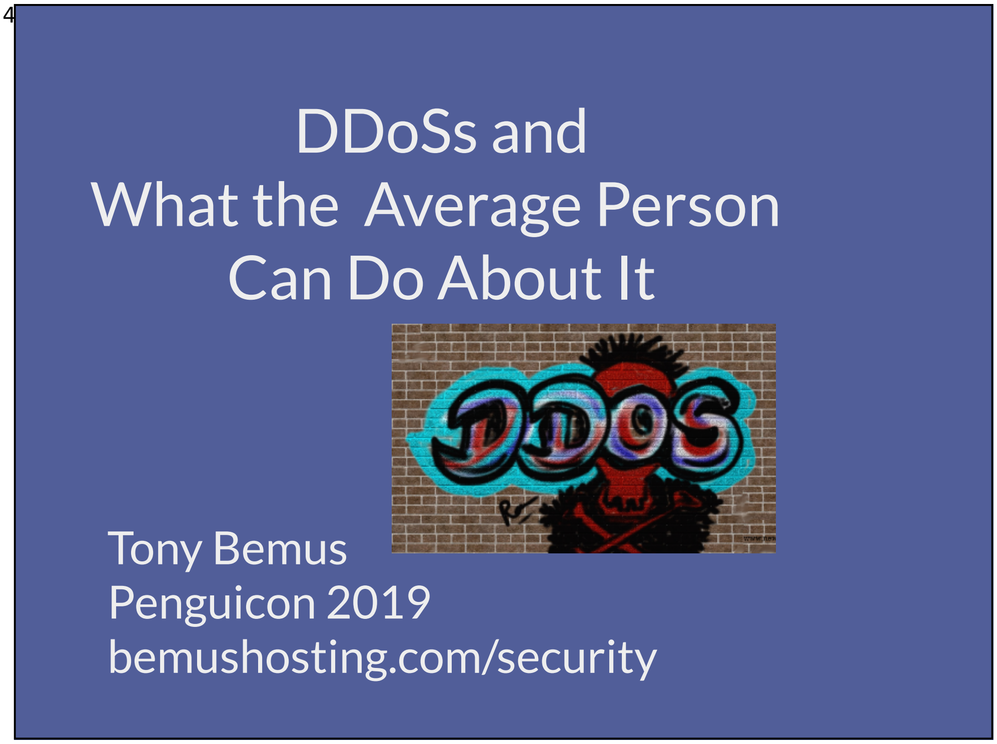
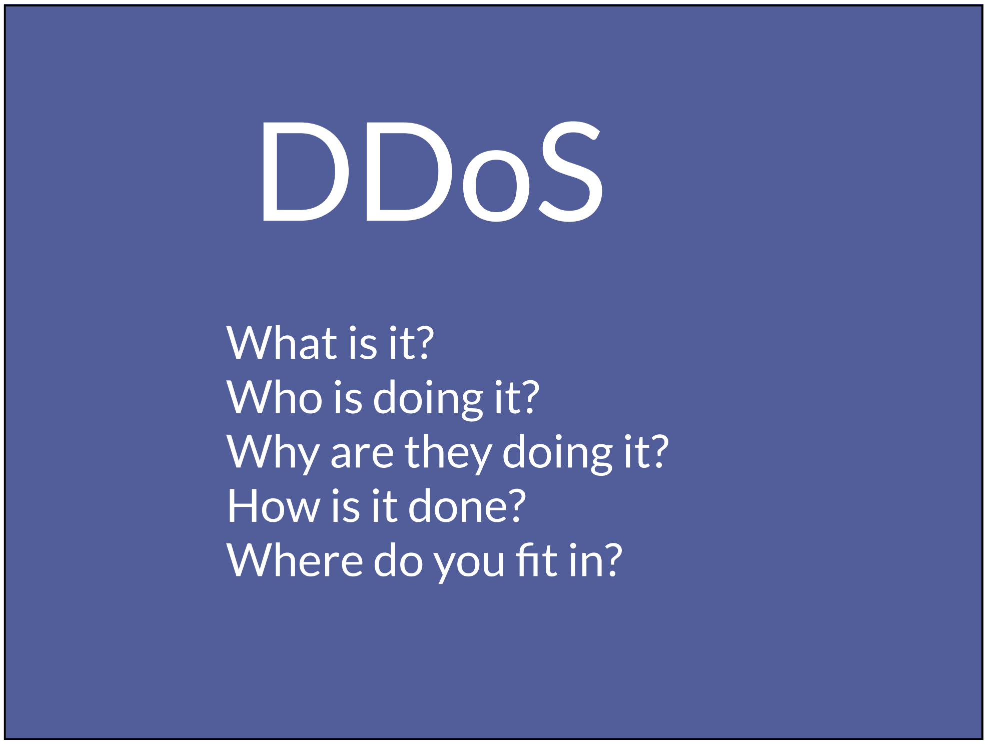


DDoSs and What the Average Person Can Do About It

Tony Bemus
Penguicon 2019
bemushosting.com/security

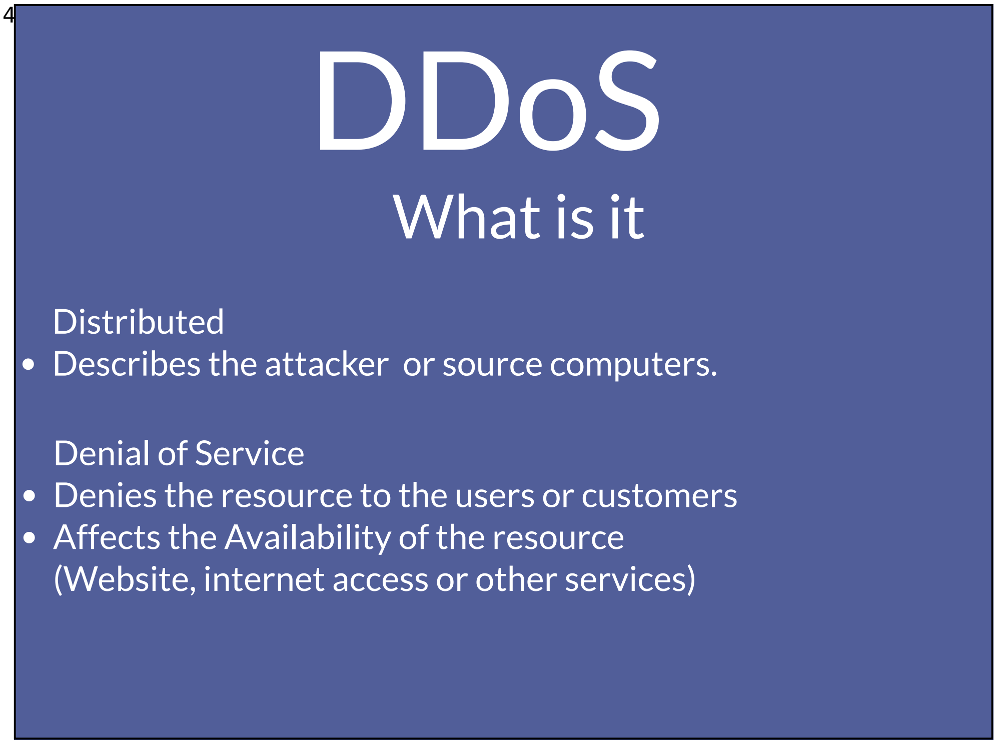
Notes:



DDoS

What is it?
Who is doing it?
Why are they doing it?
How is it done?
Where do you fit in?

Notes:



DDoS

What is it

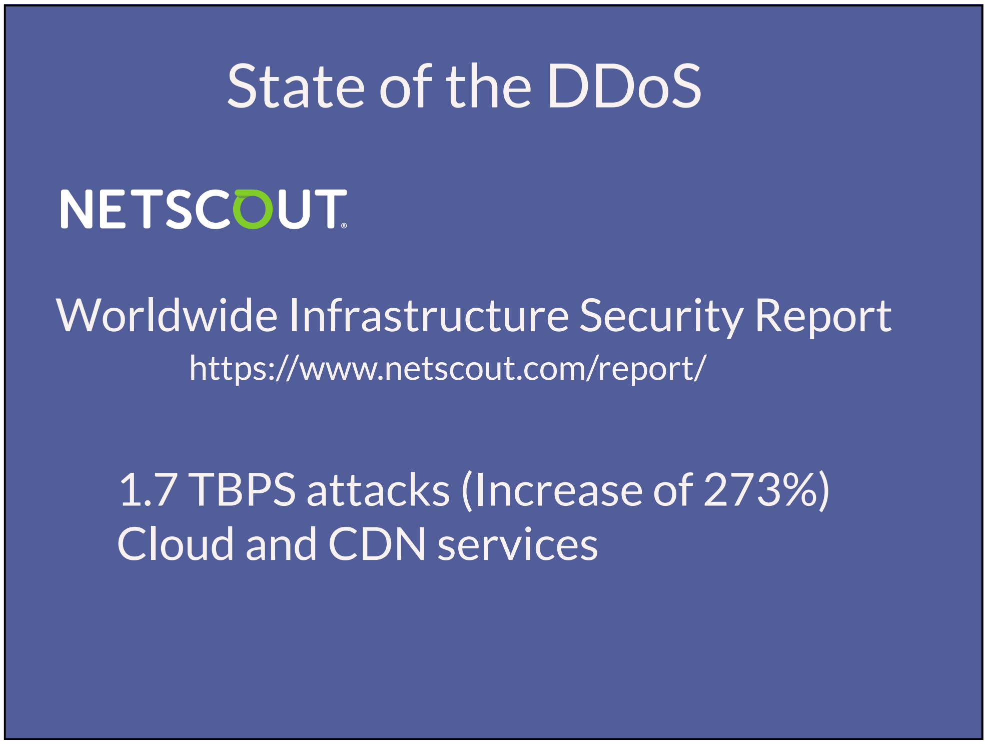
Distributed

- Describes the attacker or source computers.

Denial of Service

- Denies the resource to the users or customers
- Affects the Availability of the resource (Website, internet access or other services)

Notes:



State of the DDoS

NETSCOUT

Worldwide Infrastructure Security Report
https://www.netscout.com/report/

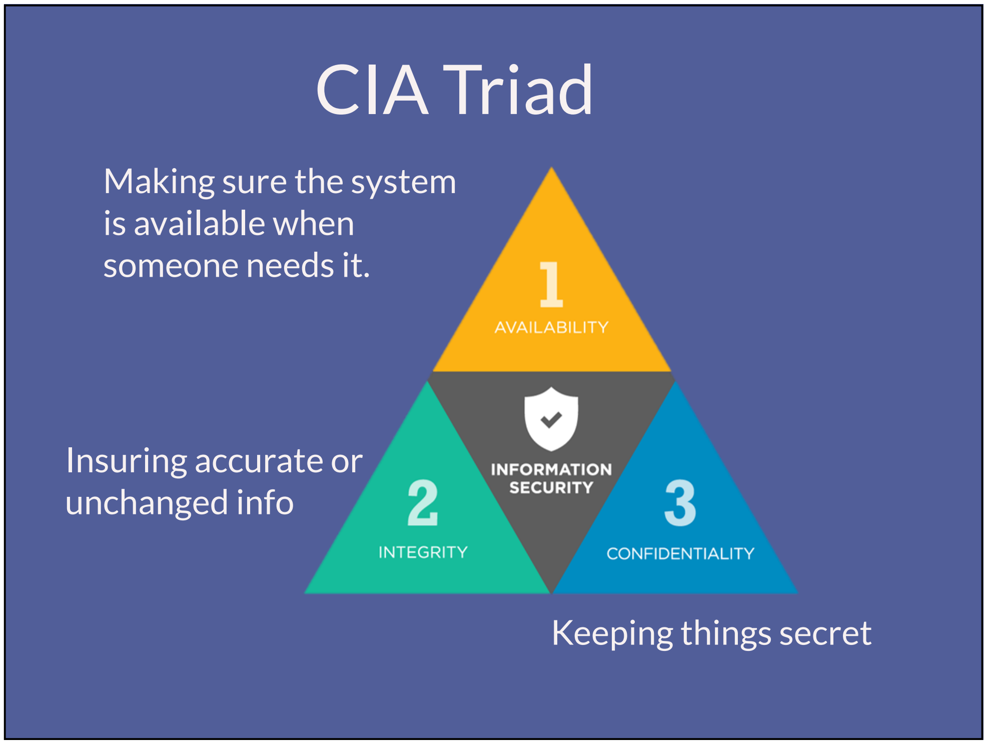
1.7 TBPS attacks (Increase of 273%)
Cloud and CDN services

Notes:

4

Availability?

Notes:



CIA Triad

Making sure the system is available when someone needs it.

Insuring accurate or unchanged info

Keeping things secret

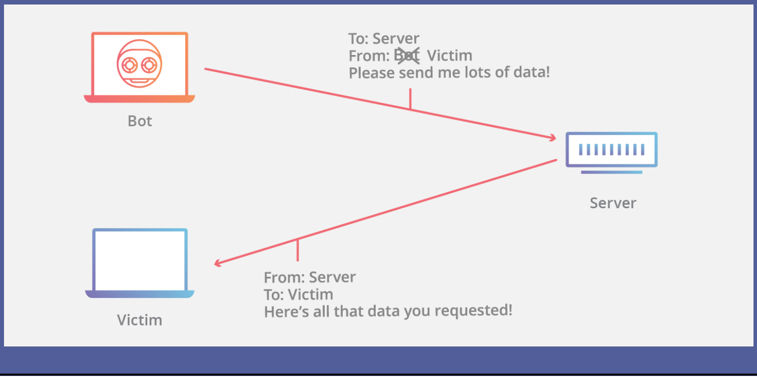
Notes:

Who is doing it?

- Attackers
- Script kiddies
- Hired thugs

Who are they really?

- Botnets are distributed hijacked IOT connected devices
- Spoofed IP addresses



To: Server
From: ~~Bot~~ Victim
Please send me lots of data!

From: Server
To: Victim
Here's all that data you requested!

Notes:

Why?

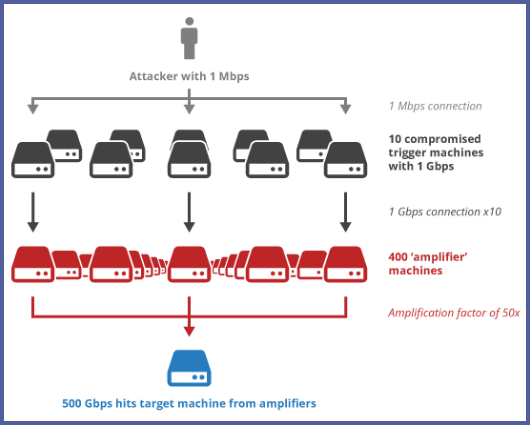
- Extortion
- Vandalism
- Distraction

Notes:

HOW is it done?

High Bandwidth Attacks

Traffic flood
    ICMP/Ping
Reflection,
Amplification
    UDP: DNS, NTP


Attacker with 1 Mbps
1 Mbps connection
10 compromised trigger machines with 1 Gbps
1 Gbps connection x10
400 'amplifier' machines
Amplification factor of 50x
500 Gbps hits target machine from amplifiers

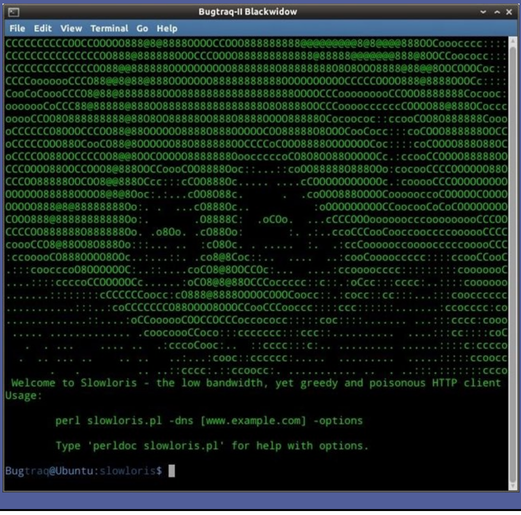
Notes:

HOW is it done?

Low Bandwidth Attacks

Application attacks (L7)

- Slow Loris,
- HTTP GET flood,
- SIP invite flood,
- dns amplification



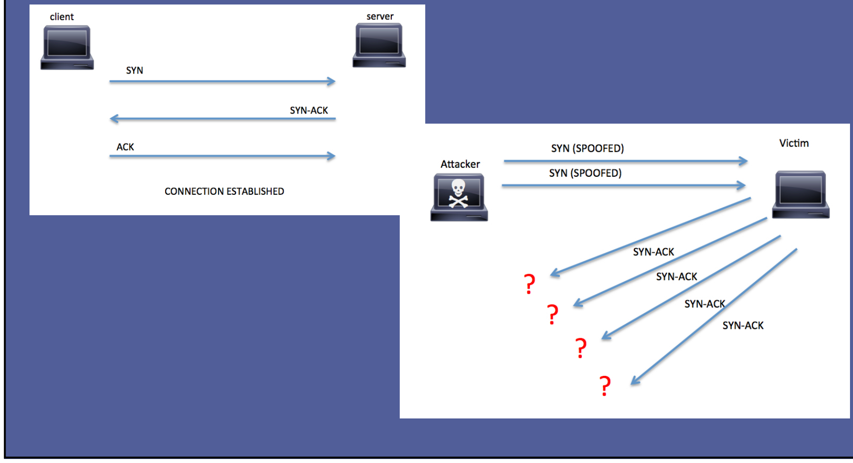
```
CCCCCCCCCC00CC00000888@8@88880000CC00088888888@@@@@@@@@8@8@@@@88800Cooocccc::::
CCCCCCCCCCCCCC00888@888888000CCC000088888888888@88888@@@@@@@888@800CCoococc:::
CCCCCCCCCCCCC0088@@8888880000000000888888808888888808080008888@88@@800C000Coc::
CCCCooooooCCC088@@8@88@88800000000888888888880000000000CCCC0000888@8888000Cc::::
CooCoCoooCCC08@88@88888880008888888888888888880000CCCoooooooooCC0008888888Cocooc:
ooooooCoCCC88@88888@8880088888888888888880808888800CCCoooocccccC000088@8880Coccc
ooooCC0080888888888@88080088888008880888800008888 80Cocoococ::ccooC0080888888Cooo
oCCCCCC08000CCC0088@88000000888808880000 0C008888808000CooCocc:::coC000888888800CC
oCCCCC000880CooC088@800000088088888800CCCCoC00088880000000Coc::::coC0000888088 0C
oCCCC008800CCCC008@@800C00000888888 80ooccccccoC08080088800000Cc.:ccooCC00008888800
CCC00008800CC0008@88800CCoooC0088880oc::...::co008888808880 0o:cocooCCCC000000880
CCC00888800C008@@8880Ccc:::cC008880c..... ....cC00000000000c.:cooooCCC000000000
00000088888000 08@8@80oc:.:...c008088c.      .  .co0008880000CooooccoC00000C0000
00000888@8@888888880o:. .  ...c08880c..          :o000000000CCoocooCoCoC00000000
C000888@88888888888 0o:.          .08888C:  .oC0o.  ...cCCC000ooooooccoooooooooCCC00
CCCC0088888808888880o. .o80o. .c0880o:          :. .:..ccoCCCooCooccoocccoooooCCCC
coooCC08@8800808880o::.... ..  :c080c. . .....  :.  .:ccCoooooccooooccccooooCCC
:ccooooC08880000800c..:...::. .co8@8Coc::..  ....  ..:cooCoooocccc::::ccooCCooC
.:::cooccco08000000C:..::.....coC08@800CC0c:...   ....:ccoooocccc::::::::coooooooC
....::::ccccoCC00000Cc......:oC08@8@880CCCocccccc::c::.:oCcc:::cccc:..::::coooooo
.......::::::::cCCCCCCoocc:c0888@88880000C000Coocc::.:cocc::cc::...:::coocccccc
...........::::..:coCCCCCCC08800008000CCooCCCooccc::::ccc::::::.......:ccocccc:co
.............:.....:oCCoooooC00CC0CCCoccococc::::coc:::.......  ...:::cccc:cooo
 .....  ............  .coocoooCCoco:::ccccccc:::ccc::..........   ....:::cc::::coC
   .  . ...    .... ..  .:cccoCooc:..  ::cccc:::c:.. .........  .......::::c:cccco
  .  .. ... ..    .. ..   ..:...:cooc::cccccc:.....  .........  .....:::::ccoocc
      .   .          .. ..::cccc:.::ccoocc:. ........... ..  . ..::.::::::ccco
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:

        perl slowloris.pl -dns [www.example.com] -options

        Type 'perldoc slowloris.pl' for help with options.

Bugtraq@Ubuntu:slowloris$ 
```

Notes:

HOW is it done?

Low Bandwidth Attacks

TCP Attack Flood: TCP SYN, TCP FIN, TCP RST, TCP Flags



Notes:

(Wireshark Example of good TCP connections)
PCAPs/http.cap

(Wireshark pcap example of syn attack)
PCAPs/SynFloodSample.pcap

Notes:

Defensive Countermeasures

When an attack hits

- More bandwidth
- Work with ISP to block the traffic
  (very difficult when the sources are distributed)
- Stateless packet filtering
  Hardware appliance (Not Firewall or IPS)
  Proxy / Cloud / CDN redirect service

Notes:

Where do you fit in

Proactive Countermeasures

Take steps to not become part of a bot net

Patch your devices
Enable firewalls
Change Default passwords
Be vigilant against phishing attacks
Update your anti-virus and anti-maleware

Notes:

Sources

A Cisco Guide to Defending Against Distributed Denial of Service Attacks
https://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html

Arbor Networks and Silver Back communications
http://sbnetworkit.com/arbor-networks/

NetScout DDoS and Network Visibility
https://www.netscout.com/arbor-ddos

NetScout WISR
https://www.netscout.com/report/

Notes:

About me

Tony Bemus

Bemushosting
https://bemushosting.com
Sunday Morning Linux Review
https://smlr.us
NetScout Arbor Cloud SOC
https://www.netscout.com/arbor-ddos

This Presentation:
https://bemushosting.com/

Notes: