Denial-of-Service (DoS)

CS 161: Computer Security

Prof. Vern Paxson

TAs: Paul Bramsen, Apoorva Dornadula,
David Fifield, Mia Gil Epner, David Hahn, Warren He,
Grant Ho, Frank Li, Nathan Malkin, Mitar Milutinovic,
Rishabh Poddar, Rebecca Portnoff, Nate Wang

http://inst.eecs.berkeley.edu/~cs161/

April 4, 2017

General Communication Security Goals: CIA

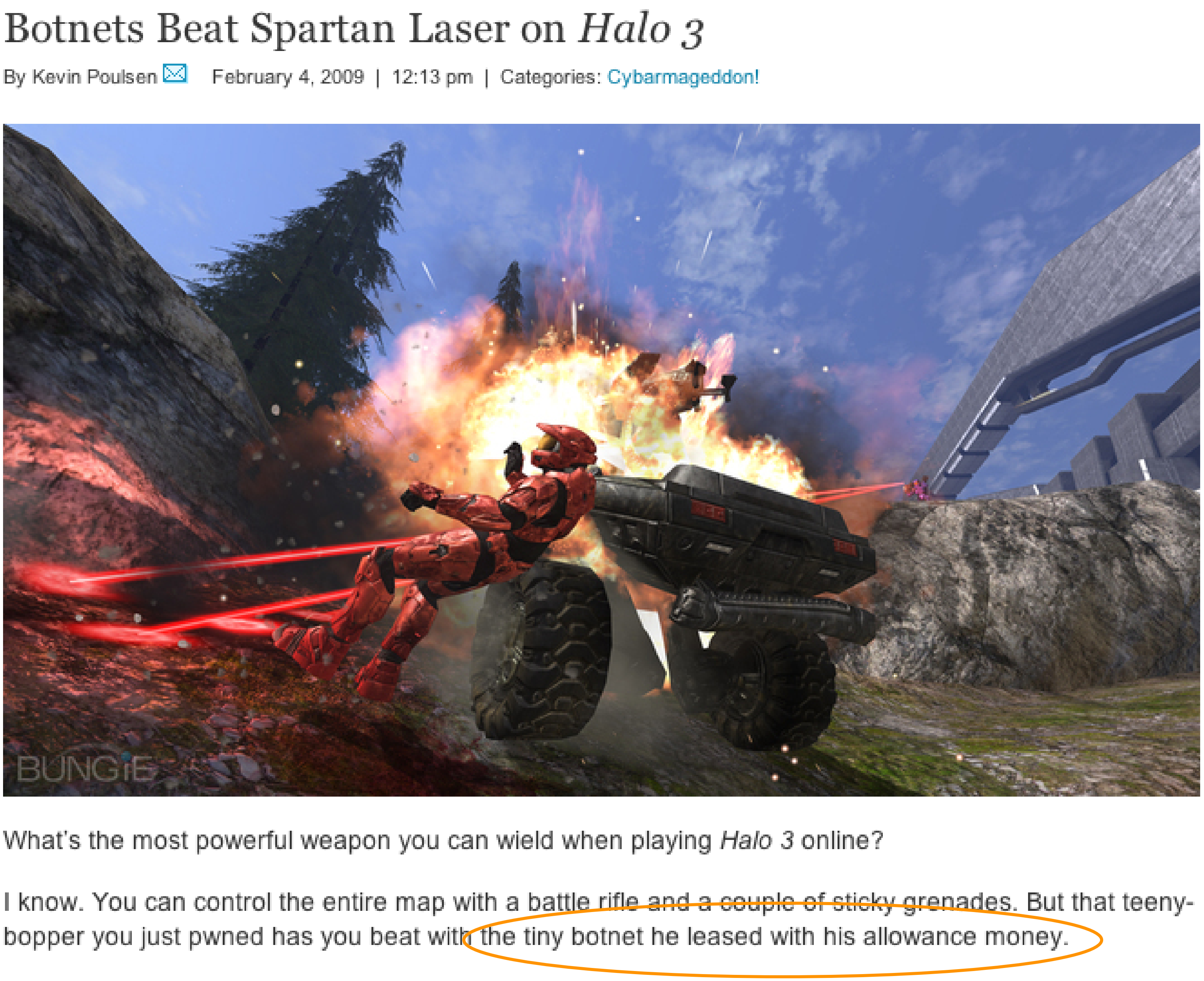
- Confidentiality
  - No one can *read* our data / communication unless we want them to
- Integrity
  - No one can *manipulate* our data / processing / communication unless we want them to
- Authentication
  - We can determine who created a given message / data

General Communication Security Goals: CIAA

- Confidentiality
  - No one can *read* our data / communication unless we want them to
- Integrity
  - No one can *manipulate* our data / processing / communication unless we want them to
- Authentication
  - We can determine who created a given message / data
- Availability
  - We can *access* our data / conduct our processing / use our communication capabilities when we want to

Attacks on Availability

- Denial-of-Service (DoS, or "*doss*"): *keeping someone from using a computing service*
- How broad is this sort of threat?
  - *Very*: **huge** attack surface
- We do though need to consider our threat model …
  - What might motivate a DoS attack?

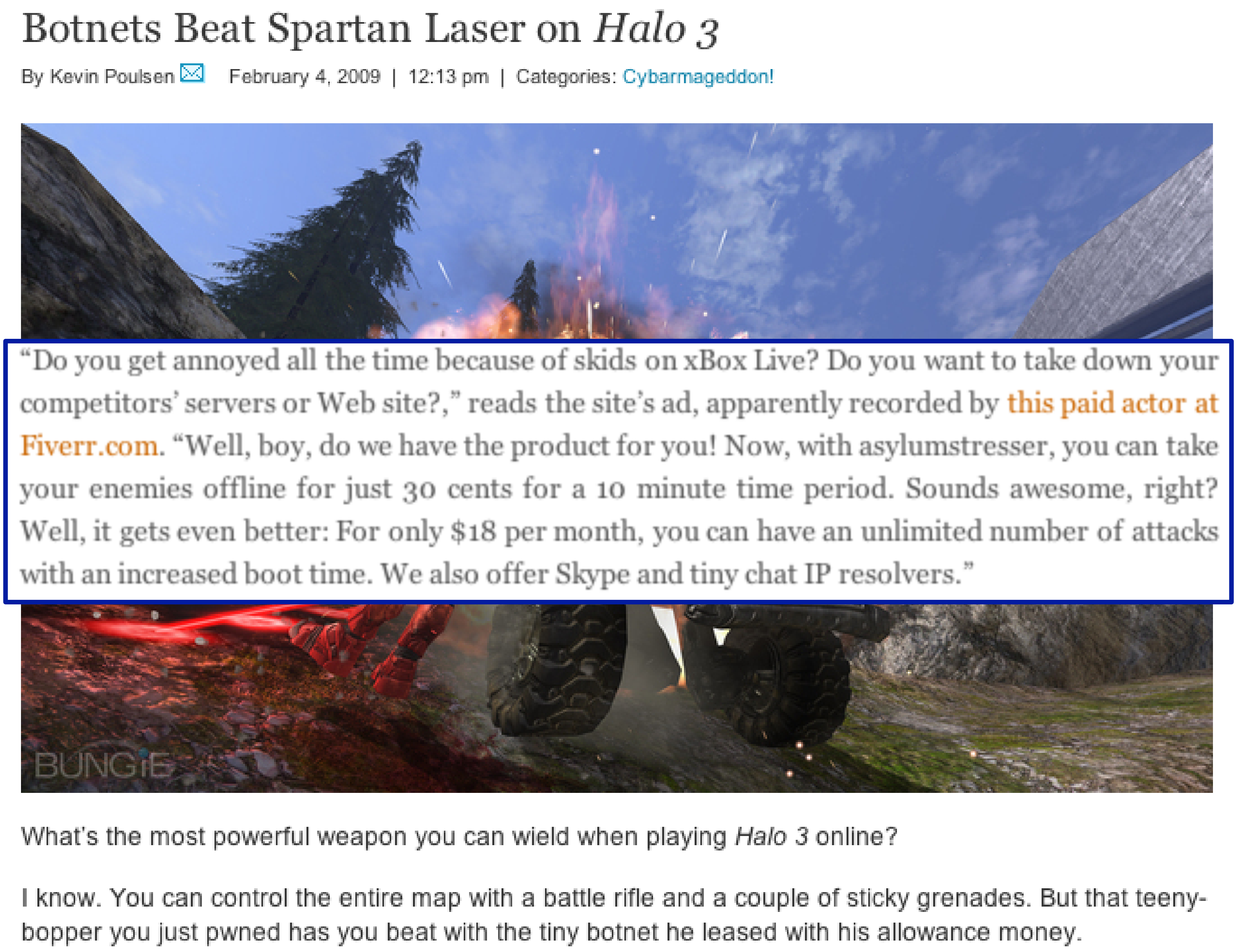


Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen ✉ February 4, 2009 | 12:13 pm | Categories: Cybarmageddon!

What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle ~~and a couple of sticky grenades~~. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.



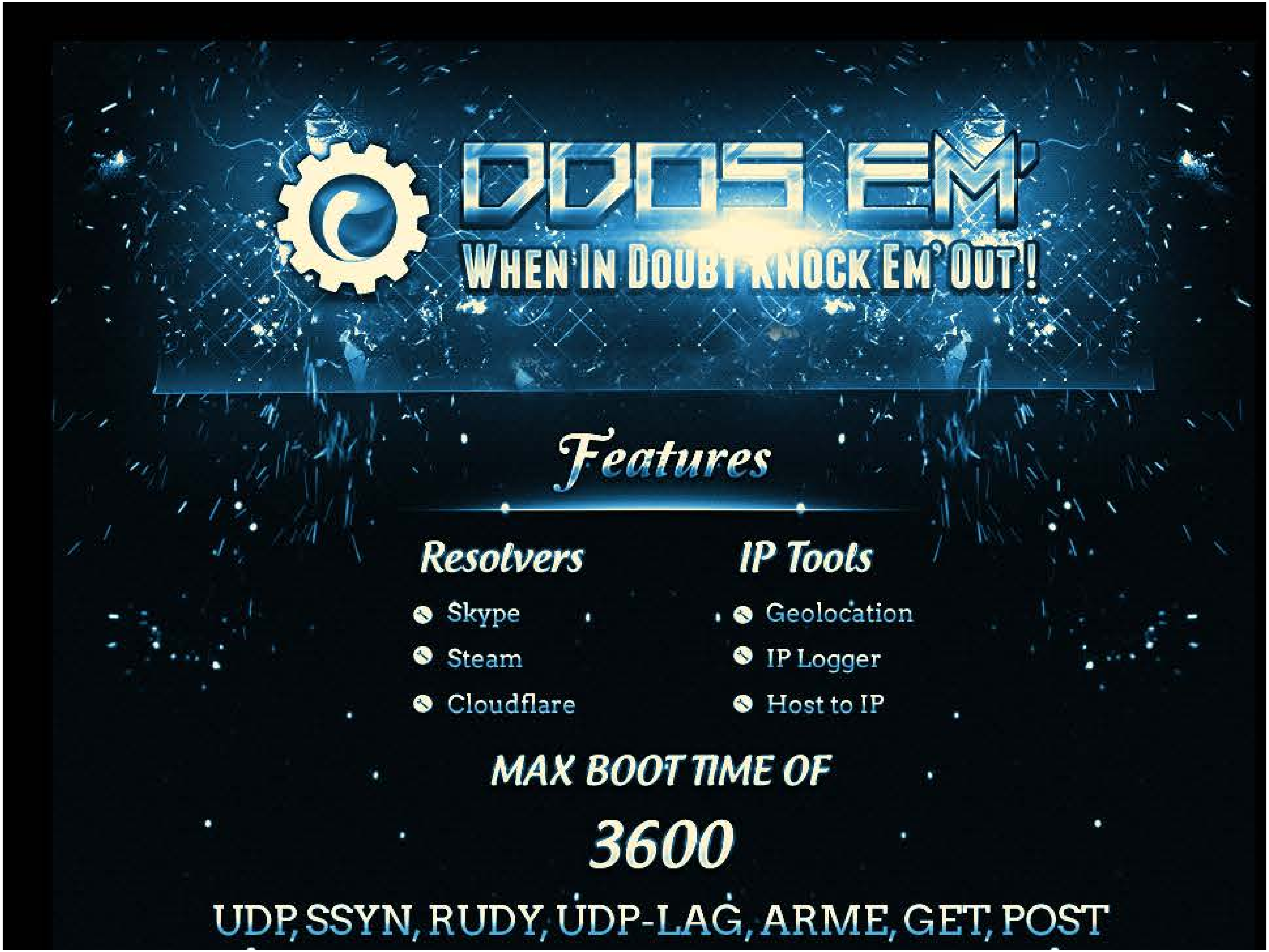
Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen February 4, 2009 | 12:13 pm | Categories: Cybarmageddon!

"Do you get annoyed all the time because of skids on xBox Live? Do you want to take down your competitors' servers or Web site?," reads the site's ad, apparently recorded by this paid actor at Fiverr.com. "Well, boy, do we have the product for you! Now, with asylumstresser, you can take your enemies offline for just 30 cents for a 10 minute time period. Sounds awesome, right? Well, it gets even better: For only $18 per month, you can have an unlimited number of attacks with an increased boot time. We also offer Skype and tiny chat IP resolvers."

What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.



DDOS EM'

WHEN IN DOUBT KNOCK EM' OUT!

Features

Resolvers

- Skype
- Steam
- Cloudflare

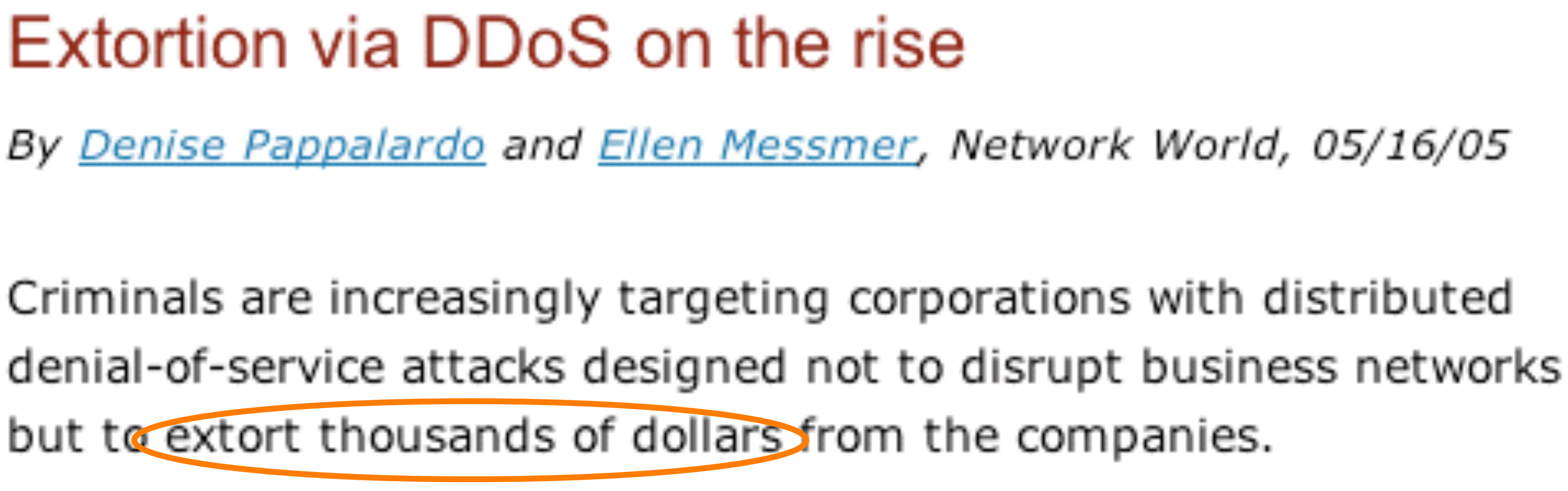
IP Tools

- Geolocation
- IP Logger
- Host to IP

MAX BOOT TIME OF

3600

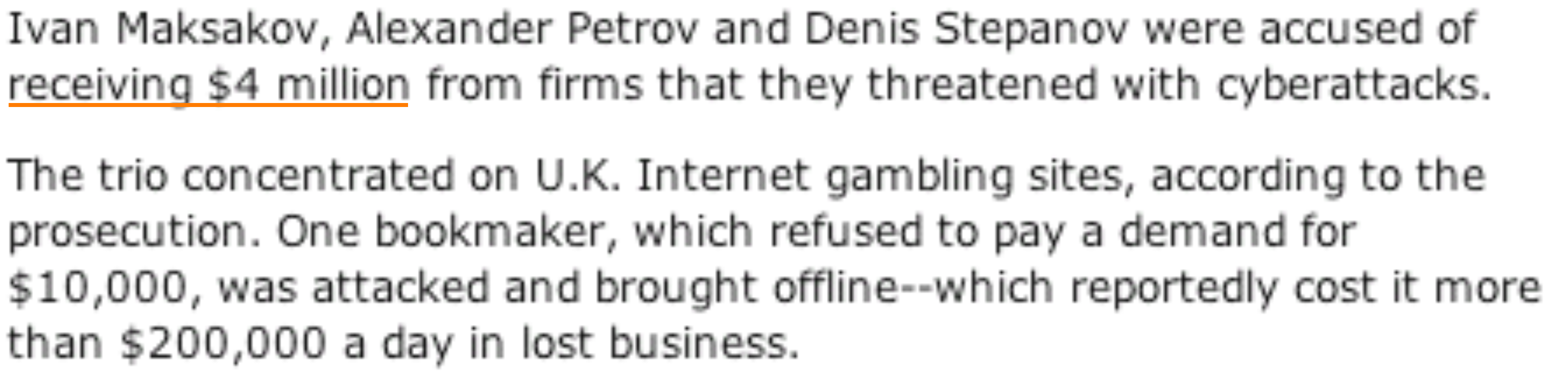
UDP, SSYN, RUDY, UDP-LAG, ARME, GET, POST



Extortion via DDoS on the rise

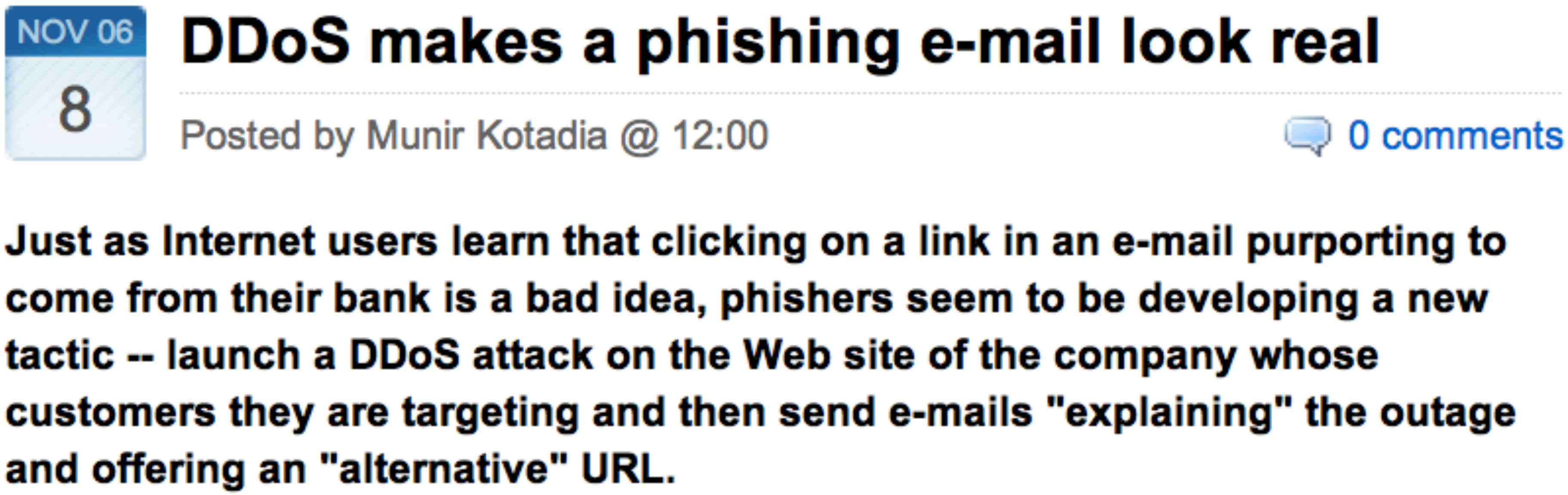
By Denise Pappalardo and Ellen Messmer, Network World, 05/16/05

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.

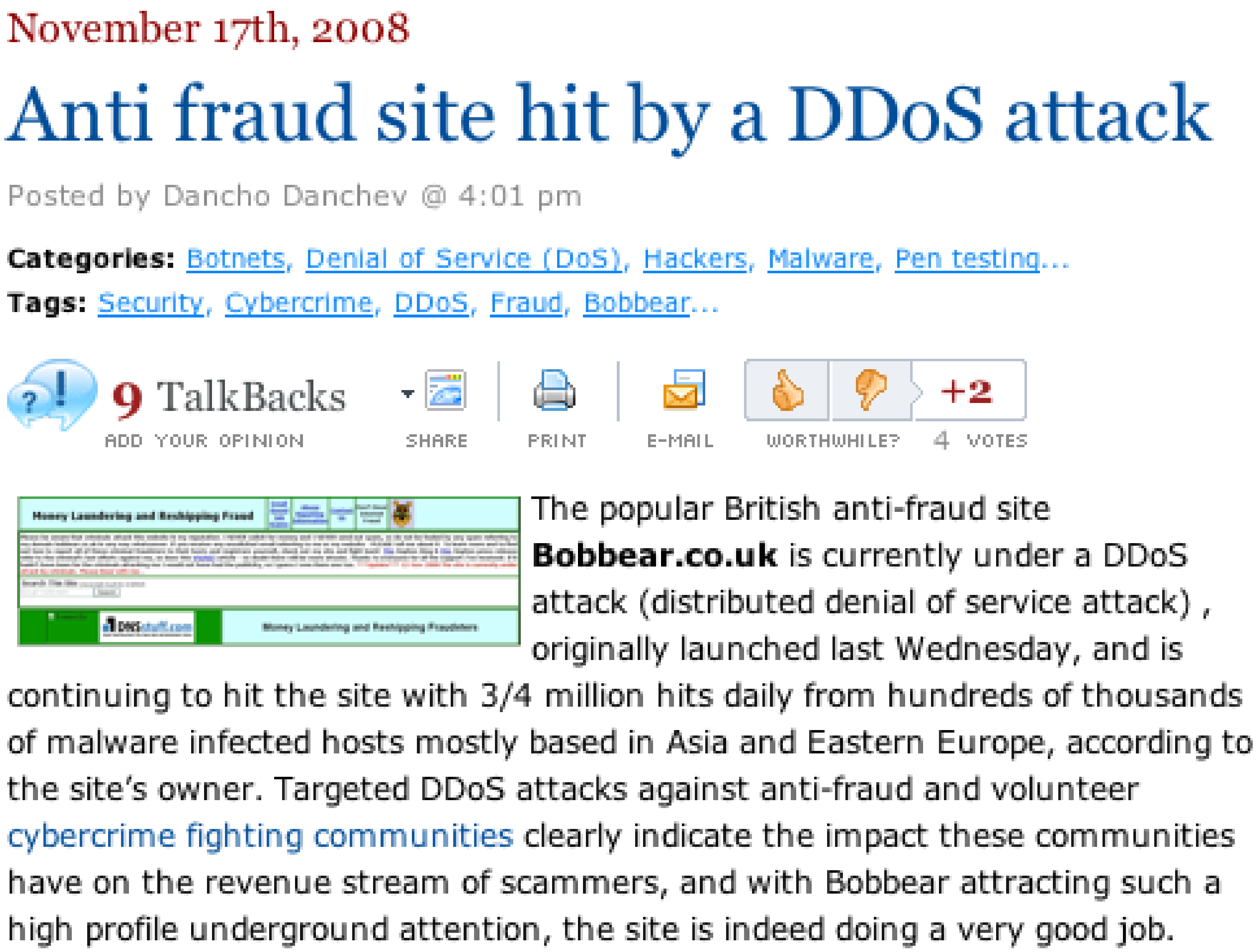


NOV 06
8

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

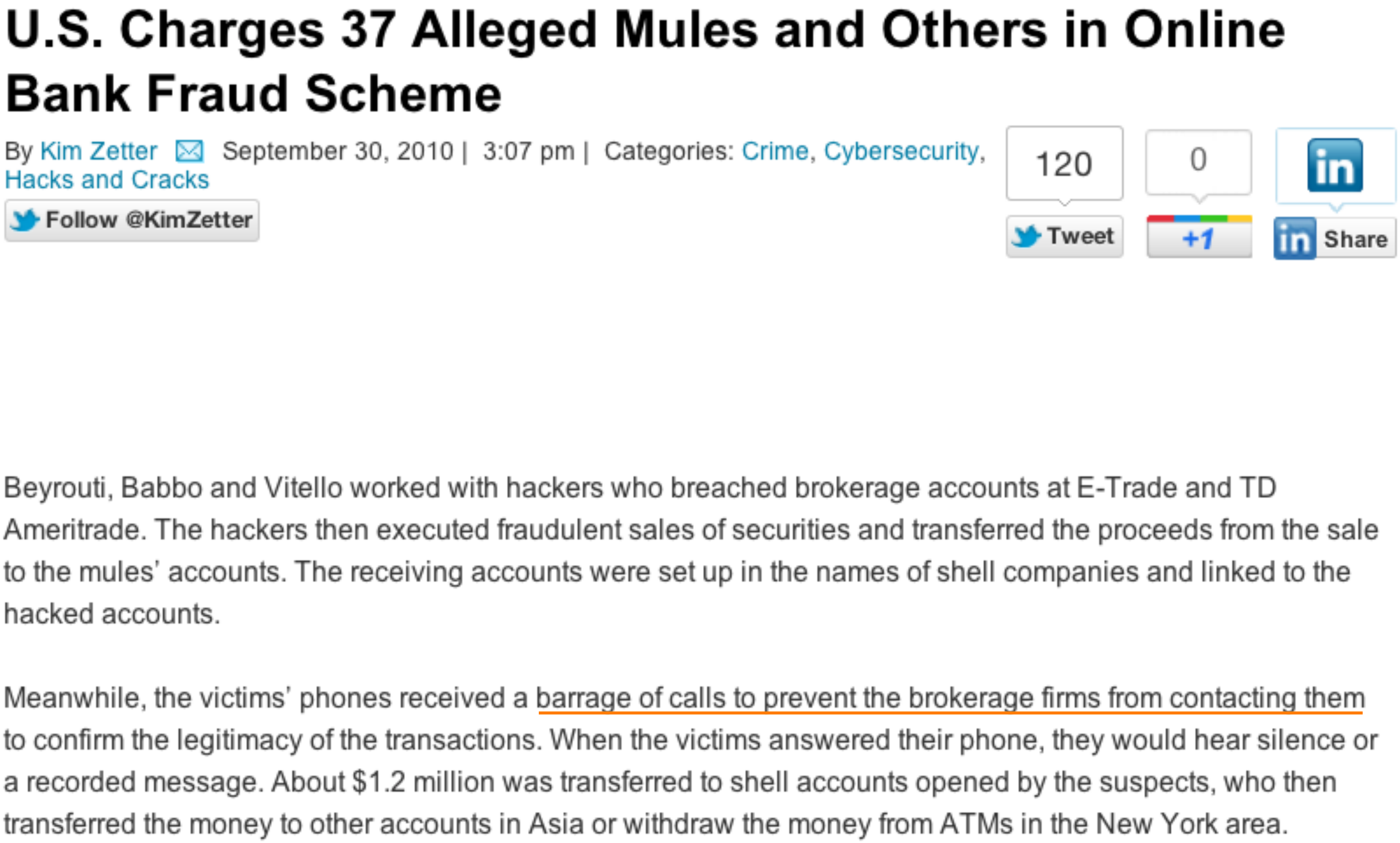
Posted by Dancho Danchev @ 4:01 pm

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

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

9 TalkBacks
ADD YOUR OPINION
SHARE
PRINT
E-MAIL
+2
WORTHWHILE?
4 VOTES
Money Laundering and Reshipping Fraud
Money Laundering and Reshipping Fraudsters

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.



U.S. Charges 37 Alleged Mules and Others in Online Bank Fraud Scheme

By Kim Zetter September 30, 2010 | 3:07 pm | Categories: Crime, Cybersecurity, Hacks and Cracks

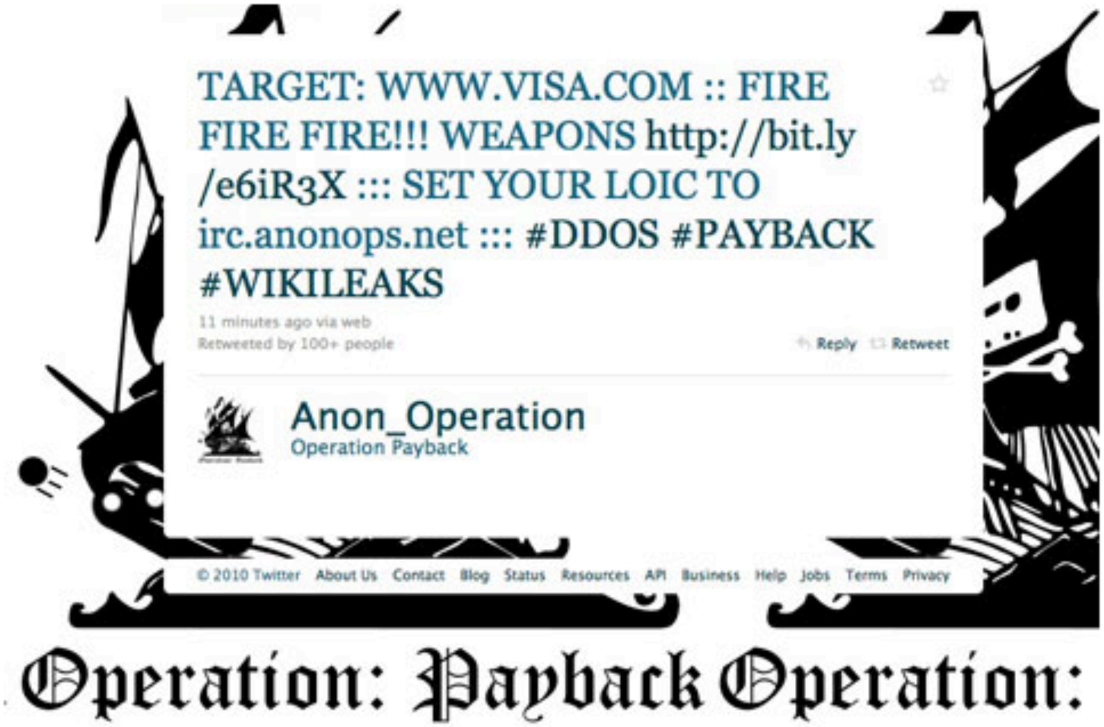
Beyrouti, Babbo and Vitello worked with hackers who breached brokerage accounts at E-Trade and TD Ameritrade. The hackers then executed fraudulent sales of securities and transferred the proceeds from the sale to the mules' accounts. The receiving accounts were set up in the names of shell companies and linked to the hacked accounts.

Meanwhile, the victims' phones received a barrage of calls to prevent the brokerage firms from contacting them to confirm the legitimacy of the transactions. When the victims answered their phone, they would hear silence or a recorded message. About $1.2 million was transferred to shell accounts opened by the suspects, who then transferred the money to other accounts in Asia or withdraw the money from ATMs in the New York area.

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

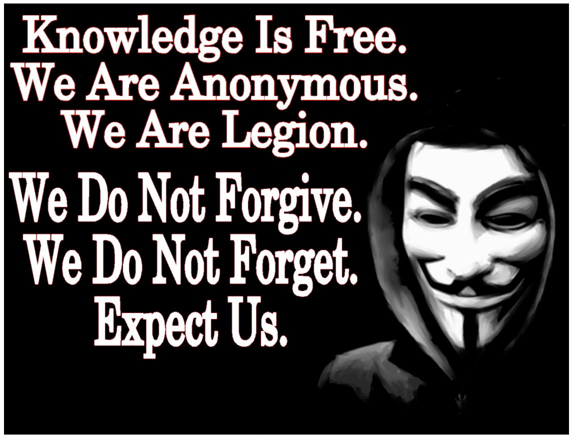
Anon_Operation
Operation Payback

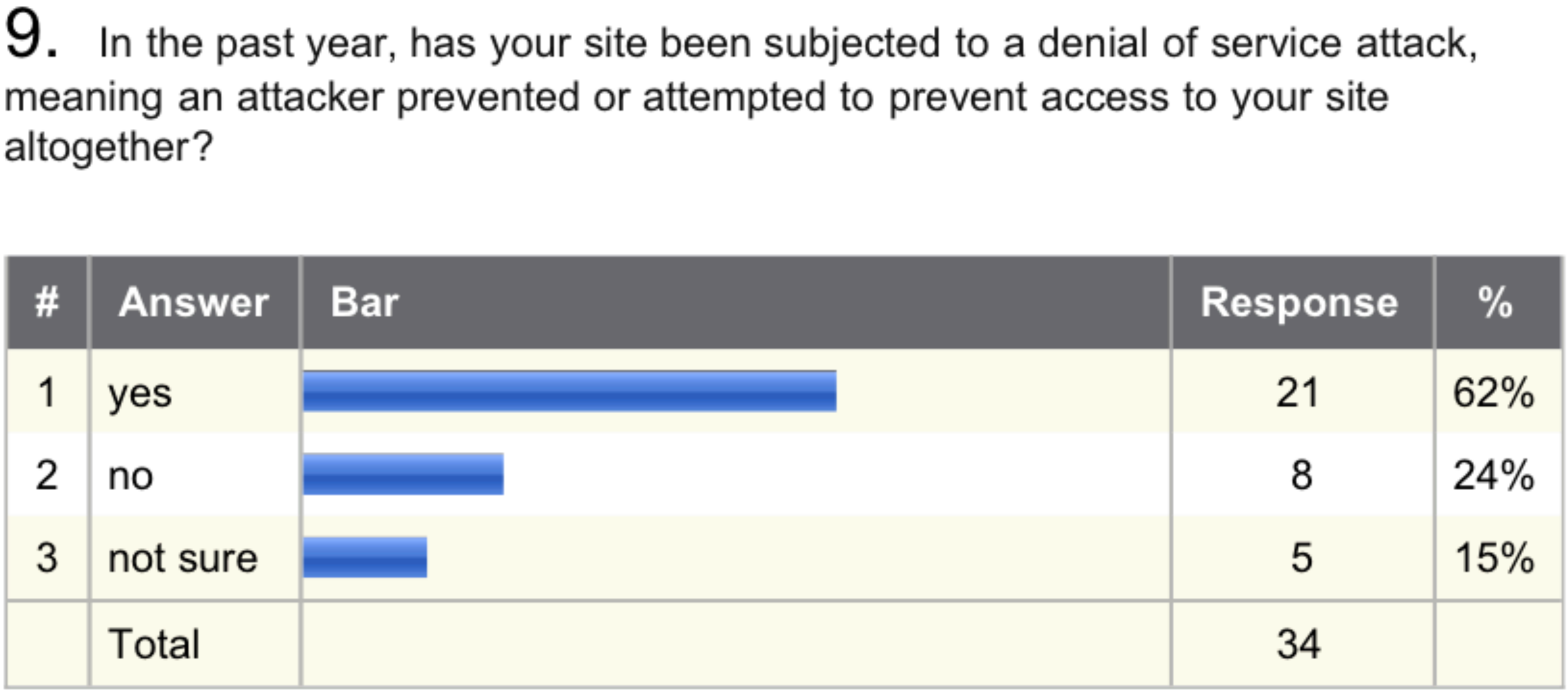
Reply
Retweet
© 2010 Twitter About Us Contact Blog Status Resources API Business Help Jobs Terms Privacy
Operation: Payback Operation:

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.

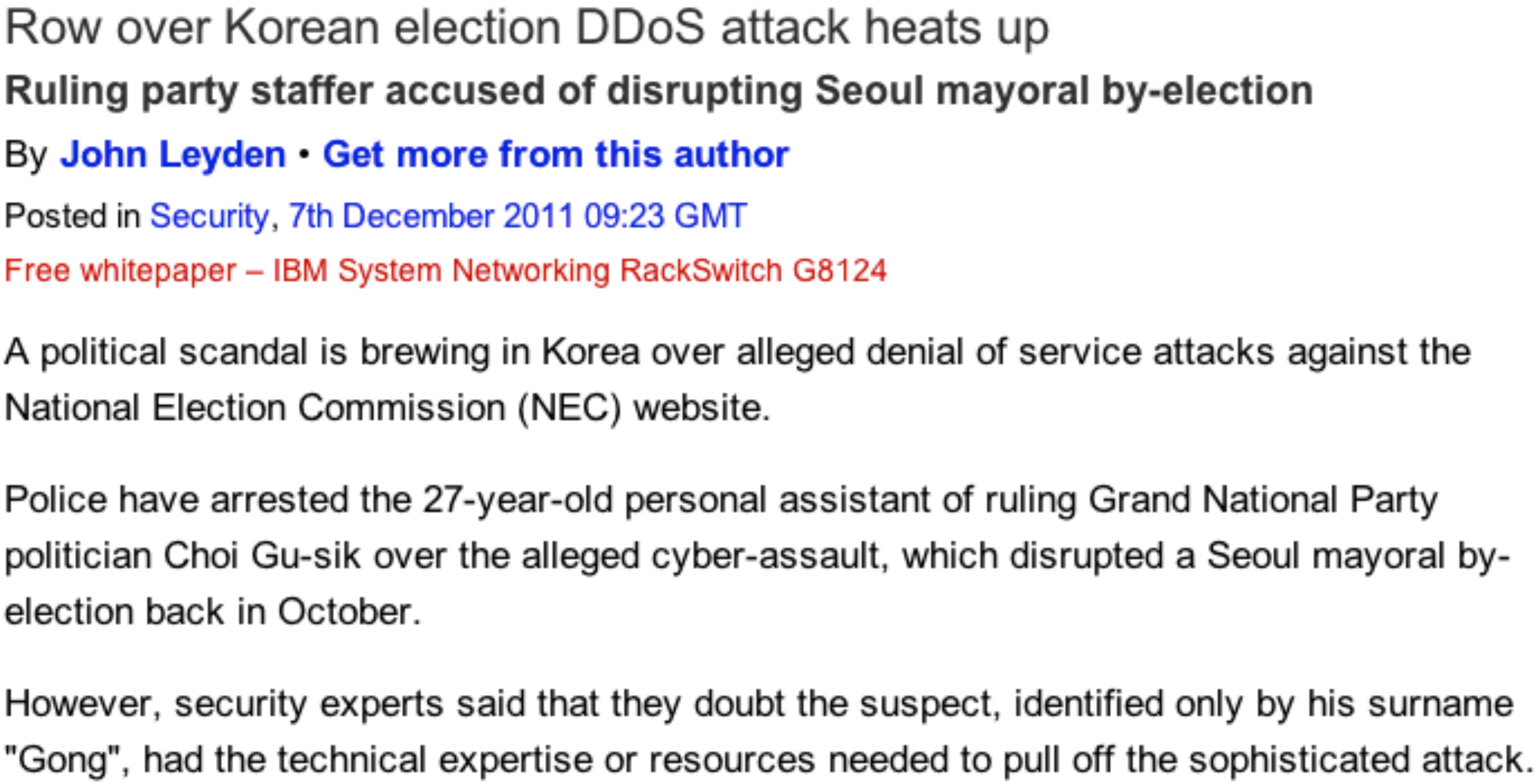
The group explained that its distributed denial of service attacks — in which they essentially flood Web sites site with traffic to slow them down or knock them offline — were part of a broader effort called Operation Payback, which





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

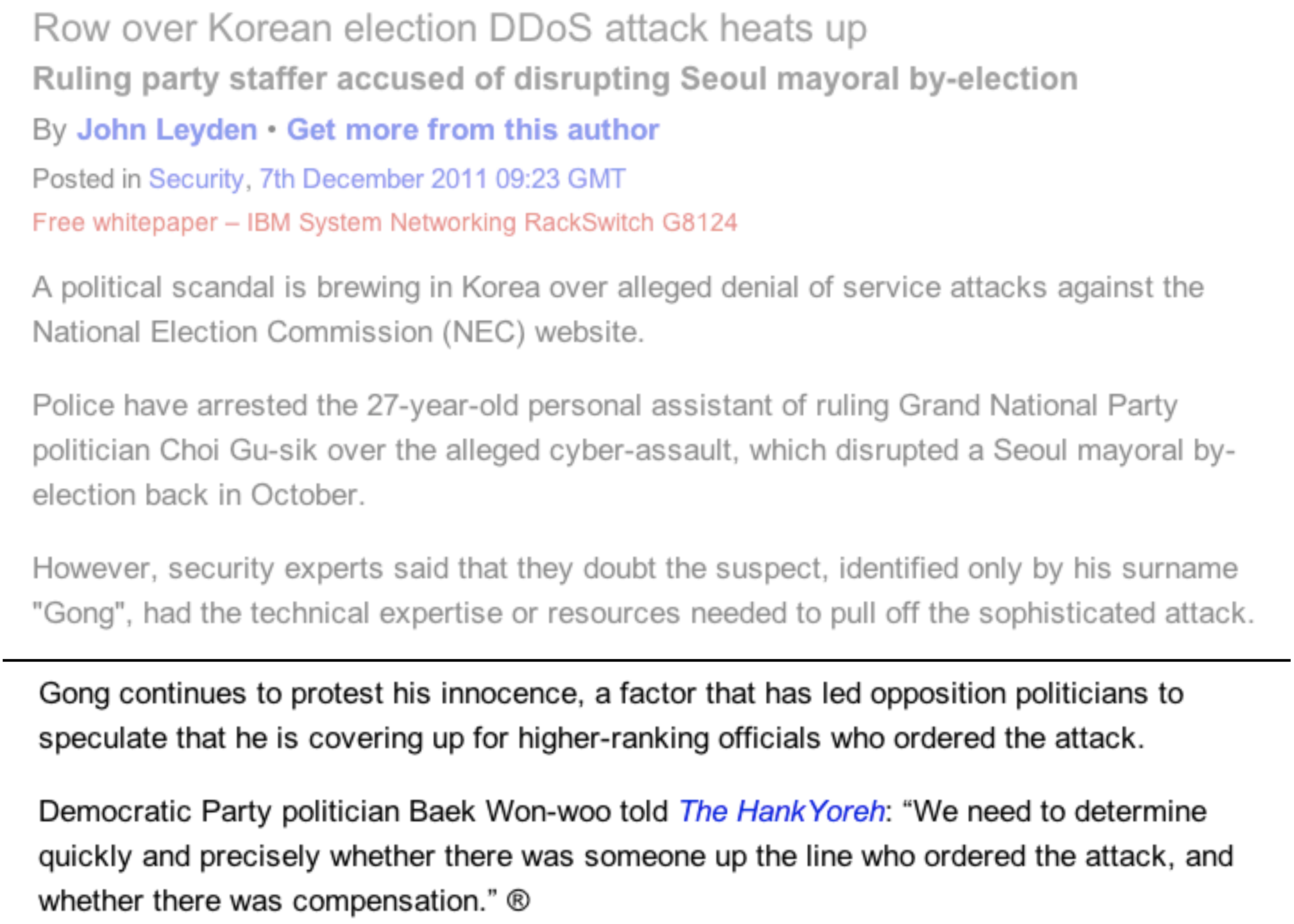
By **John Leyden** • **Get more from this author**

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

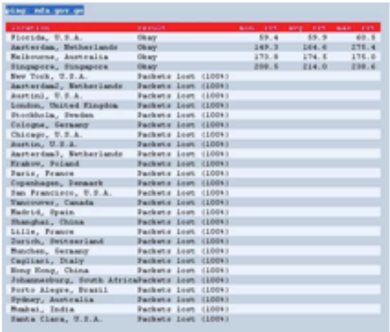
Coordinated Russia vs Georgia cyber attack in progress

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...

62 TalkBacks ADD YOUR OPINION | SHARE | PRINT | E-MAIL | WORTHWHILE? +18 24 VOTES

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



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	208.5	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%)			

Motivations for DoS

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

Attacks on Availability

- Denial-of-Service (DoS, or "*doss*"): *keeping someone from using a computing service*
- How broad is this sort of threat?
  - *Very*: **huge** attack surface
- We do though need to consider our threat model …
  - What might motivate a DoS attack?
- Two basic approaches available to an attacker:
  - 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

DoS Defense in General Terms

- Defending against program flaws requires:
  - Careful coding/testing/review
  - Careful *authentication*
    - Don’t obey shut-down orders from imposters
  - 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 mechanisms*
    - Keep adversary’s consumption from affecting others
  - *Reliable identification* of different users
    - Know who the adversary is in the first place!

DoS & Operating Systems

- How could you DoS a multi-user Unix system on which you have a login?
  - `# rm -rf /`
    - (if you have root - but then just “halt” works well!)

  -
    ```
    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
  - … doubtless many more
- Defenses?
  - Isolate users / impose quotas

5 Minute Break

Questions Before We Proceed?

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 packet pattern* in the flooding traffic that’s not in benign traffic
  - Filter = *isolation mechanism*
  - Attacker’s IP address = means of *identifying* misbehaving user

Filtering Sounds Pretty Easy …

- … but it's not. What steps can the attacker take to defeat the filtering?
  - 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
    - How does a defender filter this?
      - They don't! (Unless the traffic has some sort of identifying quirk)
      - Best they can hope for is that operators around the world implement anti-spoofing mechanisms (today about 1/3rd do nothing)

Filtering Sounds Pretty Easy …

- … but it's not. What steps can the attacker take to defeat the filtering?
  - 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
    - How does a defender filter this?
      - They don't! (Unless the traffic has some sort of identifying quirk)
      - Best they can hope for is that operators around the world implement anti-spoofing mechanisms (today about 1/3rd do nothing)
  - Use many hosts to send traffic rather than just one
    - Distributed Denial-of-Service = **DDoS** ("dee-doss")
    - Requires defender to install complex filters
    - How many hosts are "enough" for the attacker?
      - Today they are very cheap to acquire … :-(

Survey Peak Attack Size Year Over Year

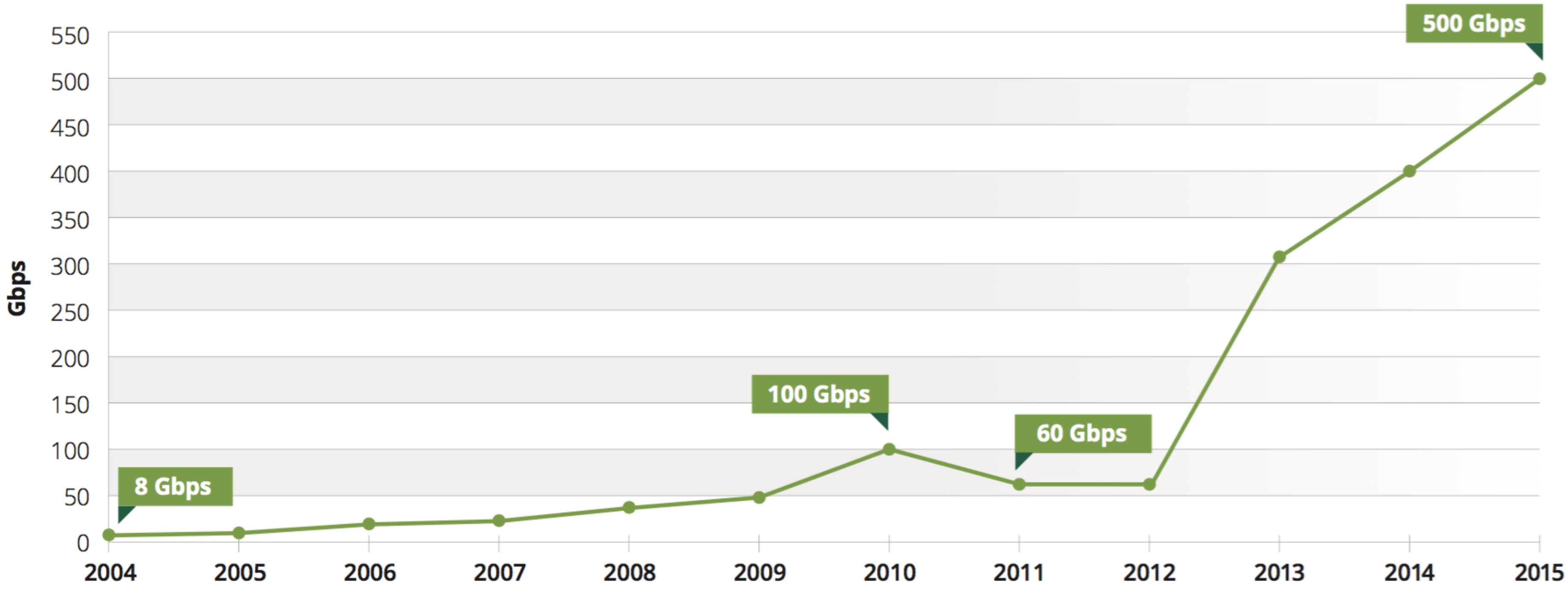


Figure 14 *Source: Arbor Networks, Inc.*

Oct 2016: 1.2 Tbps

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

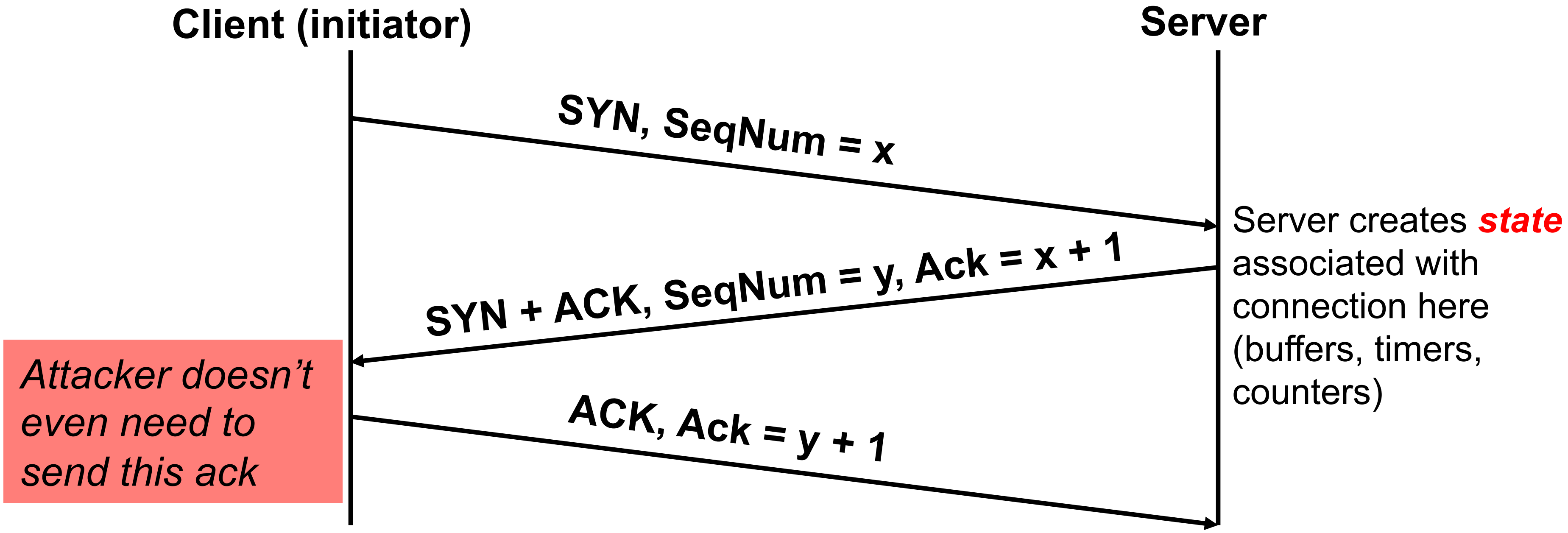
Amplification Vector: DNS / UDP

- Consider DNS lookups:
  - *Reply is generally much bigger than request*
    - Since it includes a copy of the reply, plus answers etc.

  ⇒ Attacker spoofs request seemingly from the target
    - Small attacker packet yields large flooding packet
    - Doesn't increase # of packets, but **total byte volume**
  - Works for other request/response protocols too
- Note #1: attacks 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

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



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

Attacker doesn't even need to send this ack

TCP *SYN Flooding*

- Attacker targets *memory* rather than network capacity
- Every (unique) SYN that the attacker sends burdens the target
  - Potentially cheaper attack than acquiring tons of bots
- 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, con’t

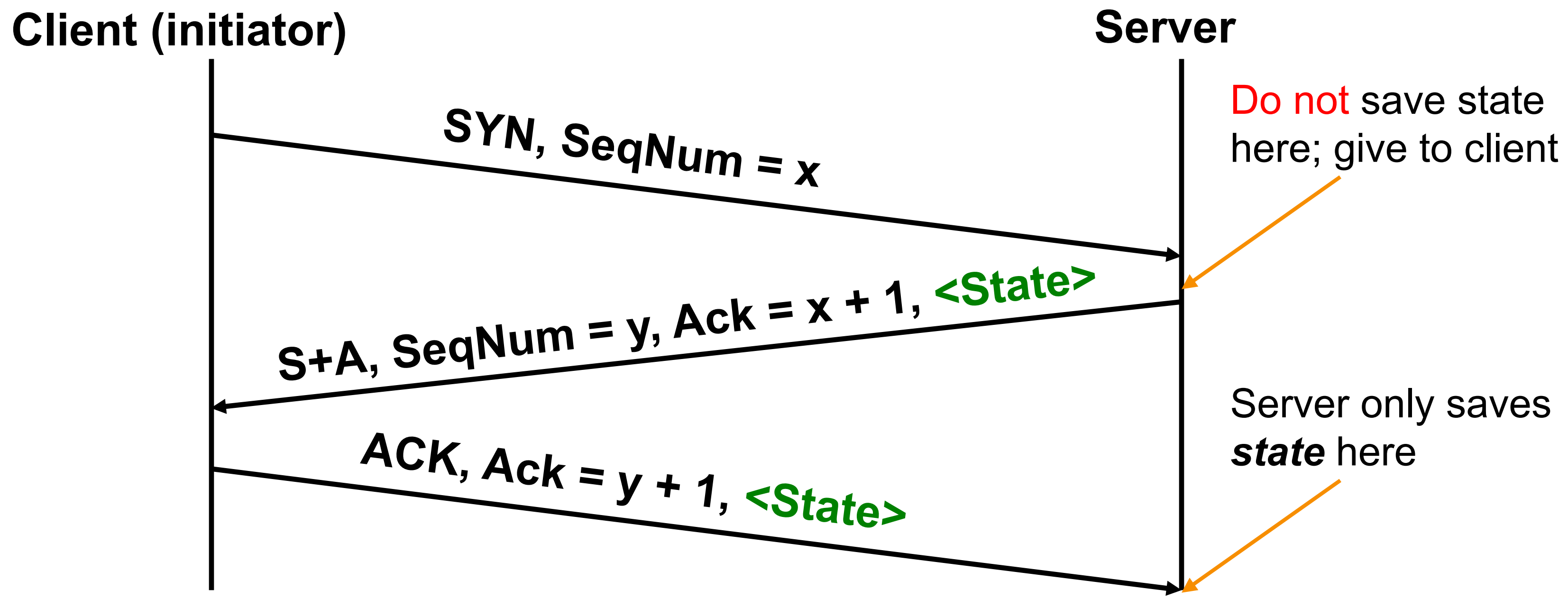
- How can the target defend itself?
- Approach #1: make sure they have **tons of memory!**
  - How much is enough?
  - Depends on resources attacker can bring to bear (threat model)
    - Which might be hard to know

TCP SYN Flooding, con't

- 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 critical state to the client* …
- Client needs to ***return** the critical state* in order to established connection


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

Do not save state here; give to client

Server only saves ***state*** here

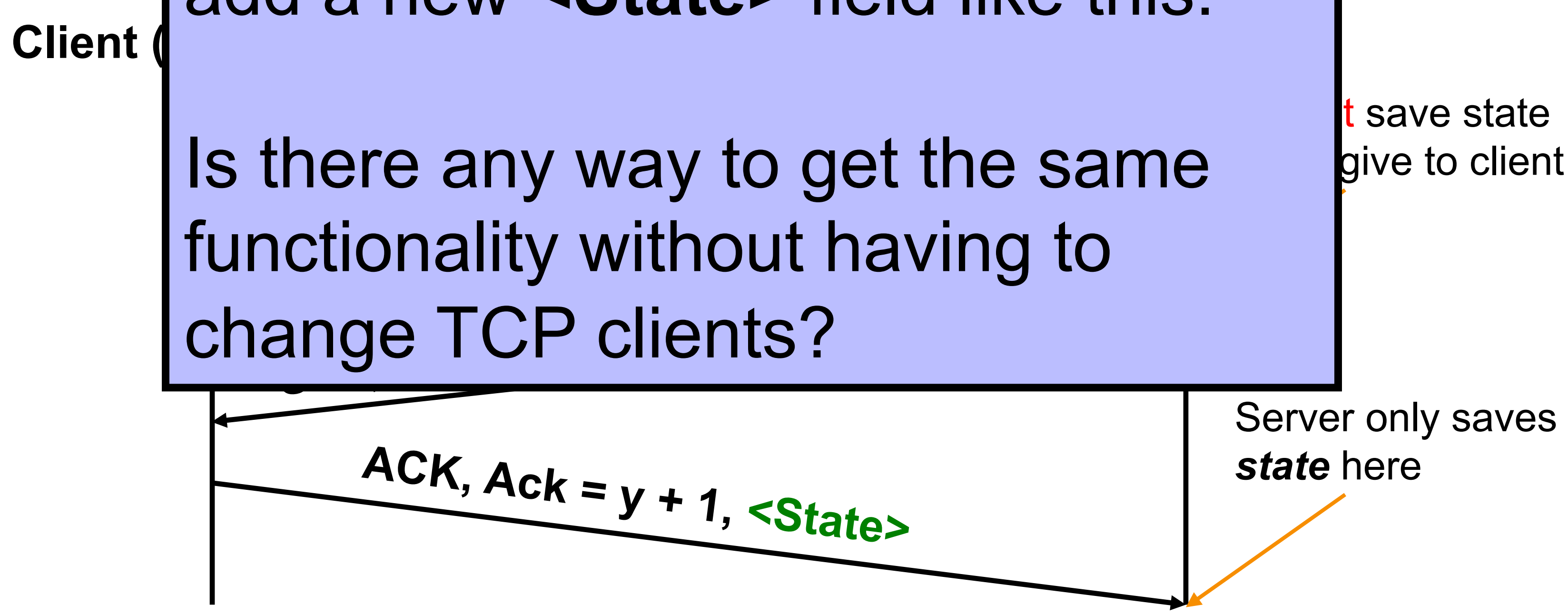
SYN Flooding Defense: *Idealized*

- Server: when SYN arrives, rather than keeping state locally, *send critical state to the client* …
- Client
der to
establ

Problem: the world isn't so ideal!

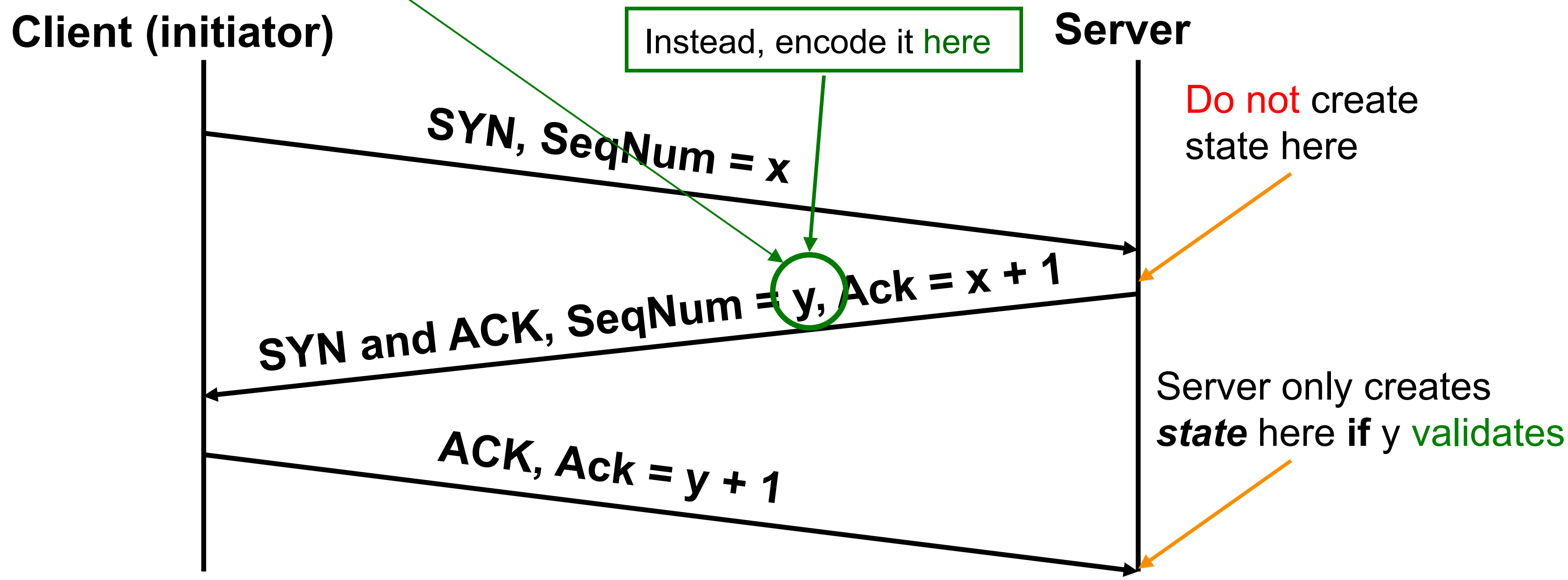
TCP doesn't include an easy way to add a new **<State>** field like this.

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



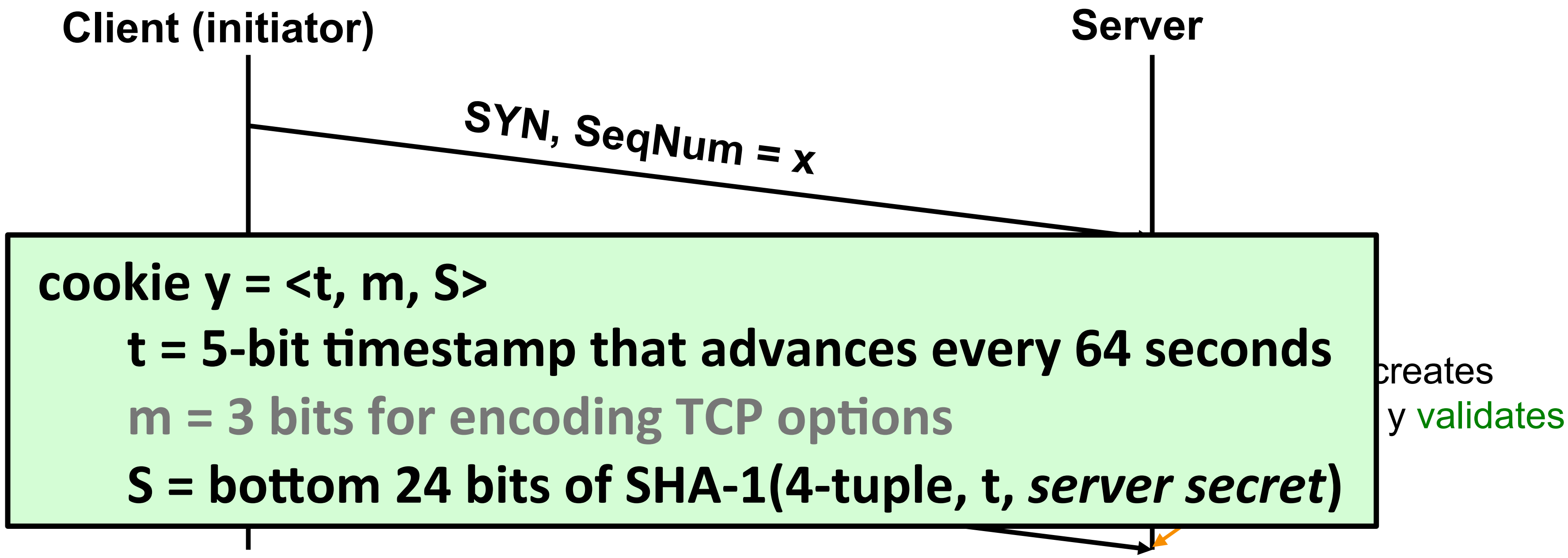
Practical Defense: *SYN Cookies*

- Server: when SYN arrives, encode critical state entirely within SYN-ACK's sequence # y !
  - y = *encoding* of necessary state, using server secret
- When ACK of SYN-ACK arrives, server only creates state ***if*** value of **y** from it agrees w/ secret



Practical Defense: *SYN Cookies*

- Server: when SYN arrives, encode critical state entirely within SYN-ACK's sequence # y !
  - y = *encoding* of necessary state, using server secret
- When ACK of SYN-ACK arrives, server only creates state ***if*** value of **y** from it agrees w/ secret



cookie y = <t, m, S>

t = 5-bit timestamp that advances every 64 seconds

m = 3 bits for encoding TCP options

S = bottom 24 bits of SHA-1(4-tuple, t, *server secret*)