DDoS e Correios 2020:

Atuais e Futuros Desafios

Marcos Cícero

GRIS Correios

Marcos Cícero

Analista de Sistemas (Fundador GRIS Correios)

Professor / Coordenador de Pós-Graduação (**Centro Universitário IESB**)

Instrutor **ESR/RNP (Análise Forense)**

Fundador (**DEFCON Group Brasilia – DC5561**)

M.Sc. "candidate" in Computer Security (University of Liverpool - UK)

Certificações ativas:

GIAC Reverse Engineering Malware (GREM)

Certified Ethical Hacker (C|EH)

Correios

Agenda

- Revisão sobre DDoS
- Correios (estrutura e visão de futuro - 2020)
- Atuais desafios
- Desafios futuros
- Melhores práticas

Distributed Denial-of-Service (DDoS)

Estamos preparados para o pior cenário ?

Lembremos que alguns do últimos ataques de grande porte não envolveram o uso massivo de BOTNETs.

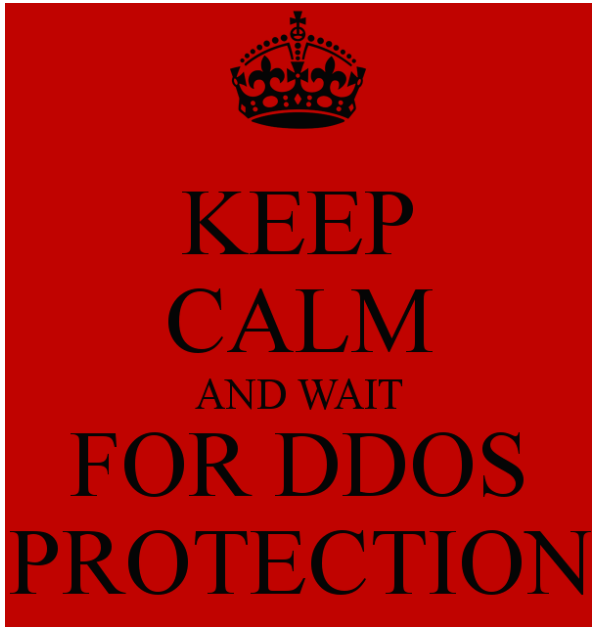
Correios

Distributed Denial-of-Service (DDoS)

Ponto pacífico:

DDoS ainda é um problema de segurança

sem solução definitiva.



Correios

Distributed Denial-of-Service (DDoS)

Ataque cujo objetivo é “simplesmente” tirar os recursos computacionais “do ar”

#TangoDown

Correios

Distributed Denial-of-Service (DDoS)

- “Flood” ⌦ “inundação de pacotes”
- “Slow DoS” ⌦ “slow approach”

Obs 1: google “th3j3st3r”

Obs 2: Ataques “IPv6 Router Advertise (RA)”

Distributed Denial-of-Service (DDoS)

Atingimos o limite ?

Aparentemente, não!

- 2013: 309 Gbps (DNS) (a warning shot)
- 2014: 400 Gbps (NTP)
- 2014: 500 Gbps (DNS)

Correios

Distributed Denial-of-Service (DDoS)

IP Spoofing
+
Fator de Amplificação

Distributed Reflection Denial-of-Service (DRDoS)

Correios

- **Empresa Pública responsável pela infraestrutura postal no Brasil**
- **Presente em todos os municípios**
- **119.938 empregados**
- **36,5 milhões de objetos por dia**
- **7468 agências próprias e franqueadas (AGFs)**
- **Rede de computadores extremamente capilarizada**
- **2 Centros de Dados (DF e SP)**

Correios 2020

Plano estratégico de longo prazo

- **Missão:** ***"Fornecer soluções acessíveis e confiáveis para conectar pessoas, instituições e negócios, no Brasil e no mundo."***
- **Visão:** ***"Ser uma empresa de classe mundial."***

Perante o quadro caótico global de segurança da informação, trata-se de um grande desafio.

Correios

Grupo de Resposta a Incidentes de Segurança (GRIS Correios)

CSIRT híbrido (misto) / multidisciplinar

(equipes de 3 diferentes departamentos)

Formalização:

- **CTIR Gov (22/01/13)**
- **CERT.Br (15/02/13)**

Correios

DDoS e Correios

Grupo de Resposta a Incidentes de Segurança
(GRIS Correios)

Atuais desafios acerca dos ataques DDoS

- **Alguns incidentes em:**
  - **2012**
  - **2013 (05/10/2013 – marco histórico na ECT)**
  - **2014**
- **Impacto: paralisação total dos serviços Internet**

Correios

DDoS e Correios

Grupo de Resposta a Incidentes de Segurança
(GRIS Correios)

Atuais desafios acerca dos ataques DDoS

- **Picos de 600 Mbps**
  - **Ataques volumétricos**
  - **“Slow DoS”**
- **Contra-medida: atuação conjunta com a operadora (Embratel)**

DDoS e Correios

Grupo de Resposta a Incidentes de Segurança
(GRIS Correios)

Reais Desafios Futuros

- **Adquirir "solução Anti-DDoS"**
  - **Parceria inevitável com a operadora**
  - **Solução que contemple "Slow DoS"**
- **Tornar-se um sistema autônomo (AS)**
- **"Fortalecer" a infraestrutura de Internet**

Correios

DDoS e Correios

Grupo de Resposta a Incidentes de Segurança
(GRIS Correios)

Desafios “Futurísticos”

- **Continuar “*não sendo*” um alvo em potencial**
- **Capacitar a equipe em tópicos avançados**
- **Colaborar ativamente com outros CSIRTs**
- **Investir em inteligência cibernética**
- **“Prever” o próximo ataque**

Correios

DDoS - Melhores práticas

FATO:

Ataques DDoS de grande porte acontecem e acontecerão com mais frequência.

POR QUÊ ?

Porque ainda há recursos para isso:

BOTNETs, DNS, NTP, SNMP, Chargen, SSDP, BitTorrent

Correios

DDoS - Melhores práticas

DILEMAS/SOLUÇÕES:

Cortar o mal pela raiz.

COMO ?

- **Combater C2 (C&C)**
- **“Cuidar” dos serviços: NTP, SNMP, Chargen, SSDP, etc.**

DDoS - Melhores práticas

- **DNS: outro patamar porque é um serviço crítico.**
  - **Desabilitar recursividade dos "*open resolvers*"**
    - **Cerca de 240.000 servidores no Brasil. *Shadowserver* reporta 398.000. Como ????**
    - **AS18881: ~ 63.000 servidores recursivos abertos**
  - **Habilitar DNS RRL (Response Rate Limiting)**

Correios

DDoS - Melhores práticas

- **BCP38/84: implementação em todos os pontos de presença, última milha, PTTs**
- **Evitar o anúncio BGP de prefixos utilizados para "infraestrutura"**
- **Para reflexão: IPv6 tende a piorar o cenário ?**

Correios

Obrigado!

csirt@correios.com.br