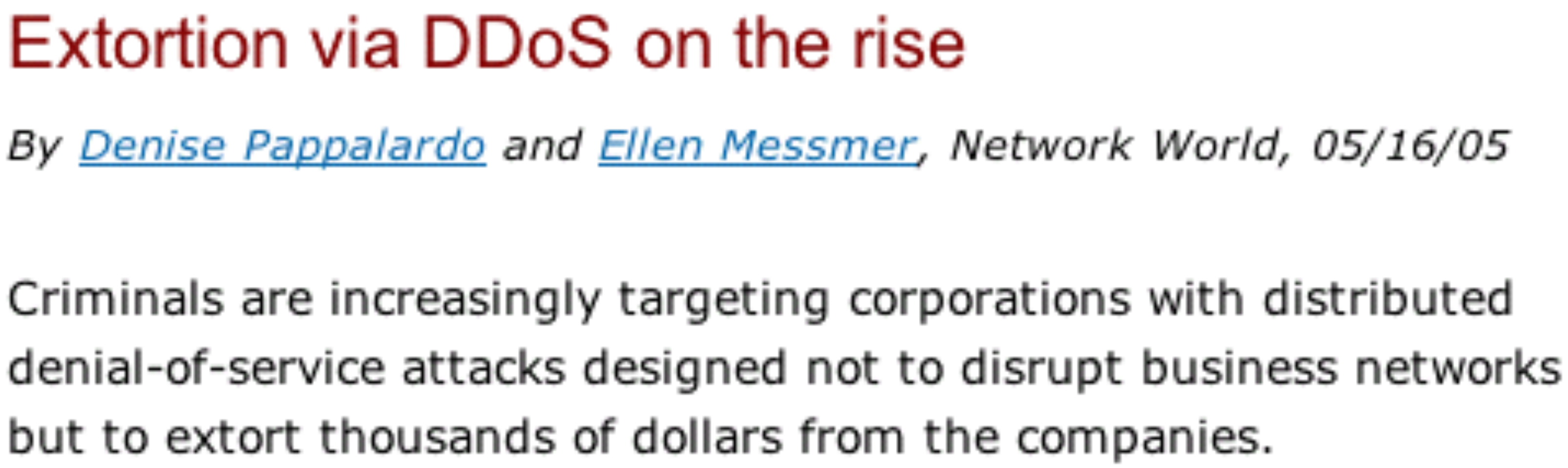
Botnets Beat Spartan Laser on *Halo 3*

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?

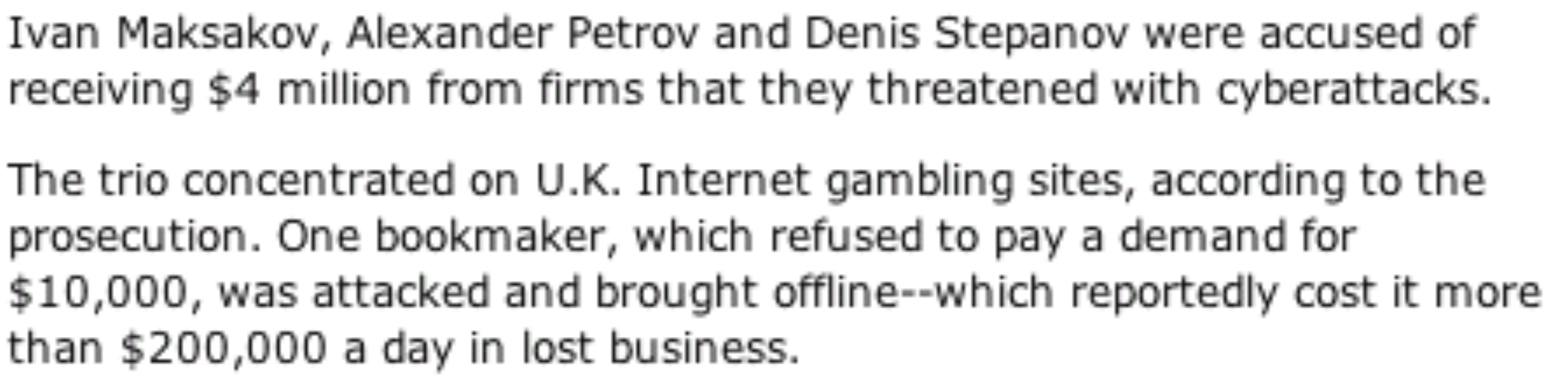
I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.



Extortion via DDoS on the rise

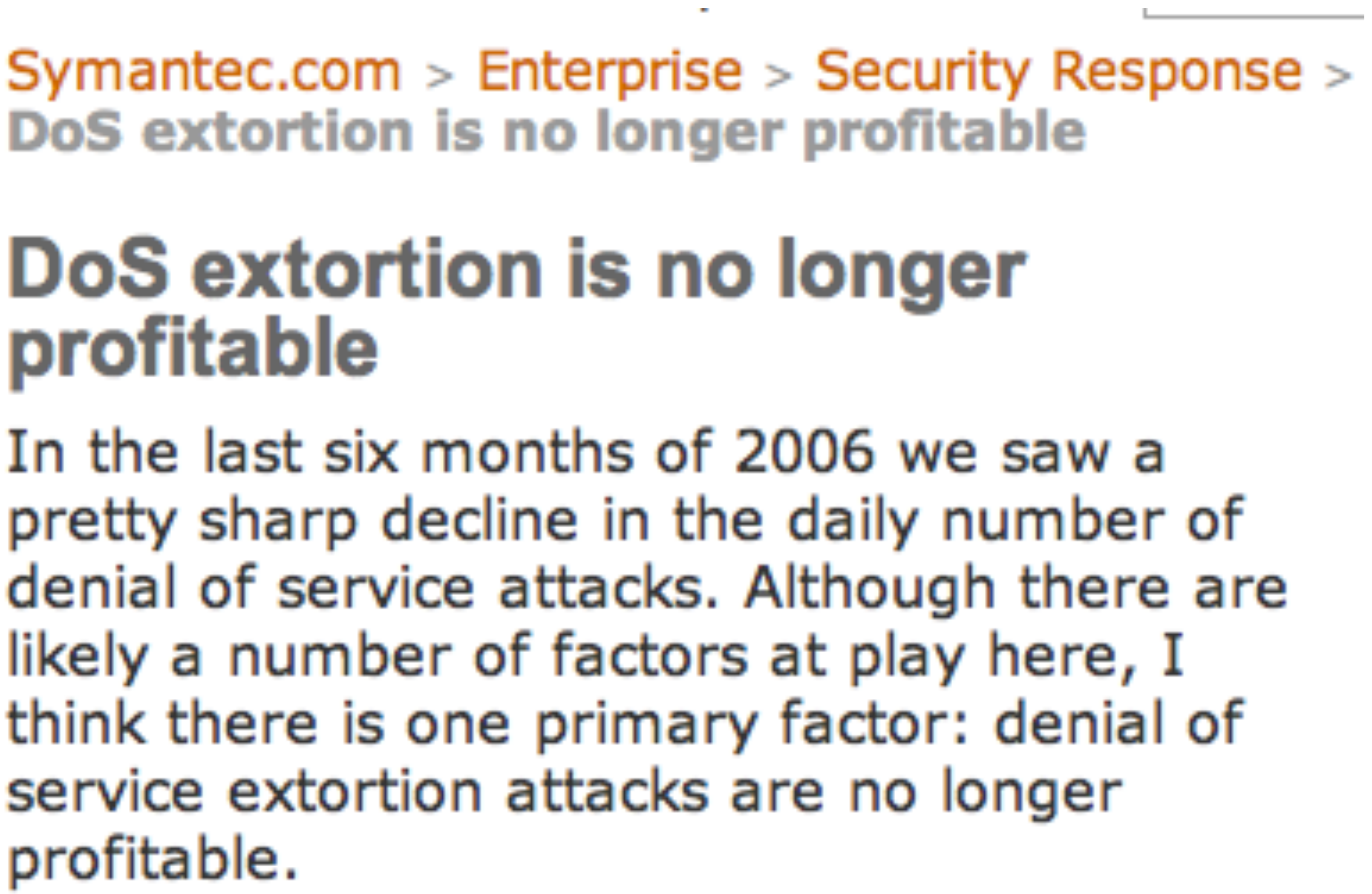
By Denise Pappalardo and Ellen Messmer, Network World, 05/16/05

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.

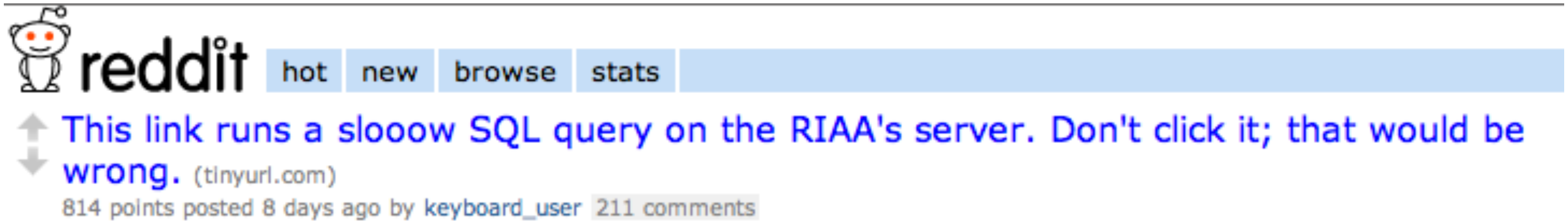
The trio concentrated on U.K. Internet gambling sites, according to the prosecution. One bookmaker, which refused to pay a demand for $10,000, was attacked and brought offline--which reportedly cost it more than $200,000 a day in lost business.



Symantec.com > Enterprise > Security Response > DoS extortion is no longer profitable

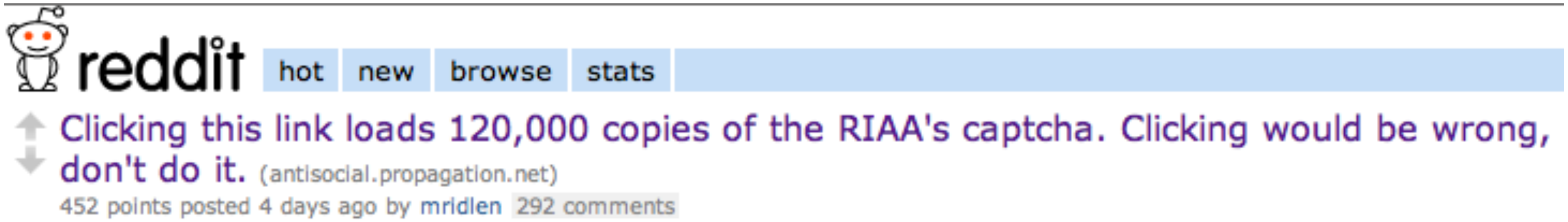
DoS extortion is no longer profitable

In the last six months of 2006 we saw a pretty sharp decline in the daily number of denial of service attacks. Although there are likely a number of factors at play here, I think there is one primary factor: denial of service extortion attacks are no longer profitable.



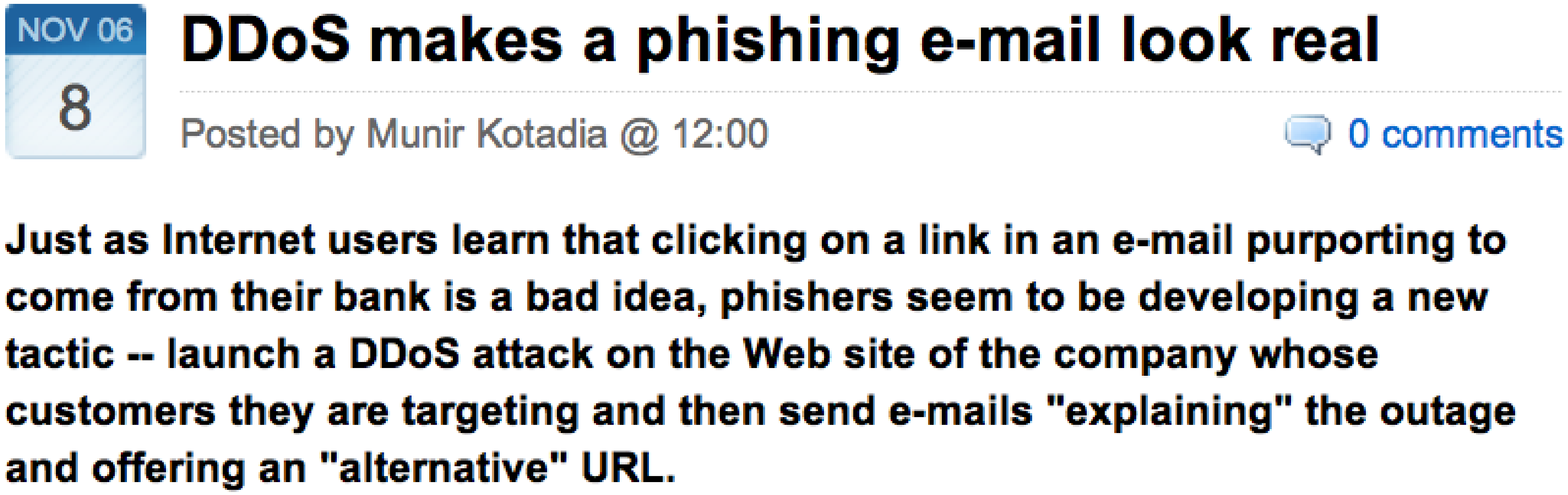
This link runs a slooow SQL query on the RIAA's server. Don't click it; that would be wrong. (tinyurl.com)

814 points posted 8 days ago by keyboard_user 211 comments



Clicking this link loads 120,000 copies of the RIAA's captcha. Clicking would be wrong, don't do it. (antisocial.propagation.net)

452 points posted 4 days ago by mrdlen 292 comments



NOV 06

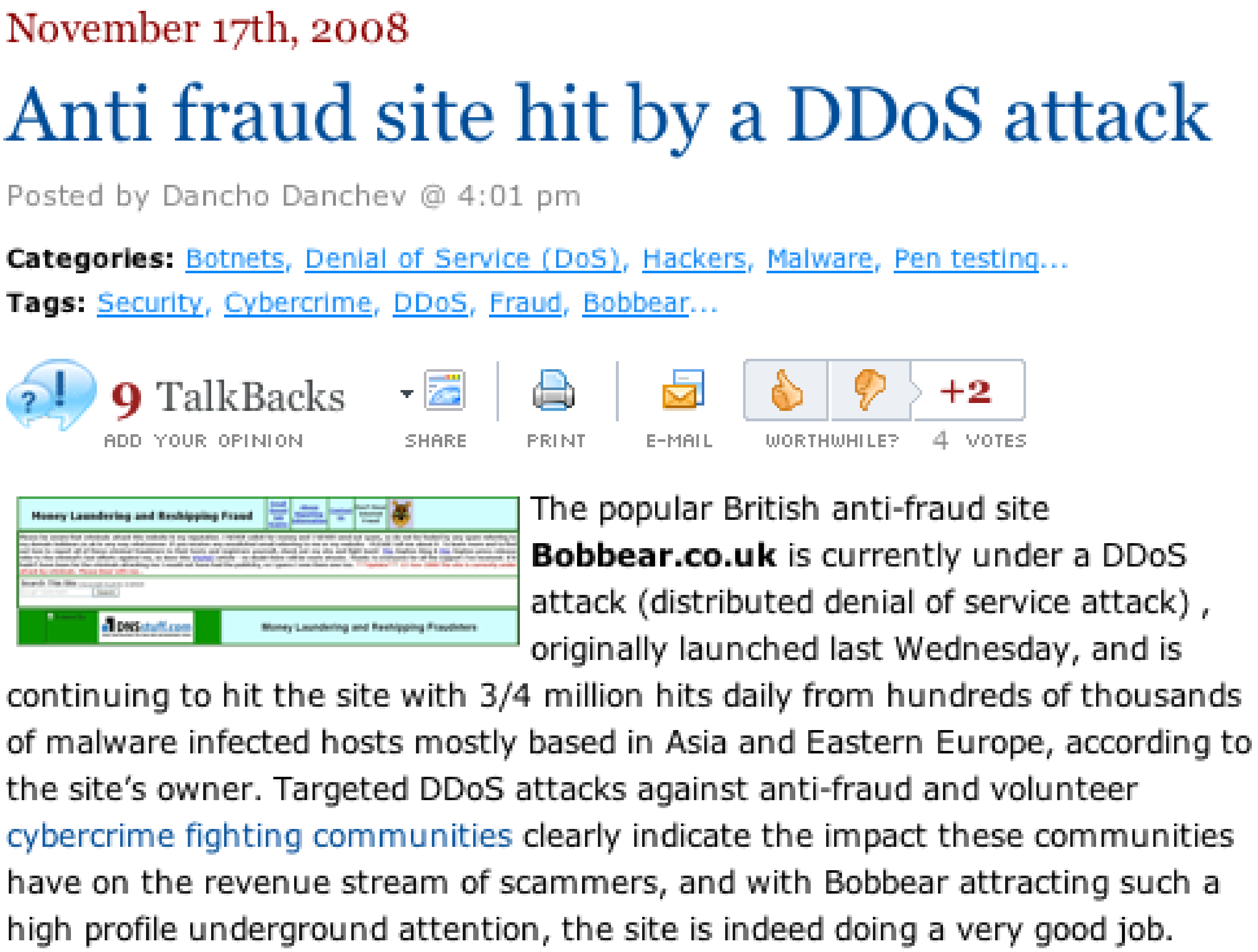
8

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.

UK Anti-Fraud Crusader BobBear STILL Under Attack. No Abatement.

By Marc Handelman on December 8th, 2008

0 tweet

BobBear, an anti-fraud site based in the UK is still (*first reported here at Infosecurity.US on November 19th*) under constant distributed denial of service attack (**DDoS**), reports The Shadowserver Foundation. More information regarding BobBear, and the unfortunate attacks they are being subjected to appears after the break.

Russia accused of unleashing cyberwar to disable Estonia

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

Ian Traynor in Brussels
Thursday May 17, 2007
The Guardian

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.

Kremlin-backed youths launched Estonian cyberwar, says Russian official

Mea Culpa without the *culpa*

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 11th March 2009 19:11 GMT

Members of a Kremlin-backed youth group spearheaded the cyberattacks that paralyzed Estonia's internet traffic in May of 2007, a Russian government official has admitted.

Until recently, Russia has denied any involvement in the DDoS (or distributed denial of service) attacks, which followed a diplomatic row between the two countries. But in an interview with *The Financial Times*, a "commissar" in a Kremlin-backed youth group known as Nashe unapologetically said he and other associates were behind the month-long assault.

"I wouldn't have called it a cyber attack; it was cyber defence," the official, Konstantin Goloskokov, told the paper. "We taught the Estonian

Kids responsible for Estonia attack

Author: Ian Grant
Posted: 15:25 13 Mar 2009
Topics: Security

The distributed denial of service attack that took down Estonia was run by a bunch of kids, it has emerged.

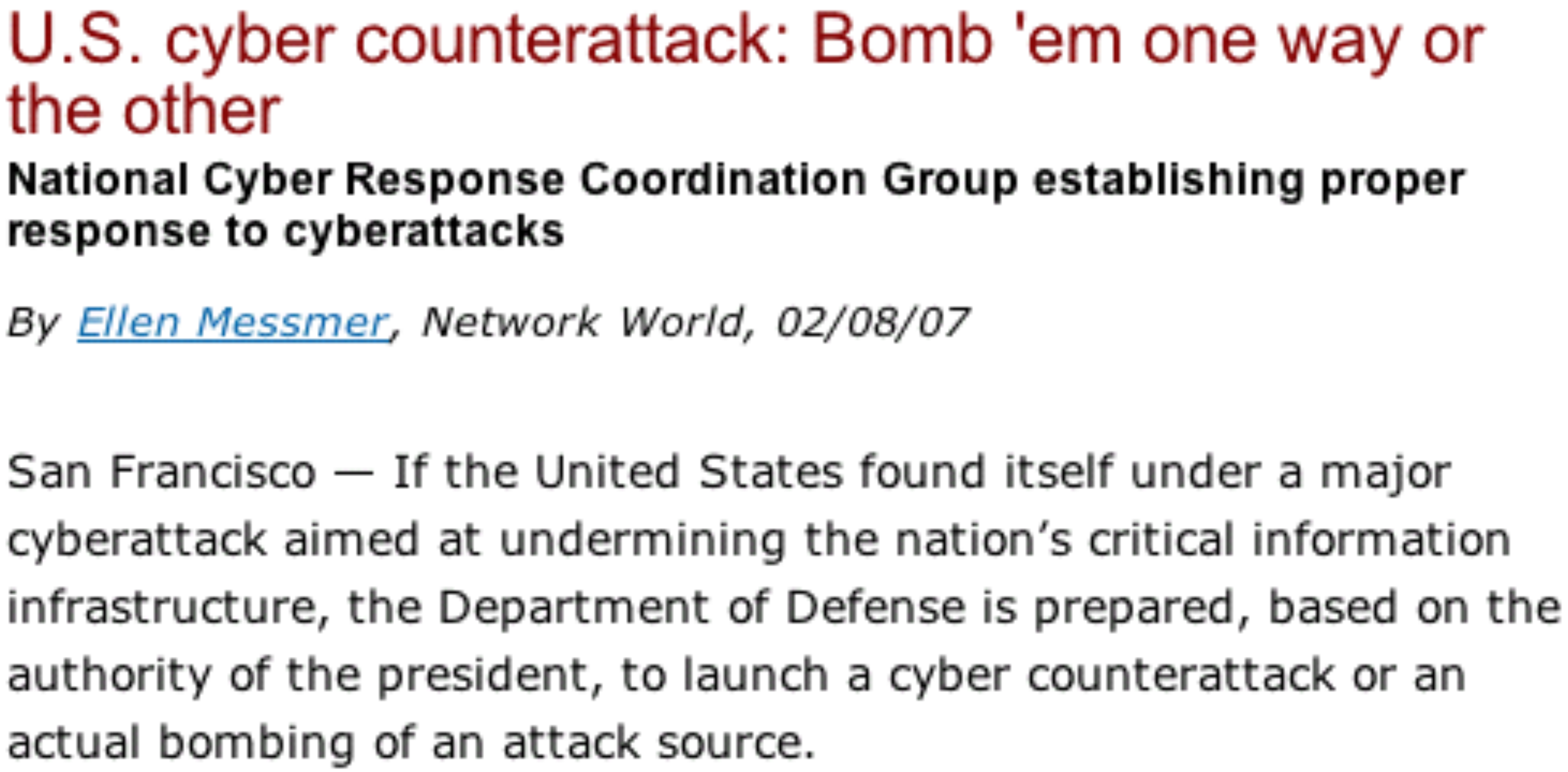
Two years ago, the former Soviet satellite found its banking and government websites paralysed for several weeks by a distributed denial-of-service (DDoS) attack.

The incident prompted a massive reorganisation and upgrade of network security and early warning systems among Nato members, and Nato even set up a cyber-security research house in Estonia.

At the time Russia was suspected of orchestrating the attack, but Moscow always denied it, and indeed Estonian officials never accused the Kremlin directly.

Yesterday, Konstantin Goloskokov (22) claimed he and some friends set up the attack to protest the removal of a Red Army monument from a downtown site in Estonia's capital Tallinn. The move had earlier led to rioting by pro-Soviet protesters.

Goloskokov told Reuters the attack was an act of civil disobedience, and, therefore, completely legal. "I was not involved in any cyber-attack," he said.

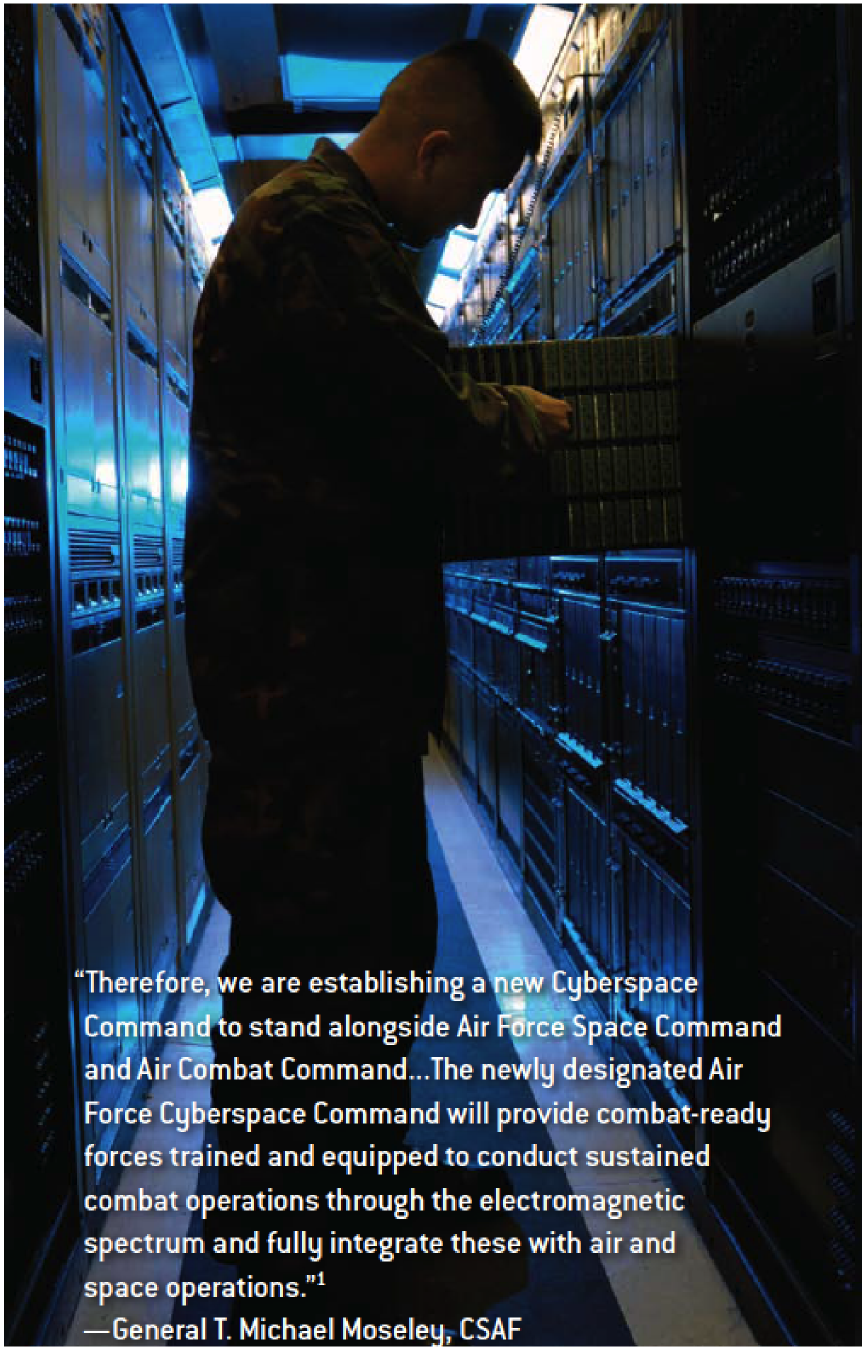


U.S. cyber counterattack: Bomb 'em one way or the other

National Cyber Response Coordination Group establishing proper response to cyberattacks

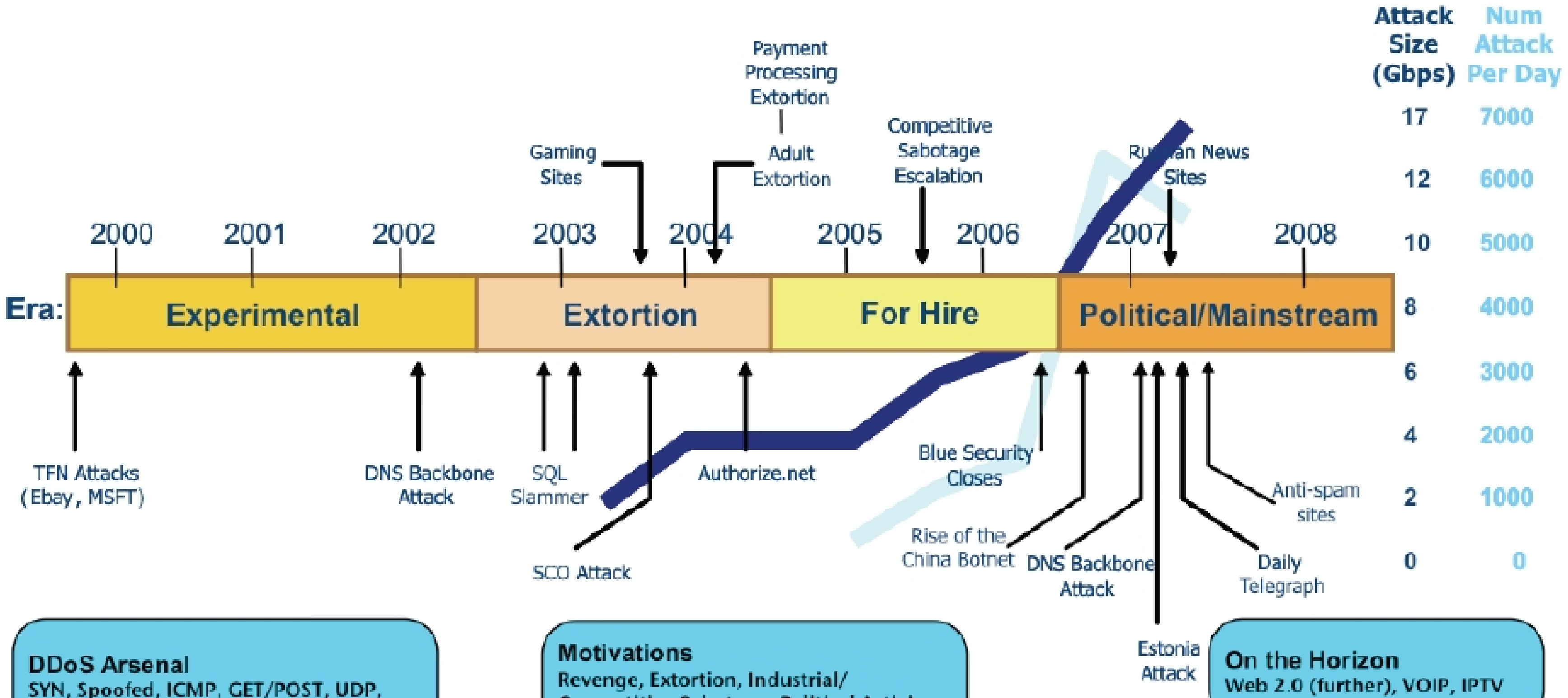
By Ellen Messmer, Network World, 02/08/07

San Francisco — If the United States found itself under a major cyberattack aimed at undermining the nation’s critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source.



"Therefore, we are establishing a new Cyberspace Command to stand alongside Air Force Space Command and Air Combat Command…The newly designated Air Force Cyberspace Command will provide combat-ready forces trained and equipped to conduct sustained combat operations through the electromagnetic spectrum and fully integrate these with air and space operations."[1]

—General T. Michael Moseley, CSAF

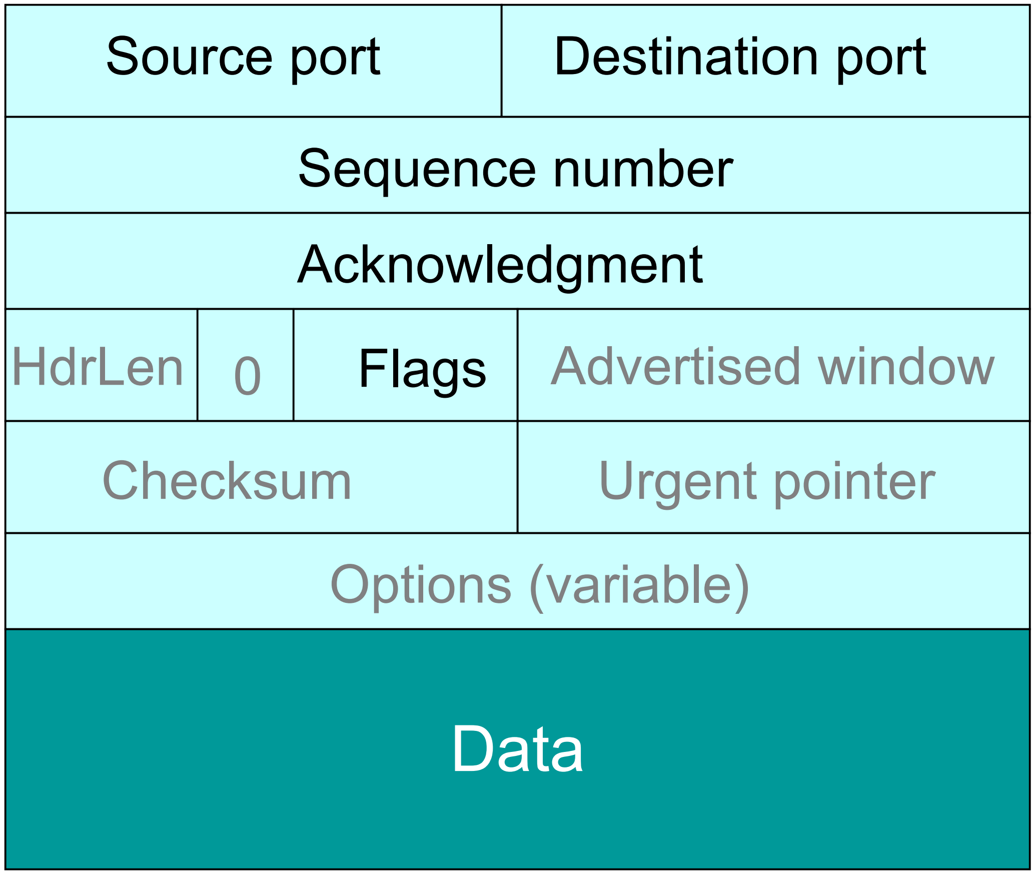


DDoS Arsenal
SYN, Spoofed, ICMP, GET/POST, UDP, Bad Protocols, Connection Floods, Application Back-end, P2P, Browser Malware

Motivations
Revenge, Extortion, Industrial/ Competitive Sabotage, Political Activism, Terrorism

On the Horizon
Web 2.0 (further), VOIP, IPTV

TCP Header



Source port

Destination port

Sequence number

Acknowledgment

HdrLen

0

Flags

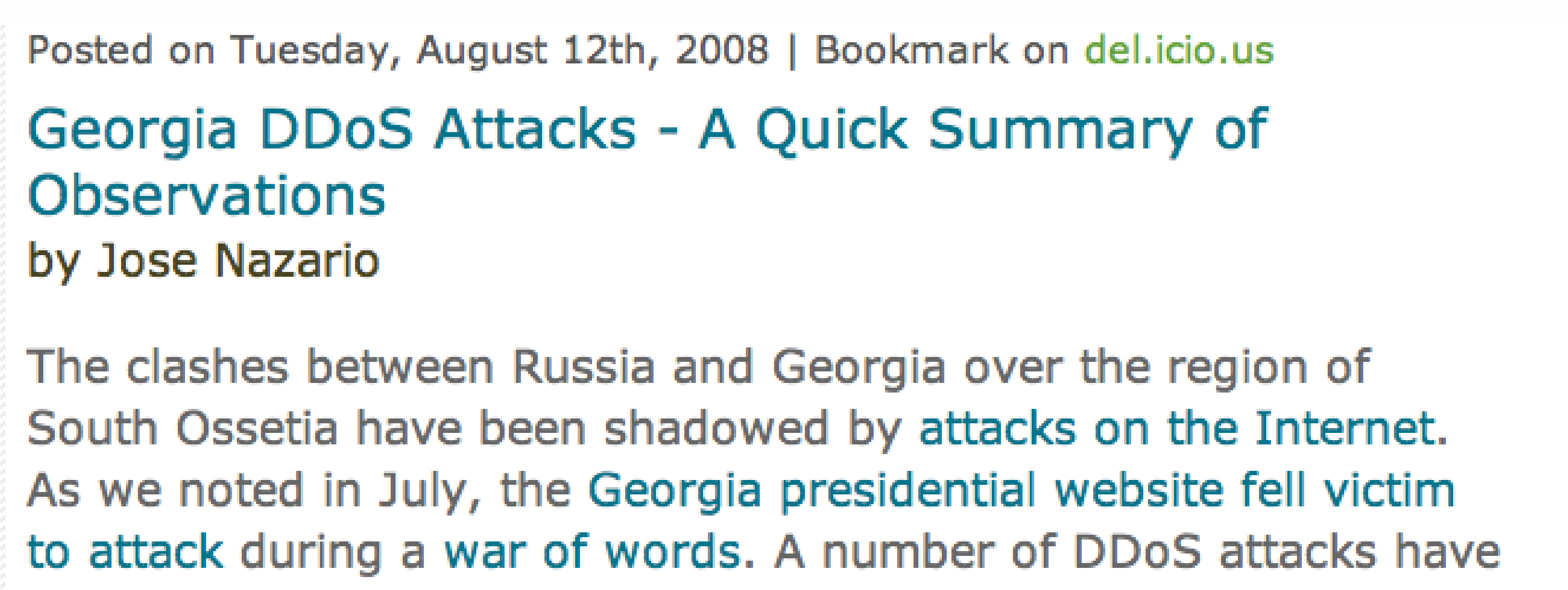
Advertised window

Checksum

Urgent pointer

Options (variable)

Data

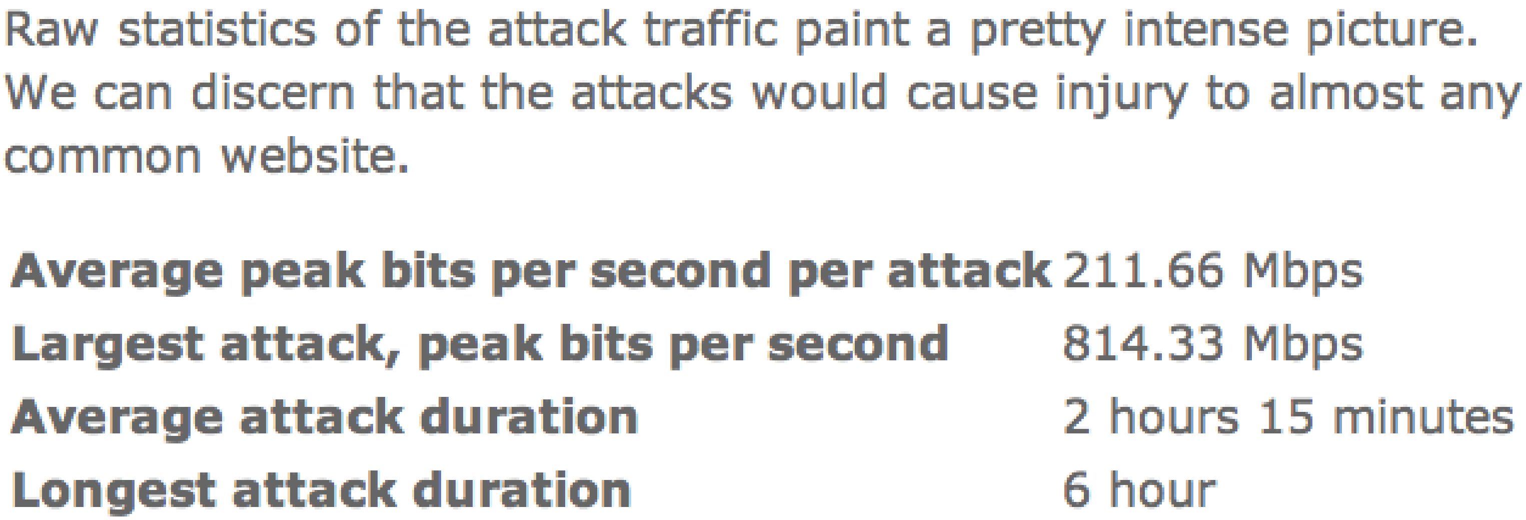


Posted on Tuesday, August 12th, 2008 | Bookmark on del.icio.us

Georgia DDoS Attacks - A Quick Summary of Observations

by Jose Nazario

The clashes between Russia and Georgia over the region of South Ossetia have been shadowed by attacks on the Internet. As we noted in July, the Georgia presidential website fell victim to attack during a war of words. A number of DDoS attacks have



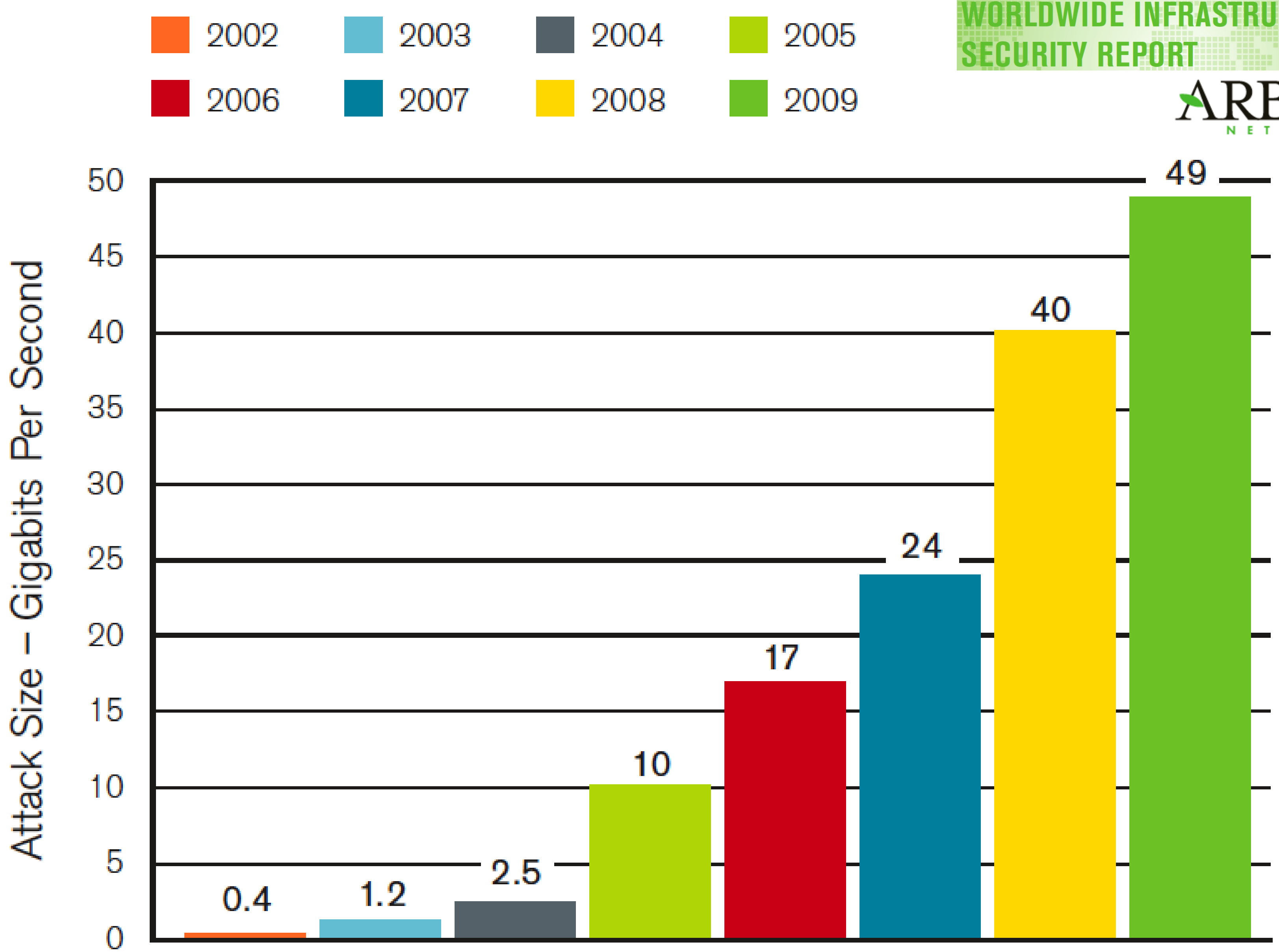
Raw statistics of the attack traffic paint a pretty intense picture. We can discern that the attacks would cause injury to almost any common website.

Average peak bits per second per attack	211.66 Mbps
Largest attack, peak bits per second	814.33 Mbps
Average attack duration	2 hours 15 minutes
Longest attack duration	6 hour

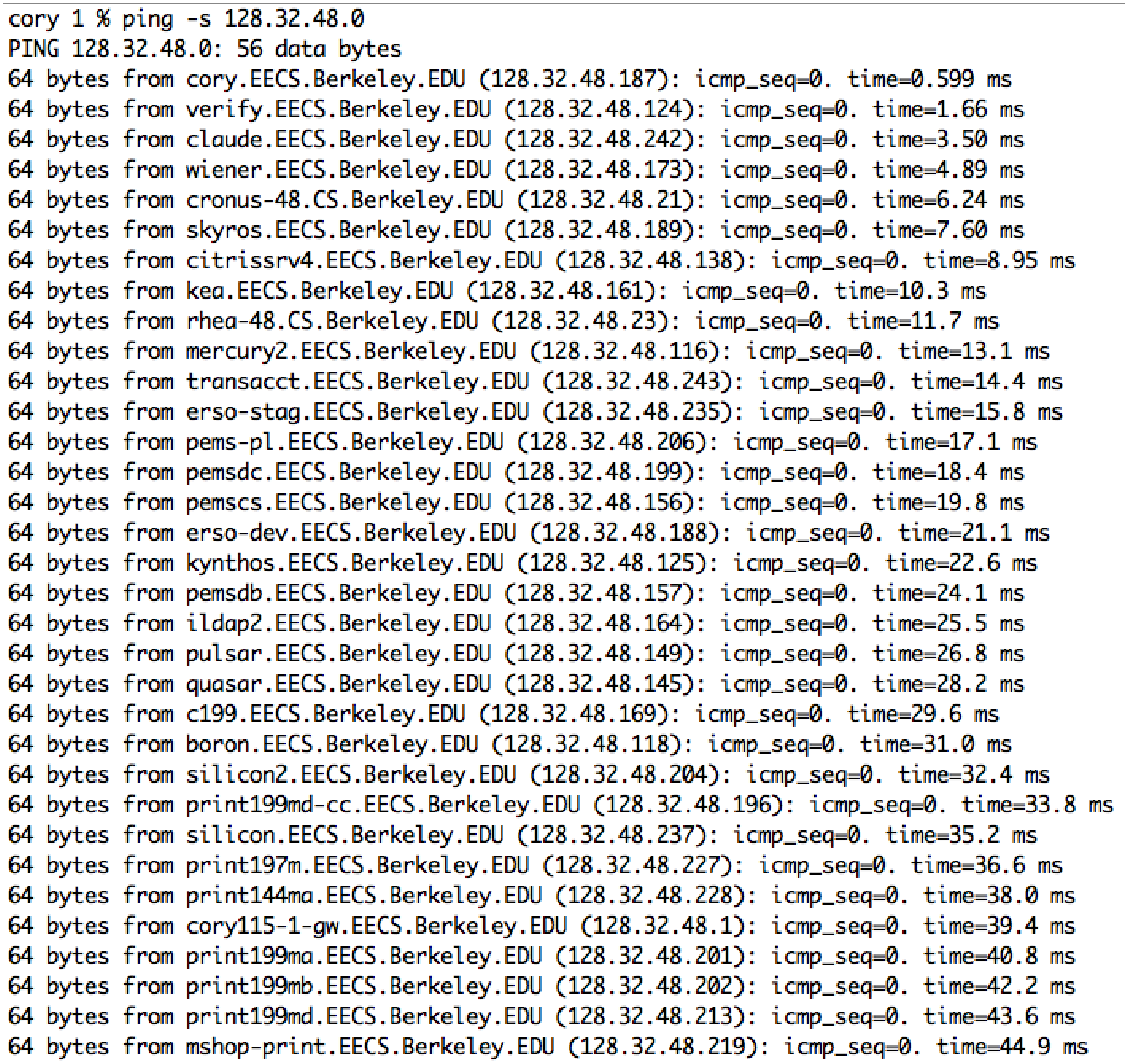
Largest DDoS Attack – 49 Gigabits Per Second

WORLDWIDE INFRASTRUCTURE SECURITY REPORT

ARBOR NETWORKS



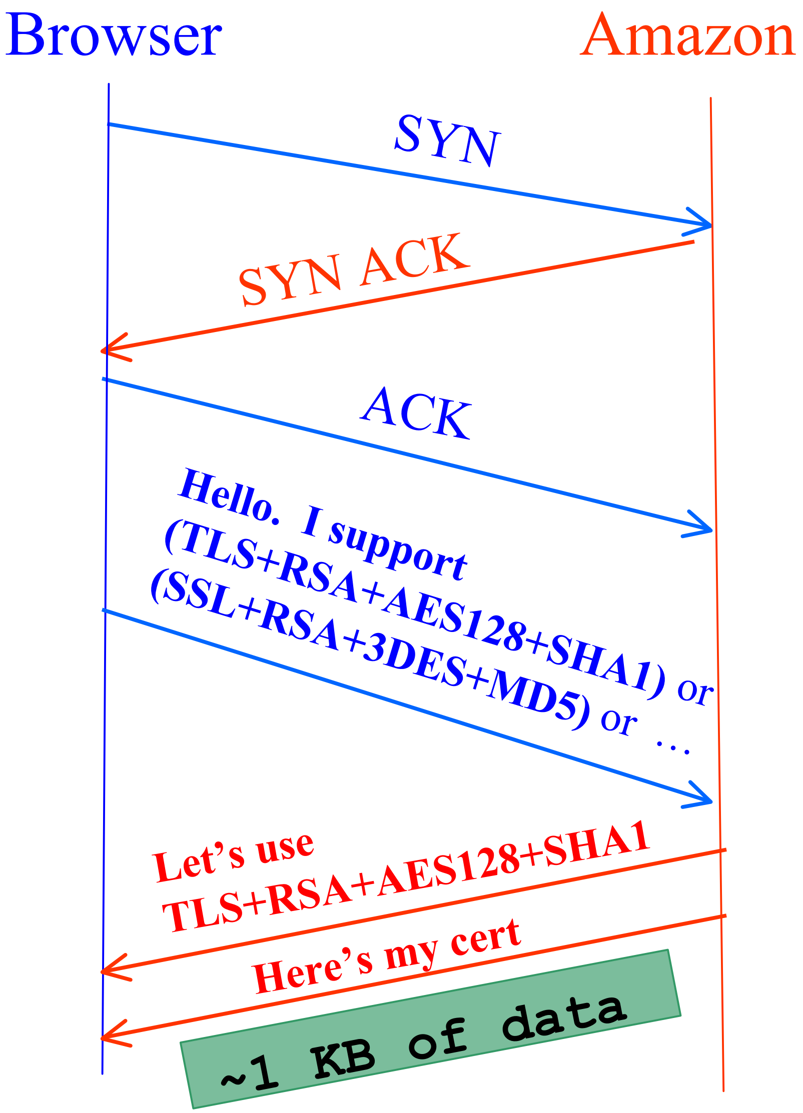
```
cory 1 % ping -s 128.32.48.0
PING 128.32.48.0: 56 data bytes
```



```
cory 1 % ping -s 128.32.48.0
PING 128.32.48.0: 56 data bytes
64 bytes from cory.EECS.Berkeley.EDU (128.32.48.187): icmp_seq=0. time=0.599 ms
64 bytes from verify.EECS.Berkeley.EDU (128.32.48.124): icmp_seq=0. time=1.66 ms
64 bytes from claude.EECS.Berkeley.EDU (128.32.48.242): icmp_seq=0. time=3.50 ms
64 bytes from wiener.EECS.Berkeley.EDU (128.32.48.173): icmp_seq=0. time=4.89 ms
64 bytes from cronus-48.CS.Berkeley.EDU (128.32.48.21): icmp_seq=0. time=6.24 ms
64 bytes from skyros.EECS.Berkeley.EDU (128.32.48.189): icmp_seq=0. time=7.60 ms
64 bytes from citrissrv4.EECS.Berkeley.EDU (128.32.48.138): icmp_seq=0. time=8.95 ms
64 bytes from kea.EECS.Berkeley.EDU (128.32.48.161): icmp_seq=0. time=10.3 ms
64 bytes from rhea-48.CS.Berkeley.EDU (128.32.48.23): icmp_seq=0. time=11.7 ms
64 bytes from mercury2.EECS.Berkeley.EDU (128.32.48.116): icmp_seq=0. time=13.1 ms
64 bytes from transacct.EECS.Berkeley.EDU (128.32.48.243): icmp_seq=0. time=14.4 ms
64 bytes from erso-stag.EECS.Berkeley.EDU (128.32.48.235): icmp_seq=0. time=15.8 ms
64 bytes from pems-pl.EECS.Berkeley.EDU (128.32.48.206): icmp_seq=0. time=17.1 ms
64 bytes from pemsdc.EECS.Berkeley.EDU (128.32.48.199): icmp_seq=0. time=18.4 ms
64 bytes from pemscs.EECS.Berkeley.EDU (128.32.48.156): icmp_seq=0. time=19.8 ms
64 bytes from erso-dev.EECS.Berkeley.EDU (128.32.48.188): icmp_seq=0. time=21.1 ms
64 bytes from kynthos.EECS.Berkeley.EDU (128.32.48.125): icmp_seq=0. time=22.6 ms
64 bytes from pemsdb.EECS.Berkeley.EDU (128.32.48.157): icmp_seq=0. time=24.1 ms
64 bytes from ildap2.EECS.Berkeley.EDU (128.32.48.164): icmp_seq=0. time=25.5 ms
64 bytes from pulsar.EECS.Berkeley.EDU (128.32.48.149): icmp_seq=0. time=26.8 ms
64 bytes from quasar.EECS.Berkeley.EDU (128.32.48.145): icmp_seq=0. time=28.2 ms
64 bytes from c199.EECS.Berkeley.EDU (128.32.48.169): icmp_seq=0. time=29.6 ms
64 bytes from boron.EECS.Berkeley.EDU (128.32.48.118): icmp_seq=0. time=31.0 ms
64 bytes from silicon2.EECS.Berkeley.EDU (128.32.48.204): icmp_seq=0. time=32.4 ms
64 bytes from print199md-cc.EECS.Berkeley.EDU (128.32.48.196): icmp_seq=0. time=33.8 ms
64 bytes from silicon.EECS.Berkeley.EDU (128.32.48.237): icmp_seq=0. time=35.2 ms
64 bytes from print197m.EECS.Berkeley.EDU (128.32.48.227): icmp_seq=0. time=36.6 ms
64 bytes from print144ma.EECS.Berkeley.EDU (128.32.48.228): icmp_seq=0. time=38.0 ms
64 bytes from cory115-1-gw.EECS.Berkeley.EDU (128.32.48.1): icmp_seq=0. time=39.4 ms
64 bytes from print199ma.EECS.Berkeley.EDU (128.32.48.201): icmp_seq=0. time=40.8 ms
64 bytes from print199mb.EECS.Berkeley.EDU (128.32.48.202): icmp_seq=0. time=42.2 ms
64 bytes from print199md.EECS.Berkeley.EDU (128.32.48.213): icmp_seq=0. time=43.6 ms
64 bytes from mshop-print.EECS.Berkeley.EDU (128.32.48.219): icmp_seq=0. time=44.9 ms
```

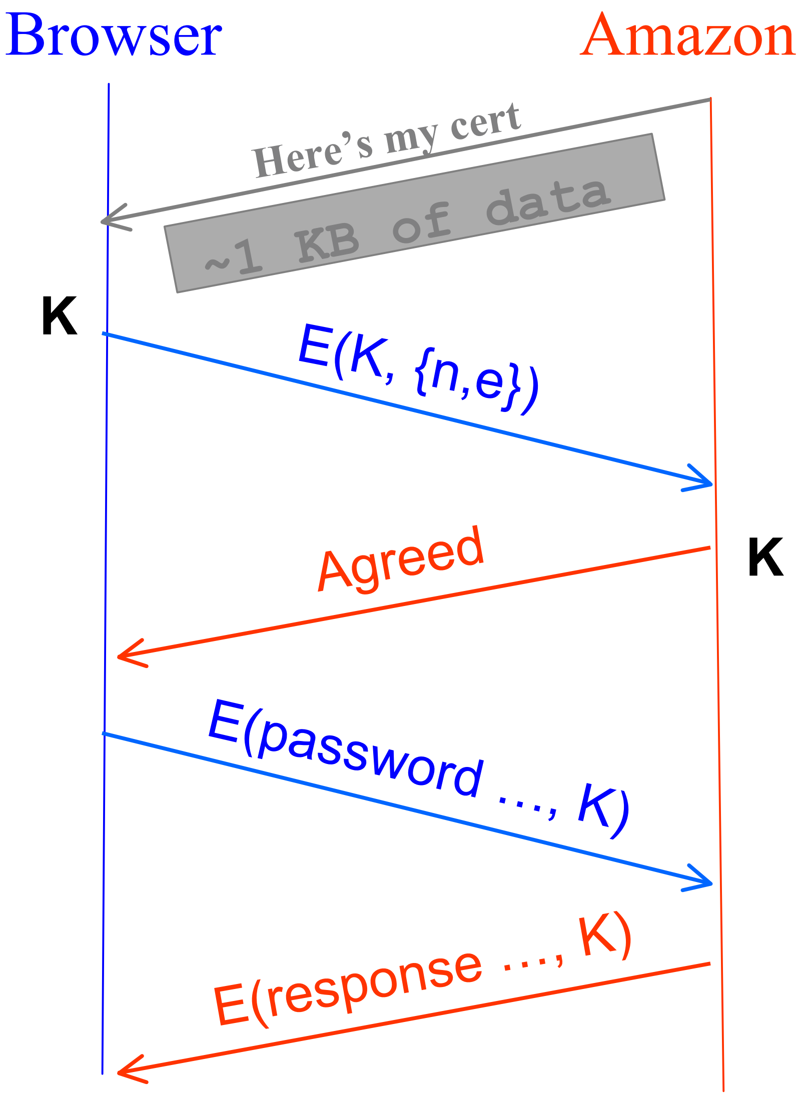
SSL/TLS Handshake

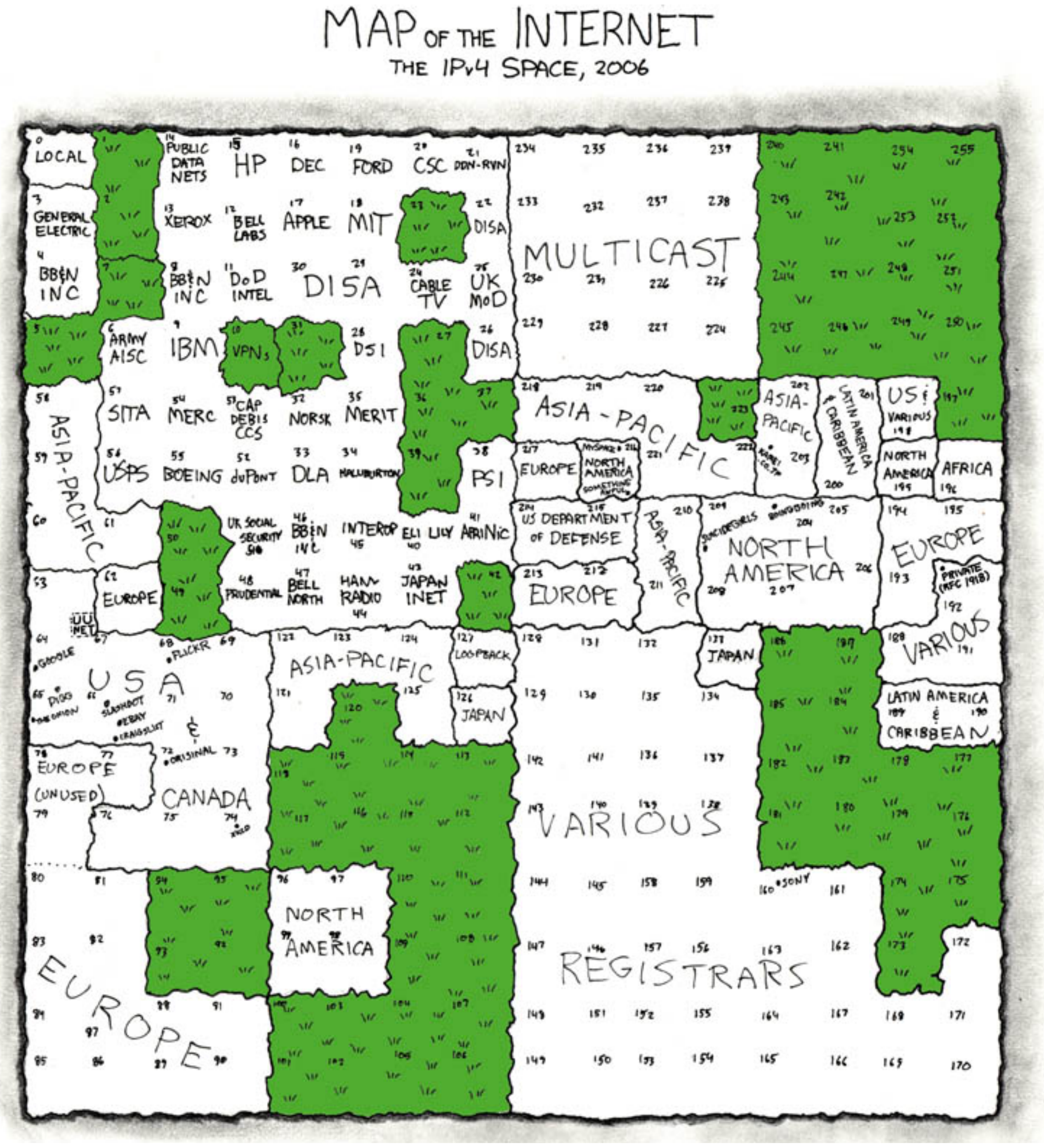
- Browser (client) connects via TCP to Amazon's **`HTTPS`** server
- Client sends over list of crypto protocols it supports
- Server picks protocols to use for this session
- Server sends over its certificate
- (all of this is in the clear)



SSL/TLS Handshake, con’t

- Browser constructs a random *session key* K
- Browser encrypts K using Amazon’s public key
- Browser sends E(K, {**n**, **e**}) to server
- Browser displays 🔒
- All subsequent communication encrypted w/ symmetric cipher (e.g., AES128) using key K
  - E.g., client can authenticate using a password





Interactive Map

Packet sent	Response from victim
TCP SYN (to open port)	TCP SYN/ACK
TCP SYN (to closed port)	TCP RST (ACK)
TCP ACK	TCP RST (ACK)
TCP DATA	TCP RST (ACK)
TCP RST	no response
TCP NULL	TCP RST (ACK)
ICMP ECHO Request	ICMP Echo Reply
ICMP TS Request	ICMP TS Reply
UDP pkt (to open port)	protocol dependent
UDP pkt (to closed port)	ICMP Port Unreach
...	...

Table 1: A sample of victim responses to typical attacks.

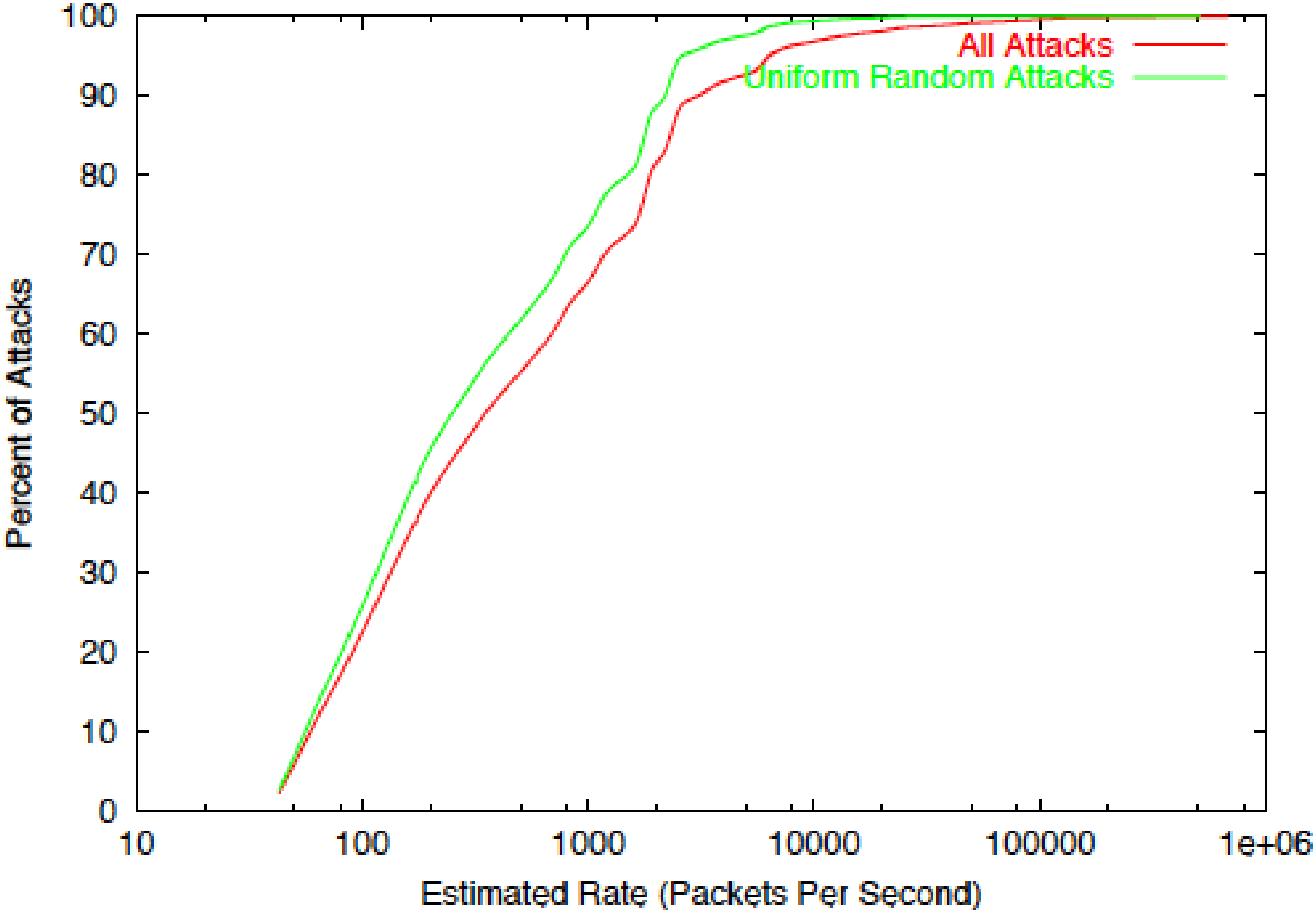


Figure 4: Cumulative distributions of estimated attack rates in packets per second.