisitos de segurança

- não aprendem
- aprendem só nos últimos anos
- cobram mais caro

# Ataques DDoS e aplicações Web

cert.br nic.br cgi.br

# Auto DDoS

- **Porque ocorrem**
  - falhas de programação
  - falta de testes adequados
  - excesso de complexidade
  - mal-dimensionamento
  - campanhas de *marketing*

- **Empresas não costumam:**
  - admitir o problema
  - reconhecer como sendo negação de serviço

# Aplicações como origem dos ataques

- **Servidores invadidos**
- **Exploração de vulnerabilidades**
  - JavaScript-based  DDoS
    - inclusão de JavaScripts maliciosos
    - invasão de *sites* de terceiros que hospedam JavaScripts
  - *Plugins*


https://www.helpnetsecurity.com/2014/09/23/jquerycom-compromised-to-serve-malware-via-drive-by-download/

# Aplicações como origem dos ataques Operação Ababil

## Lessons learned from the U.S. financial services DDoS attacks

BY: ARBOR NETWORKS - 12/13/2012

**By Dan Holden and Curt Wilson of Arbor's Security Engineering & Response Team (ASERT)**

During the months of September and October we witnessed targeted and very serious DDoS attacks against U.S. based financial institutions. They were very much premeditated, focused, advertised before the fact, and executed to the letter.

In the case of the September 2012 DDoS attack series, many compromised PHP Web applications were used as bots in the attacks. Additionally, many WordPress sites, often using the out-of-date TimThumb plugin, were being compromised around the same time. Joomla and other PHP-based applications were also compromised. Unmaintained sites running out-of-date

***... compromised PHP Web applications were used as bots in the attacks ..***
***... many WordPress sites, often using the out-of-date TimThumb plugin ...***
***... Joomla and other PHP-based applications were also compromised ...***
***... Unmaintained sites running out-of-date extensions are easy targets and the attackers to upload various PHP webshells which were then used to further deploy attack tools ...***

http://www.arbornetworks.com/asert/2012/12/lessons-learned-from-the-u-s-financial-services-ddos-attacks/

# Aplicações como origem dos ataques
# Força bruta em conta admin - *Botnets*

Mathew J. Schwartz
News

Connect Directly

2 COMMENTS
COMMENT NOW

Login

50% 50%

Tweet

**Thousands of WordPress sites with accounts that use the common default username 'admin' have been hacked. One theory: the creation of a large WordPress botnet.**

Attention, WordPress users: If you have a WordPress username set to "admin," change it immediately.

That warning was issued Friday by WordPress founder Matt Mullenweg, in the wake of reports that thousands of WordPress sites with an administrator username set to "admin" or "Admin" had been compromised via large-scale brute force attacks. Service provider HostGator, notably, reported Thursday that "this attack is well organized and ... very, very distributed; we have seen over 90,000 IP addresses involved in this attack."

**Anonymous: 10 Things We Have Learned In 2013**

*(click image for larger view and for*

http://www.darkreading.com/attacks-and-breaches/wordpress-hackers-exploit-username-admin/d/d-id/1109538/

# Aplicações como origem dos ataques


## Google Maps Plugin Vulnerability Leveraged in DDoS Attacks

By Brian Prince on February 25, 2015

Share 44 G+1 6 Tweet Recomendar 13 RSS

**Hackers are exploiting a known vulnerability in a Google Maps plugin for Joomla to launch distributed denial-of-service attacks against enterprises.**

In February 2014, multiple vulnerabilities were discovered in the Google Maps plugin for Joomla. Among the vulnerabilities is a bug that allows the plugin to act as a proxy. According to Akamai, attackers have been leveraging the vulnerable installations en masse for reflected floods using tools such as DAVOSET and UFONet. With help from PhishLabs' R.A.I.D (Research, Analysis, and Intelligence Division), Akamai matched DDoS signature traffic originating from multiple Joomla sites and ultimately identified more than 150,000 potential Joomla reflectors on the Web.

http://www.securityweek.com/google-maps-plugin-vulnerability-leveraged-ddos-attacks/

NEWS

# Update: Malware-infected home routers used to launch DDoS attacks

## Researchers found a botnet of more than 40,000 routers being used to launch the attacks

The researchers said they don't believe the routers were hacked through a vulnerability in their firmware, but because they had been deployed in an insecure manner: with their management interfaces exposed to the Internet via SSH and HTTP using default credentials.

In addition to DDoS attacks, compromised routers are used to redirect users to malicious websites, intercept online banking sessions, inject rogue ads into Web traffic, steal credentials for various online accounts and perform other illegal activities.

http://www.computerworld.com/article/2921559/malware-vulnerabilities/malware-infected-home-routers-used-to-launch-ddos-attacks.html

# Largest Video Site Source of Massive DDoS Attack via XSS Vulnerability?!

CHRISTOPHOR RICK × APRIL 4, 2014

One of my websites was the target of several DDoS attacks in the past, but I have never been the source of one. Not all video-centric websites can say the same according to PCWorld reporting on research from web security company Incapsula. Apparently, someone left a gaping hole in their code that was found and exploited. Oops!

> Because of that code injection malicious users were able to inject Javascript code into the profile picture img tag. Every time that picture was found in a page somewhere, the code was lurking, prepared to execute and hijack a user's browser. The result, says Incapsula, was over 20M HTTP GET requests from more than 22,000 users.

http://tubularinsights.com/video-site-source-of-ddos-attack/

# Alvo dos ataques

- **Tango Down**
  - organizados via IRC, redes sociais, etc
- **Principais motivações**
  - hacktivismo
    - #OpOlympicHacking, #OpOperadoras, #OpIcarus
  - extorsão
    - ArmadaCollective, DD4BC
  - política
    - partidos, governo
  - censura
    - midia em geral, *blogs* de jornalistas

# 620Gbps contra o Blog do Brian Krebs

BBC NEWS

## Massive web attack hits security blogger

22 September 2016 | Technology

The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

http://www.bbc.co.uk/news/amp/37439513

# Source code of Mirai botnet responsible for Krebs On Security DDoS released online

Now anyone can use the IoT-based botnet for their own destructive purposes.

By Charlie Osborne for Zero Day | October 3, 2016 -- 08:43 GMT (01:43 PDT) | Topic: Security

The source code for the botnet which disrupted Krebs On Security has been published online, leading to fears that the botnet will soon be used by practically anyone to flood the internet with powerful -- and expensive -- attacks.

This month, security expert Brian Krebs' blog, Krebs On Security, was struck with one of the largest distributed denial-of-service (DDoS) attacks on record.


*Europol*

At 620 Gbps, Akamai engineers were able to repel the attack, but the company -- which gave Krebs a home pro-bono -- was forced to let him go as a "business decision" since keeping the blog and weathering more DDoS attacks could have ended up costing the business a fortune.

The botnet responsible is based on malware called Mirai. The malicious code utilizes vulnerable and compromised Internet of Things (IoT) devices to send a flood of traffic against a target.

In this case, the DDoS attack included SYN Floods, GET Floods, ACK Floods, POST Floods, and GRE Protocol Floods.

http://www.zdnet.com/article/source-code-of-mirai-botnet-responsible-for-krebs-on-security-ddos-released-online/

# Mirai - IoT botnet


https://blog.cloudflare.com/say-cheese-a-snapshot-of-the-massive-ddos-attacks-coming-from-iot-cameras/

# Como melhorar o cenário

cert.br nic.br cgi.br

# Como melhorar o cenário

- **Não é possível impedir que os ataques ocorram**
  - com planejamento adequado
  - é possível torná-los menos eficazes e danosos
- **Solução depende de diversas camadas**
- **Preocupação com segurança deve estar presente em todas as partes que compõe a aplicação:**
  - servidor Web
  - framework
  - CMS
  - SGBD
- **IoT**
  - maiores preocupações com segurança

# Servidores Web (1/2)

- **Implementar boas práticas:**
  - BCP38/BCP84
  - filtrar pacotes com endereços "*spoofados*"
  - http://bcp.nic.br/entenda-o-antispoofing/
- **Manter os equipamentos atualizados**
  - sistema operacional e todos os serviços nele executados
  - serviço Web, SGBD, extensões, módulos e *plugins*
- **Desabilitar serviços desnecessários**
- **Ser cuidadoso ao usar e elaborar senhas**
  - se disponível, usar verificação em duas etapas

# Servidores Web (2/2)

- **Verificar o tráfego a procura de indícios**
  - de entrada na rede:
    - tentativas de acesso não autorizado
  - de saída da rede:
    - vazamento de dados, *scan* e acessos indevidos partindo da rede
- **Treinar pessoal para tratar incidentes de segurança**
- **Conhecer o comportamento "normal"**
- **Estar atento a *sites* e *blogs* de segurança**
  - ficar ciente de tendências de ataques e novas vulnerabilidades

# CMS

- **Manter o CMS e os *plugins* atualizados**
- **Restringir acesso à interface de administração**
  - apenas aos administradores de aplicações
- **Não usar contas padrão de administração (admin)**
- **Usar senhas fortes**
  - se disponível, habilitar a verificação em duas etapas
- **Seguir os guias de segurança dos fornecedores**
- **Utilizar *plugins* de segurança, se disponível**

# Aplicações Web (1/3)

- **Uma das principais portas de entrada para o uso indevido dos servidores Web**
- **Segurança deve ser pensada em todas as fases:**
  - projeto, desenvolvimento, testes, entrada em produção, acompanhamento de *logs*, manutenção

| OWASP Top 10 – 2013 |
| --- |
| A1 – Injeção de código |
| A2 – Quebra de autenticação e Gerenciamento de Sessão |
| A3 – *Cross-Site Scripting* (XSS) |
| A4 – Referência Insegura e Direta a Objetos |
| A5 – Configuração Incorreta de Segurança |
| A6 – Exposição de Dados Sensíveis |
| A7 – Falta de Função para Controle do Nível de Acesso |
| A8 – *Cross-Site Request Forgery* (CSRF) |
| A9 – Utilização de Componentes Vulneráveis Conhecidos |
| A10 – Redirecionamentos e Encaminhamentos Inválidos |

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

# Aplicações Web (2/3)

- **Implementar a segurança no lado do servidor**
  - controles podem ser desabilitados pelos usuários
- **Considerar o uso de WAF (*Web Application Firewall*)**
  - oferece recursos extras de proteção
  - ajuda a identificar e bloquear os ataques mais comuns
  - deve ser usado como uma camada a mais de proteção
    - não como solução única de segurança
    - qualquer falha que apresente pode colocar em risco toda a aplicação
- **Não basta estar em conformidade (*compliance*)**

# Aplicações Web (3/3)

- **Estar preparado para tratar notificações de usuários**
- **Testar, testar e testar:**
  - teste de carga (*over provision*)
  - atenção ao carregar as aplicações no ambiente de produção
  - considerar que serão executadas em ambiente hostil
    - testes de abuso, não apenas de uso
  - testar de redes externas também
  - ferramentas:

    *OWASP Zed Attack Proxy Project*
    **https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project**

# Como lidar com IoT
# Usuário (1/2)

- **Assumir que os dispositivos virão com sérios problemas**
  - necessário fazer *hardening*
  - testar em ambiente controlado
  - assumir que terá um "*backdoor*" do fabricante
- **Considerar uma rede de gerência**
  - isolar os dispositivos completamente
- **Antes de comprar**
  - verificar se o fabricante possui política de atualização de *firmware*

# Como lidar com IoT
# Usuário (2/2)

- **Ao fazer a implantação, planejar**
  - se haverá algum esquema de gerência remota
  - como atualizar remotamente
- **Ser criterioso ao escolher o fornecedor**
  - fazer testes, identificar qual o *chipset*, verificar histórico de tratamento de vulnerabilidades do fabricante do *chipset*, etc
- **Dificuldades de fazer análise / perícia**

# Como lidar com IoT
# Desenvolvedores

- **Não usar protocolos obsoletos**
- **Usar criptografia e autenticação forte**
- **Não ter senha do dia, senha padrão não documentada, *reset* de configuração via rede, etc**
- ***Defaults* seguros**
- **Atualização**
  - precisa ser possível
  - necessário prever algum mecanismo de autenticação
- **Usar práticas de desenvolvimento seguro**

# Referências e Leituras recomendadas

cert.br nic.br cgi.br

# Referências e Leituras recomendadas

- **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**
  - http://www.cert.br/docs/whitepapers/ddos/
- **Dicas para manter um ambiente Web seguro**
  - https://www.security.unicamp.br/31-dicas-para-manter-seu-ambiente-web-seguro.html
- **10 Dicas para manter seu Joomla seguro**
  - https://www.security.unicamp.br/22-dicas-seguranca-joomla.html
- **Wordfence**
  - https://www.security.unicamp.br/67-wordfence-um-plugin-de-seguranca-para-wordpress.html

# Obrigada

www.cert.br

miriam@cert.br

@certbr

**14 de outubro de 2016**

nic.br cgi.br

www.nic.br | www.cgi.br