Distributed Denial of Service

Forrest Addor, Director of Technology
Orange-Ulster BOCES
Overview

- What is DDoS?
- Types of DDoS
- Recent DDoS events
- Impact on K-12 Education
- DDoS Mitigation
- Tips & Tricks
- Q & A
What is DDoS?

DDoS is a type of [DOS attack](#) where multiple compromised systems (botnet), which are often infected with a [Trojan](#), are used to target a single system causing a [Denial of Service (DoS)](#) attack. (Webopedia, 2016)
Current DDoS Events

http://www.digitalattackmap.com

Types of DDoS

- Volume Based Attacks. Includes UDP floods, ICMP floods, and other spoofed-packet floods.
- Protocol Attacks. Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more.
- Application Layer Attacks.

(Incapsula)
Simple DDoS Example
Recent Events

October 21, 2016

- Dyn
- “10s of millions of IP addresses”
- Mirai botnet
- “Internet of Things” (IoT) Devices
- Twitter, Amazon, Reddit, Frontline
Recent Events

November 4, 2016

- Country of Liberia
- Single fiber connection to the Internet
- Mirai Botnet implicated
- 500-600 Gbps bursts
Impact on K-12 Education

Instructional
- Classroom resources
- Student management systems
- Learning management systems
- Online testing

Operational
- Food Service
- Payroll
- Purchasing
- Transportation
- Notification systems
DDoS Mitigation

1. *Detecting* the DDoS attack
2. *Diverting* the data traffic destined for the target device
3. *Analyzing and filtering* the bad traffic flows from the good traffic flows packets, preventing malicious traffic from impacting performance while allowing legitimate transactions to complete
4. *Forwarding* the good traffic to maintain business continuity
How do I know if I’m experiencing a DDoS Event?

1. Accessing Internet resources is slower than normal (or they may not load at all)
2. Server statistics may show large increase in visitors or data requests
3. Server logs may fill with unusual requests that do not match normal visitor usage
DDoS Mitigation Solutions

● Service Provider layer
  ○ “Blackholing” - Service provider blocks traffic as far upstream as possible to protect the customer
    - Requires coordination with service provider
    - All traffic to the specific destination is lost

● DDoS Appliance
  ○ Sits in local data center
  ○ Monitors data streams
  ○ Effective in handling application- and protocol-level threats

● Cloud-based Services
  ○ Provide solutions for diverting traffic and “scrubbing” bad data
  ○ Large network bandwidth available
Demonstration

radware

Every second counts
Tips & Tricks

Keep track of who is looking for your NAT (Network Address Translation) IP address, they are possible internal attackers

- [http://IPChicken.com](http://IPChicken.com)
- [Google: what is my ip?](http://Google: what is my ip?)
Tips & Tricks

Network testing sites allow anyone to initiate a DDoS attack on your network:

- VDoS Stresser - vdos-s.com

Some stressing sites are legitimate network stressing tools, others are not:

- https://str3ssed.me/
- http://networkstresser.com
Tips & Tricks

Attacks may be initiated from a cell phone. The best defense is to have users be aware of their surroundings

○ Start of a class period
○ Testing day

However...

Attacks may also be random and have no connection to your organization, staff, or students.
How Your BOCES Can Help...

- Shared costs
  - DDoS mitigation solution
  - Divergent connections to the Internet
- Centralized response
  - Monitoring
  - Diversion
Questions?
Thank you!

http://www.ouboces.org/ddos