

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

Computação
Científica Nacional

Ameaças

Carlos Friaças

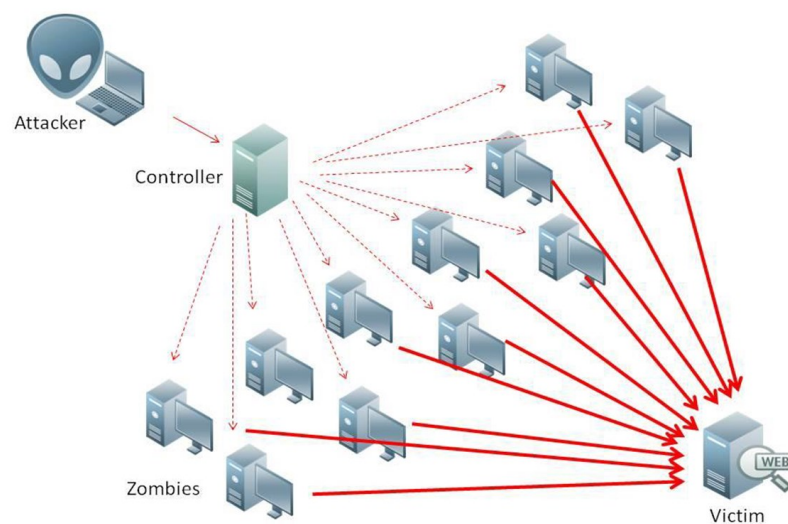


Agenda

- DDoS
- Malware
- Outras Ameaças



DDoS



Ataques mais comuns

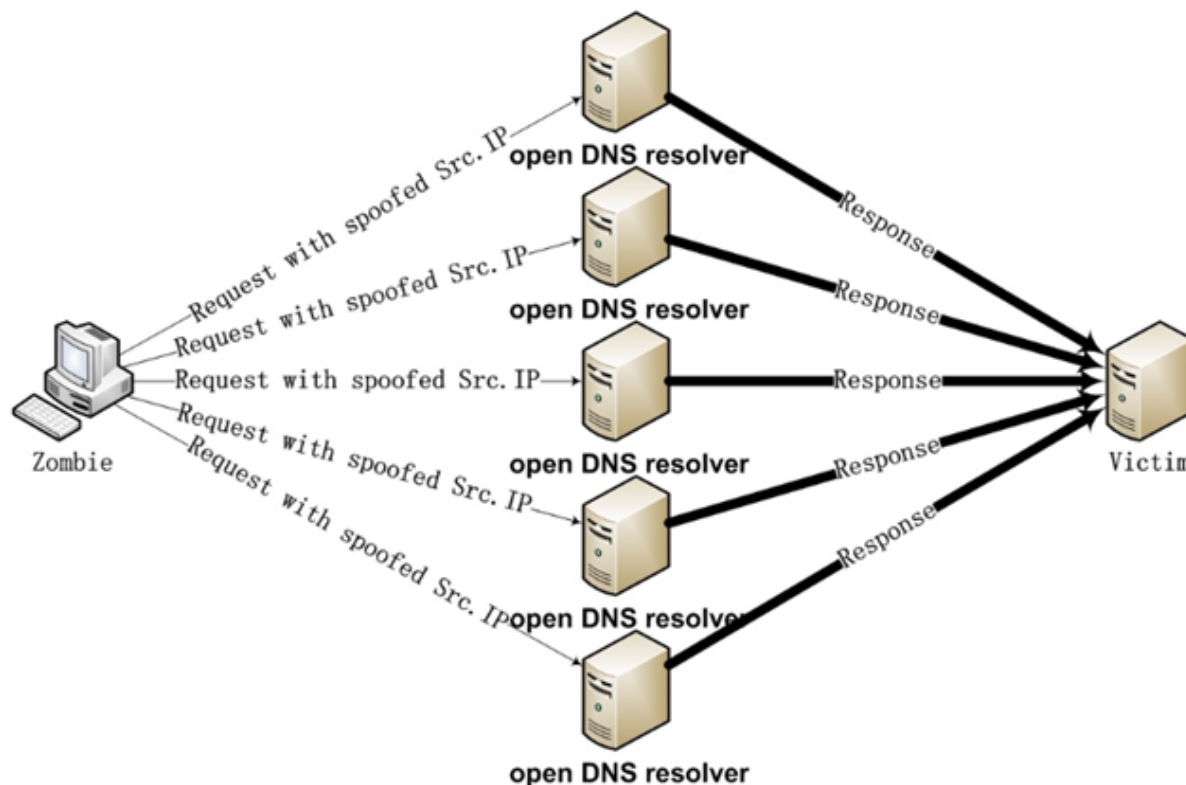
Ataques de Amplificação/Reflexão



- Tipicamente usam o protocolo UDP
- O tráfego é amplificado e refletido para a vítima
- Serviços vulneráveis ou mal configurados
ex: dns, chargen, ntp, snmp, ssdp, etc

Ataques mais comuns

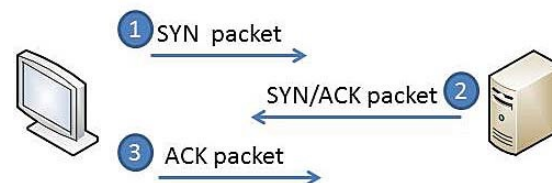
Ataques por reflexão - Exemplo



Ataques mais comuns

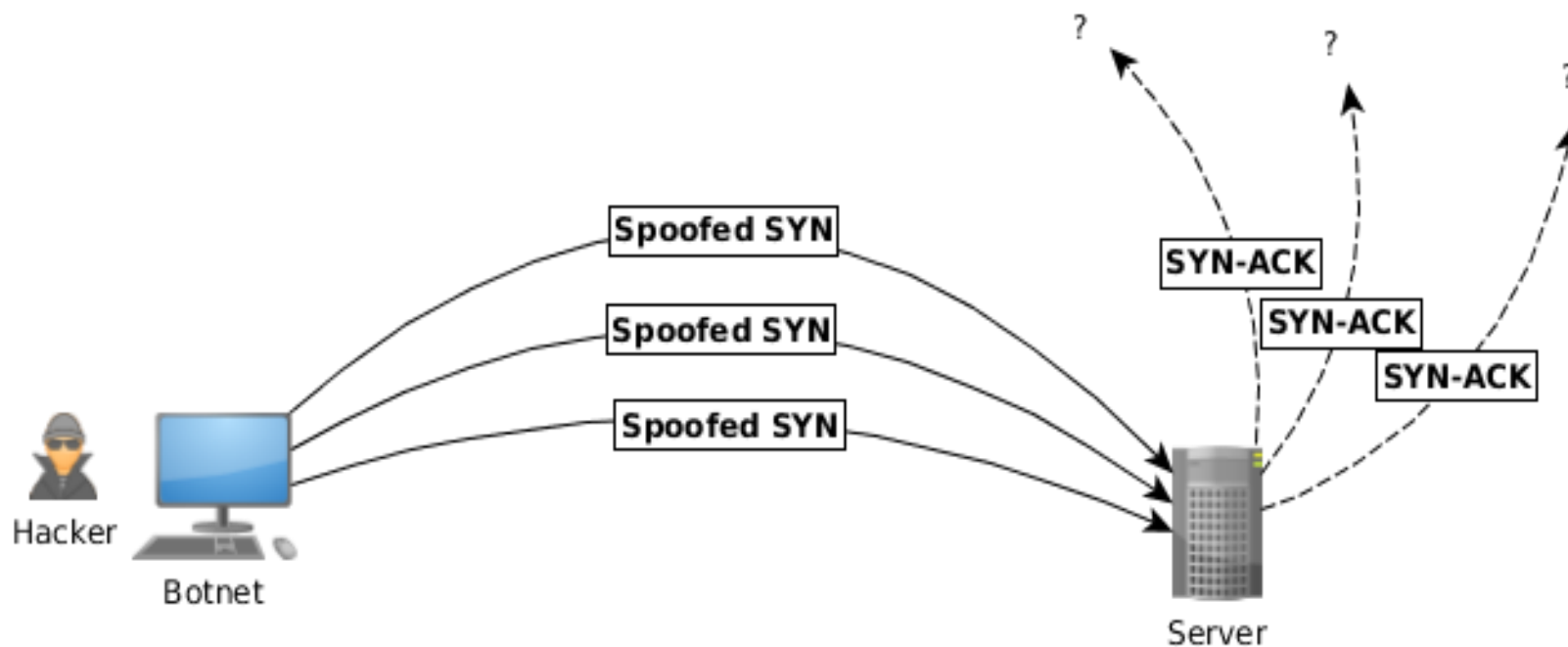
SYN Flood – Envio massivo de pacotes TCP com a *flag SYN*

- Usam o protocolo TCP
- Os ataques podem ter origem em máquinas «*zombie*», infetadas com *malware*
- Os pacotes são forjados para não denunciar os IPs de origem «reais» e dificultar a mitigação do ataque



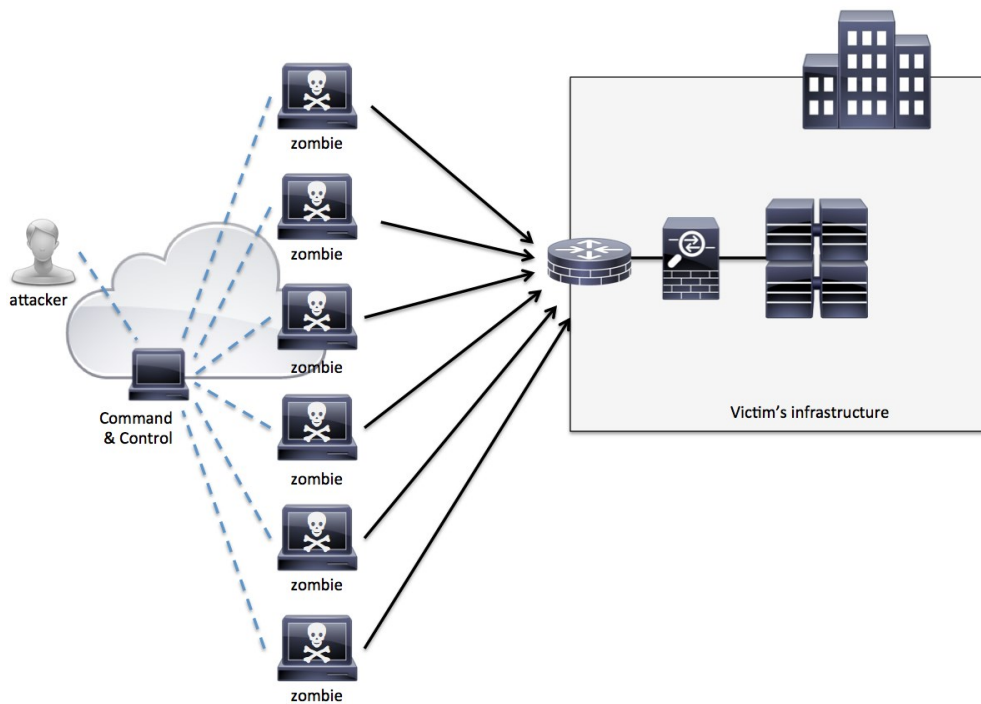
Ataques mais comuns

SYN Flood - Exemplo



Ataques mais comuns

SYN Flood - Exemplo



Ataques mais comuns

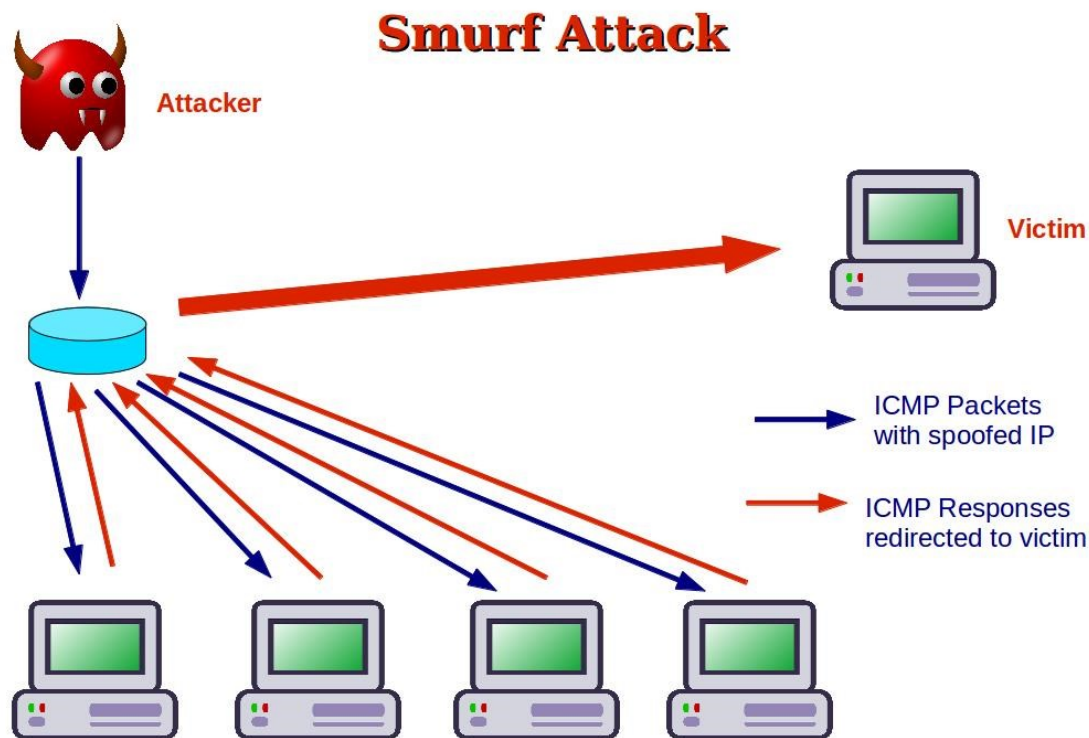
Smurf Attack – Envio massivo de pacotes ICMP “Echo request”

- Usam protocolo ICMP
- O atacante envia pacotes forjados com o IP de origem da vítima para endereços de *broadcast*



Ataques mais comuns

Smurf Attack - Exemplo



Medidas de Contenção/Mitigação

Objetivos

- Identificar o tipo de ataque
- Diferenciar o tráfego “bom” do tráfego “mau”
- Descartar o tráfego “mau” antes que chegue ao destino

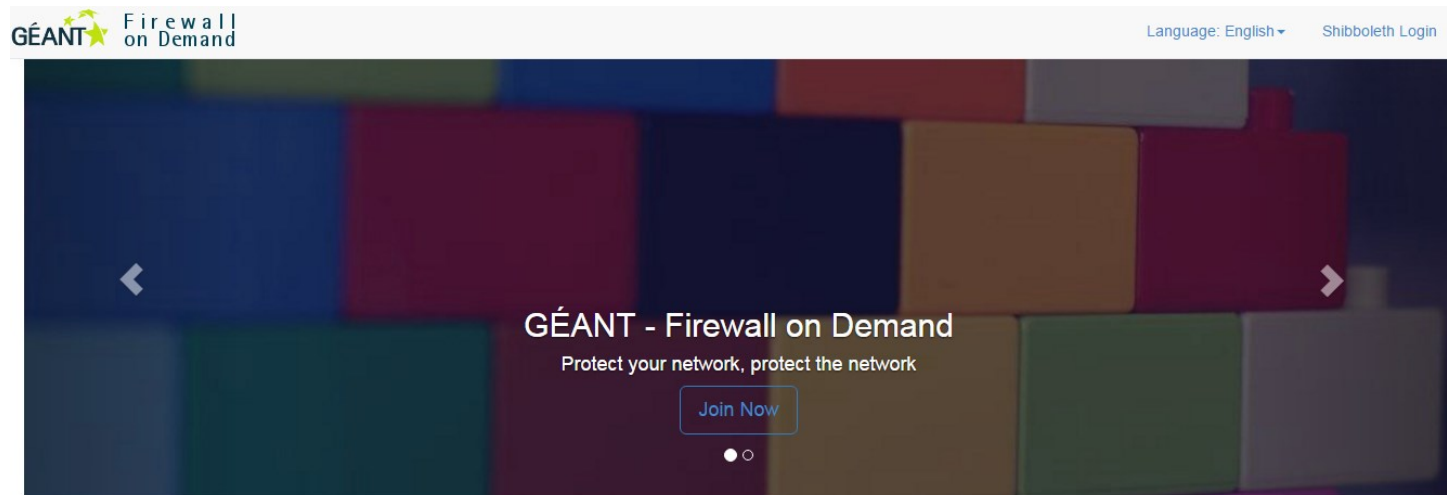
STOP **DOS**

Contenção/Mitigação (RCTS)

GÉANT - Firewall on Demand




Permite que o tráfego seja descartado antes de chegar ao *autonomous system* (AS) da RCTS, através da criação de regras de Firewall



Contenção/Mitigação (RCTS)

- RCTS CERT aplica regras, a pedido


Language: English ▾
▾

[Dashboard](#)
[Rules](#)
[Add Rule](#)
[My profile](#)

My rules

20 ▾ records per page

ACTIVE

PENDING

ERROR

DEACTIVATED

Search:

Previous
1
Next

Showing 1 to 16 of 16 entries

Name	Match	Then	Status	Expires	Actions
DDoS-20160411-gl22_UIDGVL	Dst Addr 193.137.0.0/32 Src Addr 0.0.0.0/0 Protocols icmp, tcp, udp	rate-limit 100k	DEACTIVATED	2016-04-11	Reactivate
DoS_J37VJA	Dst Addr 193.236.0.0/32 Src Addr 209.141.52.32/32 Protocols icmp, tcp, udp	discard	DEACTIVATED	2016-05-11	Reactivate

Shortcuts

[Add Rule](#)
[My Profile](#)

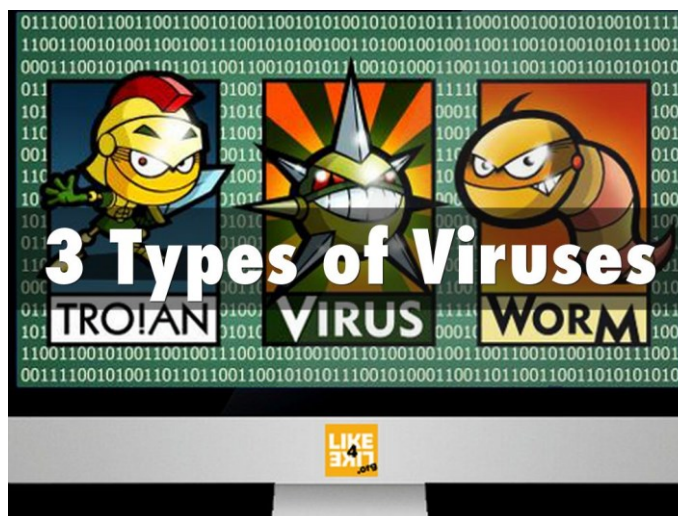
Live status

2016-09-29 11:38:10
rvx55gna4lugwgfzr2wa
Suspending rule :
Ataque_synflood_INST_
Result Successfully
committed

2016-09-29

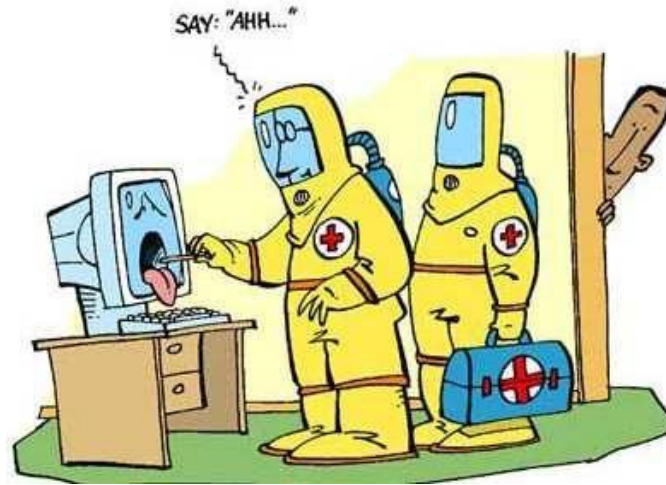


MALWARE



Malware

Vírus



- Software malicioso com capacidade de se replicar, infectando outros ficheiros, programas ou sistemas
- Concebidos para destruir dados ou influenciar o funcionamento dos sistemas

Malware

Trojan



- Aparenta ser um software inócuo para o utilizador
- As funcionalidades maliciosas são camufladas
 - roubo de informação
 - instalação de *backdoors*
- Carece da ação dos utilizadores para ser instalado

Malware



Worms

- Ao contrário dos *trojans*, não carece de ação por parte dos utilizadores
- Capacidade de replicação para infetar outros sistemas
- Vetor de ataque está sempre relacionado com vulnerabilidades no sistema

Virustotal (Google)



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE

URL

SEARCH



By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)

Choose file

 Want to automate submissions? [Check our API](#), free quota grants available for new file uploads

Virustotal.com

OUTRAS AMEAÇAS



Outras ameaças

Ataques Brute Force



Phishing



Web Hacking



Ransomware



Ataque de Brute Force



Sucessivas tentativas de login num serviço até encontrar um *username* e uma *password* válida

Solução:

- Limitar o acesso ao serviço apenas a endereços IP bem conhecidos
- Bloquear IPs após 3 tentativas de login mal sucedidas
- Usar *passwords* fortes e alterá-las periodicamente

Phishing



É um tipo de ataque cujo objetivo principal é roubar informação aos utilizadores.

Solução:

- Garantir que os websites são fidedignos (ex: Bancos, e-mail, compras on-line)
- Cuidados com e-mails suspeitos (ex: Erros ortográficos, URLs falsos, imagens com mensagens apelativas)

Web Hacking

A black rectangular box with green text that reads "YOU HAVE BEEN HACKED !".

Os Web sites vulneráveis permitem que um atacante possa atingir vários objetivos, entre os quais roubo de informação, *defacements*, uso do sistema para proveito próprio, etc.

Soluções:

- Garantir as últimas versões no software utilizado
- Realizar testes de segurança periódicos ao website
- Monitorizar os sistemas com IDS/IPS, ou outros

Ransomware



Infecção que leva a perda de informação e/ou pedidos de resgate em criptomoeda

Solução:

- Repor *backups*
- Identificar o tipo de Ransomware e procurar antídoto em *nomoreransom.org*
- Nunca tentar pagar nenhum resgate

Em Resumo



Ataques distribuídos de negação de serviço são potenciados por serviços abandonados ou sem gestão



Virustotal.com é uma ferramenta útil no combate ao *malware*



Phishing pode resultar em compromisso de dispositivos, mas também perdas reais



Obrigado