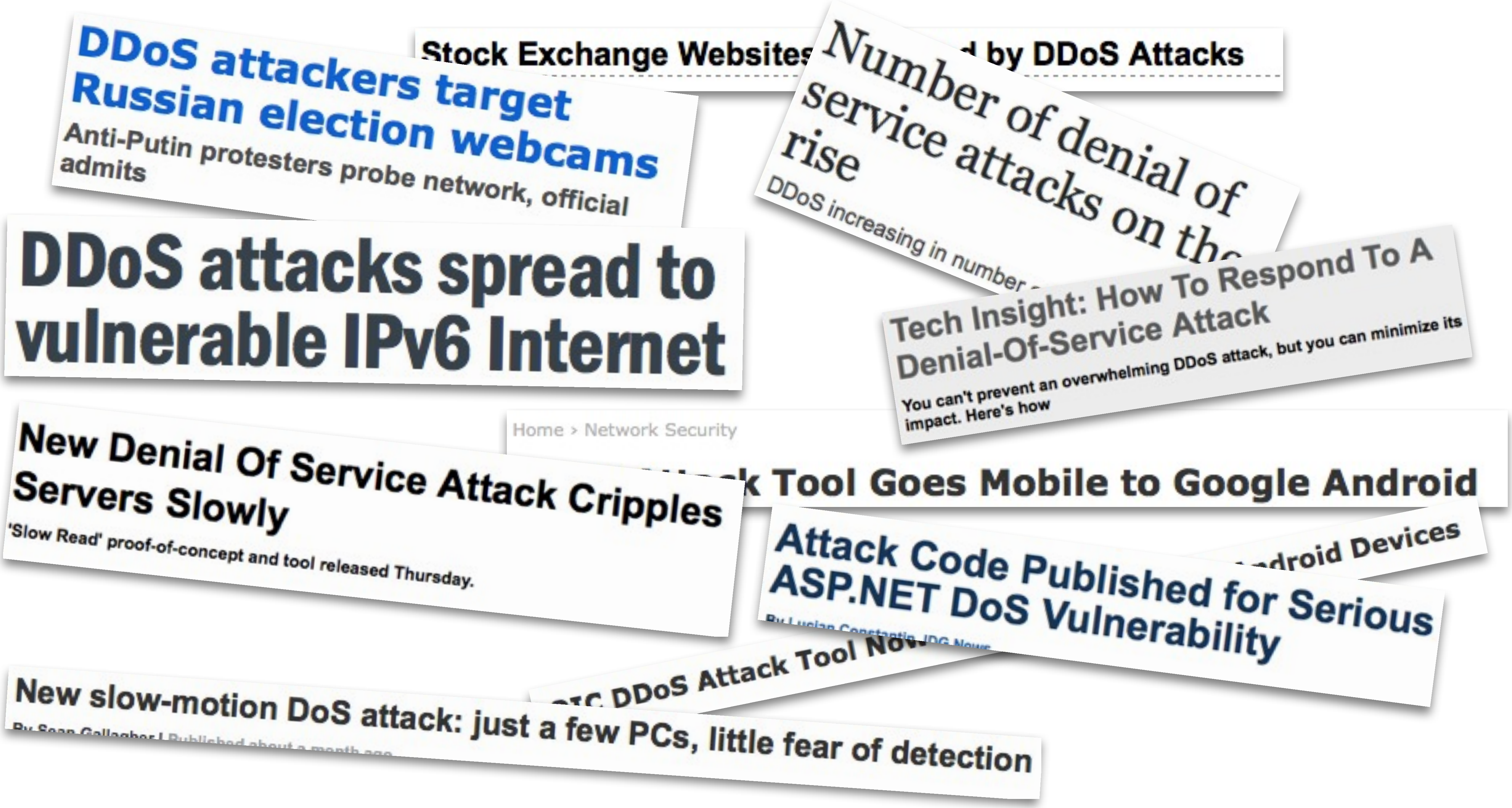
Tweaking to get away from SlowDOS

Tweaking to get away from SlowDOS
Sergey Shekyan, Senior Software Engineer
June 2nd, 2012

OWASP Kansas City
June 21st, 2012

The OWASP Foundation
http://www.owasp.org

Denial of Service Attacks



DDoS attackers target Russian election webcams

Anti-Putin protesters probe network, official admits

Stock Exchange Websites d by DDoS Attacks

Number of denial of service attacks on the rise

DDoS increasing in number

DDoS attacks spread to vulnerable IPv6 Internet

Tech Insight: How To Respond To A Denial-Of-Service Attack

You can't prevent an overwhelming DDoS attack, but you can minimize its impact. Here's how

Home › Network Security

k Tool Goes Mobile to Google Android

New Denial Of Service Attack Cripples Servers Slowly

'Slow Read' proof-of-concept and tool released Thursday.

ndroid Devices

Attack Code Published for Serious ASP.NET DoS Vulnerability

By Lucian Constantin, IDG News

IC DDoS Attack Tool Now

New slow-motion DoS attack: just a few PCs, little fear of detection

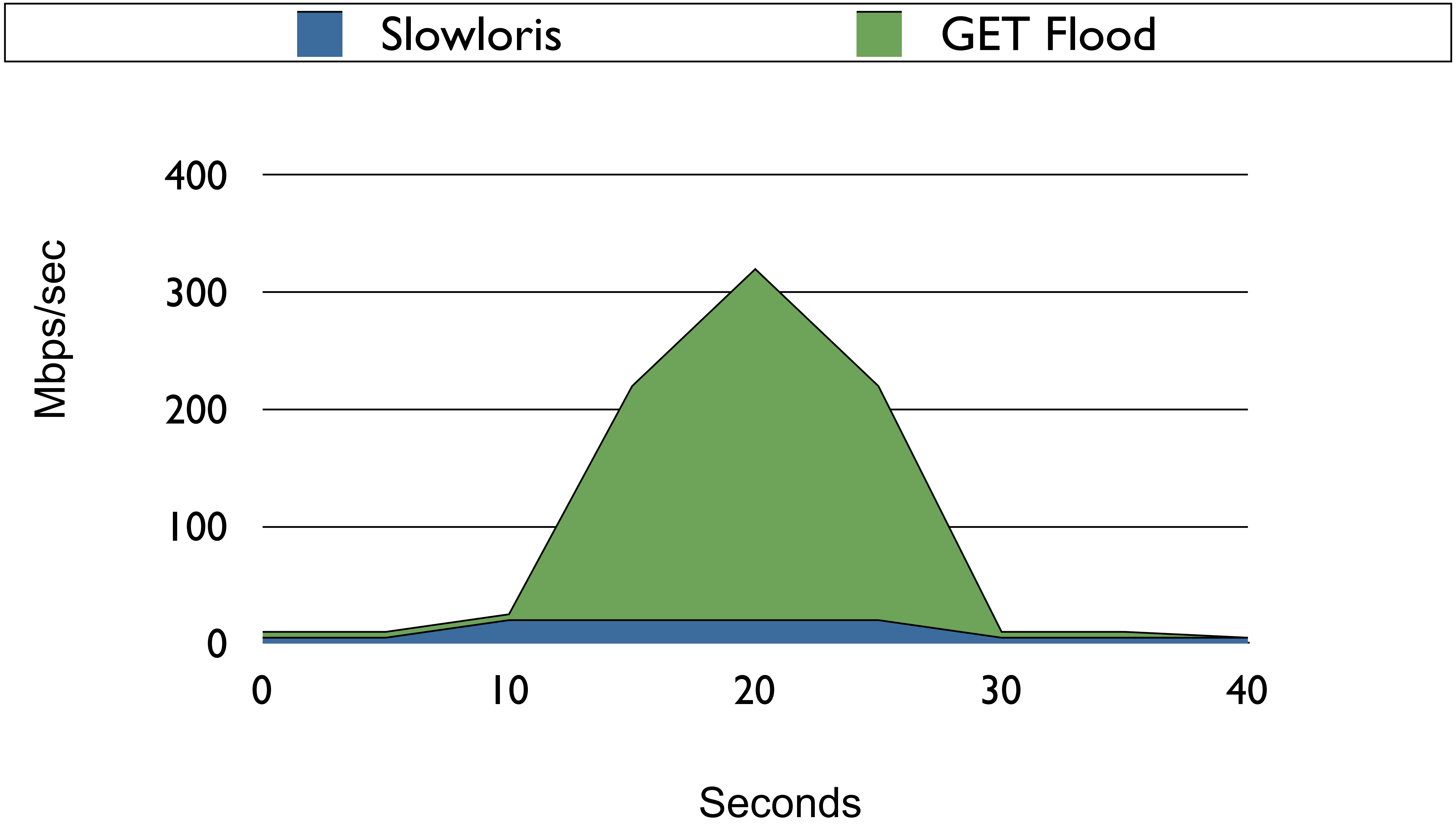
By Sean Gallagher | Published about a month ago

Types of attack

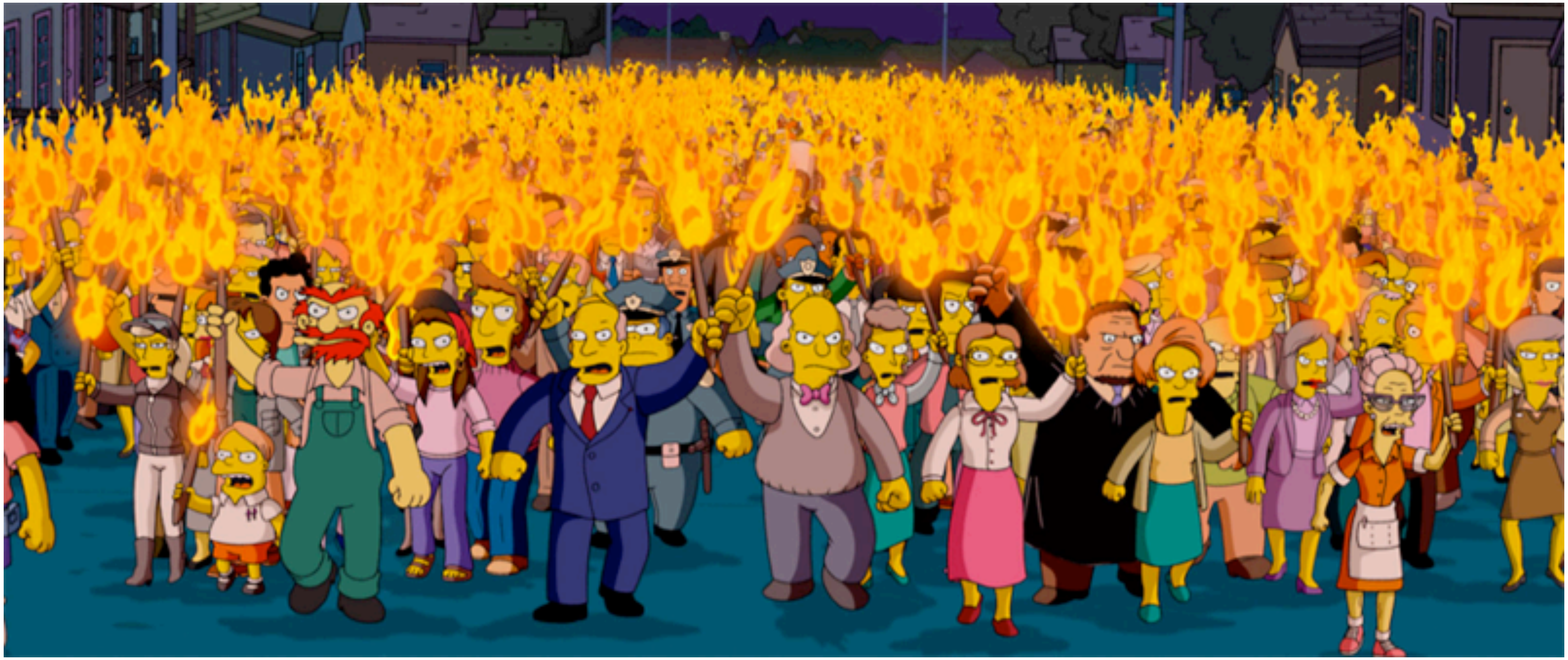
There is a variety of forms aiming at a variety of services:

- Traffic consuming attacks (DNS, firewall, router, load balancer, OS, etc.)
- Application Layer attacks (web server, media server, mail server)

What is low-bandwidth attack?



Network Layer attacks

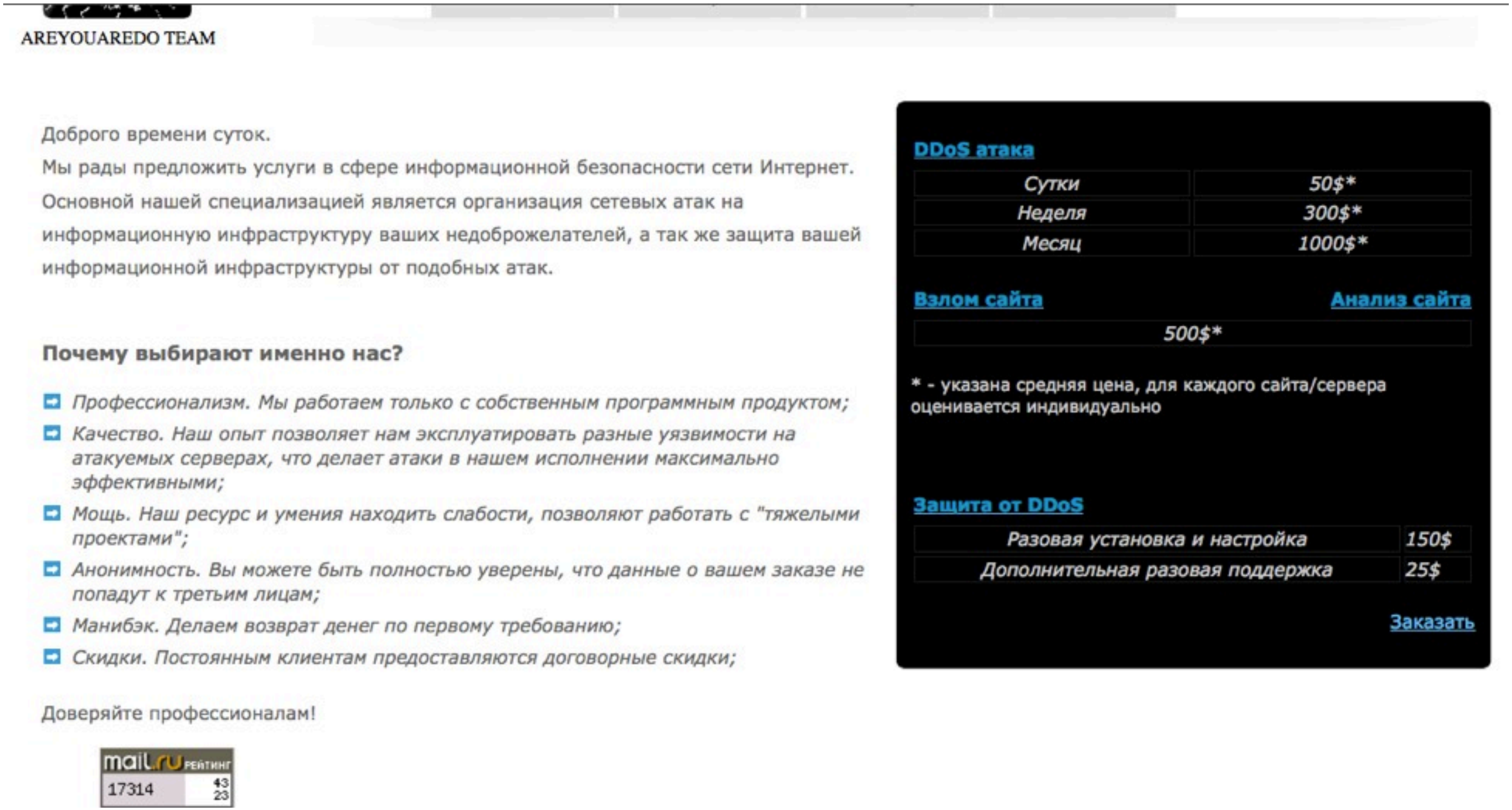


Application Layer attacks

DDoS economics

- DDoS attacks are affordable (from $5/hour)
- DDoS attack is a great way to promote your start-up (attacks on Russian travel agencies are 5 times as frequent in high season)
- Longest attack detected by Kaspersky DDos Prevention System in the second half of 2011 targeted a travel agency website and lasted 80 days 19 hours 13 minutes 05 seconds
- Akamai reports DDoS attack incidents soar 2,000 percent in the past three years

Screenshot of a “company” offering DDoS services



AREYOUAREDO TEAM

Доброго времени суток.

Мы рады предложить услуги в сфере информационной безопасности сети Интернет. Основной нашей специализацией является организация сетевых атак на информационную инфраструктуру ваших недоброжелателей, а так же защита вашей информационной инфраструктуры от подобных атак.

Почему выбирают именно нас?

- *Профессионализм. Мы работаем только с собственным программным продуктом;*
- *Качество. Наш опыт позволяет нам эксплуатировать разные уязвимости на атакуемых серверах, что делает атаки в нашем исполнении максимально эффективными;*
- *Мощь. Наш ресурс и умения находить слабости, позволяют работать с "тяжелыми проектами";*
- *Анонимность. Вы можете быть полностью уверены, что данные о вашем заказе не попадут к третьим лицам;*
- *Манибэк. Делаем возврат денег по первому требованию;*
- *Скидки. Постоянным клиентам предоставляются договорные скидки;*

Доверяйте профессионалам!

DDoS атака

Сутки	*50$**
Неделя	*300$**
Месяц	*1000$**

Взлом сайта **Анализ сайта**

*500$**

* - указана средняя цена, для каждого сайта/сервера оценивается индивидуально

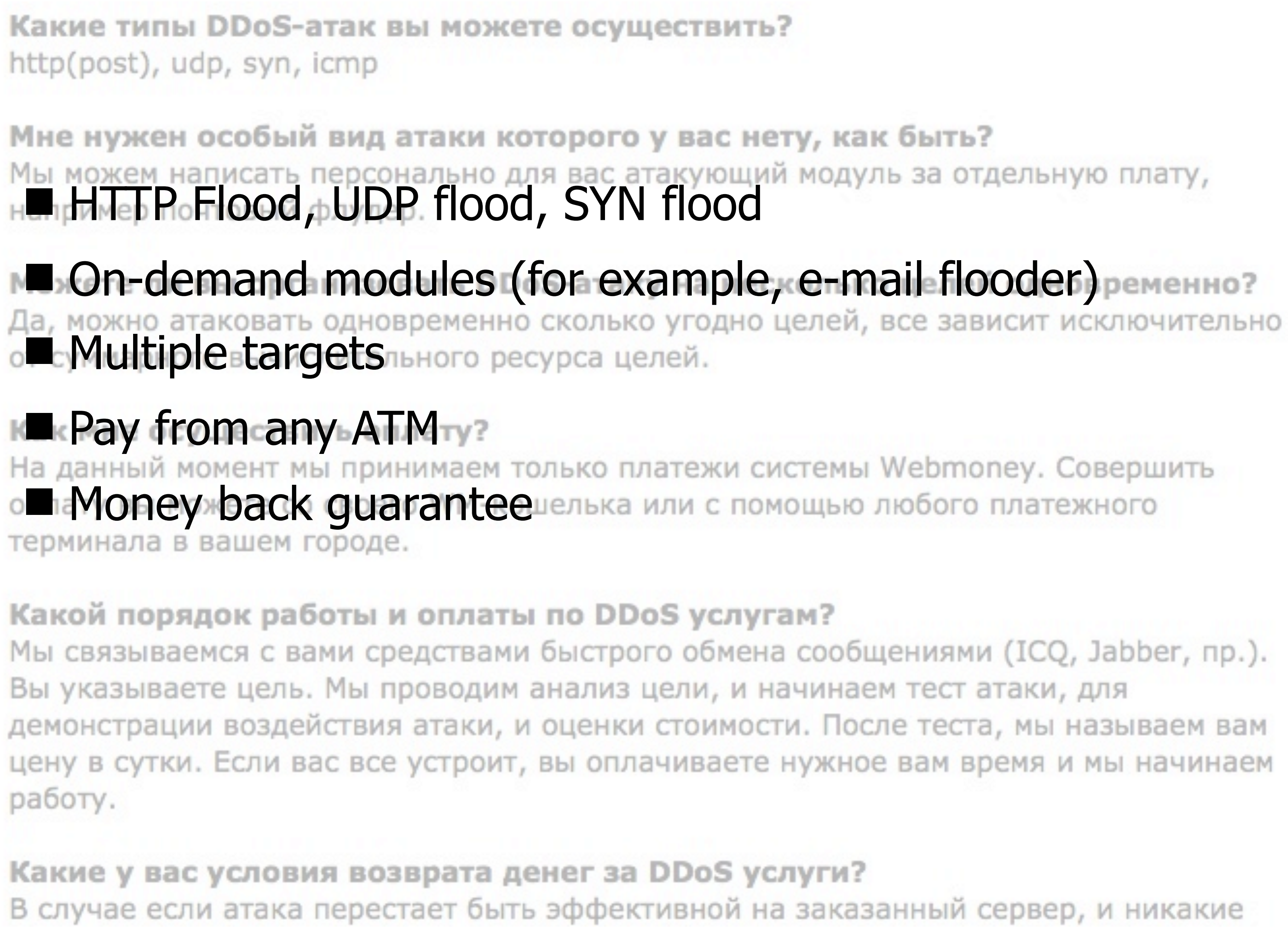
Защита от DDoS

Разовая установка и настройка	*150$*
Дополнительная разовая поддержка	*25$*

Заказать

Marketing

- HTTP Flood, UDP flood, SYN flood
- On-demand modules (for example, e-mail flooder)
- Multiple targets
- Pay from any ATM
- Money back guarantee



Какие типы DDoS-атак вы можете осуществить?
http(post), udp, syn, icmp

Мне нужен особый вид атаки которого у вас нету, как быть?
Мы можем написать персонально для вас атакующий модуль за отдельную плату, например почтовый флудер.

М[illegible]временно?
Да, можно атаковать одновременно сколько угодно целей, все зависит исключительно о[illegible]ьного ресурса целей.

К[illegible]ту?
На данный момент мы принимаем только платежи системы Webmoney. Совершить о[illegible]шелька или с помощью любого платежного терминала в вашем городе.

Какой порядок работы и оплаты по DDoS услугам?
Мы связываемся с вами средствами быстрого обмена сообщениями (ICQ, Jabber, пр.). Вы указываете цель. Мы проводим анализ цели, и начинаем тест атаки, для демонстрации воздействия атаки, и оценки стоимости. После теста, мы называем вам цену в сутки. Если вас все устроит, вы оплачиваете нужное вам время и мы начинаем работу.

Какие у вас условия возврата денег за DDoS услуги?
В случае если атака перестает быть эффективной на заказанный сервер, и никакие

Application Layer DoS attacks

- Slow HTTP headers attack (a.k.a. Slowloris)
- Slow HTTP message body attack (a.k.a Slow Post)
- Slow read HTTP attack (a.k.a. TCP Persist Timer exploit)

Demo time

What is common?

- All mentioned attacks aim at draining the pool of concurrent connections (usually relatively small)

HyperText Transfer Protocol (HTTP) Message syntax

Per RFC 2616

```
generic-message = start-line
  *(message-header CRLF)
  CRLF
  [ message-body ]
start-line = Request-Line |  Status-Line
```

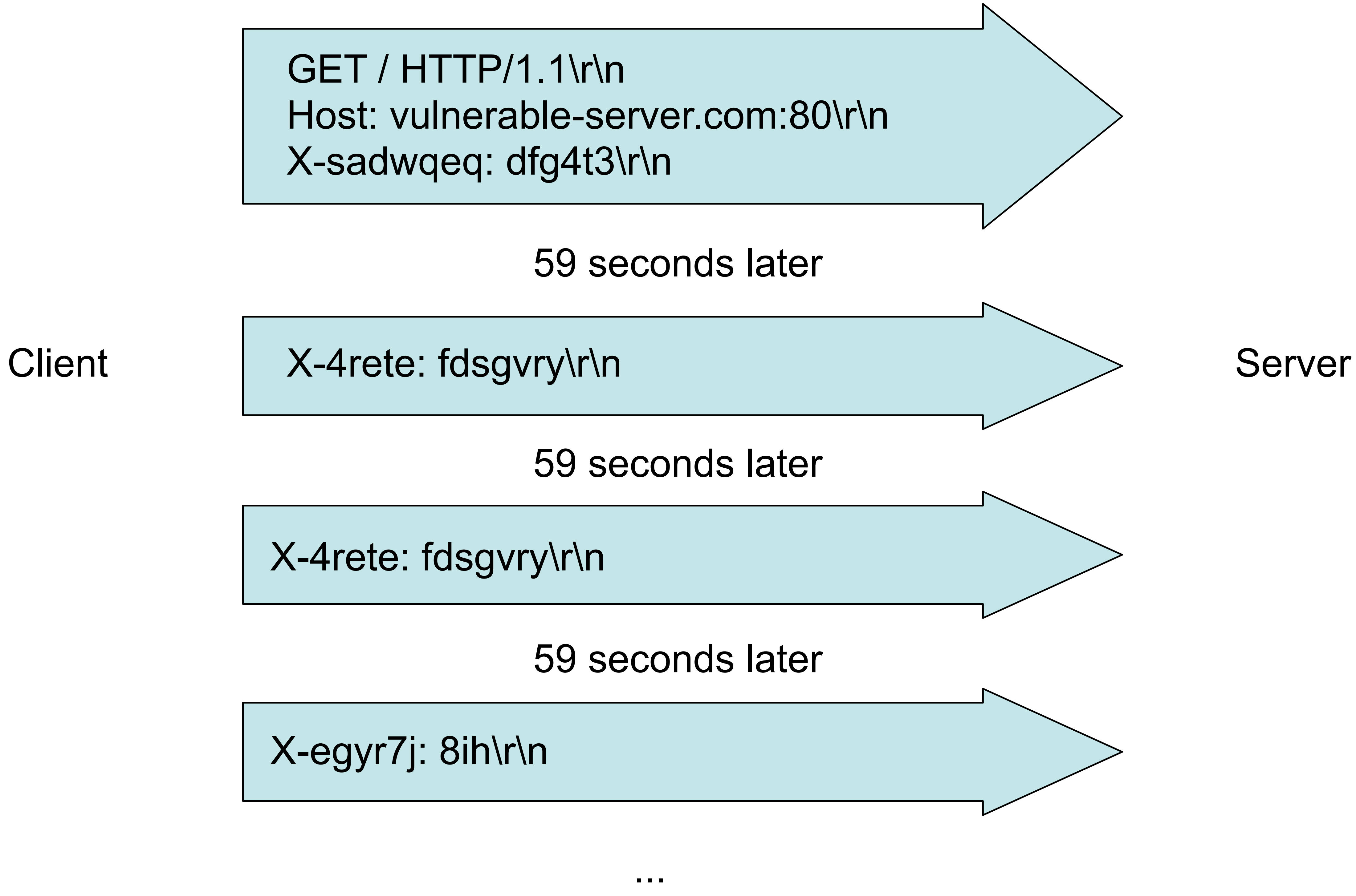
HyperText Transfer Protocol (HTTP) Message example

```
GET /page.htm HTTP/1.1CRLF
Host: www.example.com:8080CRLF
Content-Length: 25CRLF
CRLF
Optional Message Body
```

Slowloris

- Low bandwidth attack that sends HTTP requests with incomplete headers. Continues to send headers at regular intervals to keep the sockets active
- First mentioned by Adrian Ilarion Ciobanu in 2007 and implemeted by Robert Hansen in 2009

How slowloris works



Client

```
GET / HTTP/1.1\r\n
Host: vulnerable-server.com:80\r\n
X-sadwqeq: dfg4t3\r\n
```

59 seconds later

```
X-4rete: fdsgvry\r\n
```

59 seconds later

```
X-4rete: fdsgvry\r\n
```

59 seconds later

```
X-egyr7j: 8ih\r\n
```

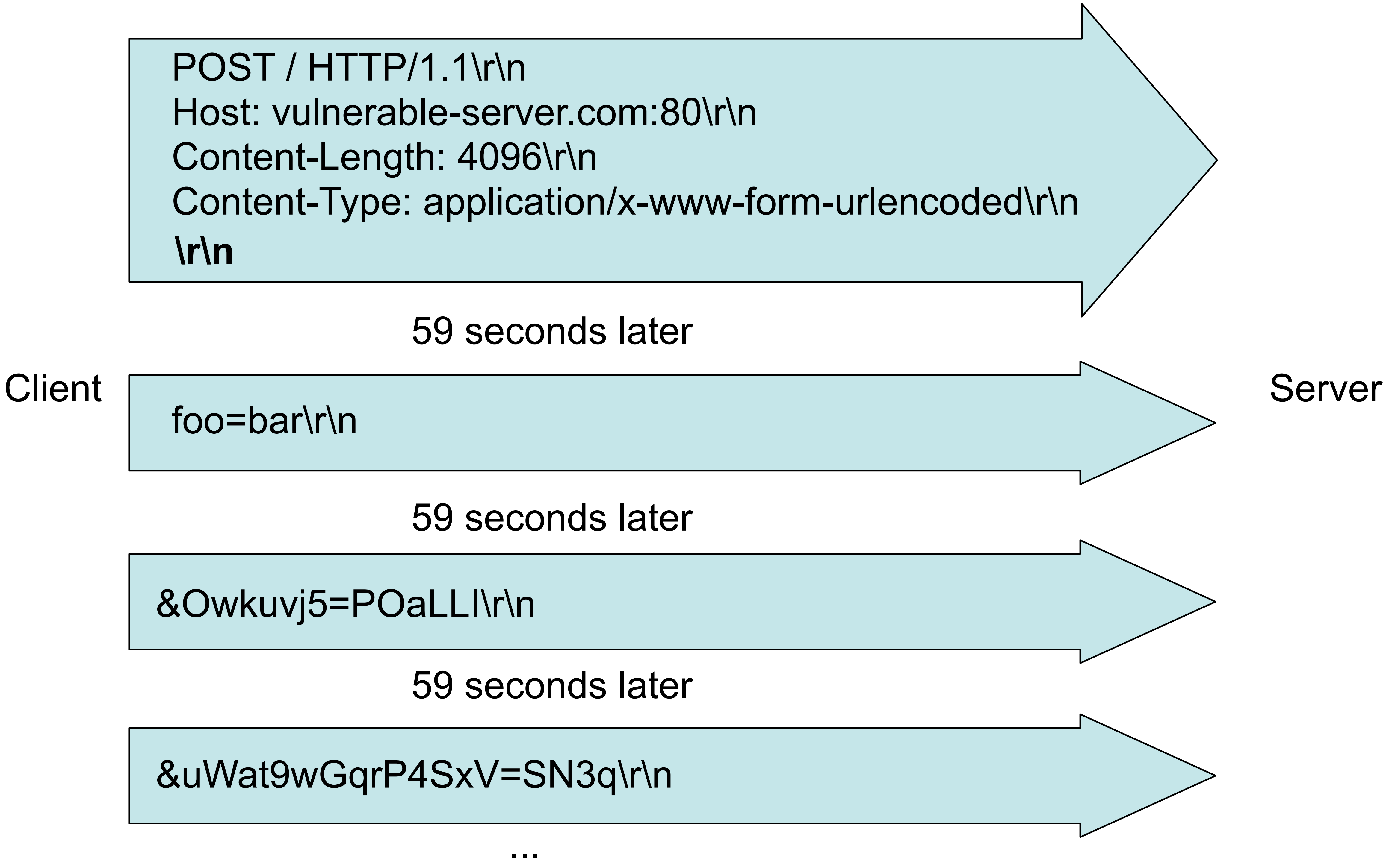
...

Server

Slow POST

- Attack that sends HTTP requests with complete headers but incomplete message body. Continues to send data at regular intervals to keep the sockets active
- Discovered by Wong Onn Chee and popularized by Tom Brennan in 2009

How Slow POST works



Client

```
POST / HTTP/1.1\r\n
Host: vulnerable-server.com:80\r\n
Content-Length: 4096\r\n
Content-Type: application/x-www-form-urlencoded\r\n
\r\n
```

59 seconds later

```
foo=bar\r\n
```

59 seconds later

```
&Owkuvj5=POaLLI\r\n
```

59 seconds later

```
&uWat9wGqrP4SxV=SN3q\r\n
```

...

Server

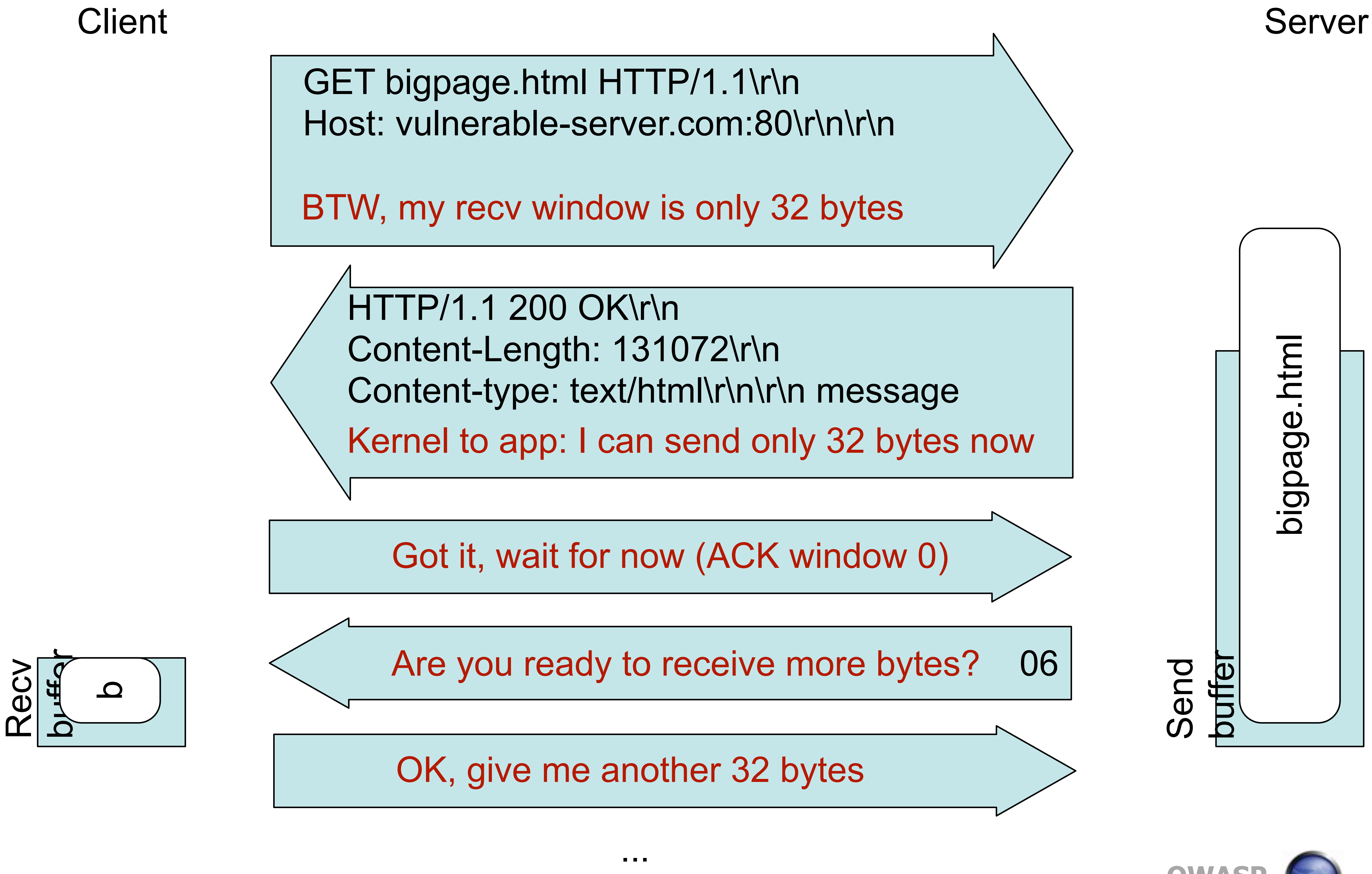
Slow Read

- Attack that keeps server sockets busy by maliciously throttling down the receipt of large HTTP responses
- Uses known Network Layer flaws to aim Application Layer
- First mentioned by Outpost24 in sockstress. Implemented as part of nkiller2 by Fotis Hantzis, a.k.a. ithilgore in 2009

Related TCP details

- "Window size (16 bits) – the size of the receive window, which specifies the number of bytes (beyond the sequence number in the acknowledgment field) that the sender of this segment is currently willing to receive" – Wikipedia

How Slow Read works



GET bigpage.html HTTP/1.1\r\n
Host: vulnerable-server.com:80\r\n\r\n

BTW, my recv window is only 32 bytes

HTTP/1.1 200 OK\r\n
Content-Length: 131072\r\n
Content-type: text/html\r\n\r\n message

Kernel to app: I can send only 32 bytes now

Got it, wait for now (ACK window 0)

Are you ready to receive more bytes? 06

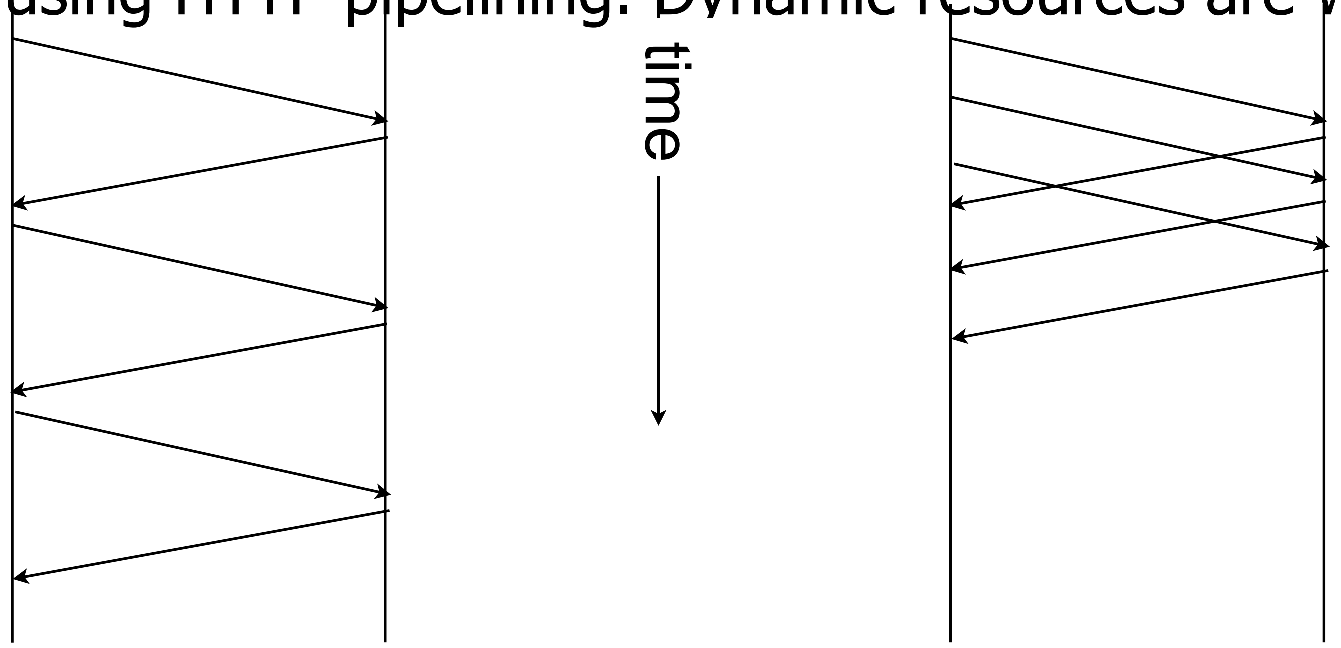
OK, give me another 32 bytes

...

Prerequisites for successful Slow Read attack

The larger server response is - increasing the chances of prolonging the connection

- make server generate a data stream that doesn't fully fit into socket's send buffer (65536 bytes is default on most Linux systems /proc/sys/net/ipv4/tcp_wmem, if server doesn't set its own value)
- Request large resource by naturally finding it and/or amplifying the response size by using HTTP pipelining. Dynamic resources are welcome.



Why is Slow Read is different? Traditional (slowloris/slowpost) DoS

- Customer stuck deciding what he wants
- Makes an order
- Pays
- Takes the order
- Next!

It is possible to identify and isolate slow client in his request state

Why Slow Read is different?
Slow Read DoS

it is quite late to do anything, as the request was already accepted and processed

- Makes an order for party of 50
- Pays
- Cannot take the entire order with him, makes several trips to the car.
- Next!

Why is Slow Read is different?

- Customer stuck deciding what he wants
- Makes an order
- Pays
- Takes the order
- Next!

- Makes an order for party of 50
- Pays
- Cannot take the entire order with him, makes several trips to the car
- Next!

Why is Slow Read is different? (continued)

- Defense mechanisms expect the crushing fist of malice to appear in the request

- Instead, the entire transaction should be monitored

Am I vulnerable?

- There is a good chance that you are. Default configurations of nginx, lighttpd, IIS, Apache, Varnish cache proxy, Shoutcast streaming server - are vulnerable to at least one of the mentioned attacks

What should I do?

- Use available tools to simulate attacks. SlowHTTPTest covers all mentioned attacks and some more at http://slowhttptest.googlecode.com
- Check out http://slowhammer.me soon to get access to your own whitehat botnet in the cloud
- Use Qualys WAF or other firewalls that are supposed to protect, but test before you pay!

Detection and Mitigation

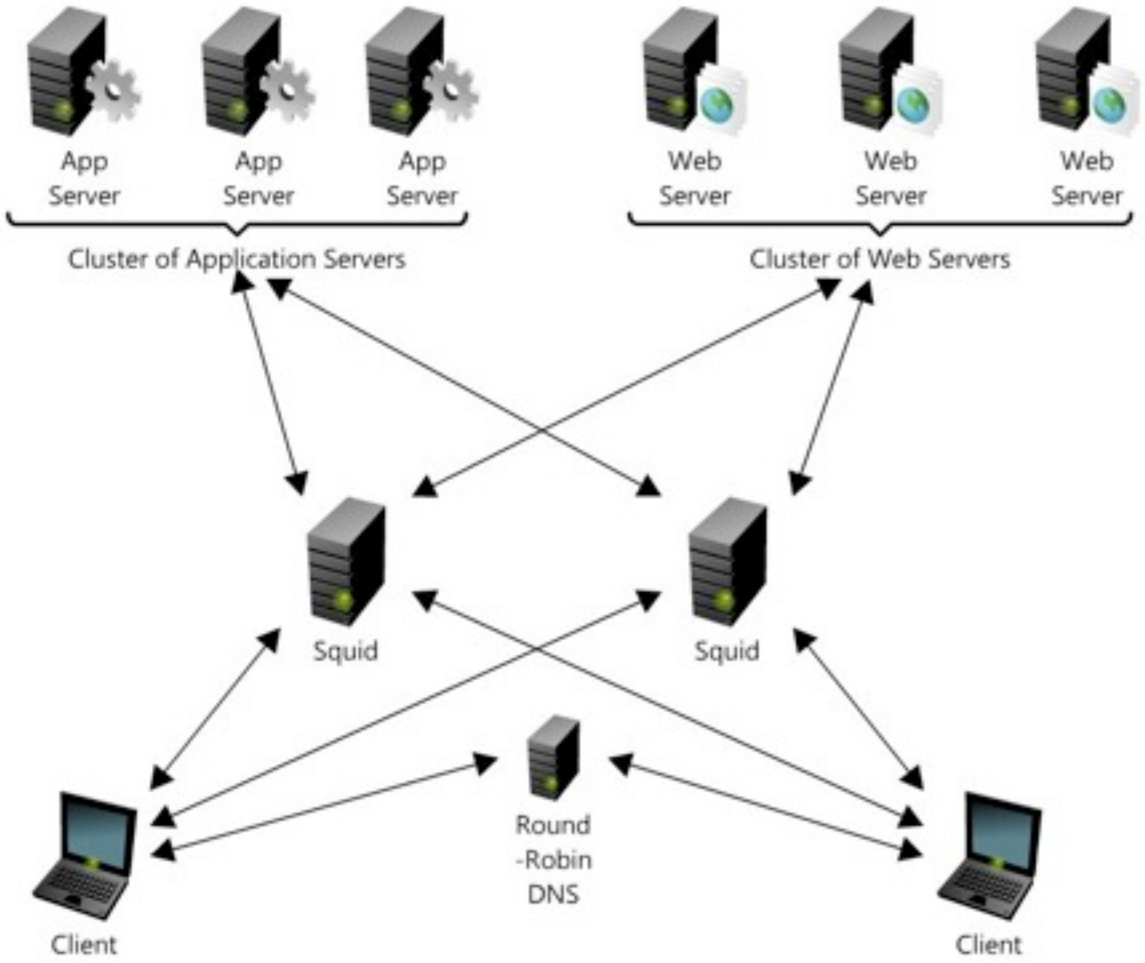
- Drop connections with abnormally small TCP advertised window(s)
- Set an absolute connection timeout, if possible
- Limit length, number of headers to accept
- Limit max size of message body to accept
- Drop connections with HTTP methods (verbs) not supported by the URL
- Limit accepted header and message body to a minimal reasonable length
- Define the minimum data rate, and drop connections that are slower than that rate

Detection and Mitigation continued

- Qualys Web Application Scanner passively detects the slow attack vulnerabilities
- ModSecurity v2.6 introduced a directive called SecWriteStateLimit that places a time limit on the concurrent number of threads (per IP address)
- Snort is working on detecting connections with small TCP advertised window(s)
- Christian Folini introduced Flying Frog script at https://www.netnea.com

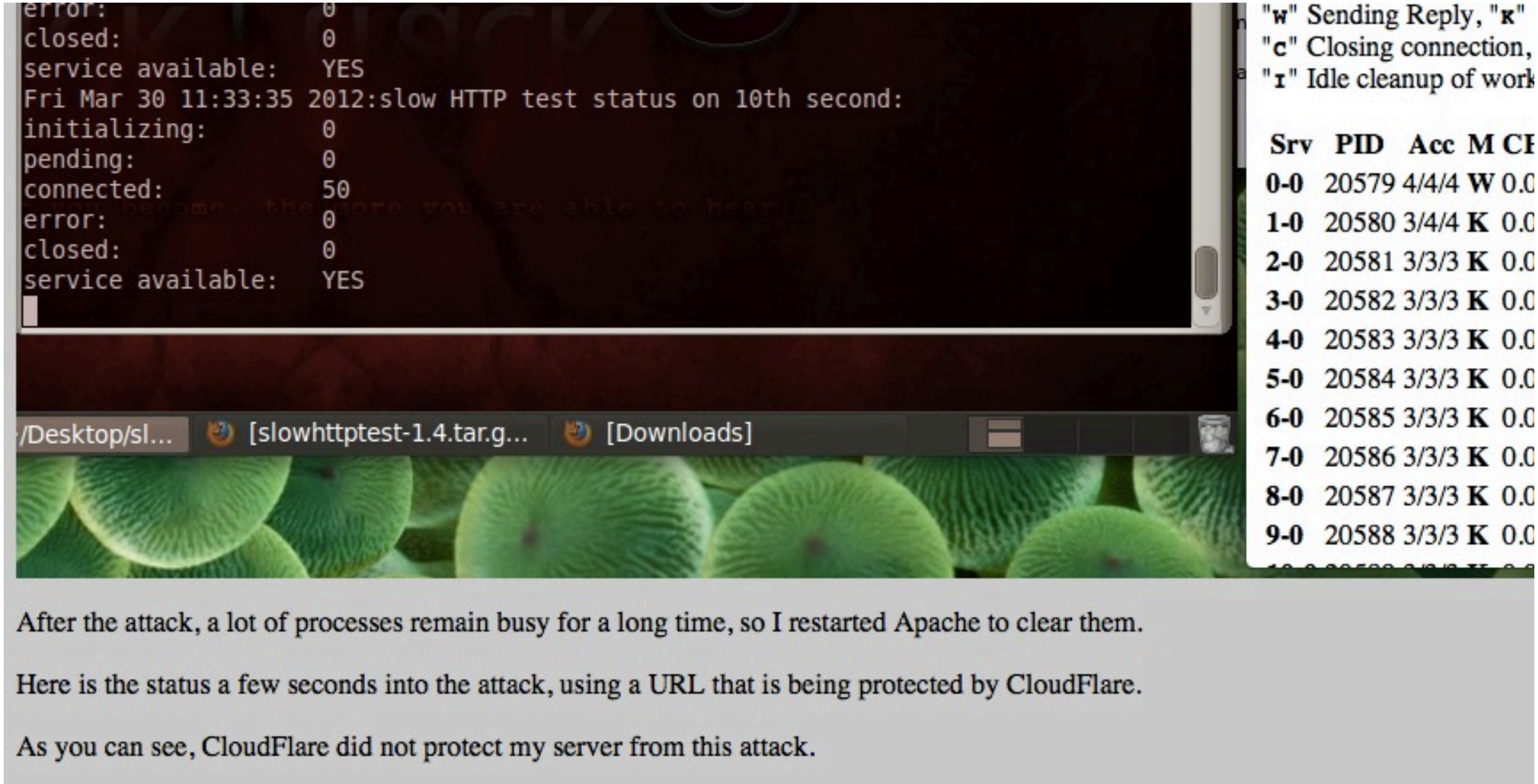
Example of misconfiguration

- Even if the server is configured to handle tens of thousands of concurrent connections, the OS might still create a bottleneck by limiting the server by the number of open file descriptors



Are anti-DoS solutions going to help?

- Have no idea, test yourself!



```
error:               0
closed:              0
service available:   YES
Fri Mar 30 11:33:35 2012:slow HTTP test status on 10th second:
initializing:        0
pending:             0
connected:           50
error:               0
closed:              0
service available:   YES
```

"W" Sending Reply, "K"
"C" Closing connection,
"I" Idle cleanup of work

Srv	PID	Acc	M	CF
0-0	20579	4/4/4	W	0.0
1-0	20580	3/4/4	K	0.0
2-0	20581	3/3/3	K	0.0
3-0	20582	3/3/3	K	0.0
4-0	20583	3/3/3	K	0.0
5-0	20584	3/3/3	K	0.0
6-0	20585	3/3/3	K	0.0
7-0	20586	3/3/3	K	0.0
8-0	20587	3/3/3	K	0.0
9-0	20588	3/3/3	K	0.0

After the attack, a lot of processes remain busy for a long time, so I restarted Apache to clear them.

Here is the status a few seconds into the attack, using a URL that is being protected by CloudFlare.

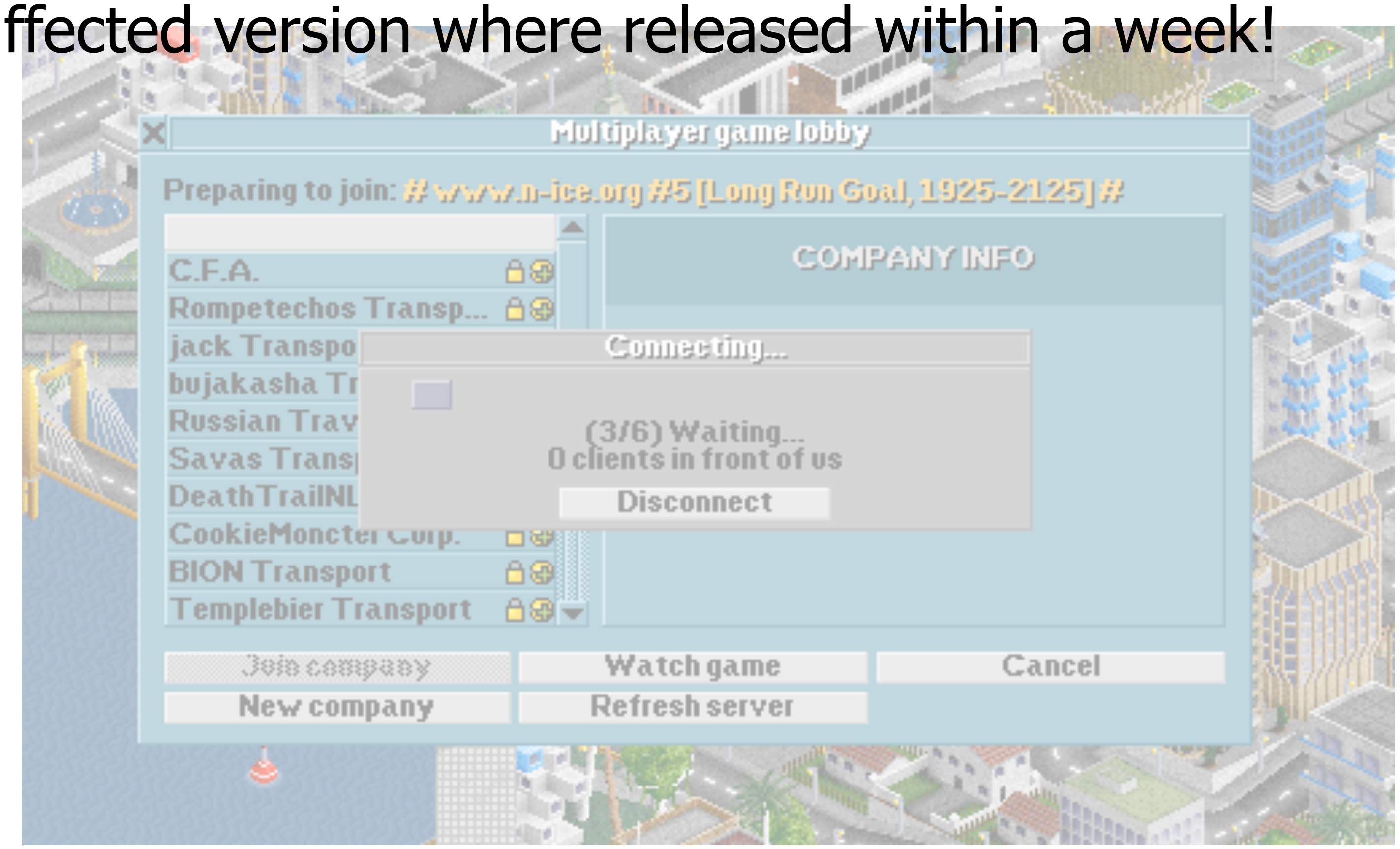
As you can see, CloudFlare did not protect my server from this attack.

Who reacted first?

Those who really care - gamers!

Open Transport Tycoon Deluxe found that by using a slow read type attack, it is possible to prevent anyone from joining a game server with virtually no resources.

Patches for all affected version where released within a week!



Multiplayer game lobby

Preparing to join: # www.n-ice.org #5 [Long Run Goal, 1925-2125] #

C.F.A.
Rompetechos Transp...
jack Transpo
bujakasha Tr
Russian Trav
Savas Trans
DeathTrailNL
CookieMoncter Corp.
BION Transport
Templebier Transport

Connecting...

(3/6) Waiting...
0 clients in front of us

Summary

- Even though the simpliest distributed DoS attacks are enough to knock down most web sites today, the nature of the attack will be sure to improve, and it’s better to be ready or, at least be aware of upcoming problems.

References

ModSecurity Advanced Topic of the Week: Mitigation of 'Slow Read" Denial of Service Attack

http://blog.spiderlabs.com/2012/01/modsecurity-advanced-topic-of-the-week-mitigation-of-slow-read-denial-of-service-attack.html

DDoS attacks in H2 2011

http://www.securelist.com/en/analysis/204792221/DDoS_attacks_in_H2_2011

The State of the Internet

http://www.akamai.com/stateoftheinternet/

Evaluation of slowhttptest against servers protected by CloudFlare

http://samsclass.info/123/proj10/slow-read.html

Blog posts on hardening web servers

https://community.qualys.com/blogs/securitylabs/

Thank you!

- sshekyan@qualys.com
- @sshekyan