A evolução dos ataques de negação de serviço (DoS).

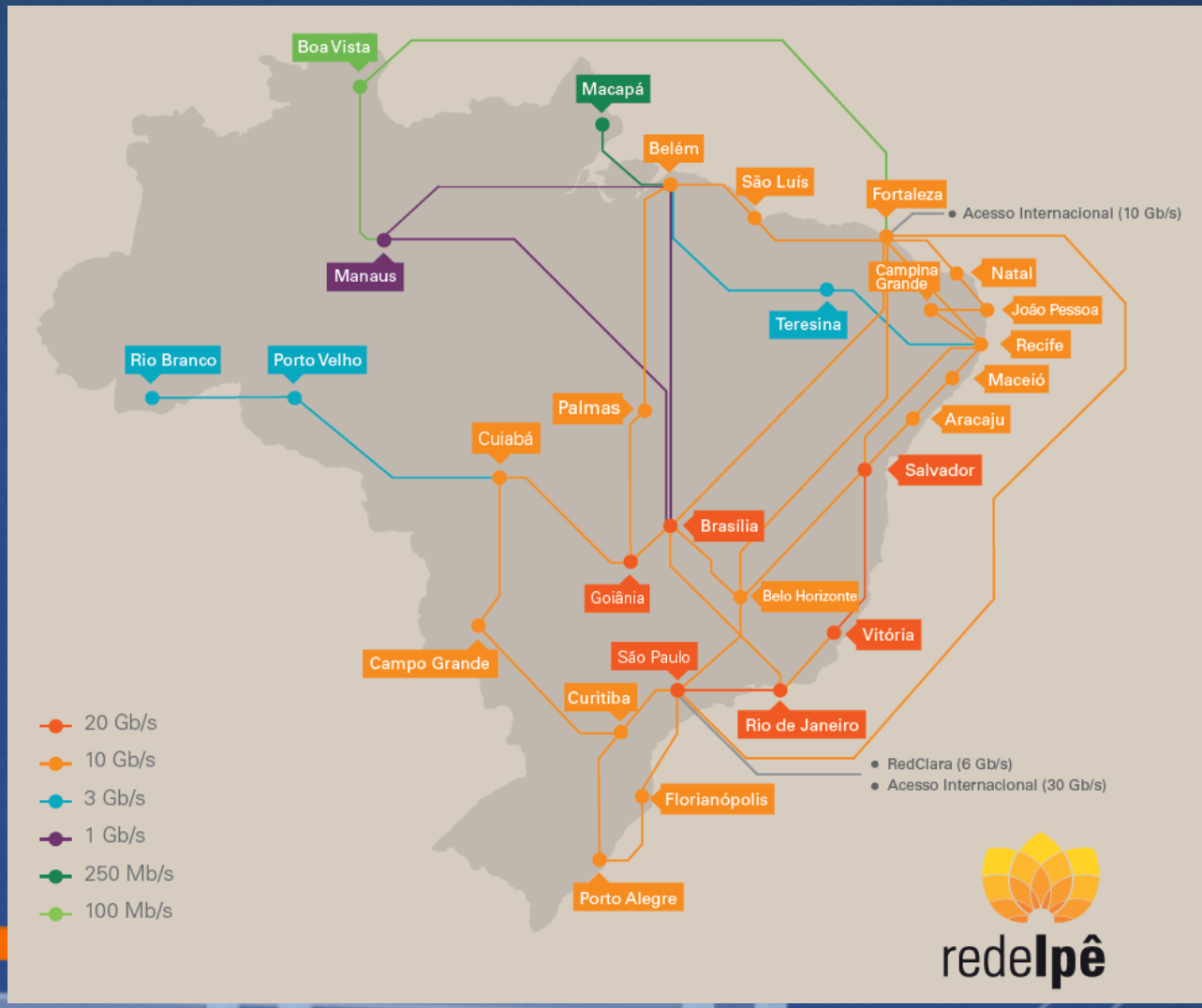
Por: Rildo Antonio de Souza - CAIS/RNP

RNP
MINISTÉRIO DA DEFESA
MINISTÉRIO DA CULTURA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
BRASIL GOVERNO FEDERAL

RNP

Rede Nacional de Ensino e Pesquisa (RNP), criada pelo MCTI em 1989, para construir uma infraestrutura de internet acadêmica.

Desde então, participa do desenvolvimento da internet no Brasil, com a introdução de novas tecnologias e a implantação da primeira rede óptica acadêmica da América Latina, em 2005, batizada de Ipê.



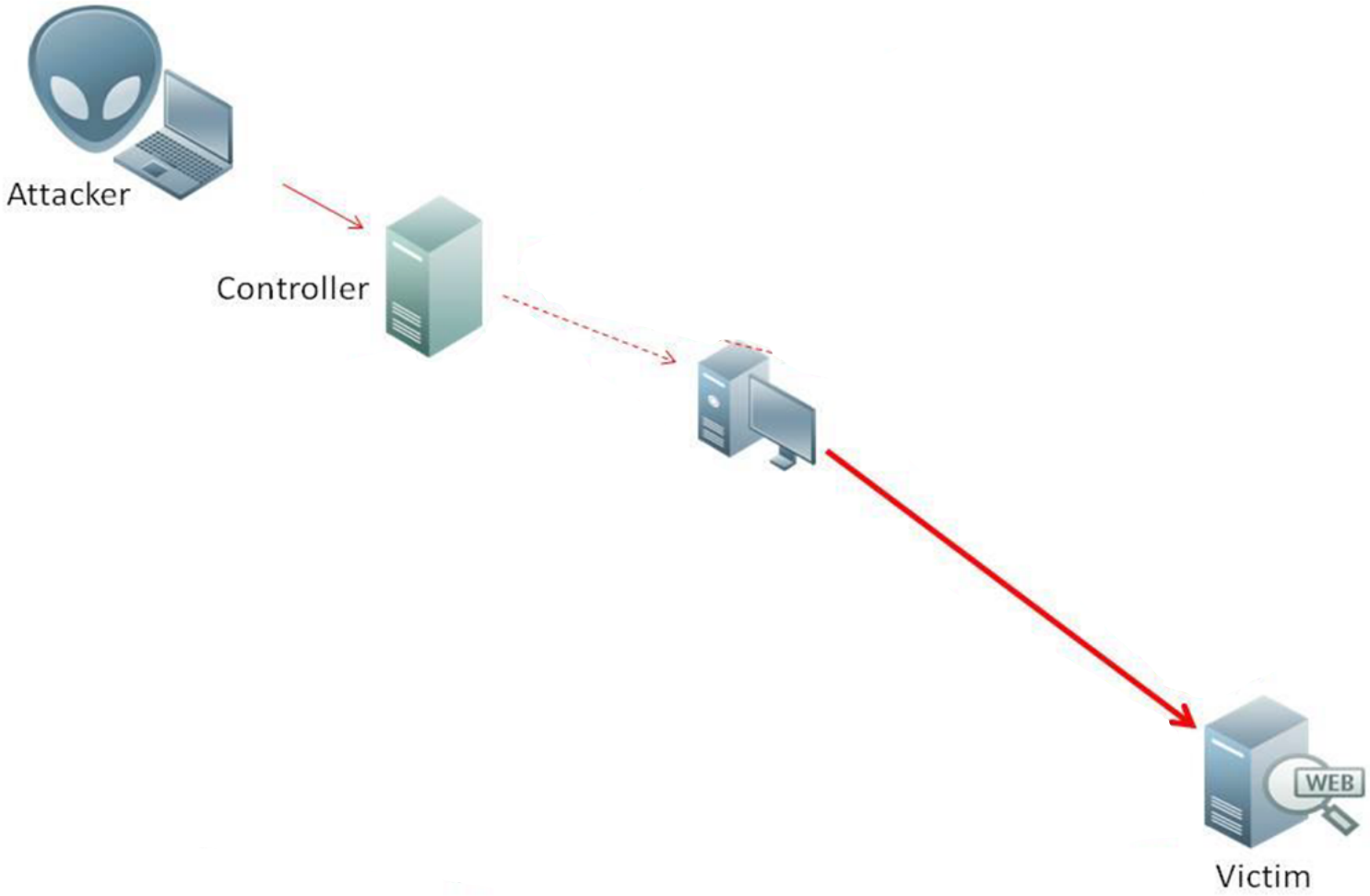
CSIRT de coordenação da rede acadêmica brasileira, a Rede Ipê, desde 1997.

Atua na detecção, resolução e prevenção de incidentes de segurança de rede, além de elaborar, promover e disseminar práticas de segurança na RNP e instituições a ela vinculadas.

O que é DoS ?

Denial of Service

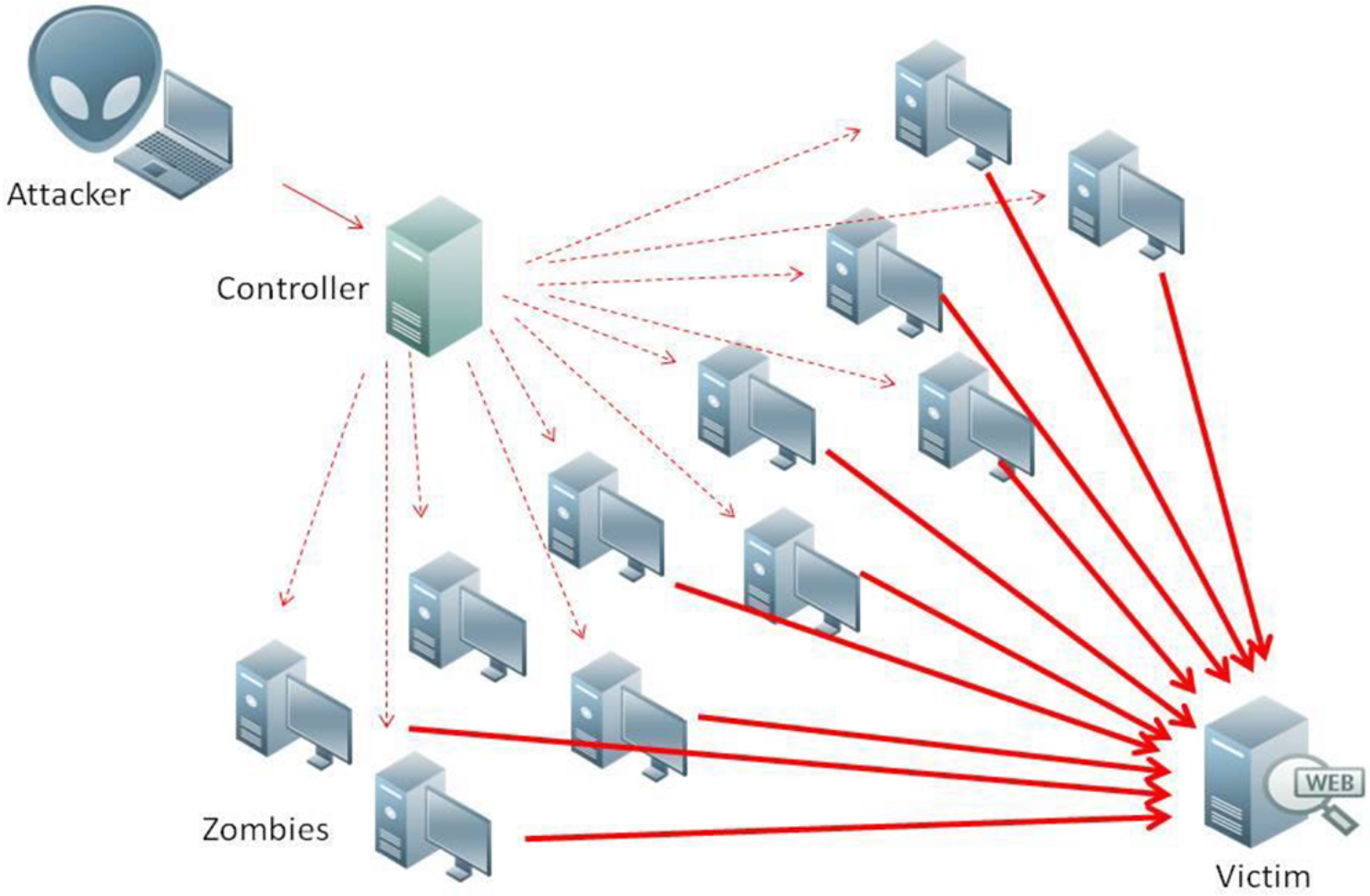
Ataque de negação de serviço



O que é DDoS ?

Distributed Denial of Service

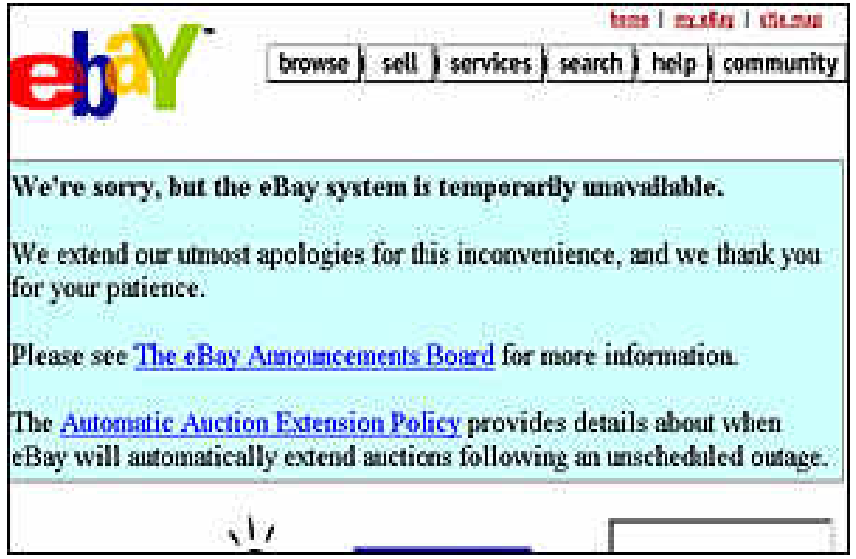
Ataque de negação de serviço distribuído



Primeiro DDoS?

The first documented DoS-style attack occured during the week of February 7, 2000, when "mafiaboy," a 15-year-old Canadian hacker, orchestrated a series of DoS attacks against several e-commerce sites, including Amazon.com and eBay.com. These attacks used computers at multiple locations to overwhelm the vendors' computers and shut down their World Wide Web (WWW) sites to legitimate commercial traffic. The attacks crippled Internet commerce, ... (100 of 487 words)

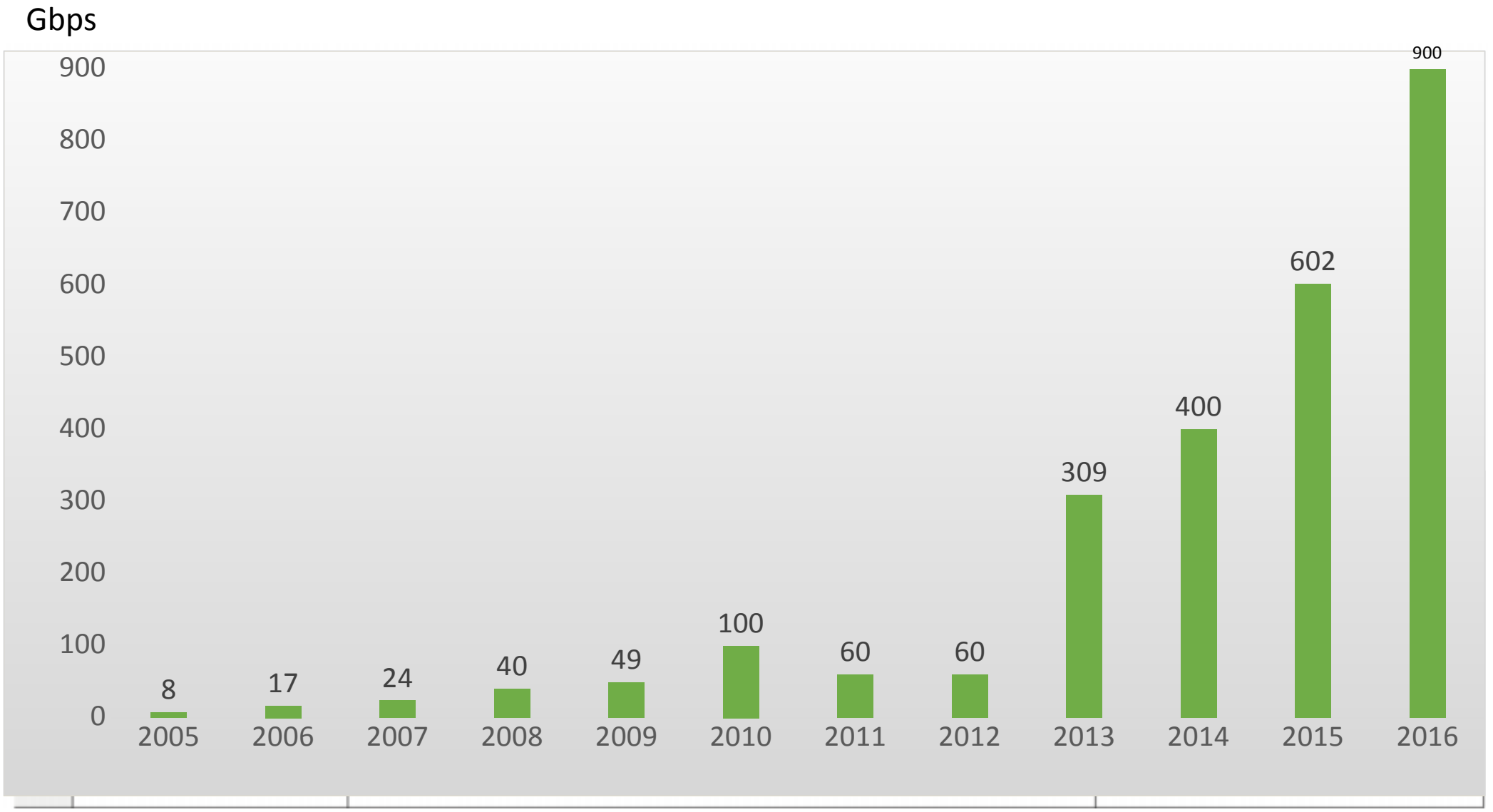
Fonte: https://blog.fortinet.com/2013/03/25/ddos-a-brief-history



amazon

CNN

Evolução DDoS no Mundo



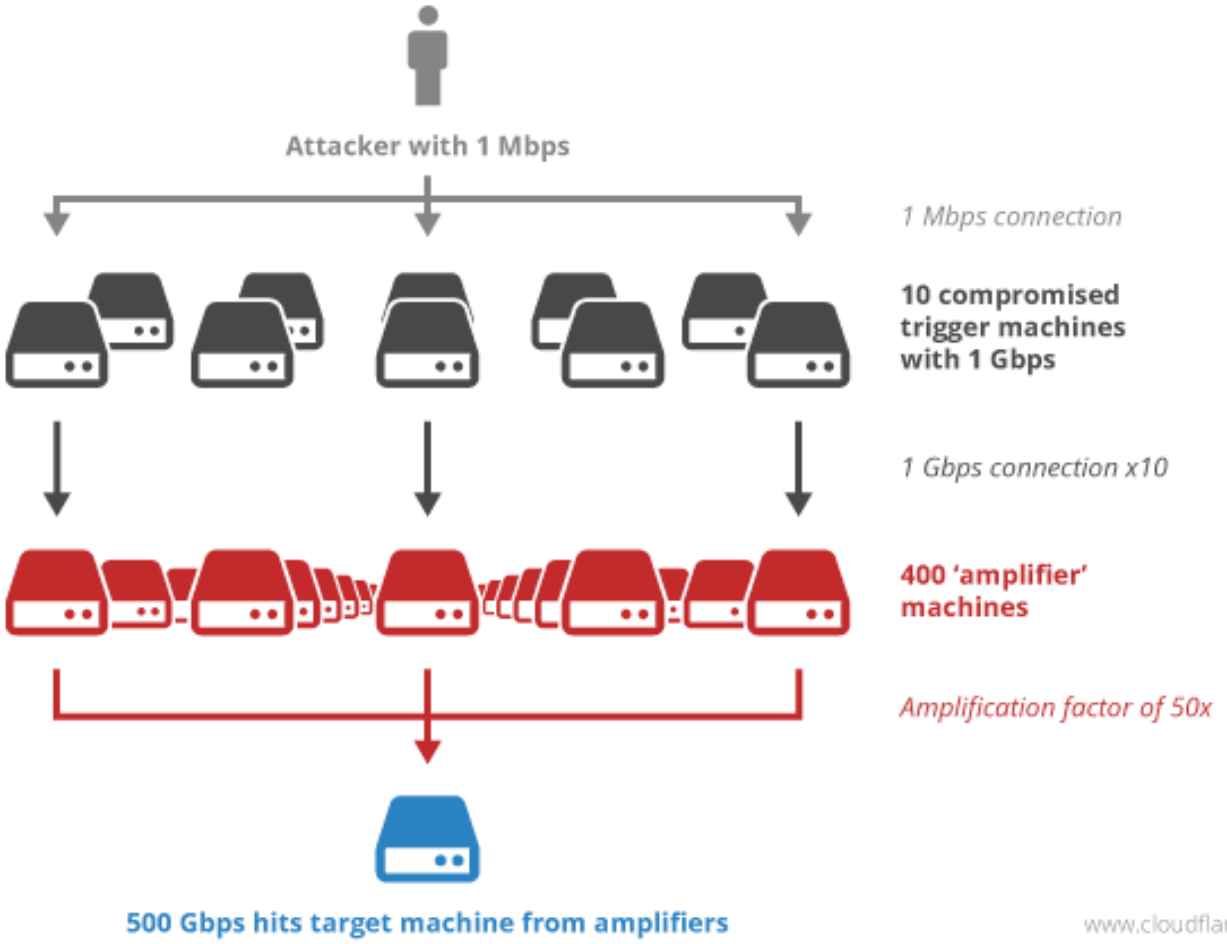
Fonte: https://www.sinog.si/wp-content/uploads/2015/04/Arbor_Gianola.pdf

Histórico de DDoS na Rede Ipê

- 2011 • Ataques do grupo Anonymous aos nossos clientes
- 2012 • Início do apoio ao MEC contra DDoS
- 2013 • Primeira detecção de ataques DRDoS na rede Ipê
- 2014 • Aumento expressivo de ataques de Amplificação
- 2015 • Recorde de ataques detectados > 5 mil
- 2016 • Detecção de ataques maiores que 4Gbps e 1.5Mpps
- 2017 • Ataques envolvendo IoT

O que é DRDoS ?

Ataque de negação de serviço reflexivo distribuído



Fonte: https://www.cloudflare.com

Como funciona o DRDoS ?

- Uso do protocolo UDP
- Utiliza IP Spoofing
- Explora vulnerabilidades em protocolos da internet
- Alta taxa de amplificação

Ataques DRDoS: Fator de amplificação

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Fonte: US-CERT

Tipos de Vulnerabilidades mais exploradas em Ataques DRDoS

- DNS Recursivo Aberto

  Servidor que permite ser utilizado por qualquer host na Internet para resolver nomes

- NTP Aberto

  Servidor que permite consultas de qualquer host da Internet,especialmente do tipo “monlist” e “readvar”

- SNMP

  Dispositivo que responde a consultas SNMP para qualquer host na Internet, especialmente em comunidades padrão “public”

- SSDP

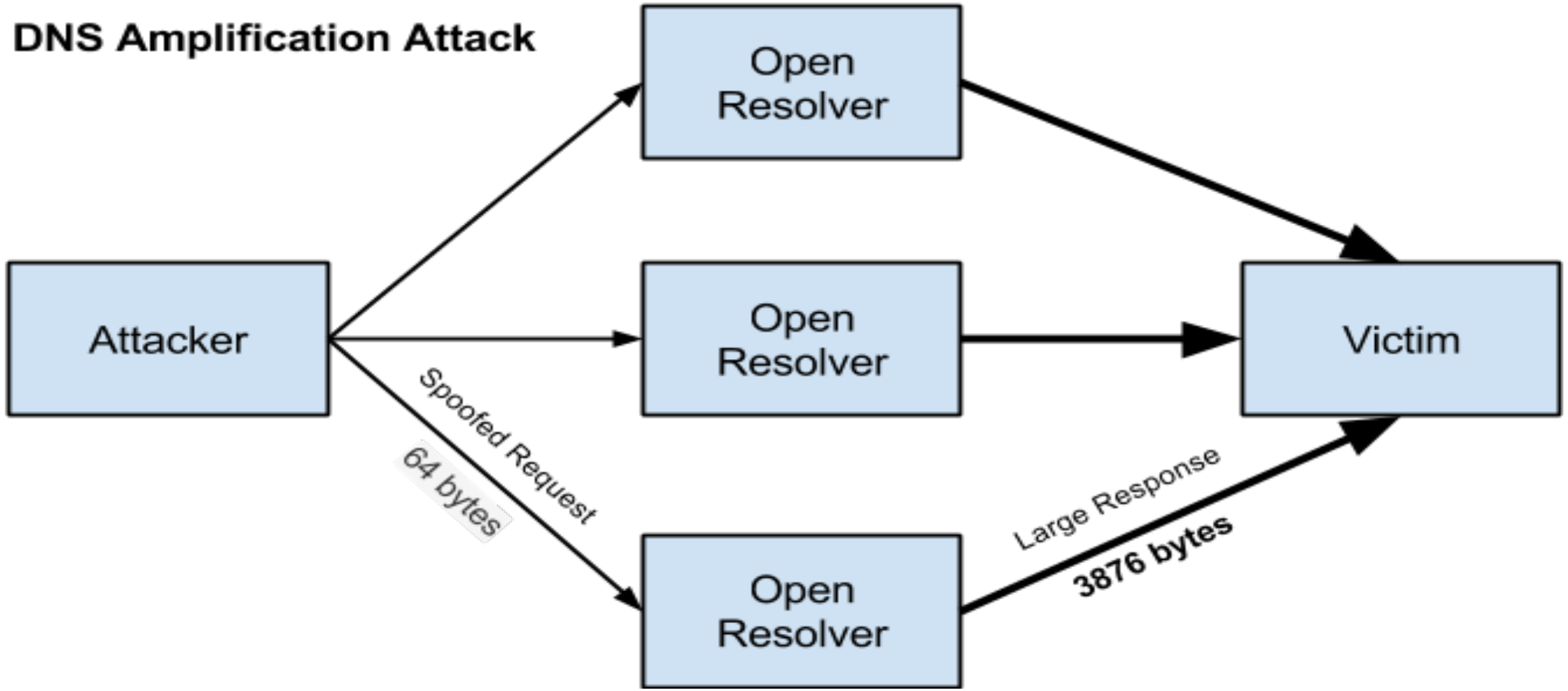
  Protocolo que permite aos usuários de rede descobrirem serviços de rede

- Netbios

  Especificação criada para prover acesso a serviços de redes em uma rede pessoal

DNS Recursivo Aberto

Como ocorre o Ataque ?



Podem ser amplificados em até 70x

Fonte: https://umbrella.cisco.com/blog/blog/2014/03/17/dns-amplification-attacks/

DNS Recursivo Aberto

Melhores Práticas:

1 - Separar servidor autoritativo do recursivo

2 - Atribuir políticas de acesso diferentes para cada servidor

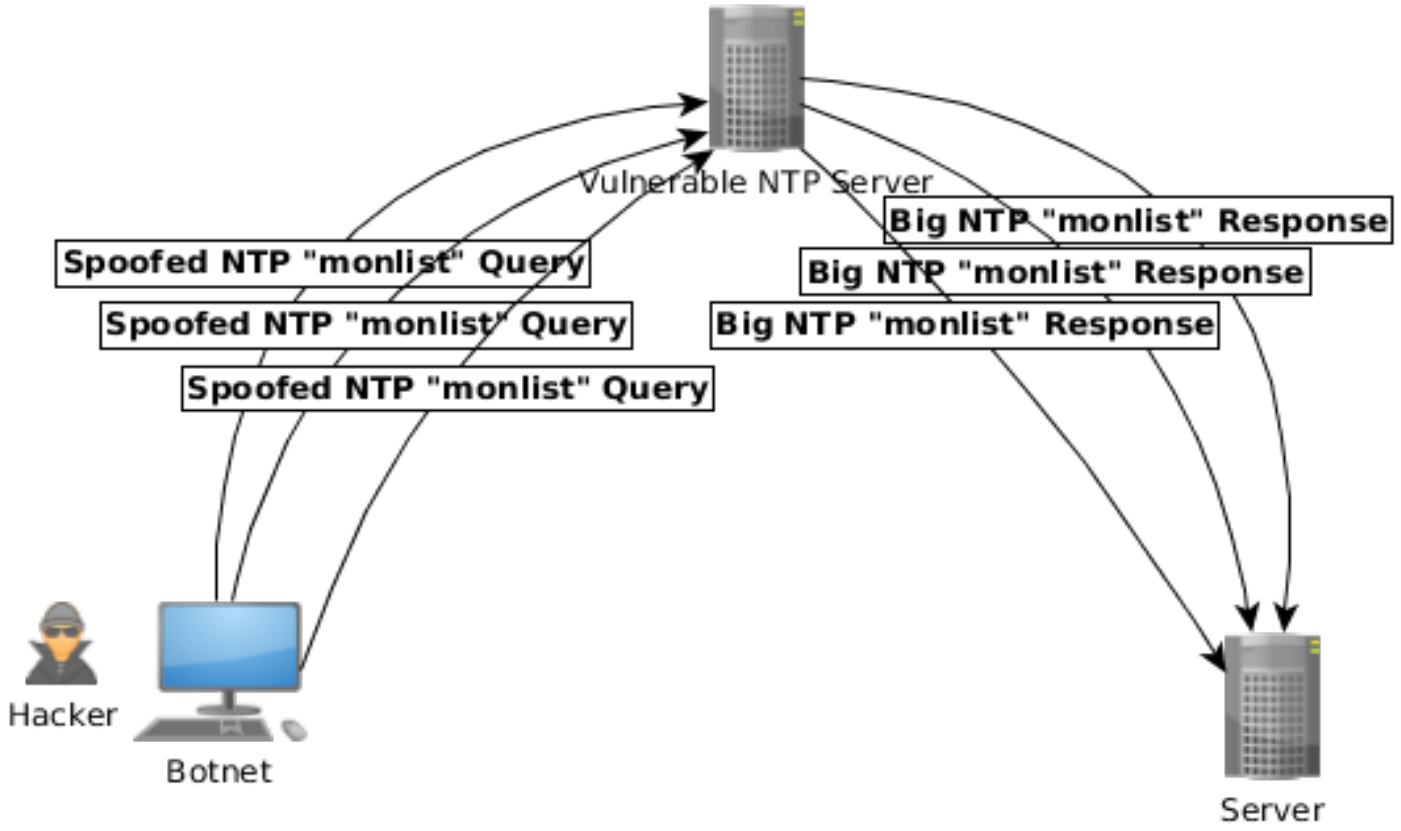
3 - Restringir consultas recursivas

Como identificar vulnerabilidade:

1 - Executar o comando abaixo em um host com Linux:
dig @"IP" www.google.com A

NTP Aberto

Como ocorre o Ataque ?



Podem ser amplificados em até 500x

Fonte: https://r00t-services.net/knowledgebase/19/What-are-NTP-Amplification-DDoS-Attacks-DrDoS-on-Websites.html

NTP Aberto

Melhores Práticas:

1 - Atualização para a versão mais nova do NTP

2 - Bloquear consultas do tipo “readvar” externas

3 - Implementar ACLs

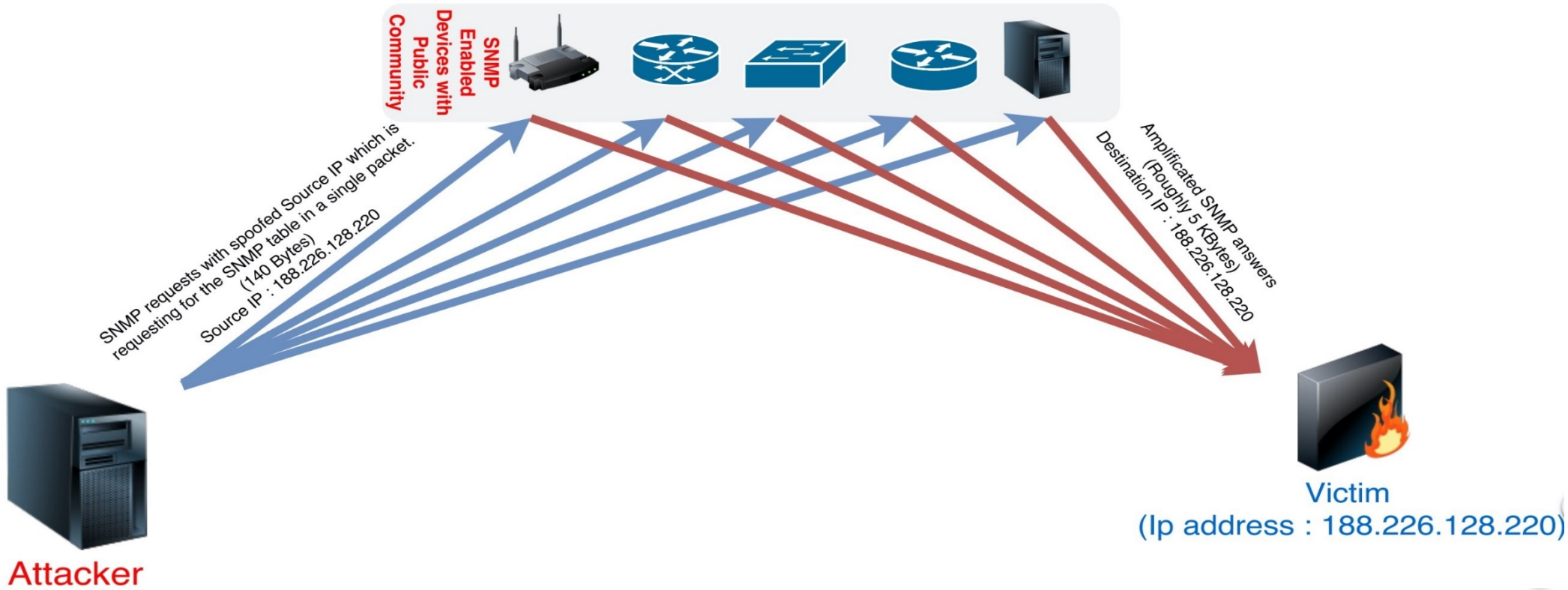
Como identificar vulnerabilidade:

1 - Executar o comando em um host Linux: ntpdc –n –c monlist “IP”

2 - Executar o comando em um host Linux: ntpq -c rv “IP”

SNMP Aberto

Como ocorre o Ataque ?



Podem ser amplificados em até 600x

Fonte: http://alibay.com.tr/approaching-danger-snmp-amplification-attacks/

SNMP Aberto

Melhores Práticas:

1 - Utilizar comunidades privadas e autenticação

2 - Restringir consultas para redes externas

3 - Desabilitar o serviço

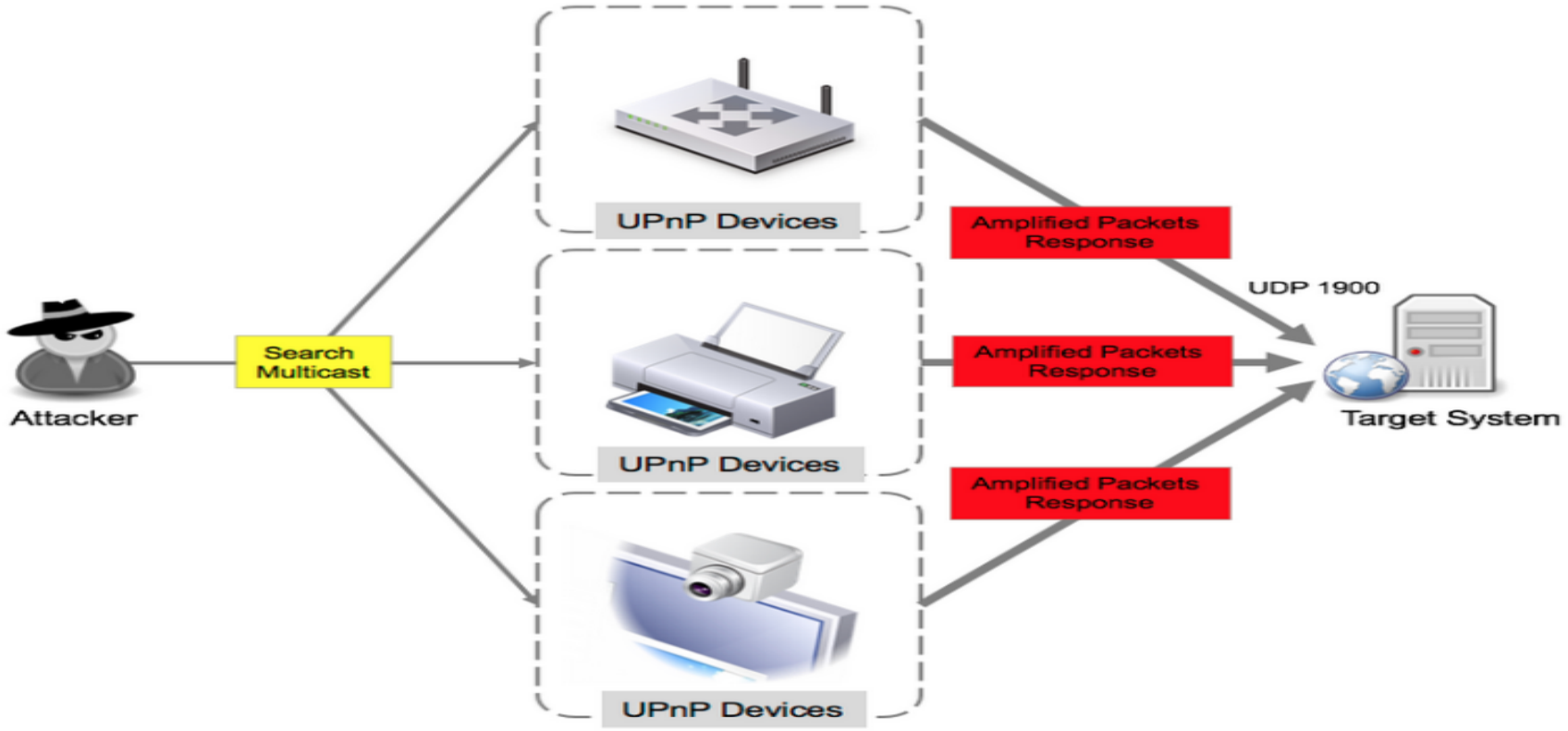
Como identificar vulnerabilidade:

1 - Executar um dos comandos abaixo em um host Linux:

snmpget –c public –v 2c “IP” 1.3.6.1.2.1.1.1.0
snmpget –c public –v 2c “IP” 1.3.6.1.2.1.1.5.0

SSDP Aberto

Como ocorre o Ataque ?



(SSDP Reflection DDoS Attack Diagram)

Podem ser amplificados em até 30x

Fonte: https://www.linkedin.com/pulse/ddos-attack-vector-ssdp-flood-junghyun-yang

SSDP Aberto

Melhores Práticas:

1 - Responder apenas consultas internas

2 - Desabilitar o UPnP quando possível

3 - Implementar BCP38

Como identificar vulnerabilidade:

1 - Executar o script do Nmap “upnp-info.nse”

NetBios Aberto

Como ocorre o Ataque ?

Podem ser amplificados em até 4x

Fonte: https://f5.com/labs/articles/threat-intelligence/ddos/old-protocols-new-exploits-ldap-unwittingly-serves-ddos-amplification-attacks-22609

NetBios Aberto

Melhores Práticas:

1 - Desabilitar consultas externas

2 - Desabilitar o compartilhamento de arquivos quando possível

3 - Implementar BCP38

Como identificar vulnerabilidade:

1 - Executar o comando abaixo em um host Linux:

nbtscan “IP”

News & Updates

To: [redacted]

Subject: Re: DDOS ATTACK!

You are ignoring us.

never give up.

ve never attack the same

pay more.

We will give you another 24 hours to decide.

Pesquisadores da UFPB desenvolvem ferramenta de defesa contra ataques DDoS

[15.9.2016]

O Brasil é um dos países com maior incidência de ataques de negação de serviço (DoS), que geralmente ocorrem quando a rede é sobrecarregada por um volume de tráfego acima do normal, provocado intencionalmente para prejudicar a disponibilidade de um sistema. Na rede acadêmica, que atende a universidades e institutos de pesquisa no país, esses tipos de ataques chegam a representar 84% do total de incidentes registrados.

A fim de proteger instituições desse risco, pesquisadores do Laboratório de Redes da Universidade Federal da Paraíba (UFPB) estão desenvolvendo, em parceria com a RNP, uma plataforma de defesa para uma variação desses ataques, os de negação de serviço distribuído (DDoS), que exploram vulnerabilidades mais sofisticadas na camada de aplicação, como, por exemplo, em sites e servidores web. A plataforma, chamada de SeVen, é capaz de identificar esses ataques, que geralmente passam despercebidos, e de mitigá-los em tempo real, evitando assim que os sites fiquem indisponíveis para o acesso.

Segundo o coordenador da pesquisa, Iguatemi E. Fonseca, os ataques que atingem sites institucionais e governamentais exploram vulnerabilidades específicas no protocolo HTTP e, devido à sua grande capacidade de mudança, são mais difíceis de serem detectados. "Os atacantes podem fazer um ataque DDoS misto, atingindo a camada de rede e a de aplicação ao mesmo tempo, para despistar o administrador da rede e o serviço ficar fora do ar", alerta o pesquisador.

Fonte:https://jidentify-theft-scout/DDOS-attack-mitigation.html

Fonte:https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf

Fonte:https://www.arbornetworks.com/blog/asert/ddos-attacks-as-attacks-rise-20150924-gjucv8


What Can I do?

Recomendações contra Ataques de Negação de Serviço:

1 – Contactar o ISP

2 - Implementar BCP 38 - Tratamento de Spoofing

3 - Implementar BCP 140 – Tratamento de servidores recursivos de DNS

4 – Realizar Hardening nos serviços de rede

5 – Implementar BCP 55 - Coleta e armazenamento de provas

6 – Implementar BCP 162 – Armazenamento de Logs

Dúvidas

Agradecimentos

OBRIGADO PELA ATENÇÃO!!!

Rildo Souza

rildo.souza@rnp.br