Abusing Public Third-Party Services for EDoS Attacks

Huangxin Wang*, Zhonghua Xi, Fei Li and Songqing Chen

August 9, 2016, Austin, TX





Outline

- Introduction
- Threat Model
- Third-party Services Characterization
- An EDoS Attack
- Defense Strategies
- Conclusion

Introduction

- Cloud service
  - Low cost
  - Pay as you go
  - Auto scalable

Perfect targets for EDoS attacks

amazon web services™ | EC2



Google Cloud Platform

Introduction (Cont'd)

- Cloud Attack Example
  - GreatFire.org in Amazon EC2
    - 2500x increase in traffic
    - **$30,000/day** under attack



- Economic Denial of Sustainability (EDoS)
  - Long-term, slowly drain the budget of the victim
  - Hard to detect

Related Work

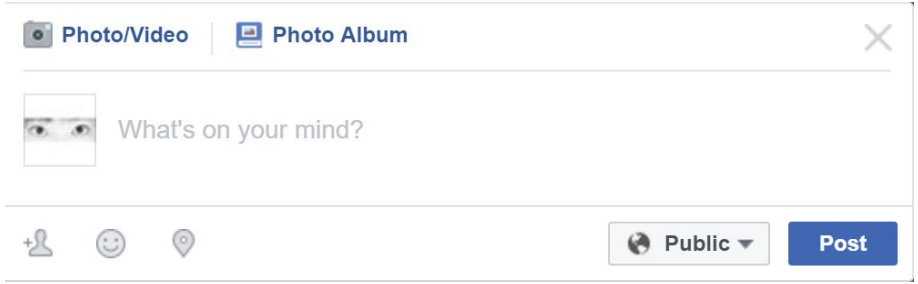
- CAPTCHA / Puzzle
  - [Kumar 2012]
  - [Masood 2013]
- Cloud weak protection
  - Budget limit alert

Objective

- Reveal the severity of the EDoS problem
- How EDoS attacks can be conducted
  - Easily
  - Low cost

Background

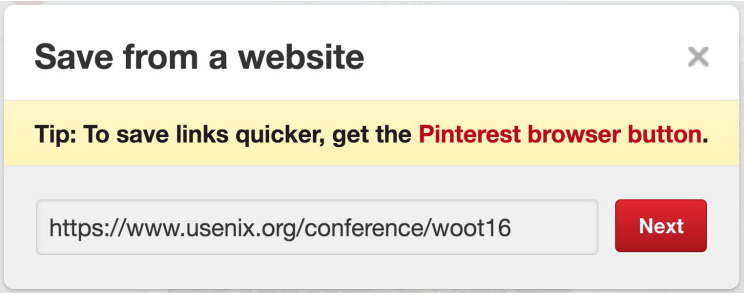
- Pre-fetching services (Facebook)

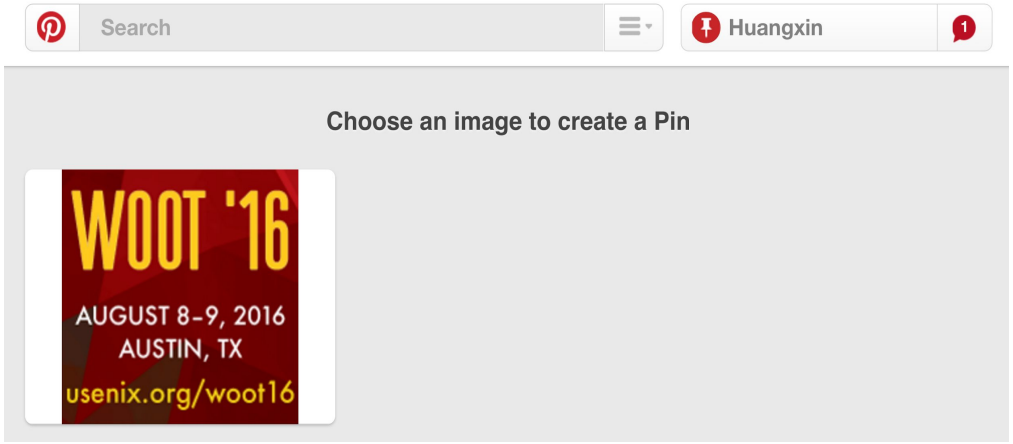




Background (Cont'd)

- Pre-fetching services (Pinterest)

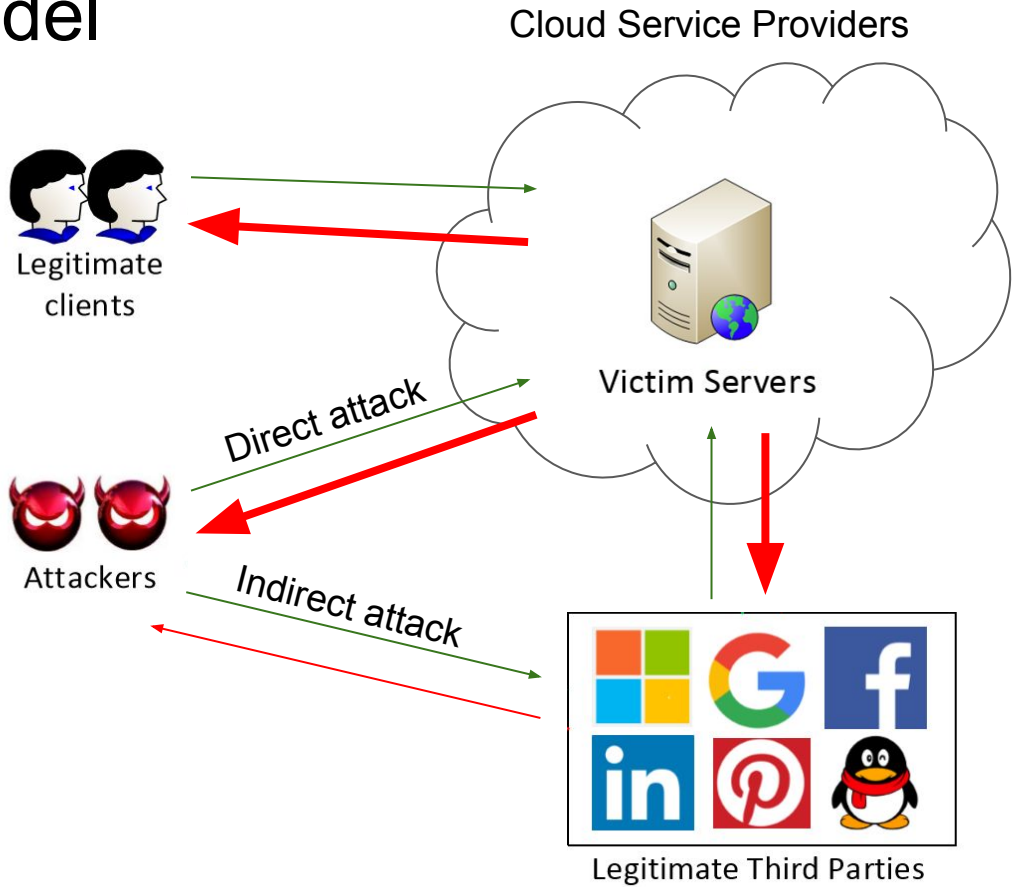




Outline

- Introduction
- **Threat Model**
- Third-party Services Characterization
- An EDoS Attack
- Defense Strategies
- Conclusion

Thread Model



Cloud Utility Model

CSP	Server Price	Traffic Egress to Internet
Amazon Cloud	$0.12/hr	$0.09/GB
Google Cloud	$0.10/hr	$0.12/GB
Microsoft Azure	$0.12/hr	$0.087/GB

Table 1: The charging model of different cloud service providers.

Outline

- Introduction
- Threat Model
- Third-party Services Characterization
- An EDoS Attack
- Defense Strategies
- Conclusion

Characterization of Third-party Services

- Identity
  - IPs / User-Agent / Cloud-based?
- Request/Response size
  - Max fetch size
  - Bandwidth / Timeout
- Caching
- Registration Cost and Anonymity

Characterization of Third-party Services (Cont'd)

- Experiment Setup

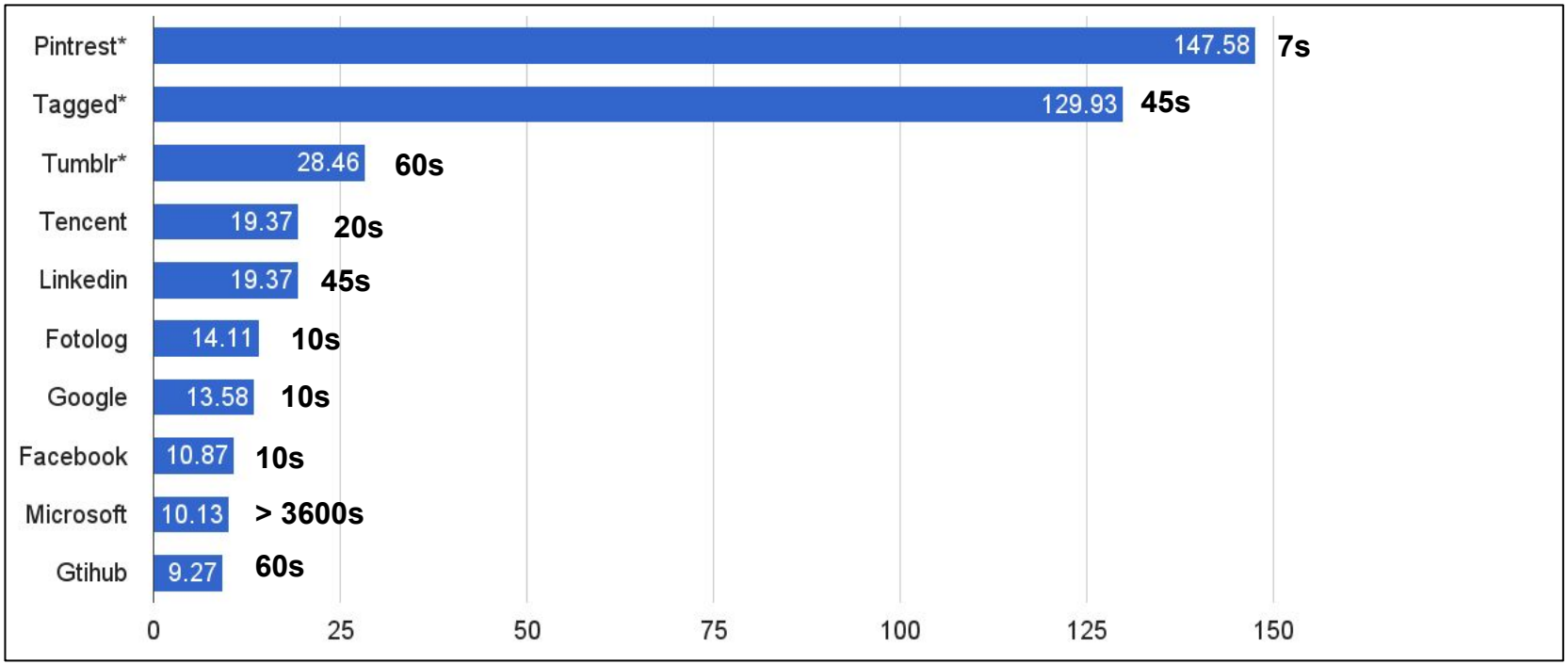


Characterization of Third-party Services (Cont'd)

- Social network
  - Facebook, Fotolog, LinkedIn, Pinterest, Tencent, Tagged 
- Mail service
  - Outlook 
- Online document/repo services
  - Google Docs, Github 

Characterization of Third-party Services (Cont'd)

- Max Fetch Size (MB) and Timeout



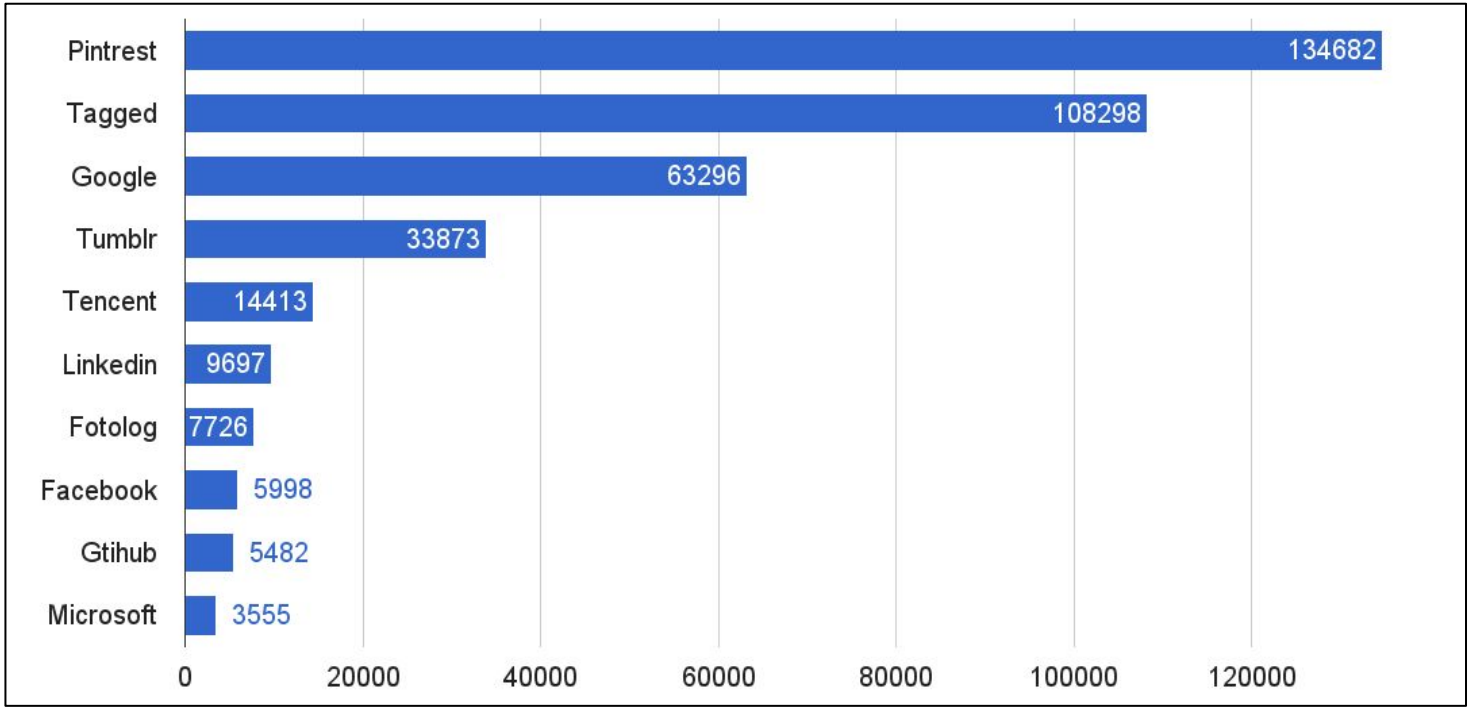
Amplification Factor

- Bandwidth amplification factor (BAF)

$$BAF = \frac{Traffic_{victim}}{Traffic_{attacker}}$$

Characterization of Third-party Services (Cont'd)

- Max Bandwidth Amplification Factor



Characterization of Third-party Services (Cont'd)

Provider	User-Agent	Fetch file type	Cache Resource	IPs*	In the public cloud
Facebook	facebookexternalhit/1.1	any	✓	175	-
	visionutils/0.2	any	✓	32	-
Fotolog	fotolog	images**	✗	1	-
Github	Camo Asset Proxy 2.2.0	images**	✓	40	Amazon Cloud
Google	Feedfetcher-Google	any	✓	3	-
LinkedIn	Embedly/0.2	any	✓	6	Amazon Cloud
Microsoft	BingPreview/1.0b	any	✓	409	-
Pinterest	Pinterest/0.2	any	✓	728	Amazon Cloud
Tagged	-	any	✓	2	-
Tencent	Mozilla/5.0 AppleWebKit/537.36 Chrome/31.0.1650.57 Safari/537.36	any	✓	1	-
Tumblr	Tumblr/14.0.835.186	any	✓	2	-

Table 3: Characteristics of the fetching services. *unique number of IPs used to serve 2000 requests. **file types based on extensions.

Characterization of Third-party Services (Cont'd)

- Registration Cost and Anonymity
  - All are free
  - All are anonymous
  - Registration is not required for Google

Outline

- Introduction
- Threat Model
- Third-party Services Characterization
- **An EDoS Attack**
- Defense Strategies
- Conclusion

An EDoS Attack

- Attack Settings
  - Single IP/Account
  - Request for 2000 times with interval 10s
  - Append an unique query string to cause cache missing

```
http://victim/img.jpg?s=pinterest&id=1
http://victim/img.jpg?s=pinterest&id=2
...
http://victim/img.jpg?s=pinterest&id=2000
```

An EDoS Attack (Cont'd)

- Attack traffic observed in the victim server

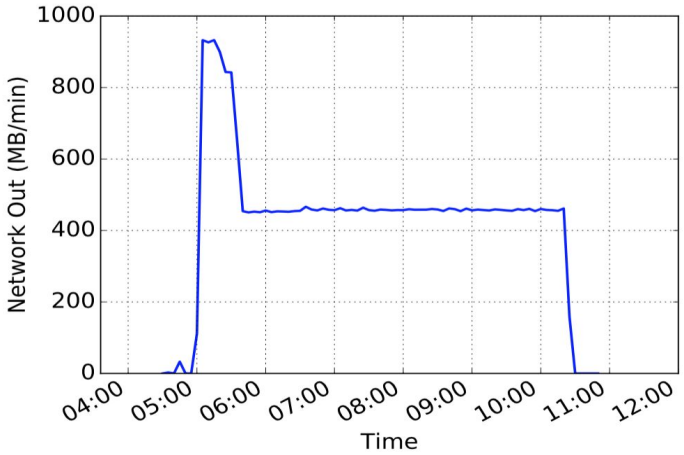


Figure 4: Average network out traffic of the victim server under requests from 10 third-party service providers with a 10-second request interval. Each sample point is the average value within a 5-minute window.

Cost:
$11.78 for 166GB traffic
$1545.07/month at the same attack rate

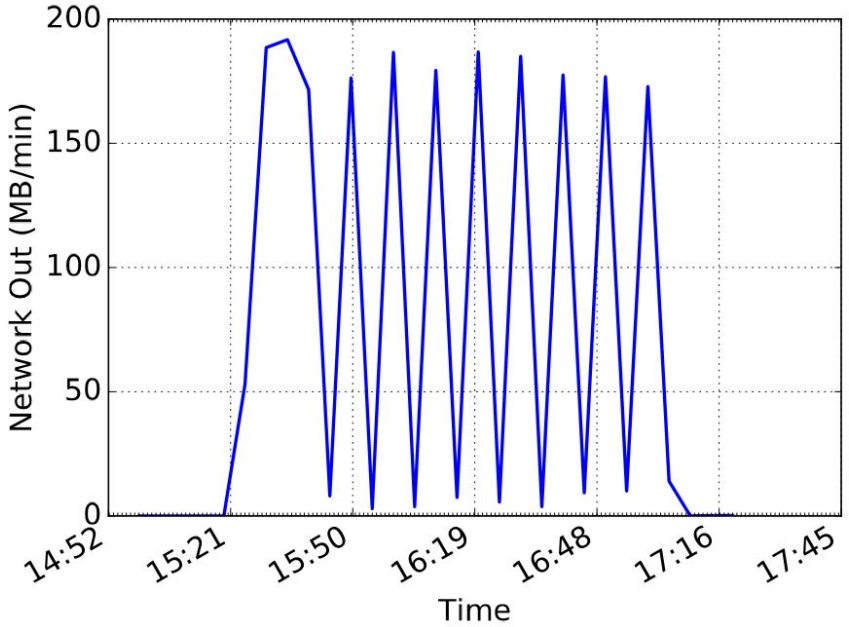
Note: it is only single IP, single account!

Outline

- Introduction
- Threat Model
- Third-party Services Characterization
- An EDoS Attack
- **Defense Strategies**
- Conclusion

Defense Strategies

- Third-parties
  - Capacity >> Cloud users
  - Rate limit
  - Forward HEAD requests



Microsoft block the requests periodically

Defense Strategies (Cont'd)

- Cloud users
  - Rate limit
    - IP/User-Agent-based filtering
  - Same-zone/region severing
    - E.g., 3 service providers are in the cloud
      - Lower-to-free traffic cost

Current Deployed Model



Key	Value
http://victim/ img.jpg	image_bytes
http://victim/img.jpg ?id=1	image_bytes

Cache

Proposed Model



Key	Value
http://victim/ img.jpg	image_bytes

Cache

Victim server:
Redirect to final url

Third-party services:
Check the cache again

Proposed Model (Cont'd)

- Results
  - Tagged works under our proposed scheme
    - Dropping the avg BAF from 15464.11 -> 0.43
  - Other service providers
    - Not check the cache

Outline

- Introduction
- Threat Model
- Third-party Services Characterization
- An EDoS Attack
- Defense Strategies
- **Conclusion**

Conclusion & Future work

- Conclusion
  - Third-party services make EDoS attacks easy/cheap
  - Effective defense strategy requires cooperations
- Future work
  - Exploring different attack approaches
  - Defense strategy for general EDoS attack is demanded

Thank you!