# Lecture 22:
# Denial of Service

https://cs161.org

# Announcements

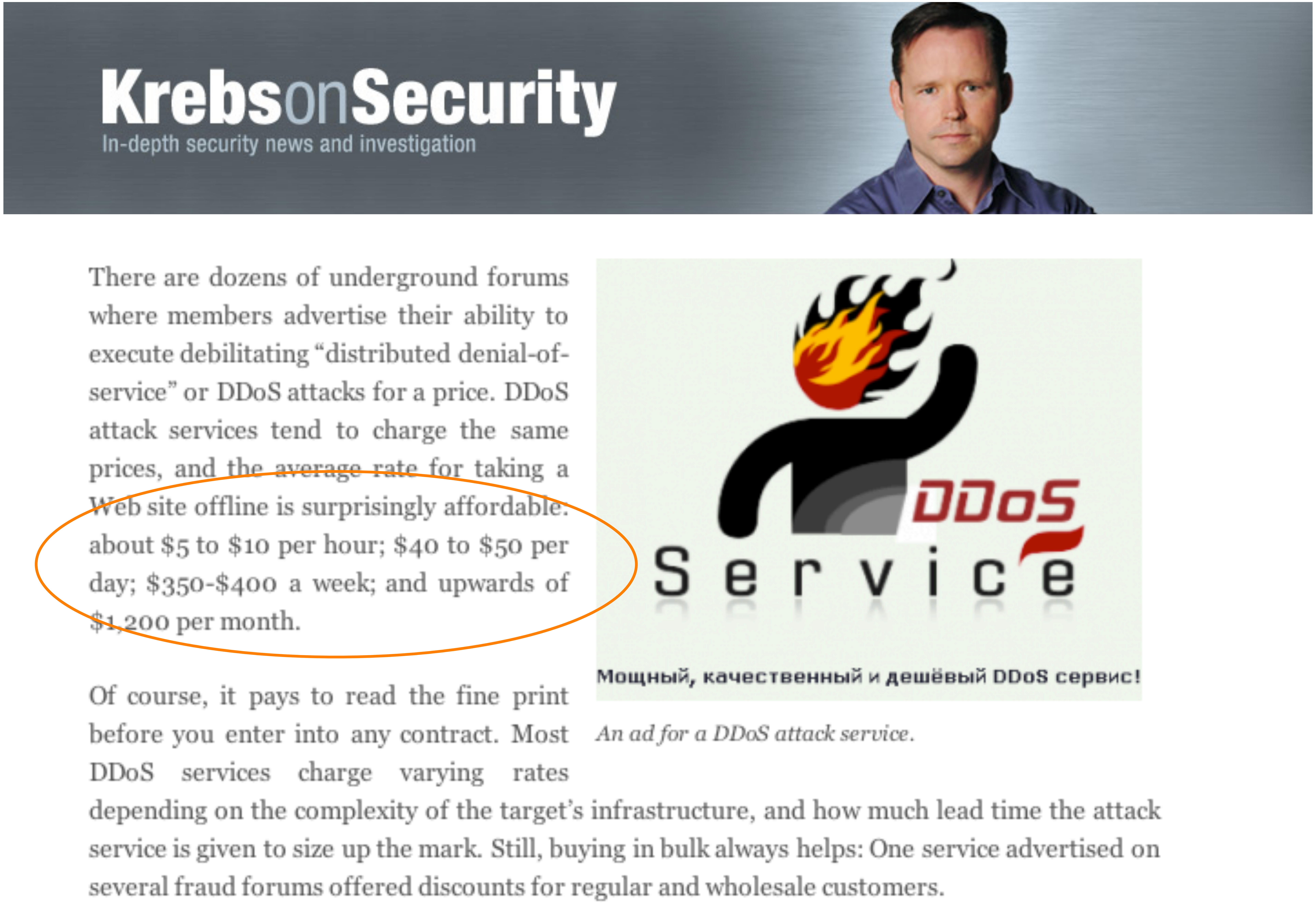
- I welcome your questions and feedback during lecture in Zoom's text chat

# Attacks on Availability

- Denial-of-Service (DoS): preventing legitimate users from using a computing service
- Distributed Denial-of-Service (DDoS) occurs when a server is flooded with traffic from many different devices

# Motivations for DoS

- Showing off / entertainment / ego
- Competitive advantage
  - Maybe commercial, maybe just to win
- Vendetta / denial-of-money
- Extortion
- Political statements
- Impair defenses
- Espionage
- Warfare



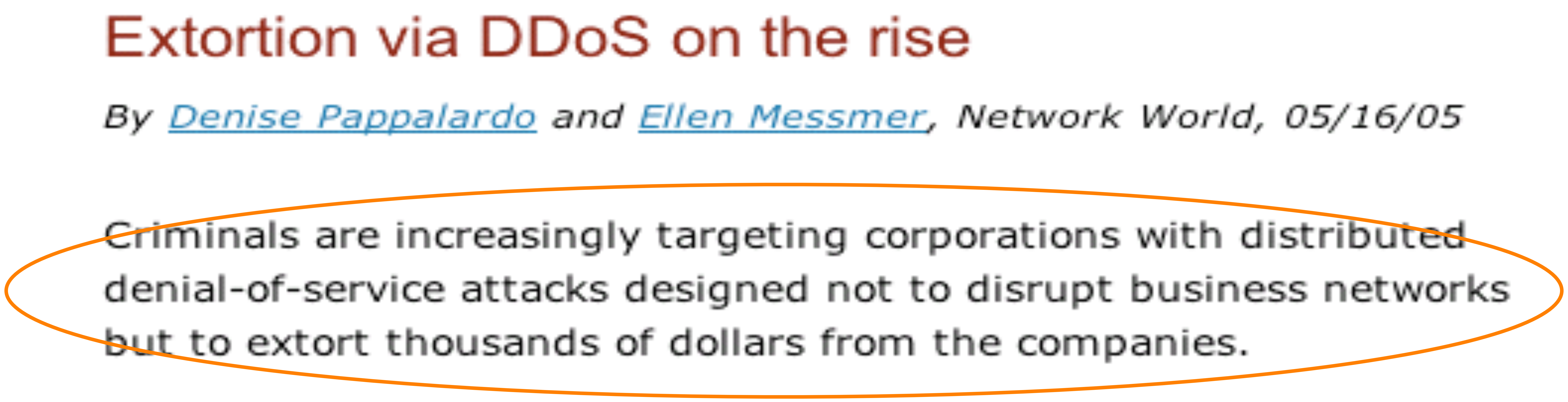
KrebsonSecurity

In-depth security news and investigation

There are dozens of underground forums where members advertise their ability to execute debilitating "distributed denial-of-service" or DDoS attacks for a price. DDoS attack services tend to charge the same prices, and the average rate for taking a Web site offline is surprisingly affordable: about $5 to $10 per hour; $40 to $50 per day; $350-$400 a week; and upwards of $1,200 per month.

*An ad for a DDoS attack service.*

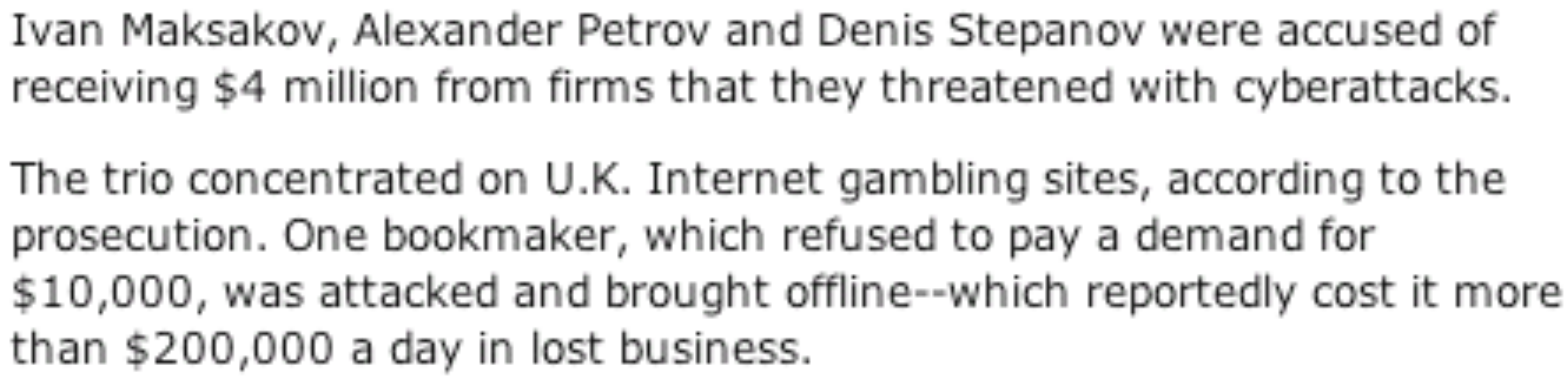
Of course, it pays to read the fine print before you enter into any contract. Most DDoS services charge varying rates depending on the complexity of the target's infrastructure, and how much lead time the attack service is given to size up the mark. Still, buying in bulk always helps: One service advertised on several fraud forums offered discounts for regular and wholesale customers.



# Extortion via DDoS on the rise

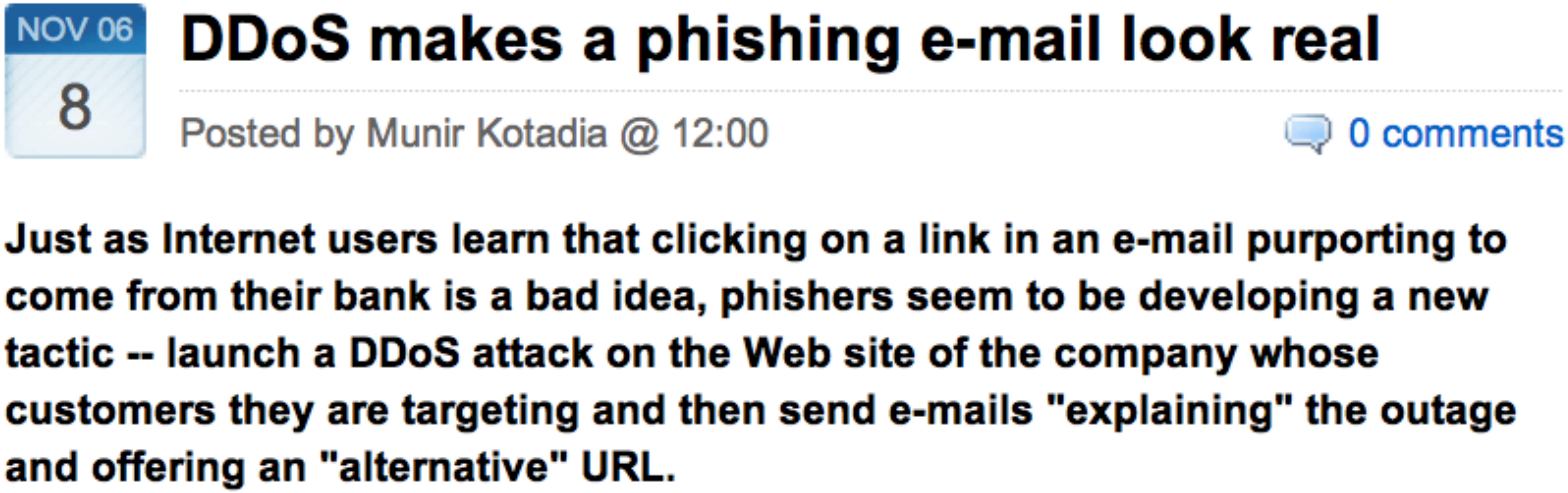
*By Denise Pappalardo and Ellen Messmer, Network World, 05/16/05*

Criminals are increasingly targeting corporations with distributed denial-of-service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies.



Ivan Maksakov, Alexander Petrov and Denis Stepanov were accused of receiving $4 million from firms that they threatened with cyberattacks.

The trio concentrated on U.K. Internet gambling sites, according to the prosecution. One bookmaker, which refused to pay a demand for $10,000, was attacked and brought offline--which reportedly cost it more than $200,000 a day in lost business.



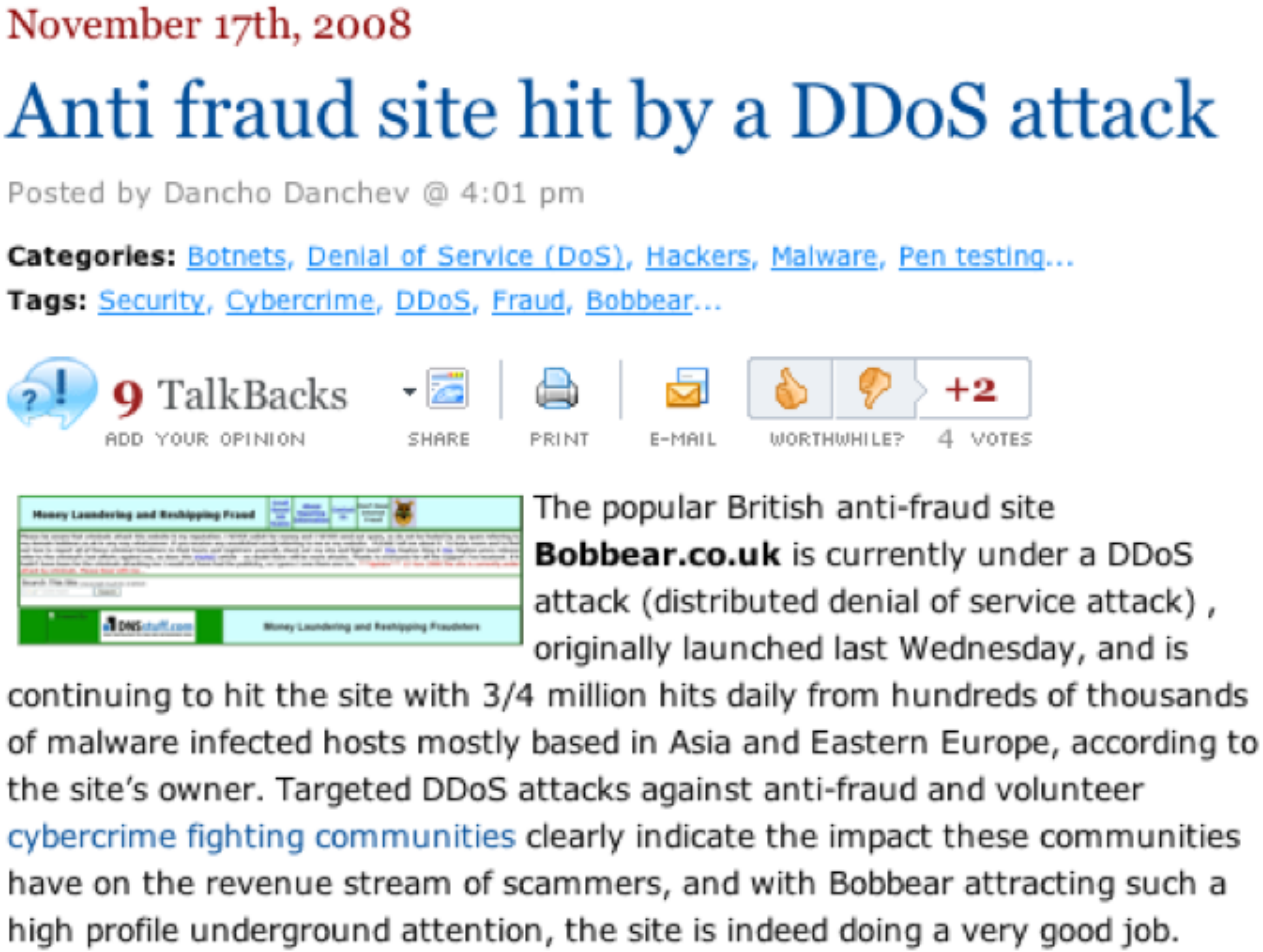
NOV 06
8

## DDoS makes a phishing e-mail look real

Posted by Munir Kotadia @ 12:00

0 comments

**Just as Internet users learn that clicking on a link in an e-mail purporting to come from their bank is a bad idea, phishers seem to be developing a new tactic -- launch a DDoS attack on the Web site of the company whose customers they are targeting and then send e-mails "explaining" the outage and offering an "alternative" URL.**



November 17th, 2008

# Anti fraud site hit by a DDoS attack

Posted by Dancho Danchev @ 4:01 pm

**Categories:** Botnets, Denial of Service (DoS), Hackers, Malware, Pen testing...

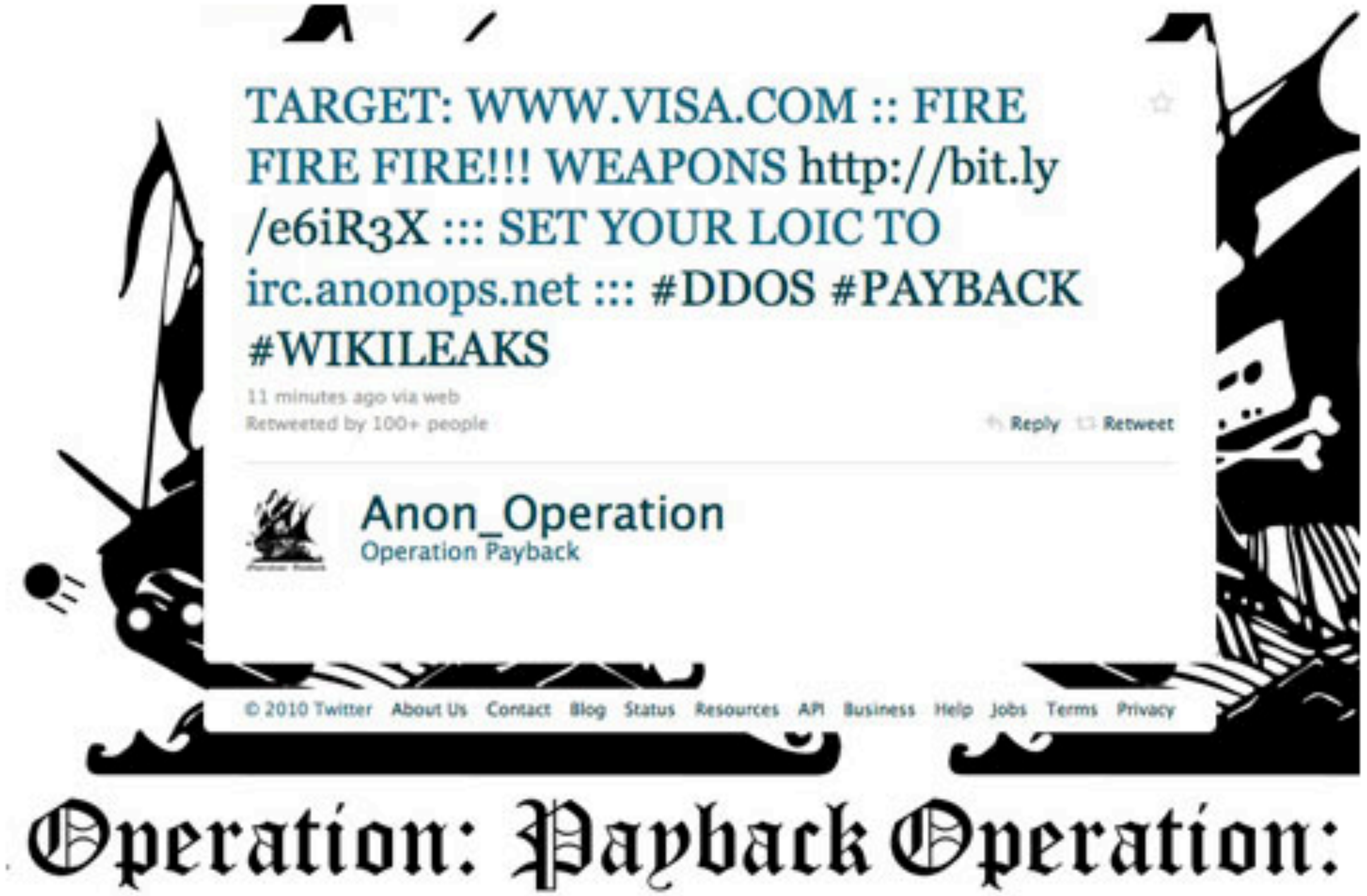
**Tags:** Security, Cybercrime, DDoS, Fraud, Bobbear...

The popular British anti-fraud site **Bobbear.co.uk** is currently under a DDoS attack (distributed denial of service attack) , originally launched last Wednesday, and is continuing to hit the site with 3/4 million hits daily from hundreds of thousands of malware infected hosts mostly based in Asia and Eastern Europe, according to the site's owner. Targeted DDoS attacks against anti-fraud and volunteer cybercrime fighting communities clearly indicate the impact these communities have on the revenue stream of scammers, and with Bobbear attracting such a high profile underground attention, the site is indeed doing a very good job.

December 8, 2010, 4:18 PM

# ‘Operation Payback’ Attacks Fell Visa.com

By ROBERT MACKEY



TARGET: WWW.VISA.COM :: FIRE FIRE FIRE!!! WEAPONS http://bit.ly/e6iR3X ::: SET YOUR LOIC TO irc.anonops.net ::: #DDOS #PAYBACK #WIKILEAKS

11 minutes ago via web
Retweeted by 100+ people

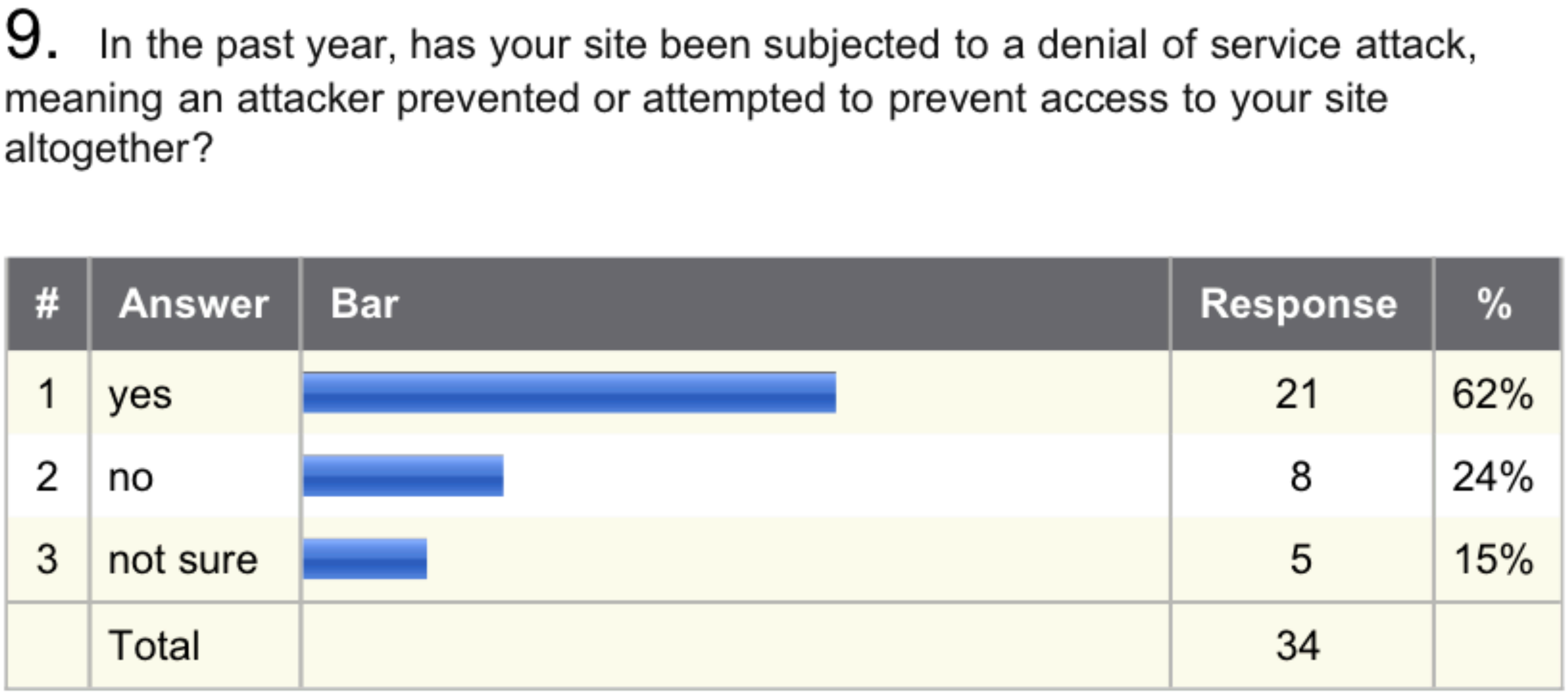
Anon_Operation
Operation Payback

Reply
Retweet
© 2010 Twitter About Us Contact Blog Status Resources API Business Help Jobs Terms Privacy
Operation: Payback Operation:

A message posted on Twitter by a group of Internet activists announcing the start of an attack on Visa’s Web site, in retaliation for the company’s actions against WikiLeaks.

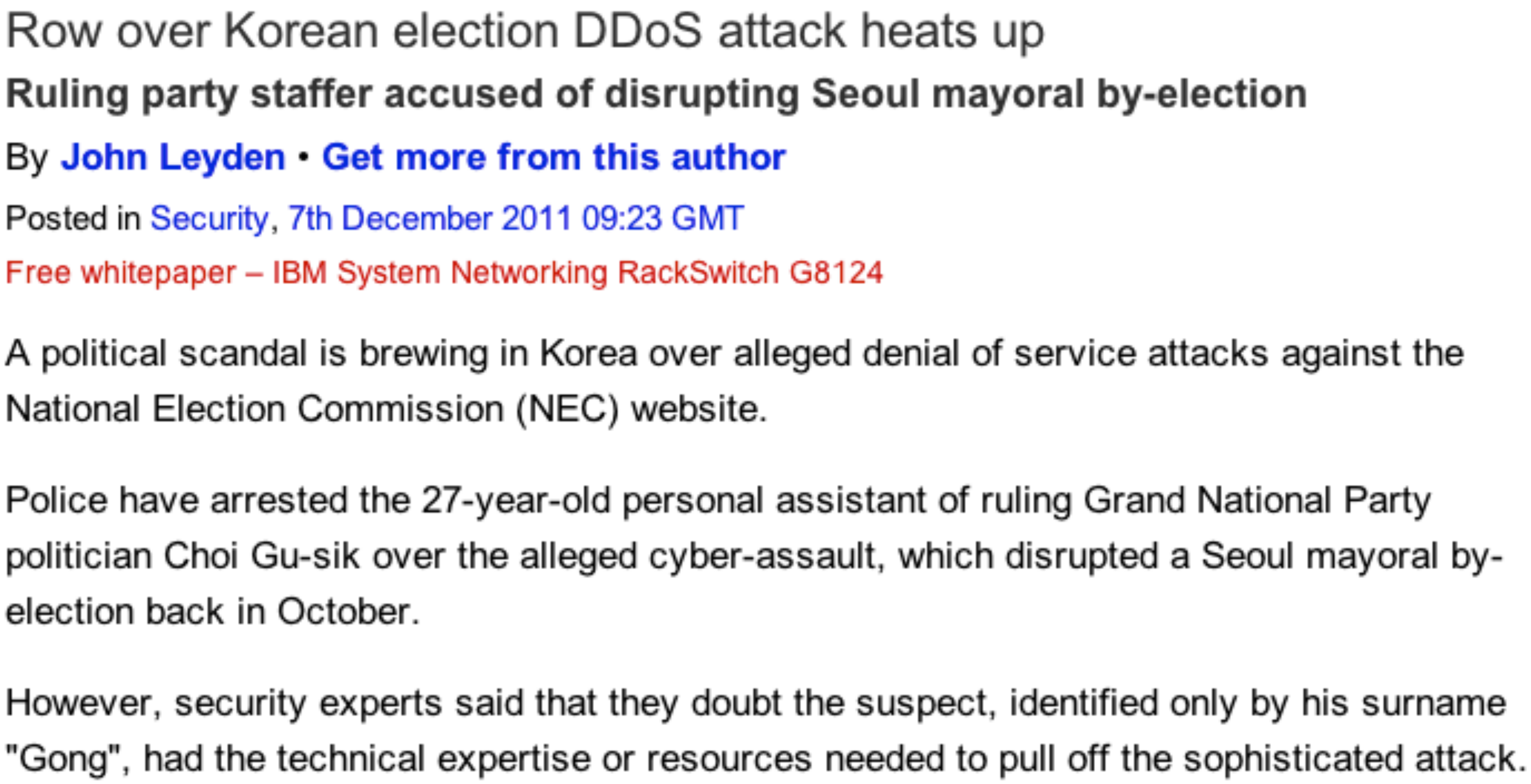
**Last Updated | 6:54 p.m.** A group of Internet activists took credit for crashing the Visa.com Web site on Wednesday afternoon, hours after they launched [a similar attack on MasterCard](). The cyber attacks, by activists who call themselves Anonymous, are aimed at punishing companies that have acted to stop the flow of donations to WikiLeaks in recent days.

The group explained that its [distributed denial of service attacks]() — in which they essentially flood Web sites site with traffic to slow them down or knock them offline — were part of a broader effort called Operation Payback, which



9. In the past year, has your site been subjected to a denial of service attack, meaning an attacker prevented or attempted to prevent access to your site altogether?

| # | Answer | Bar | Response | % |
|---|---|---|---|---|
| 1 | yes | | 21 | 62% |
| 2 | no | | 8 | 24% |
| 3 | not sure | | 5 | 15% |
| | Total | | 34 | |



# Row over Korean election DDoS attack heats up

## Ruling party staffer accused of disrupting Seoul mayoral by-election

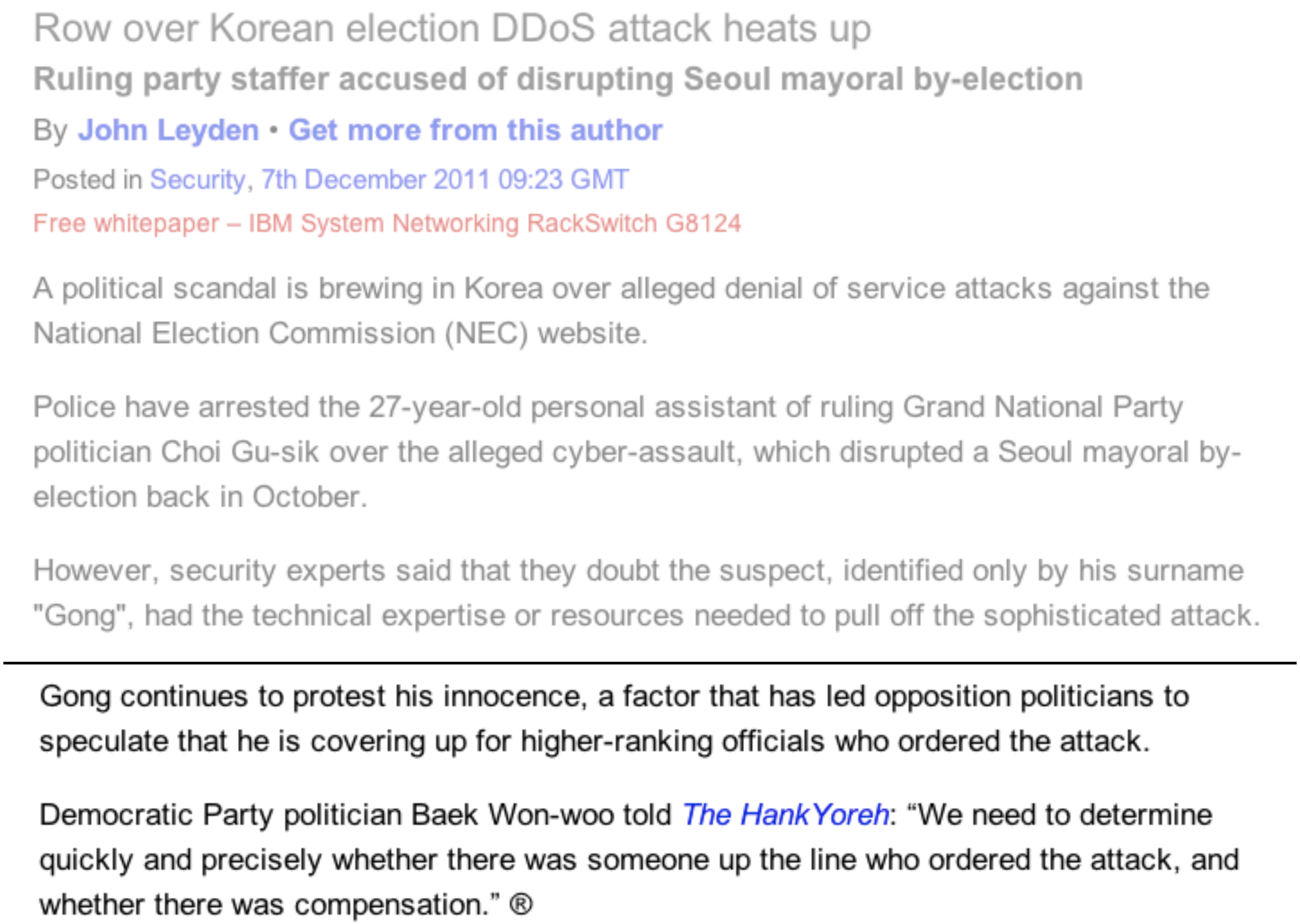
By **John Leyden** • **Get more from this author**

Posted in Security, 7th December 2011 09:23 GMT

A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.



# Row over Korean election DDoS attack heats up

**Ruling party staffer accused of disrupting Seoul mayoral by-election**

By **John Leyden** • **Get more from this author**

Posted in Security, 7th December 2011 09:23 GMT

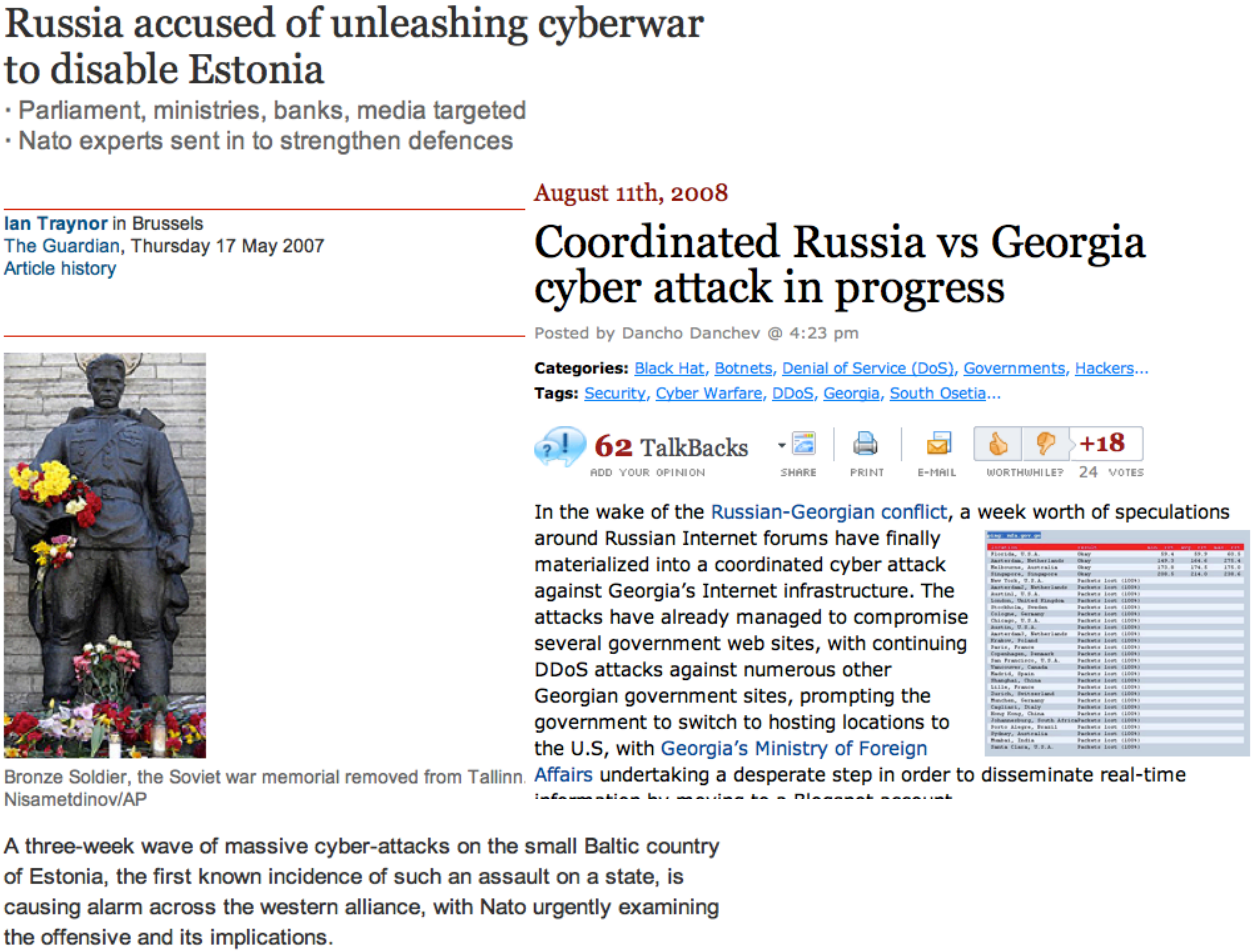
A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.

Gong continues to protest his innocence, a factor that has led opposition politicians to speculate that he is covering up for higher-ranking officials who ordered the attack.

Democratic Party politician Baek Won-woo told *The HankYoreh*: “We need to determine quickly and precisely whether there was someone up the line who ordered the attack, and whether there was compensation.” ®



# Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

Ian Traynor in Brussels
The Guardian, Thursday 17 May 2007
Article history

Bronze Soldier, the Soviet war memorial removed from Tallinn. Nisametdinov/AP

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

August 11th, 2008

# Coordinated Russia vs Georgia cyber attack in progress

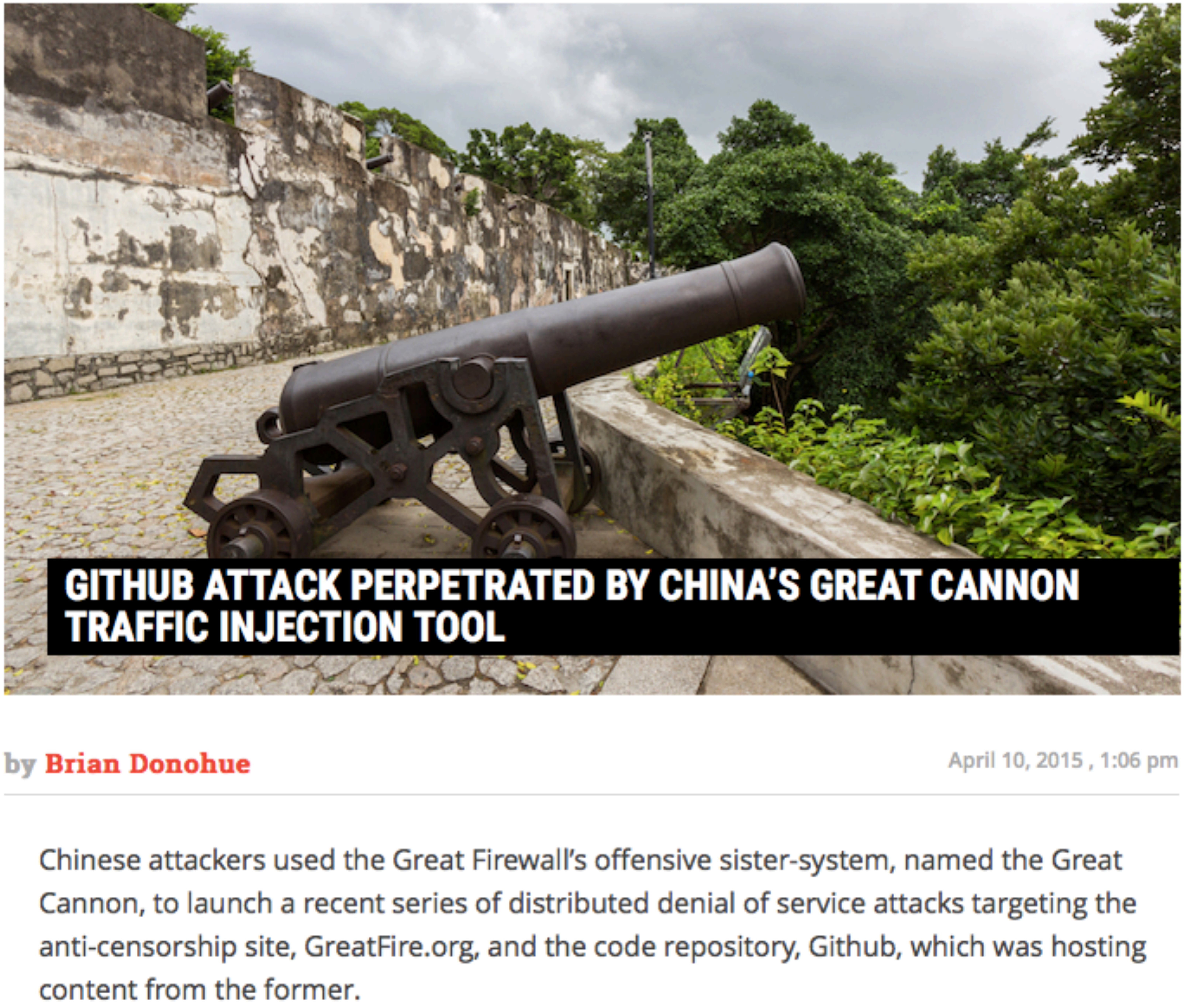
Posted by Dancho Danchev @ 4:23 pm

**Categories:** Black Hat, Botnets, Denial of Service (DoS), Governments, Hackers...
**Tags:** Security, Cyber Warfare, DDoS, Georgia, South Osetia...

In the wake of the Russian-Georgian conflict, a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with Georgia's Ministry of Foreign Affairs undertaking a desperate step in order to disseminate real-time information by moving to a Blogspot account

ping: mfa.gov.ge

| location | result | min. rtt | avg. rtt | max. rtt |
|---|---|---|---|---|
| Florida, U.S.A. | Okay | 59.4 | 59.9 | 60.5 |
| Amsterdam, Netherlands | Okay | 149.3 | 164.6 | 275.4 |
| Melbourne, Australia | Okay | 173.8 | 174.5 | 175.0 |
| Singapore, Singapore | Okay | 200.5 | 214.0 | 238.6 |
| New York, U.S.A. | Packets lost (100%) | | | |
| Amsterdam2, Netherlands | Packets lost (100%) | | | |
| Austin1, U.S.A. | Packets lost (100%) | | | |
| London, United Kingdom | Packets lost (100%) | | | |
| Stockholm, Sweden | Packets lost (100%) | | | |
| Cologne, Germany | Packets lost (100%) | | | |
| Chicago, U.S.A. | Packets lost (100%) | | | |
| Austin, U.S.A. | Packets lost (100%) | | | |
| Amsterdam3, Netherlands | Packets lost (100%) | | | |
| Krakow, Poland | Packets lost (100%) | | | |
| Paris, France | Packets lost (100%) | | | |
| Copenhagen, Denmark | Packets lost (100%) | | | |
| San Francisco, U.S.A. | Packets lost (100%) | | | |
| Vancouver, Canada | Packets lost (100%) | | | |
| Madrid, Spain | Packets lost (100%) | | | |
| Shanghai, China | Packets lost (100%) | | | |
| Lille, France | Packets lost (100%) | | | |
| Zurich, Switzerland | Packets lost (100%) | | | |
| Munchen, Germany | Packets lost (100%) | | | |
| Cagliari, Italy | Packets lost (100%) | | | |
| Hong Kong, China | Packets lost (100%) | | | |
| Johannesburg, South Africa | Packets lost (100%) | | | |
| Porto Alegre, Brazil | Packets lost (100%) | | | |
| Sydney, Australia | Packets lost (100%) | | | |
| Mumbai, India | Packets lost (100%) | | | |
| Santa Clara, U.S.A. | Packets lost (100%) | | | |



# GITHUB ATTACK PERPETRATED BY CHINA'S GREAT CANNON TRAFFIC INJECTION TOOL

by **Brian Donohue**

April 10, 2015 , 1:06 pm

Chinese attackers used the Great Firewall's offensive sister-system, named the Great Cannon, to launch a recent series of distributed denial of service attacks targeting the anti-censorship site, GreatFire.org, and the code repository, Github, which was hosting content from the former.

# Attacks on Availability

- Deny service via a **program flaw** (“*NULL”)
  - E.g., supply an input that crashes a server
  - E.g., fool a system into shutting down

- Deny service via **resource exhaustion** (“while(1);”)
  - E.g., consume CPU, memory, disk, network

- Network-level DoS vs application-level DoS

# DoS & Operating Systems

- How could you DoS a multi-user Unix system on which you have a login?
    - Open lots of connections/ports
    - Start lots of processes
    - Take up a lot of CPU
    - Look for an input that causes something critical to crash
    - Create lots of /tmp files
    - rm -rf /* ??

# DoS & Operating Systems

- How could you DoS a multi-user Unix system on which you have a login?

  -
    ```
    char buf[1024];
    int f = open("/tmp/junk");
    while (1) write(f, buf,
    sizeof(buf));
    ```
    - Gobble up all the disk space!

  -
    ```
    while (1) fork();
    ```
    - Create a zillion processes!
  - Create zillions of files, keep opening, reading, writing, deleting
    - Thrash the disk

Defenses?

Isolate users / impose quotas

# Network-level DoS

- Can exhaust network resources by
  - Flooding with lots of packets (brute-force)
  - DDoS: flood with packets from many sources
  - Amplification: Abuse patsies who will amplify your traffic for you

# DoS & Networks

- How could you DoS a target's Internet access?
  - Send a zillion packets at them
  - Internet lacks isolation between traffic of different users!
- What resources does attacker need to pull this off?
  - At least as much sending capacity ("bandwidth") as the bottleneck link of the target's Internet connection
    - Attacker sends maximum-sized packets
  - Or: overwhelm the rate at which the bottleneck router can process packets
    - Attacker sends minimum-sized packets! (in order to maximize the packet arrival rate)

# Defending Against Network DoS

- Suppose an attacker has access to a beefy system with high-speed Internet access (a “big pipe”).
- They pump out packets towards the target at a very high rate.
- What might the target do to defend against the onslaught?
  - Install a network filter to discard any packets that arrive with attacker’s IP address as their source
    - E.g., `drop * 66.31.1.37:* -> *:*`
    - Or it can leverage any other pattern in the flooding traffic that’s not in benign traffic
  - Attacker’s IP address = means of identifying misbehaving user

# Filtering Sounds Pretty Easy …

- … but DoS filters can be easily evaded:
- Make traffic appear as though it's from many hosts
  - Spoof the source address so it can't be used to filter
    - Just pick a random 32-bit number of each packet sent
  - Defender can't filter this — best they can hope for is that operators around the world implement anti-spoofing mechanisms (today ≥ 75% do)
- Use many hosts to send traffic rather than just one
  - Distributed Denial-of-Service = DDoS
  - No longer possible to filter based on source IP address
  - Very cheap to acquire many hosts … :-(

# It’s Not A “Level Playing Field”

- When defending resources from exhaustion, need to beware of asymmetries, where attackers can consume victim resources with little comparable effort
  - Makes DoS easier to launch
  - Defense costs much more than attack

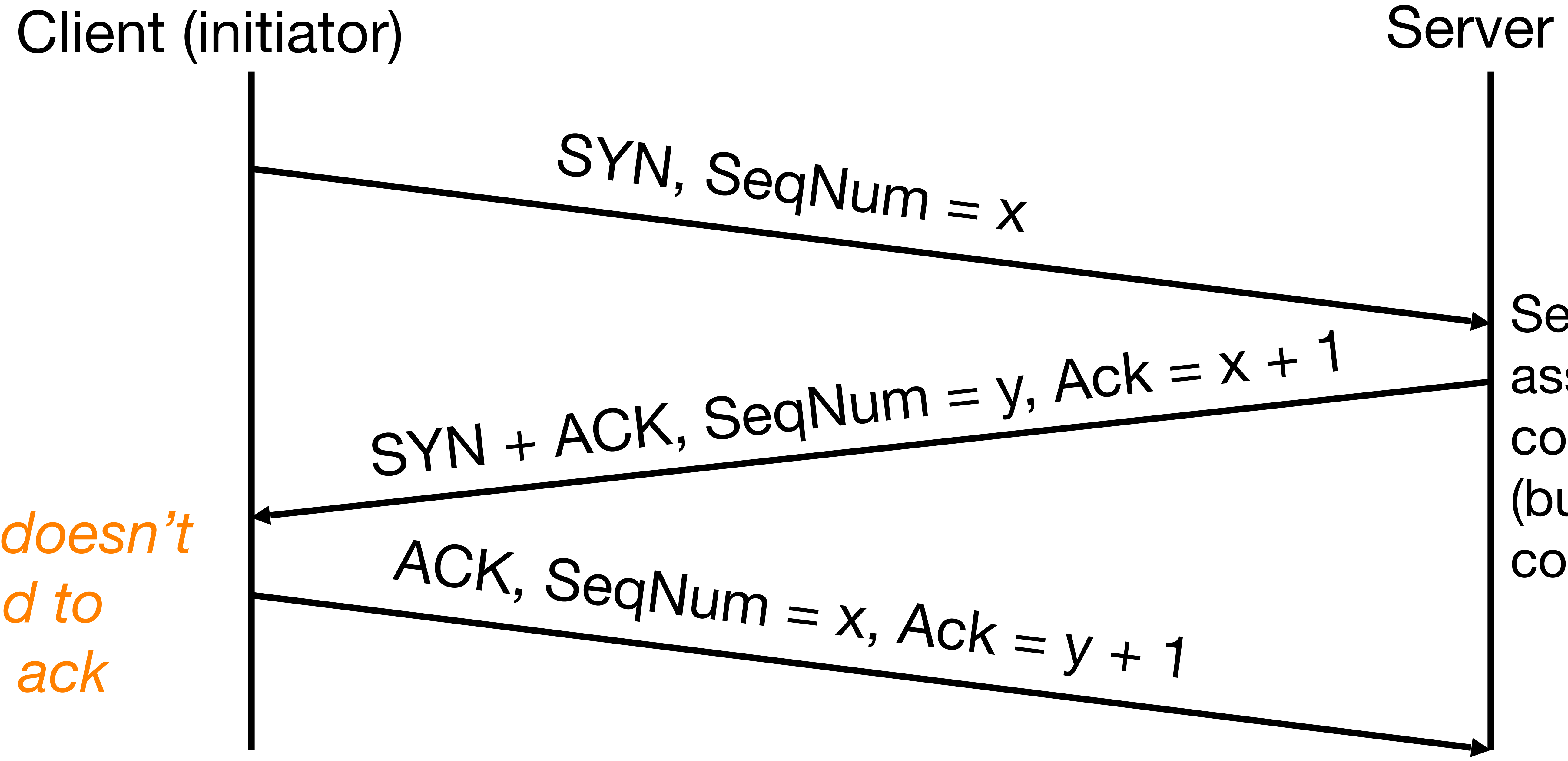
- Particularly dangerous form of asymmetry: amplification
  - Attacker leverages system’s own structure to pump up the load they induce on a resource

# Amplification

- Example of amplification: DNS lookups
  - Reply is generally much bigger than request (since it includes a copy of the reply, plus answers etc.)
  - Attacker spoofs DNS request to a patsy DNS server, seemingly from the target
  - Small attacker packet yields large flooding packet
  - Doesn’t increase # of packets, but total volume
- Note #1: these examples involve blind spoofing
  - So for network-layer flooding, generally only works for UDP-based protocols (can’t establish TCP conn.)
- Note #2: victim doesn’t see spoofed source addresses
  - Addresses are those of actual intermediary systems

# Transport-Level Denial-of-Service

- TCP's 3-way connection establishment handshake used to agree on initial sequence numbers
- So a single SYN from an attacker suffices to force the server to spend some memory


Client (initiator)
Server
SYN, SeqNum = x
SYN + ACK, SeqNum = y, Ack = x + 1
ACK, SeqNum = x, Ack = y + 1

*Attacker doesn't even need to send this ack*

Server creates state associated with connection here (buffers, timers, counters)

# TCP SYN Flooding

- Attacker targets memory rather than network capacity
- Every (unique) SYN that the attacker sends burdens the target
- What should target do when it has no more memory for a new connection?
- No good answer!
  - Refuse new connection? Legit new users can’t access service
  - Evict old connections to make room? Legit old users get kicked off

# TCP Syn Flooding Defenses

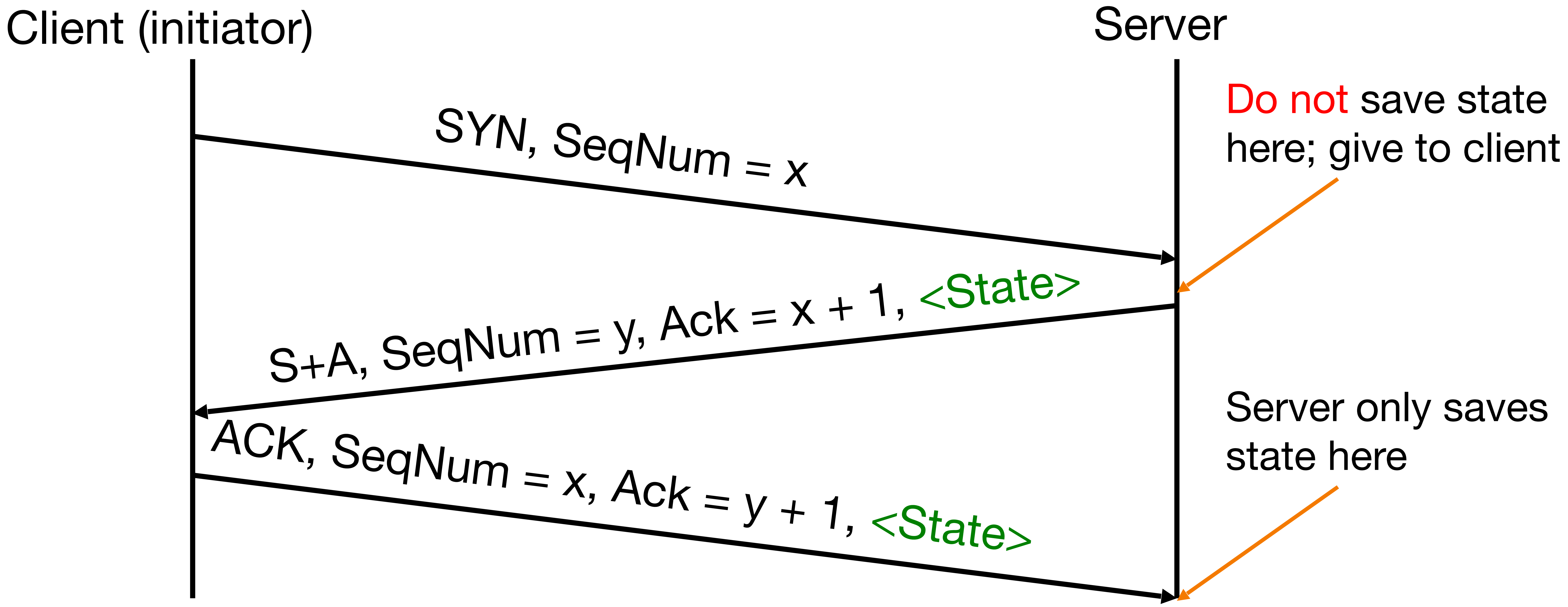
- How can the target defend itself?
- Approach #1: make sure they have tons of memory!
  - How much is enough?
  - Depends on resources attacker can bring to bear (threat model), which might be hard to know

# TCP Syn Flooding Defenses

- Approach #2: identify bad actors & refuse their connections
  - Hard because only way to identify them is based on IP address
    - We can’t for example require them to send a password because doing so requires we have an established connection!
  - For a public Internet service, who knows which addresses customers might come from?
  - Plus: attacker can spoof addresses since they don’t need to complete TCP 3-way handshake
- Approach #3: don’t keep state!  (“SYN cookies”; only works for spoofed SYN flooding)

# SYN Flooding Defense: *Idealized*

- Server: when SYN arrives, rather than keeping state locally, *send it to the client* …
- Client needs to *return the state* in order to established connection


Client (initiator)
Server
SYN, SeqNum = x
S+A, SeqNum = y, Ack = x + 1, <State>
ACK, SeqNum = x, Ack = y + 1, <State>

Do not save state here; give to client

Server only saves state here

# SYN Flooding Defense: *Idealized*

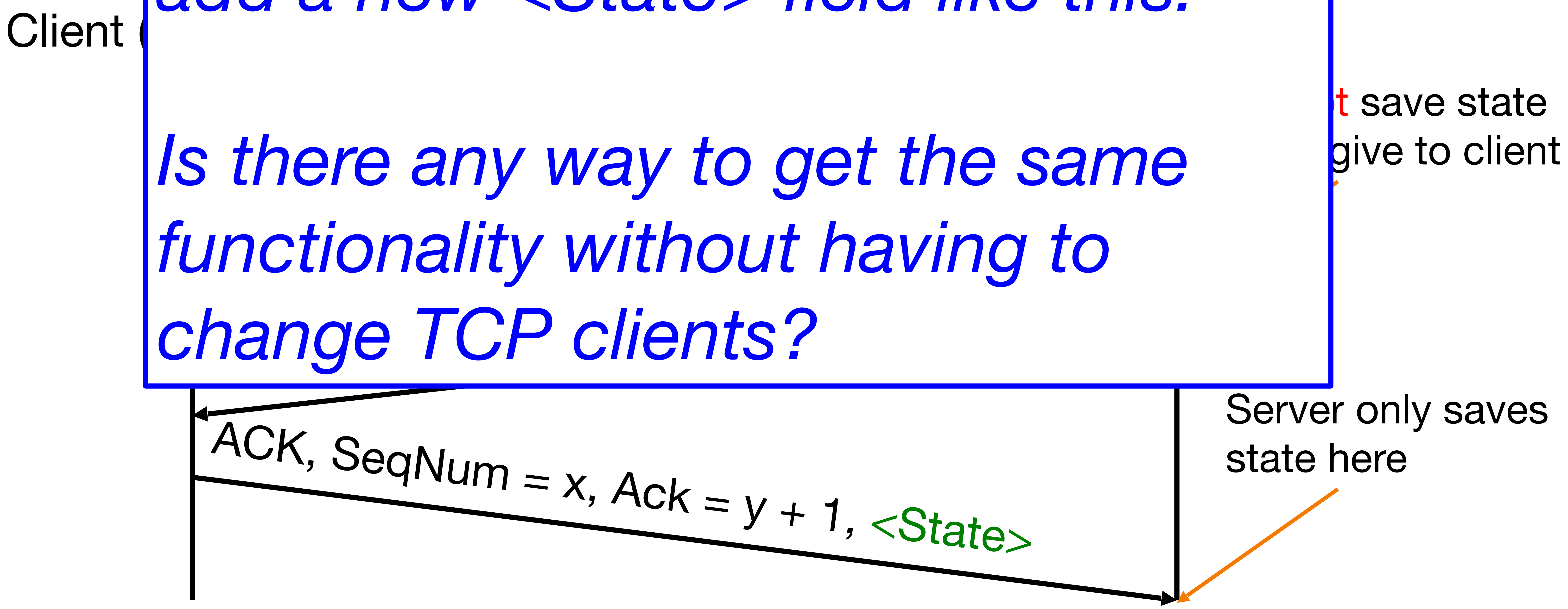
- Server: when SYN arrives, rather than keeping state locally, *send it to the client* …

- Client needs to *re* connection

*Problem: the world isn't so ideal!*

*TCP doesn't include an easy way to add a new <State> field like this.*

*Is there any way to get the same functionality without having to change TCP clients?*

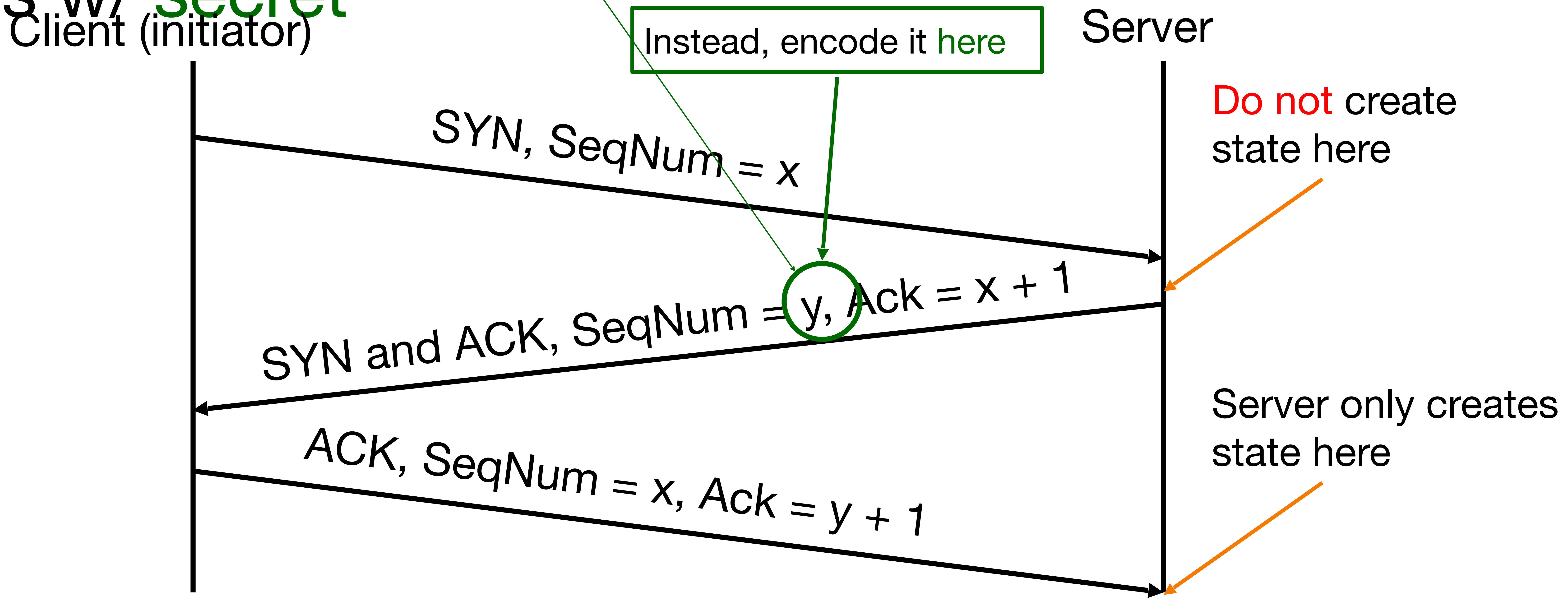

Client (
t save state
give to client
ACK, SeqNum = x, Ack = y + 1, <State>
Server only saves state here

# Practical Defense: *SYN Cookies*

- Server: when SYN arrives, encode connection state entirely within SYN-ACK's sequence # y
  - y = *encoding* of necessary state, using server secret

y = T (lower bits of timestamp), <state>,
lower bits of HMAC(key, T, <state>, x, source port & IP, destination port & IP)]

- When ACK of SYN-ACK arrives, server only creates state ***if*** value of y from it agrees w/ secret


Client (initiator)
Server
Instead, encode it here
SYN, SeqNum = x
Do not create state here
SYN and ACK, SeqNum = y, Ack = x + 1
ACK, SeqNum = x, Ack = y + 1
Server only creates state here

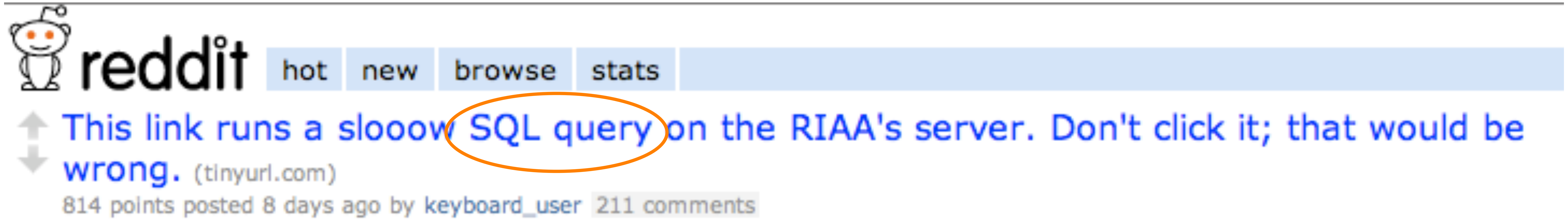
# SYN Cookies: Discussion

- Illustrates general strategy: rather than *holding* state, *encode* it so that it is returned when needed
- For SYN cookies, attacker must complete 3-way handshake in order to burden server
  - *Can't use spoofed source addresses*
- Note #1: strategy requires that you have enough bits to encode all the state
  - (This is just barely the case for SYN cookies)
- Note #2: if it's expensive to generate *or check* the cookie, then it's not a win

# Application-Layer DoS

- Rather than exhausting network or memory resources, attacker can overwhelm a service's processing capacity

- There are many ways to do so, often at little expense to attacker compared to target (*asymmetry*)



This link runs a slooow SQL query on the RIAA's server. Don't click it; that would be wrong. (tinyurl.com)

814 points posted 8 days ago by keyboard_user 211 comments

*The link sends a request to the web server that requires heavy processing by its "backend database".*

# Algorithmic complexity attacks

- Attacker can try to trigger worst-case complexity of algorithms / data structures
- Example: You have a hash table.
  Expected time: O(1). Worst-case: O(n).
- Attacker picks inputs that cause table collisions.
  Time per lookup: O(n).
  Total time to do n operations: O(n^2).
- Solution? Use algorithms with good worst-case running time.
  - E.g., universal hash function guarantees that Pr[hk(x)=hk(y)] = 1/2^b, so hash collisions will be rare.

# Application-Layer DoS

- Rather than exhausting network or memory resources, attacker can overwhelm a service's processing capacity
- There are many ways to do so, often at little expense to attacker compared to target (asymmetry)
- Defenses against such attacks?
- Approach #1: Only let legit users issue expensive requests
  - Relies on being able to identify/authenticate them
  - Note: that this itself might be expensive!
- Approach #2: Force legit users to "burn" cash
- Approach #3: massive over-provisioning ($$$)

# DoS Defense in General Terms

- Defending against program flaws requires:
  - Careful design and coding/testing/review
  - Consideration of behavior of defense mechanisms
    - E.g. buffer overflow detector that when triggered halts execution to prevent code injection ⇒ denial-of-service

- Defending resources from exhaustion can be **really** hard.  Requires:
  - *Isolation and scheduling mechanisms*
    - Keep adversary's consumption from affecting others
  - *Reliable identification* of different users