

# BCNET

Shared IT Services for Higher Education & Research

# Conference 2017

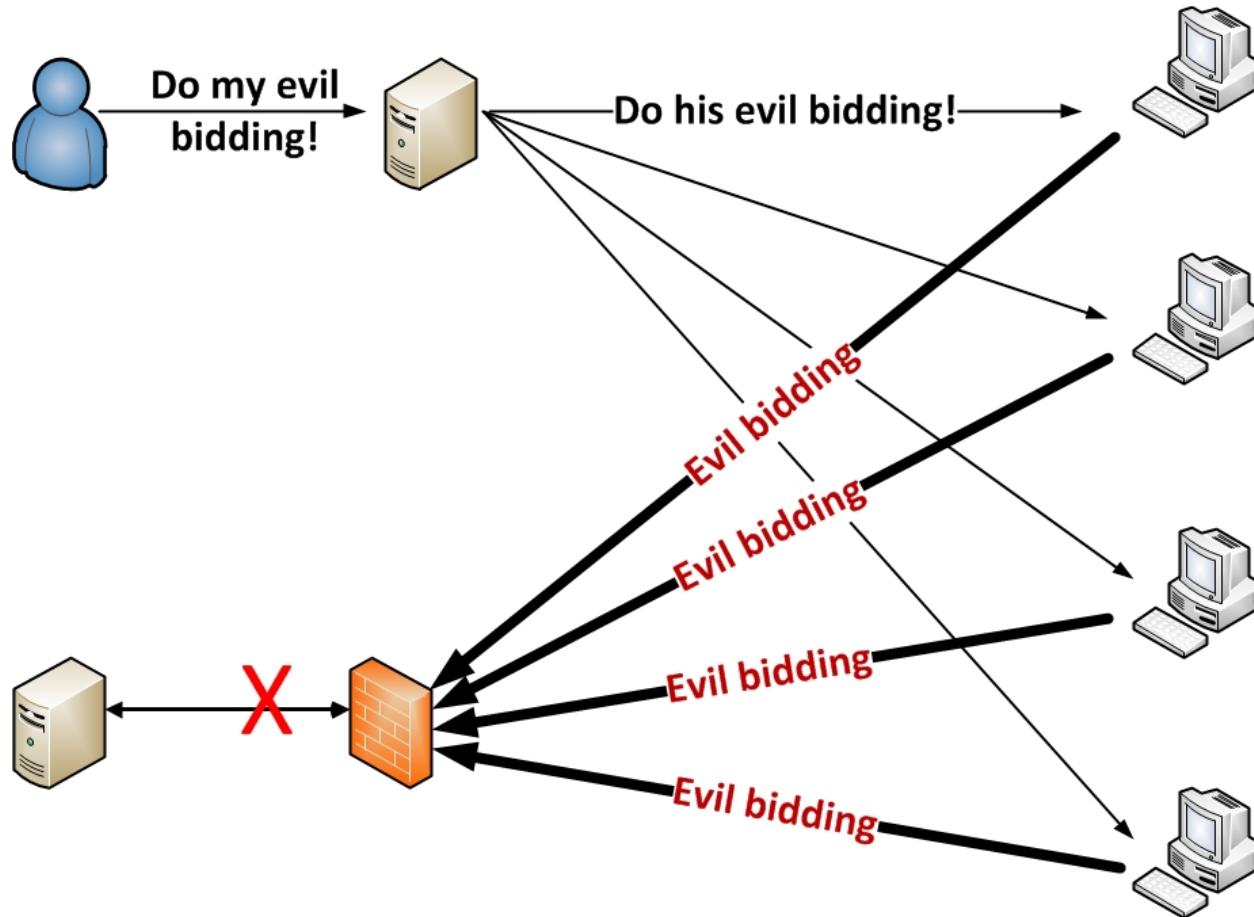


## Preparing for the Big One

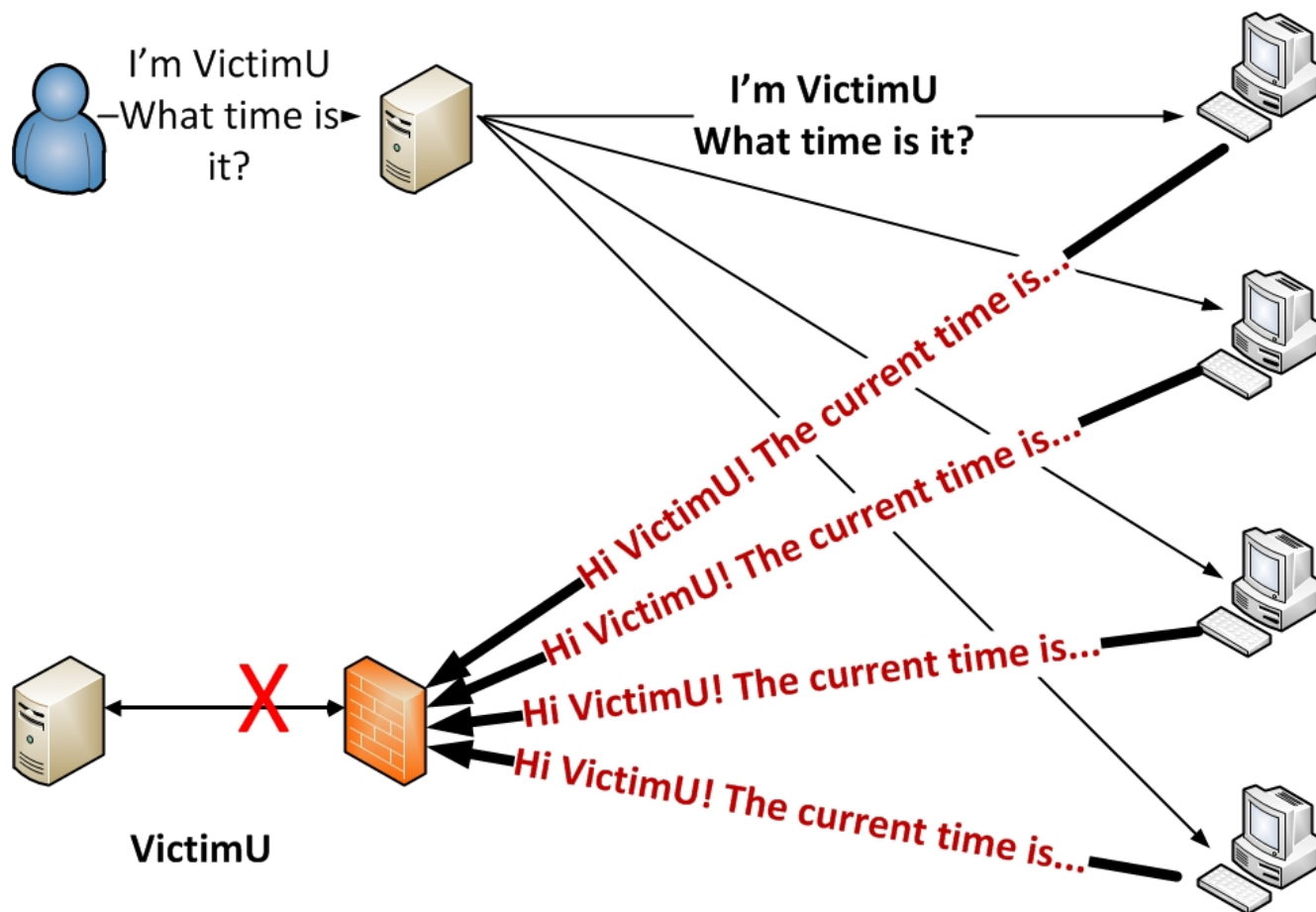
Distributed Denial of Service Attacks and  
You

- Hugh Burley, Thomson Rivers University
- Alex Doradea-Cabrera, BCNET
- Dave Kubert, University of Northern BC
- Keir Novik, Simon Fraser University

# Basic DDoS Attack



# Reflection DDoS Attack



# Arbor Networks

12<sup>th</sup> Worldwide Infrastructure Security Report 2017




The largest attack reported this year was 800 Gbps, a 60 percent increase over last year. Other respondents reported attacks of 600 Gbps, 550 Gbps and 500 Gbps. ATLAS data also shows that the frequency of extremely large attacks has increased dramatically this year.

This year's results show a 8 percent increase in education organizations



Service provider customers remain the number one target of DDoS attacks, with an increasing proportion of attacks targeting them.

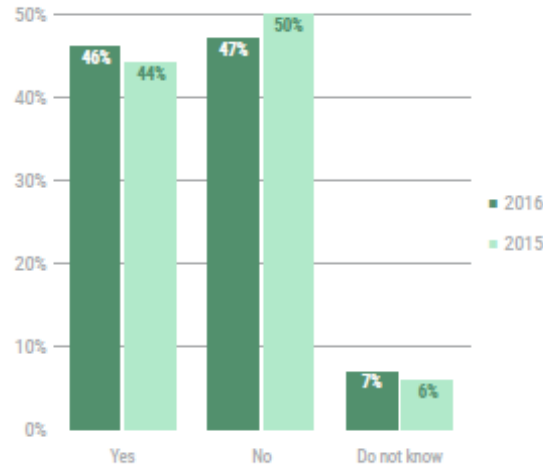


The proportion of respondents seeing attacks targeting cloud-based services has decreased significantly, down from one third last year to only one quarter this year.

# Scalar

Security Study 2017

Did your organization experience a DDoS attack that caused a disruption to business operations and/or system downtime? <sup>1</sup>



## HIGHEST REPORTED INCIDENTS OF DDoS ATTACKS\*

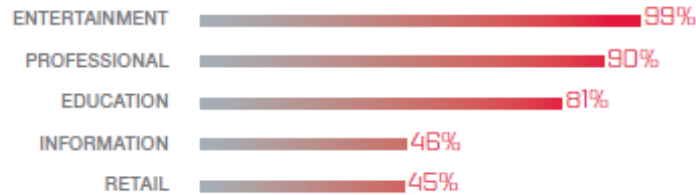


FIGURE 2. Data from 2016 Verizon Data Breach Investigations Report—security incidents by industry Regulatory compliance. Read full report for additional detail.

# Sonic Wall

2017 Annual Threat Report

Gaps in IoT devices exposed the largest DDoS attack in history via Mirai botnet



DDoS attacks are estimated to cost businesses **an average of \$22,000 per minute**

with the cost ranging as high as over \$100,000 per minute.<sup>[1]</sup>

With the average DDoS attack lasting six hours, the financial impact can be enormous.



# Defensive Measures

- Current capabilities
  - Member policers
  - Member filters
  - Port threshold alerts
  - Black hole or null route

# Defensive Measures

- Areas of improvement
  - Visibility / detection tools to gather accurate signatures
  - Tools with baselines and threat intelligence
  - Border filters based on signatures
  - Cloud based scrubbing service
  - RTBH and black hole techniques

# How can you protect?

- Patch and configure systems securely
- Prevent spoofed traffic from leaving your network (BCP38)
- Least privilege filtering
- Replace fragile systems
- Build capacity
- Network and firewalls



# How can you plan?

- Business Continuity Plan
- Disaster Recovery Plan
- Incident Response Plan
- Tolerance of service disruption
- Service prioritization
- Communications – internal and external

# How can you prepare?

- Visibility
- Monitor
  - Service response
  - Unusual traffic
- Ability to block
- Authority to act

# DDoS Survey Results

- Have DDoS attacks been discussed at your organization?
  - Yes: 6
  - No: 2
  - I don't know: 1

# DDoS Survey Results

- Has your organization been the victim of DDoS attacks?
  - Yes: 6
  - No: 1
  - I don't know: 2

# DDoS Survey Results

- If so, frequency and duration?
  - Weekly (many insignificant, more serious recently)
  - Planned to hit registration servers on reg. day
  - 1 attack in 2.5 years, about 2 hours
  - Half dozen per year, about 1 hour
  - 1 event of note lasting 2 hours
  - 3 events in 10 years, 1 to 3 days in duration

# DDoS Survey Results

- What is the estimated cost of loss of Internet?
  - 1 hour
    - \$1000 - \$10000
    - Manageable
  - 1 critical hour
    - \$10000 - \$100000
  - 1 day
    - “thousands of dollars”, “very costly”
  - 1 critical day
    - “priceless” “millions of dollars”
- “We don’t know”

# DDoS Survey Results

- What is the maximum time your organization could tolerate without Internet service?
  - Less than an hour
  - 10 minutes
  - 1 day
  - 3 hours
  - I don't know
  - 3 days
  - Have not considered
  - 4 hours

# DDoS Survey Results

- Do you consider BCNET's current DDoS Protection capability to be sufficient, keeping in mind that it does not protect the targeted service but instead protects the rest of your infrastructure from being overwhelmed?
  - Yes: 1
  - No: 3
  - Undecided: 5



# DDoS Survey Results

- Does your organization employ source address validation methods to reduce your participation in DDoS attacks?
  - Yes: 4
  - No: 2
  - I don't know: 3

# DDoS Survey Results

- What other countermeasures does your organization employ against internally-origination DDoS attacks?
  - Engaged 3<sup>rd</sup> party service
  - Next Gen firewall
  - VLANs
  - Packet-shaping
  - Nothing yet
  - Vulnerability management program

# DDoS Survey Results

- Would your organization consider a subscription to a shared BCNET DDoS scrubbing service?
  - Yes: 5
  - No: 1
  - Undecided: 3

# Questions?