

Most Significant Operational Threats

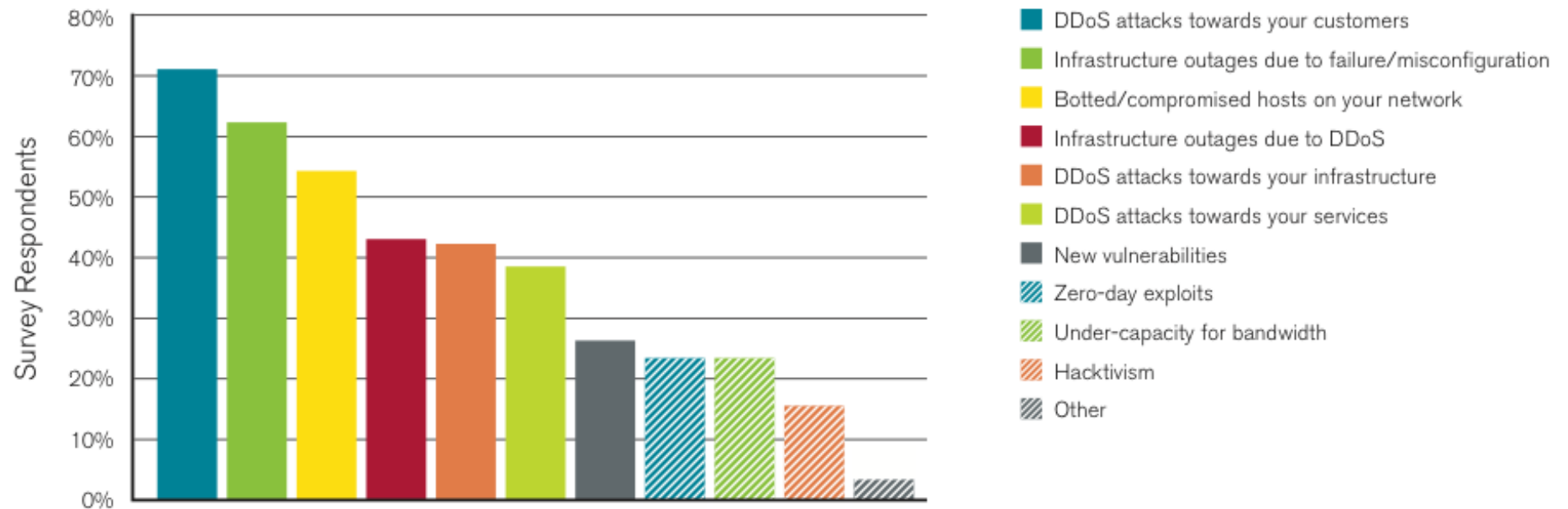


Figure 6 Source: Arbor Networks, Inc.

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.



reddit

hot

new

browse

stats



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



reddit

hot

new

browse

stats



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 mridlen 292 comments

December 8, 2010, 4:18 PM

'Operation Payback' Attacks Fell Visa.com

By ROBERT MACKEY



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

Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey[†]

The Berkman Center for Internet & Society at Harvard University

December 2010

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	

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



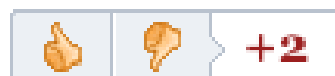
SHARE



PRINT



E-MAIL



WORTHWHILE?

4 VOTES



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.

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](#)

 Follow @KimZetter

120

 Tweet

0

+1



 Share

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.

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

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.

Coordinated Russia vs Georgia cyber attack in progress

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 race in order to disseminate real-time information by moving to a Blogger account

[illegible]

News

American Forces Press Service

 [SHARE](#)

NEWS ARTICLE

[E-MAIL A COPY](#) | [PRINTER FRIENDLY](#) | [LATEST NEWS](#)

Mullen Offers 40-year Perspective on Social, Military Issues

By Karen Parrish
American Forces Press Service

WASHINGTON, Sept. 20, 2011 – As the last month ticks down in a career that began with his graduation from the U.S. Naval Academy in 1968, Navy Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, today offered his view of how war, peace, society and the world have changed over those 40-plus years.

He's seen some of the most significant military changes ever during his tenure as chairman, he told the audience gathered here at the Carnegie Endowment for International Peace.

"I talk about two existential threats to the United States right now," he said. "One is obviously the nuclear weapons that exist in Russia; we think that we've got that well controlled inside the [current strategic arms reduction, or New START] treaty and inside the relationship."

The other is cyber attacks, which "I think ... actually can bring us to our knees," he added.

The cyber threat has no boundaries or rules, and can issue from other nations, nongovernment actors – "You pick it," – but the danger it poses warrants a structure of doctrine and regulation like that used to control the nuclear threat, he said.

"We're a long way from that right now," he said.

It Begins: Military's Cyberwar Command Is Fully Operational

By [Spencer Ackerman](#)  November 4, 2010 | 12:00 am | Categories: [Spies](#), [Secrecy and Surveillance](#)

 Follow @attackerman

92

0



 Tweet

+1

 Share

 Like

 Send

 127 likes. [Sign Up](#) to see what your friends like.



Fifteen thousand military computer networks became protected on November 3, 2010. Those ensconced within the informational phalanx [called the event Cyber Command Day](#). They lived only to face a new challenge — the war against the Machines.

In truth, yesterday wasn't quite so dramatic. The Department of Defense announced that the military's new command for protecting its networks against cyberassault had achieved "[full operational capability](#)," meaning the new U.S. Cyber Command, which [opened for business in May](#), is 100 percent ready for duty, just [a month behind schedule](#). Not that "full operational capability" fills in many of the blanks about when it's acceptable for Cyber Command to attack a foreign network or how deeply it'll be involved in the civilian internet.

US general: 'We're cleared to cyber-bomb enemy hackers'

Curiously, his command website went down after he said it

By **Brid-Aine Parnell** • **[Get more from this author](#)**

Posted in [Security](#), 17th November 2011 12:51 GMT

[Free whitepaper – Cloud-ready network architecture](#)

The US military is now legally in the clear to launch offensive operations in cyberspace, the commander of the US Strategic Command has said.

"I do not believe that we need new explicit authorities to conduct offensive operations of any kind," Air Force General Robert Kehler told [Reuters](#).

But he added that the military was still figuring out the rules of engagement for cyber-warfare outside the "area of hostilities", which are the places they've already been approved to do battle in.

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.

DDoS attacks take out Asian nation

Myanmar fades to black

By [Dan Goodin in San Francisco](#) • [Get more from this author](#)

Posted in [Crime](#), 3rd November 2010 22:26 GMT

[Free whitepaper – Low-latency switches power high-frequency trading](#)

Myanmar was severed from the internet on Tuesday following more than 10 days of distributed denial of service attacks that culminated in a massive data flood that overwhelmed the Southeast Asian country's infrastructure, a researcher said.

The DDoS assault directed as much as 15 Gbps of junk data to Myanmar's main internet provider, more than 15 times bigger than the 2007 attack that [brought some official Estonian websites to their knees](#), said Craig Labovitz, a researcher at Arbor Networks. It was evenly distributed throughout Myanmar's 20 or so providers and included multiple variations,

DDoS attacks take out Asian nation

Myanmar fades to black

By [Dan Goodin in San Francisco](#) • [Get more from this author](#)

Posted in [Crime](#), 3rd November 2010 22:26 GMT

[Free whitepaper – Low-latency switches power high-frequency trading](#)

Myanmar was severed from the internet on Tuesday following more than 10 days of distributed denial of service attacks that culminated in a massive data flood that overwhelmed the Southeast Asian country's infrastructure, a researcher said.

The DDoS assault directed as much as 15 Gbps of junk data to Myanmar's main internet provider, more than 15 times bigger than the 2007 attack that [brought some official Estonian websites to their knees](#), said Craig Labovitz, a researcher at Arbor Networks. It was evenly distributed throughout Myanmar's 20 or so providers and included multiple variations,

The attacks come ahead of the November 7 general elections set by the military junta that rules Myanmar. Many critics of the government say it launched the attacks in an attempt to manipulate the outcome. Others have blamed external forces. The data flood [began 10 days ago](#), according to *The People's Daily* in China, which borders Myanmar. ®

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

[Free whitepaper – IBM System Networking RackSwitch G8124](#)

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." ®

Attack Motivations Considered Common or Very Common

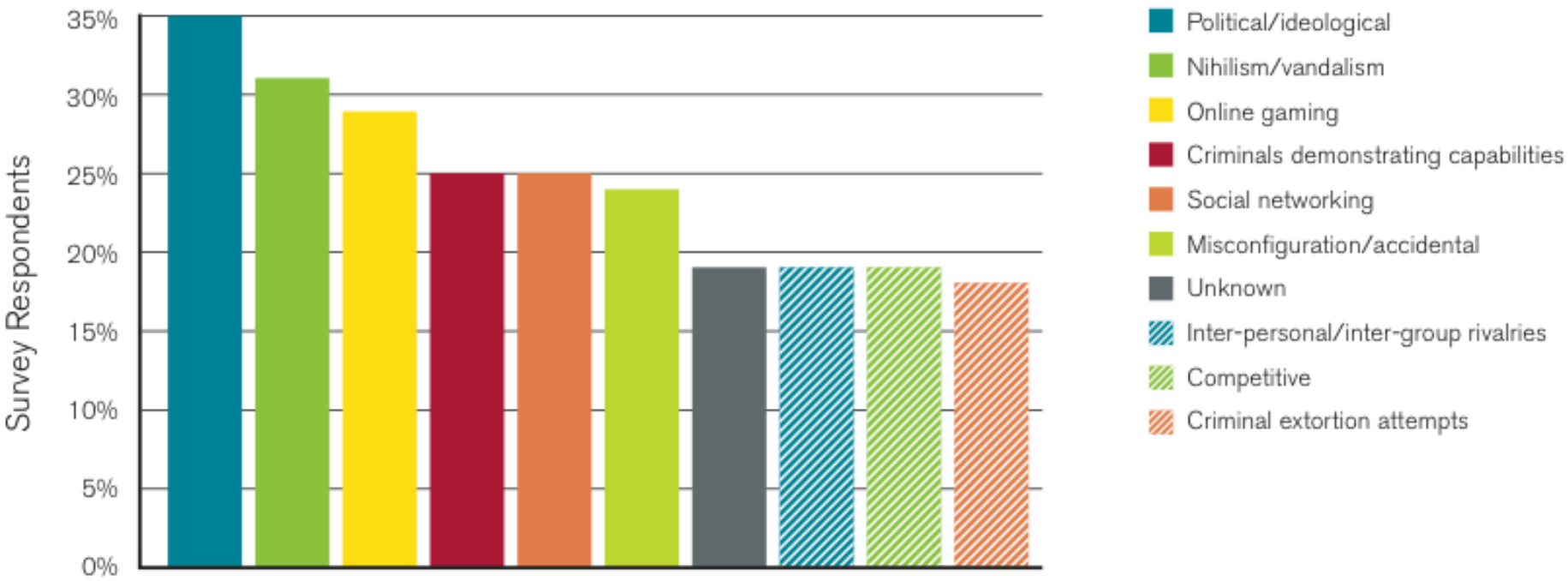


Figure 20 Source: Arbor Networks, Inc.

Average Number of DDoS Attacks per Month

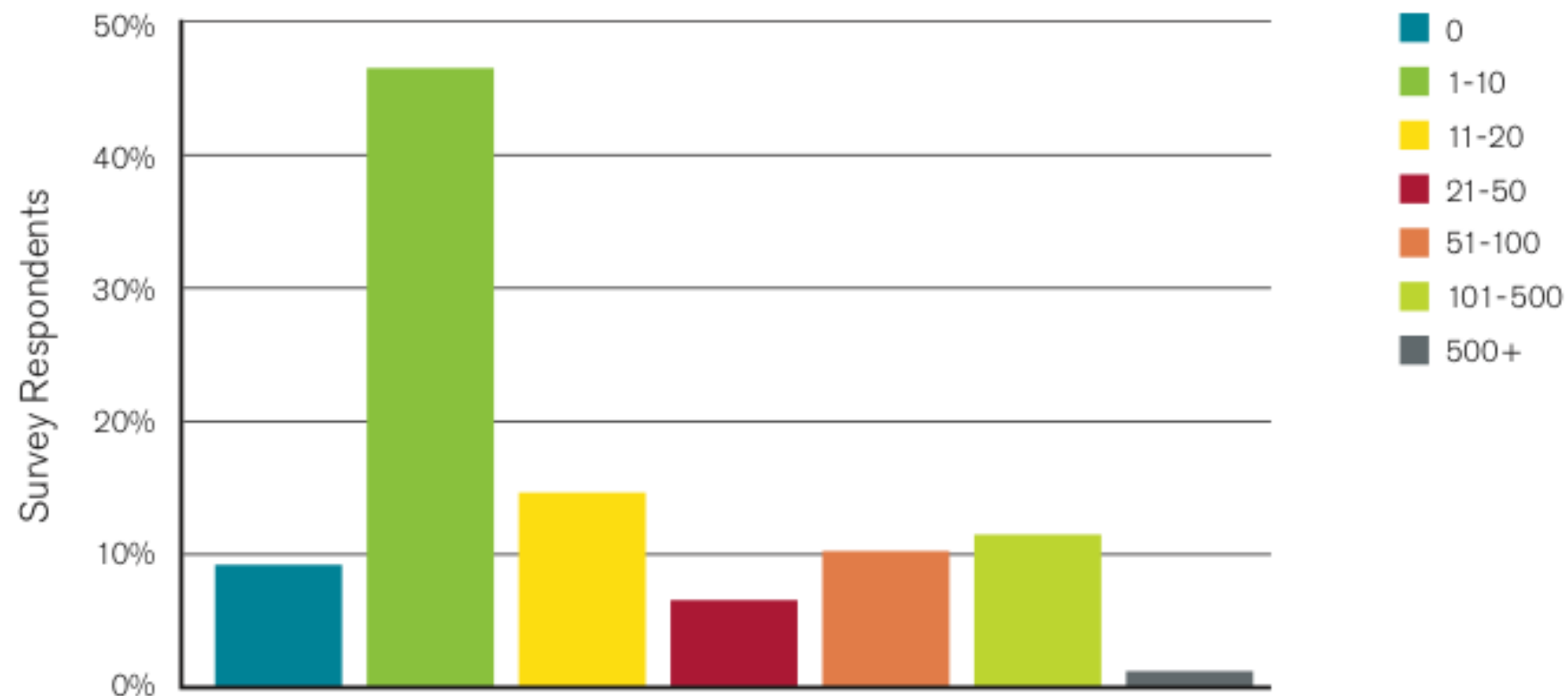


Figure 17 Source: Arbor Networks, Inc.

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 Bandwidth Attacks Reported

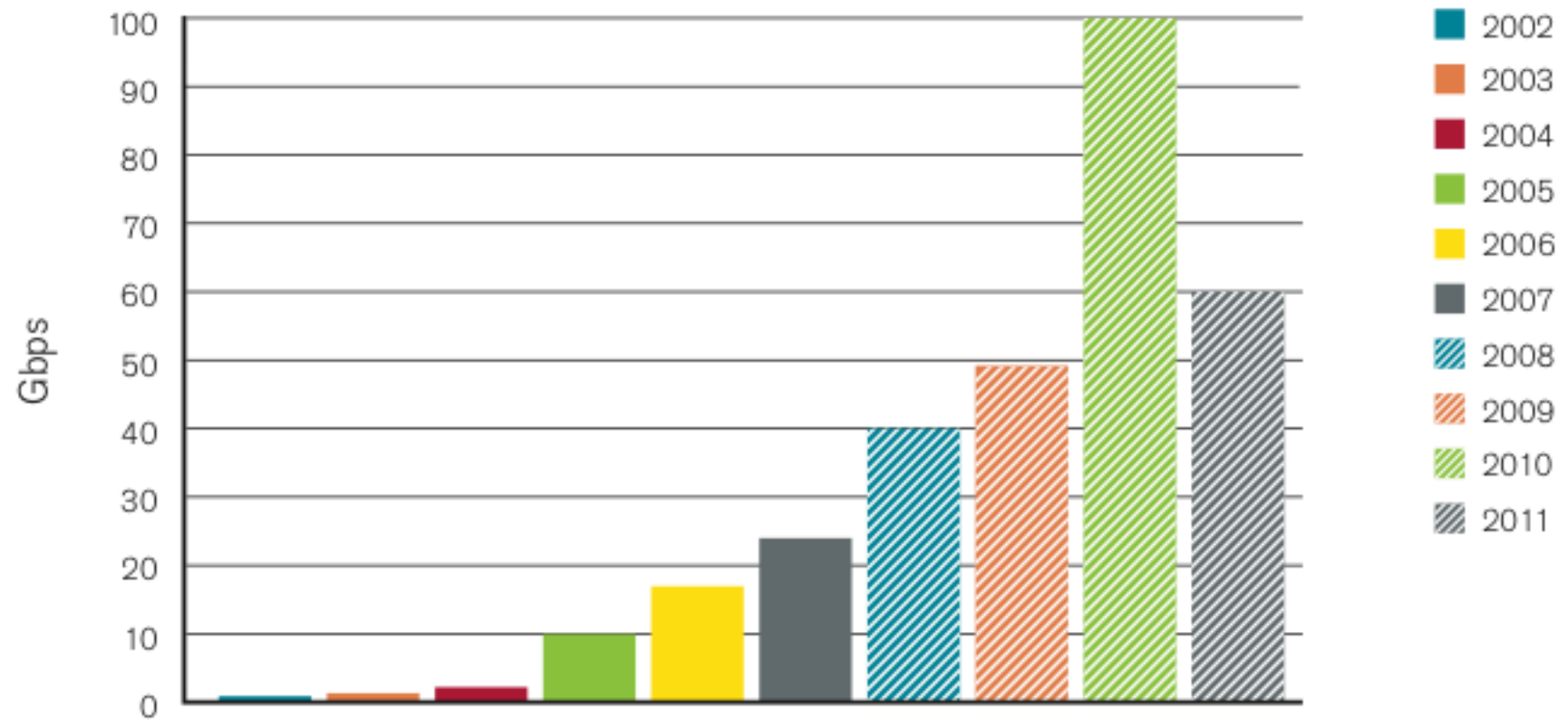


Figure 15 Source: Arbor Networks, Inc.

Application-Layer DDoS Attacks

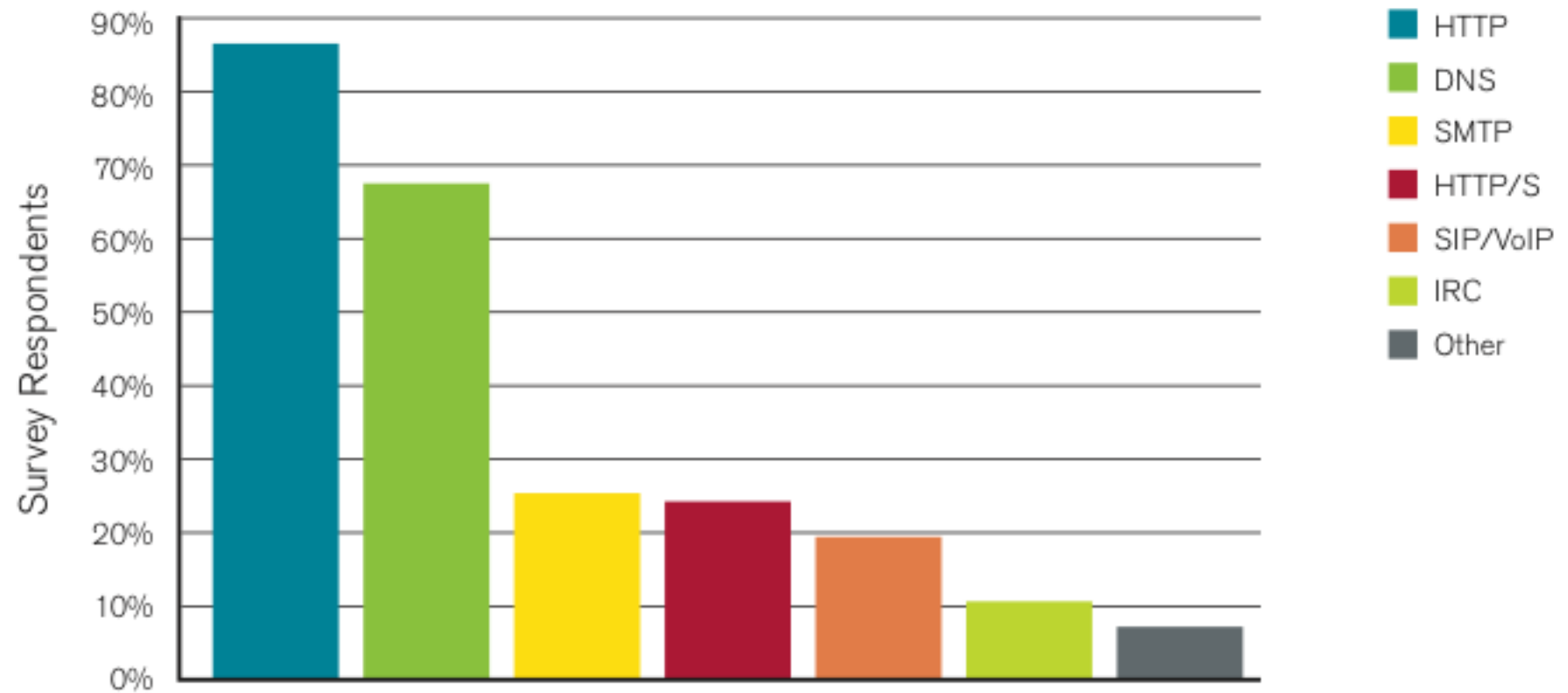
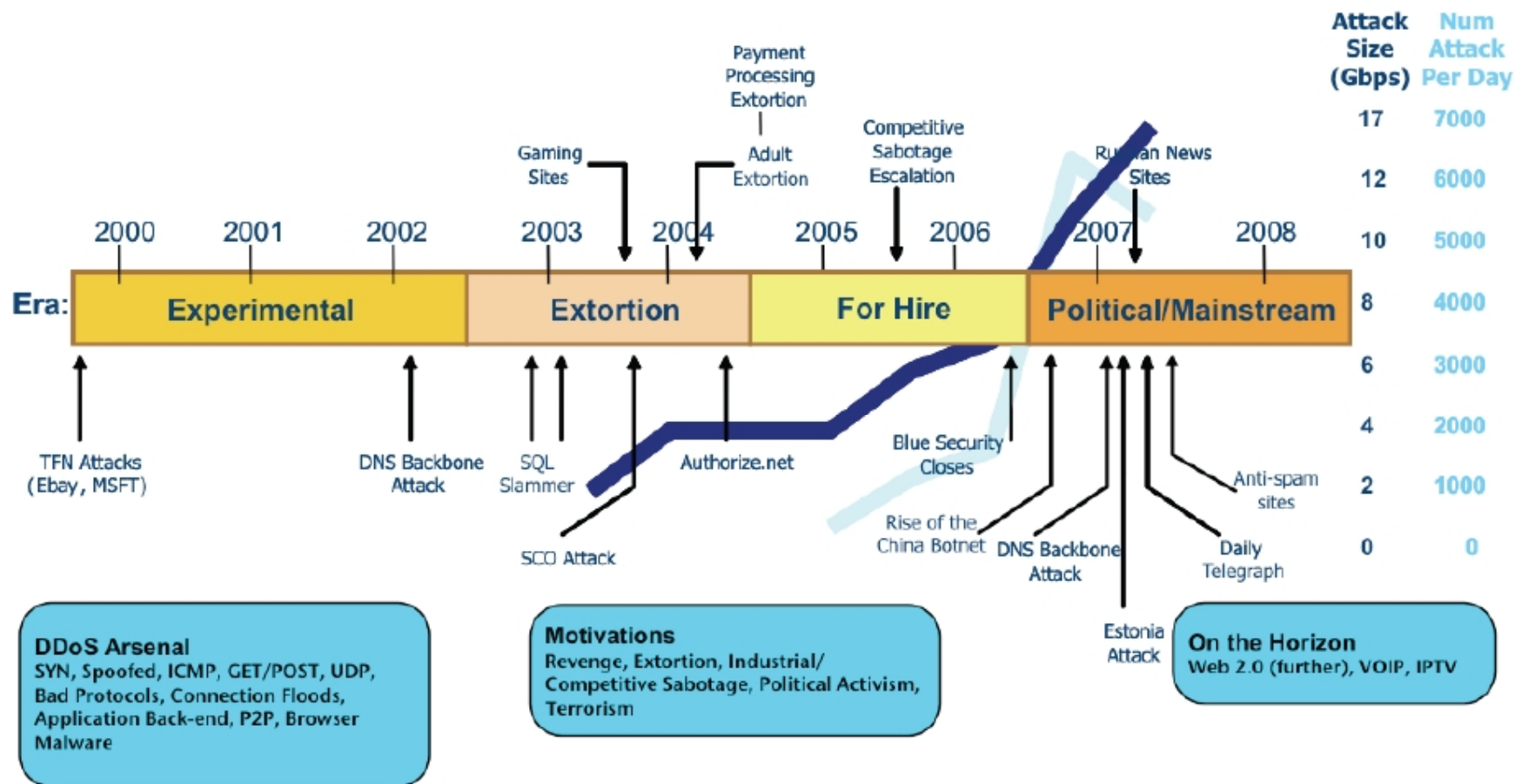


Figure 7 Source: Arbor Networks, Inc.



Krebs on Security

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.

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.



An ad for a DDoS attack service.

- “Approximately \$250,000 USD/incident.”
- “\$8,000 USD/incident.”
- “Approximately 1,000EUR/incident.”
- “Roughly \$1M USD to \$1.5M USD/incident.”
- “\$300,000 USD/incident.”
- “\$1M USD/incident.”
- “More than \$100,000 USD/month.”
- “Net revenue-generator—we offer commercial DDoS mitigation services.”



July 4th DDoS Attack Timeline

Multi-Phased Attack



1st Wave of Elevated Traffic

- 1 Day Duration
- 7.4 Billion Total Page Views
- 192.5 TB Served
- Equal 12 OC-192's & 2,500 Servers
- 99.9% BW, 96.2% Request Offload

Subsequent Waves of Elev Traffic

- Next 3 Days of Attack
- 726.6 Million Total Page Views
- 42.2 TB Served

"The first list had only five targets — all U.S. government sites. A second list used by the malware on July 6 had 21 targets, all U.S. government and commercial sector sites, including e-commerce and media sites. A list on the 7th switched out some of the U.S. sites for ones in South Korea. ...- Joe Stewart, director of malware research at SecureWorks

DDoS Mitigation Tools Used

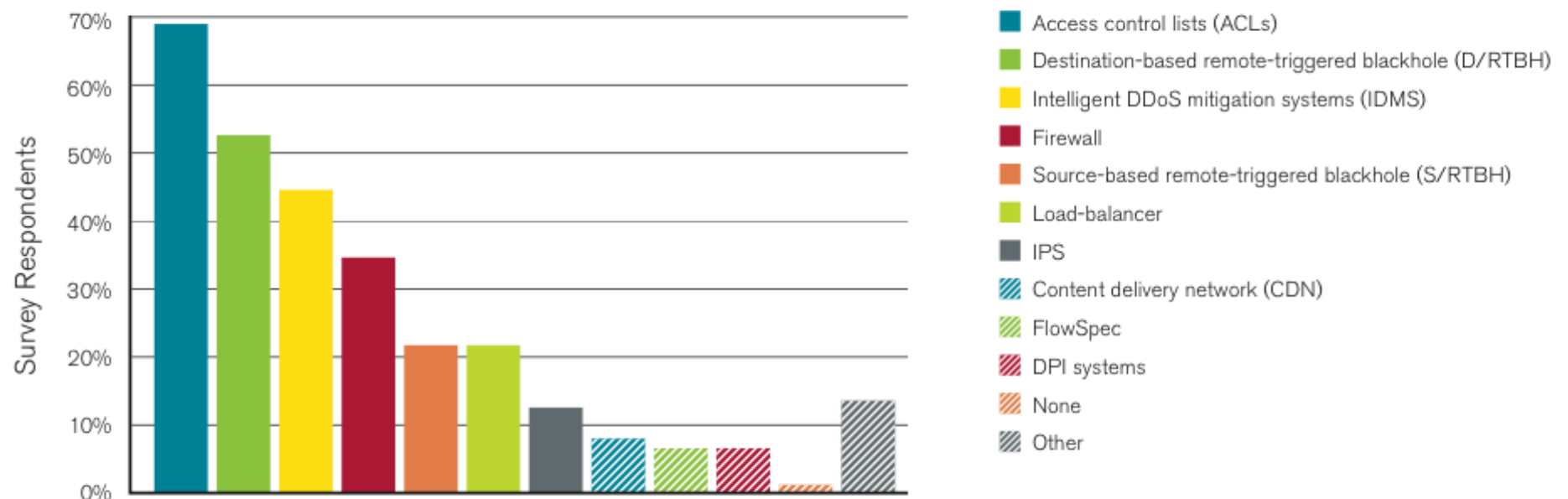


Figure 27 Source: Arbor Networks, Inc.

MAP OF THE INTERNET

THE IPv4 SPACE, 2006



[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.

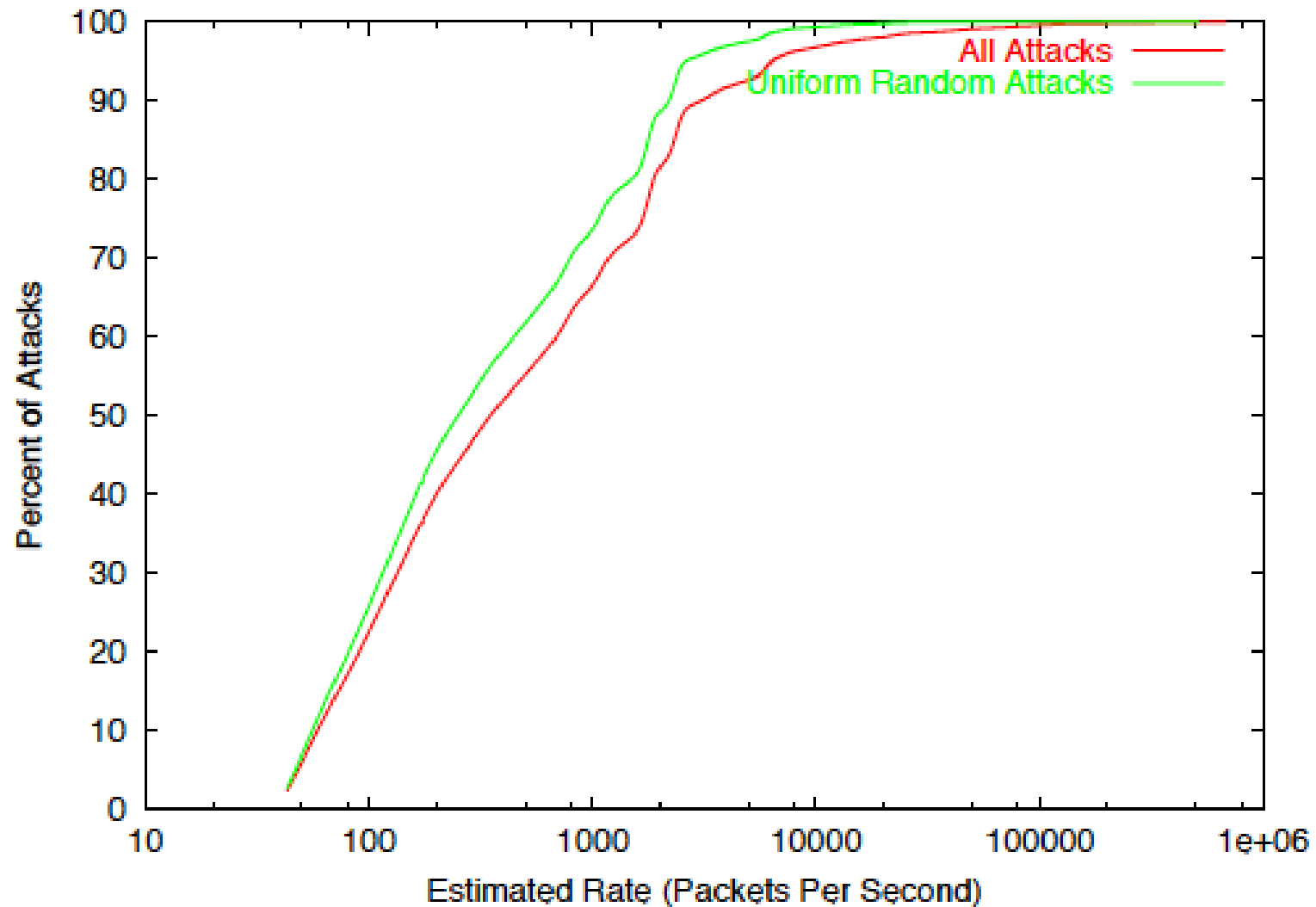


Figure 4: Cumulative distributions of estimated attack rates in packets per second.