Common Misconceptions About The Modern Day DDoS Attack

Tom Bienkowski, Director DDoS Product Marketing
Arbor Networks  The Security Division of NETSCOUT

16

Number of years Arbor has been delivering innovative security and network visibility technologies & products

#1

Arbor market position in Carrier, Enterprise and Mobile DDoS equipment market segments – [Infonetics Research Dec, 2015]

100%

Percentage of world’s Tier 1 service providers who are Arbor customers

120 Tbps

Amount of global traffic monitored by the ATLAS

http://digitalattackmap.com
Common Misconceptions About DDoS Attacks

- I have adequate DDoS protection solutions in place. (My firewall, IPS, ISP)
- Impact does not justify the cost of protection.
- The odds are we will NOT be attacked.
- DDoS is “old news” …I’m more concerned with Advanced Threats.
Common Misconceptions About DDoS Attacks

I have adequate DDoS protection solutions in place. (My firewall, IPS, ISP)

Impact does not justify the cost of protection.

DDoS is “old news” …I’m more concerned with Advanced Threats.

The odds are we will NOT be attacked.
The Cyber Reflection

Every Physical Geo-Political Event…
DDoS Attack Trends

Fact: DDoS Attacks Increasing in Size, Frequency & Complexity

*Source: Arbor Networks 11th Annual Worldwide Infrastructure Security Report

Survey Peak Attack Size Year Over Year

Multi-Vector DDoS Attacks

Demand for DDoS Detection/Mitigation Services

*Source: Arbor Networks 11th Annual Worldwide Infrastructure Security Report
Ability & Motivations

Fact: It’s never been easier to launch a DDoS attack

$5:$100sK

Cost of DDoS Service  Impact to Victim

Buy DDOS - Professional DDOS Service
Ability & Motivations

Fact: Many motivations behind DDoS attacks

**DDoS Attack Motivations**

- **42%** Criminals demonstrating DDoS attack capabilities
- **41%** Online gaming-related
- **35%** Criminal extortion attempt
- **31%** Online gambling-related
- **31%** Nihilism/vandalism
- **30%** Social networking-related
- **29%** Political/ideological disputes
- **26%** Diversion to cover compromise/data exfiltration
- **23%** Flash crowds
- **23%** Competitive rivalry between business organizations
- **21%** Inter-personal/inter-group rivalries
- **21%** Misconfiguration/accidental
- **19%** Financial market manipulation
- **9%** Intra-criminal disputes

*Source: Arbor Networks 11th Annual Worldwide Infrastructure Security Report*
Examples of The Cyber Reflection

Every Physical Geo-Political Event…

Has a Cyber Reflection…
The Gaza Strip Conflict

- **July 27th**: [Reuters] “UN Security Council Calls For Cease-Fire As Muslims Start Celebrating Eid al-Fitr” – there is a noticeable reduction in physical and DDoS attacks.

- **July 29th**: [Jewish Daily Forward] “The Palestinian Authority announced that it had brokered a 24-hour humanitarian cease-fire with all Palestinian factions with the possibility of extending it an additional 48 hours.”

- **August 1st**: [NY Times] “Gaza fighting intensifies as cease fire falls apart”

- **August 3rd**: Notice that the number of attacks rises again sharply. From July 28th through August 2nd, there were a total of 192 attacks. On August 3rd there were 268.
Flint, Michigan Water Contamination

- Michigan.gov website was attacked on Saturday, Jan. 16
- Hurley Medical Center confirmed on Thursday, Jan 21 it was the victim of a "cyber attack" a day after Anonymous hacktivists threatened action over Flint's water crisis.
Ferguson, MO & Cleveland, OH 2014

- Attack and threats against Ferguson law enforcement and town government websites.

- Tamir Rice shooting
  - Madness C2 started ordering attacks against Cleveland city websites
    - C2 appears to be associated with Anonymous
  - ATLAS also reported NTP amplification attack (Peaked at 5Gbps)
FIFA World Cup Brazil

- Over 60 World Cup related websites were attacked.
- Also threatened to take down sponsor sites.
2016 Rio Summer Olympics

People protest against the Olympic event and the interim government of Michel Temer, on the day of the inauguration at Maracana stadium of the Rio 2016 Olympic Games, Rio de Janeiro, Brazil, on 05 August 2016. EPA/Leonardo Muñoz

RIO DE JANEIRO -- Hours before it stages its Opening Ceremony, Rio’s troubled Olympics faced a big street demonstration on Friday when a few
"the more you click on the button, the more attack windows will be launched..." "have fun going to dinner, travel, work while your computer does all the work safely and anonymously..."
2016 Rio Summer Olympics

**Attack Volume**

- Pre-Olympics probing attacks using IoT botnet (200 Gbps)
- Sustained 500+Gbps attack from Opening to Closing Ceremonies (GRE, non reflection/amplification)
- Targets include Brazilian ISPs, banks, government institutions and sponsors
Common Misconceptions About DDoS Attacks

- I have adequate DDoS protection solutions in place. (My firewall, IPS, ISP)
- Impact does not justify the cost of protection.
- The odds are we will NOT be attacked.
- DDoS is “old news” …I’m more concerned with Advanced Threats.
Motivations

Fact: Many motivations behind DDoS attacks

![Graph showing DDoS Attack Motivations]

- 42% Criminals demonstrating DDoS attack capabilities
- 41% Online gaming-related
- 35% Criminal extortion attempt
- 31% Online gambling-related
- 31% Nihilism/vandalism
- 30% Social networking-related
- 29% Political/ideological disputes
- 26% Diversion to cover compromise/data exfiltration
- 23% Flash crowds
- 23% Competitive rivalry between business organizations
- 21% Inter-personal/inter-group rivalries
- 21% Misconfiguration/accidental
- 19% Financial market manipulation
- 9% Intra-criminal disputes

*Source: Arbor Networks 11th Annual Worldwide Infrastructure Security Report*
DDoS Used in Multiple Stages of Kill Chain

Advanced Attack Kill Chain

RESEARCH
Recon

INITIAL COMP
Weaponization
Delivery
Installation

SPREAD OUT
Exploitation
C&C

EXTRACT DATA
Complete Mission

Target Org

Attack Activities Over Time

Port Scanning  DDoS  Port Scanning

Phishing  Evasion  P2P  Zero Day

DDoS  Bad URL  Phishing

RAT  Evasion  Malware

Evasion  POS  Bot

TOR  Evasion  DDoS

Attackers

DDoS Used in Multiple Stages of Kill Chain
# DDoS Used in Multiple Stages of Kill Chain

## Advanced Attack Kill Chain

<table>
<thead>
<tr>
<th>RESEARCH</th>
<th>Recon</th>
</tr>
</thead>
<tbody>
<tr>
<td>INITIAL COMP</td>
<td>Weaponization Delivery Installation</td>
</tr>
<tr>
<td>SPREAD OUT</td>
<td>Exploitation C&amp;C</td>
</tr>
<tr>
<td>EXTRACT DATA</td>
<td>Complete Mission</td>
</tr>
</tbody>
</table>

## Attack Activities Over Time

- Port Scanning
- **DDoS**
- Port Scanning
- Phishing
- Evasion
- P2P
- Zero Day
- DDoS
- Bad URL
- Phishing
- RAT
- Evasion
- Malware
- Evasion
- POS
- Bot
- TOR
- Evasion
- DDoS

**Sizing up your security posture...in preparation for later weaponization/data exfiltration stage**
DDoS Used in Multiple Stages of Kill Chain

Evasion / Diversion Tactic: Overwhelming your security forensics making it harder to find indicators of compromise / breach.
DDoS Used in Multiple Stages of Kill Chain

- **Advanced Attack Kill Chain**
- **Attack Activities Over Time**
  - Port Scanning
  - DDoS
  - Port Scanning
  - Phishing
  - Evasion
  - P2P
  - Zero Day
  - DDoS
  - Bad URL
  - Phishing
  - RAT
  - Evasion
  - Malware
  - Evasion
  - POS
  - Bot
  - TOR
  - Evasion
  - DDoS

**Diversion**: Analogous to setting alarms off at one end of building while thief slips out the other with all the loot.
DDoS as Smokescreen

What type of attack was this?

According to the BBC, this was a DDoS - a distributed denial of service attack - where a website is overwhelmed by bot traffic, and breaks down. TalkTalk has not revealed how the personal data of its customers was actually stolen, but speculations suggest that the DDoS was used to distract security professionals, while the hackers compromised the personal data on the site through a different loophole.

Federal Financial Institutions Examination Council

Joint Statement

Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC) members ("members") are issuing this statement to notify financial institutions of the risks associated with the continued distributed denial-of-service (DDoS) attacks on public websites. The statement also outlines the steps that institutions are expected to take to address these attacks, and provides resources to help institutions mitigate the risks posed by such attacks.

BACKGROUND

In the latter half of 2012, an increased number of DDoS attacks were launched against financial institutions by politically motivated groups. These DDoS attacks continued periodically and increased in sophistication and intensity. These attacks caused slow website response times, intermittently prevented customers from accessing institutions’ public websites, and adversely affected back-office operations. In other cases, DDoS attacks served as a diversionary tactic by criminals attempting to commit fraud using stolen customer or bank employee credentials to initiate fraudulent wire or automated clearinghouse transfers.
Examples of Combo DDoS & Advanced Threats Tools in the Wild
The Game Has Changed

Fact:

- Advanced threats have evolved from independent DDoS attacks and malware to **attack campaigns**.
- Attack campaigns are organized human to human campaigns, using multiple tools and techniques - DDoS is a common attack tool.
Common Misconceptions About DDoS Attacks

I have adequate DDoS protection solutions in place. (My firewall, IPS, ISP)

The odds are we will NOT be attacked.

Impact does not justify the cost of protection.

DDoS is “old news” …I’m more concerned with Advanced Threats.
Misconception: Firewall / IPS Will Stop DDoS Attacks

Fact: Firewalls and IPS (load balancers, WAF etc.) are not designed to stop DDoS attacks.

- DDoS attacks use legitimate packets and do not violate protocols rules – thus many go undetected by firewalls and IPS.
- Because firewalls and IPS (load balancers, WAF) are required to track state, they are vulnerable to some DDoS attacks (e.g. HTTP/TCP SYN floods) – and routinely fail during attacks.

Completing the Security Triad:

Confidentiality
Integrity
Availability?
The Modern Day DDoS Attack Is Complex

Dynamic, multi-vector combination

TCP State-Exhaustion Attacks
- Crashes stateful devices (Load balancers, firewalls, IPSs)

Volumetric Attacks
- Large (up to 500 Gbps)
- Saturates links

Your ISP

Your Data Center

Firewall

Application Layer Attacks
- Low and Slow, Stealth attacks
- Crashes application servers

Industry Best Practices exist to stop all of these attacks
Stopping Modern Day DDoS Attacks

Layered DDoS Attack Protection

1. Stop volumetric attacks In-Cloud

2. Stop application layer DDoS attacks & other advanced threats; detect abnormal outbound activity

3. Intelligent communication between both environments

4. Backed by continuous threat intelligence

Backed by Continuous Threat Intelligence

A Recommended Industry Best Practice:
Arbor’s DDoS Protection Solution

Comprehensive DDoS Protection Products & Services

Armed with Global Visibility & Actionable Threat Intelligence
Closing Statements

Without the proper knowledge of...

1. DDoS attack trends (i.e. ease, motivations, attack types, relationship with data breach)
2. Best practices in DDoS mitigation (i.e. Products, People and Processes)
3. Impact to your business (i.e. downtime, loss revenue, mitigation costs etc.)

...You cannot accurately calculate the risk to your organization and put the proper business continuity plans in place.
Q&A / Thank You

For more info, please contact:

Tom Bienkowski
Director DDoS Product Marketing
tbienkowski@arbor.net