Service Provider Experienced Threats

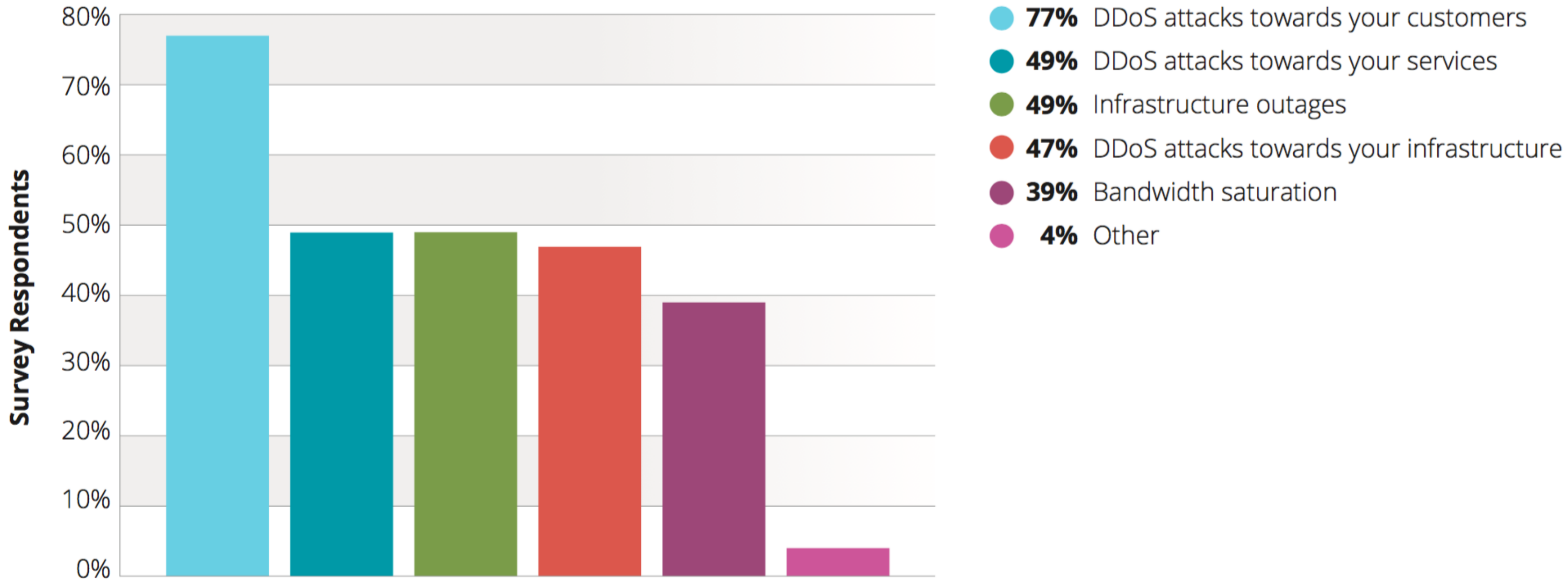


Figure 7 *Source: Arbor Networks, Inc.*

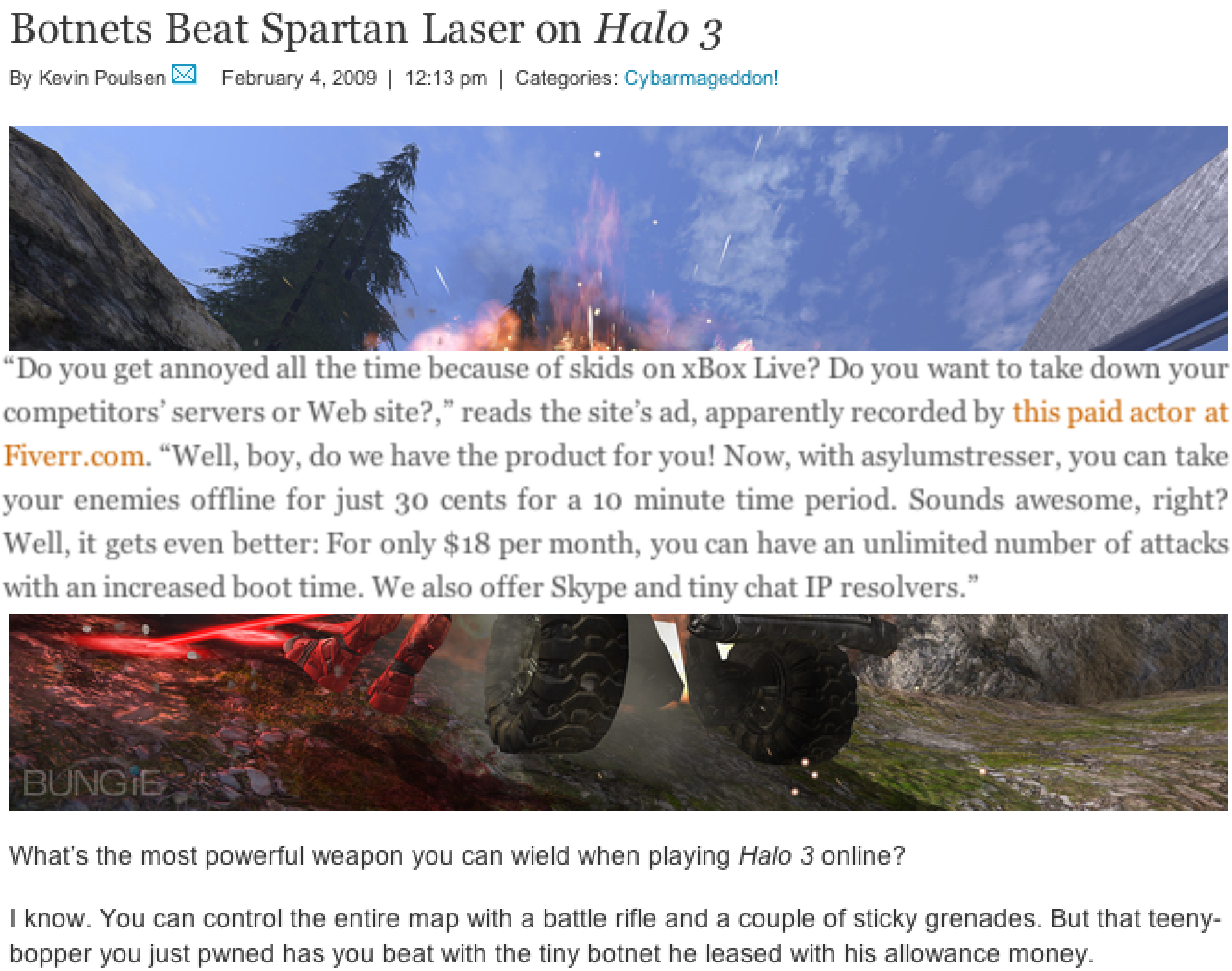
Arbor Networks 2016 Report

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.



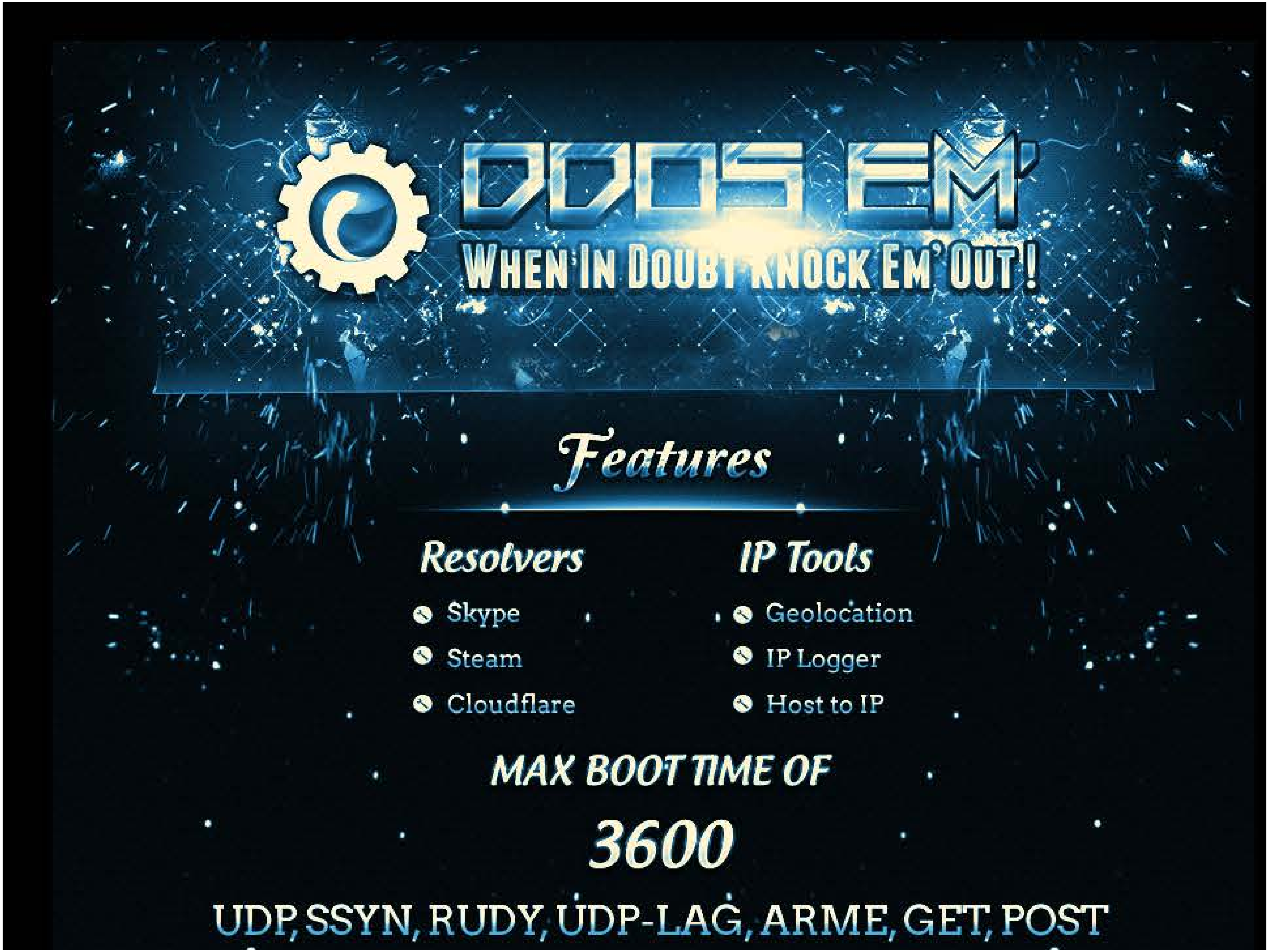
Botnets Beat Spartan Laser on *Halo 3*

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

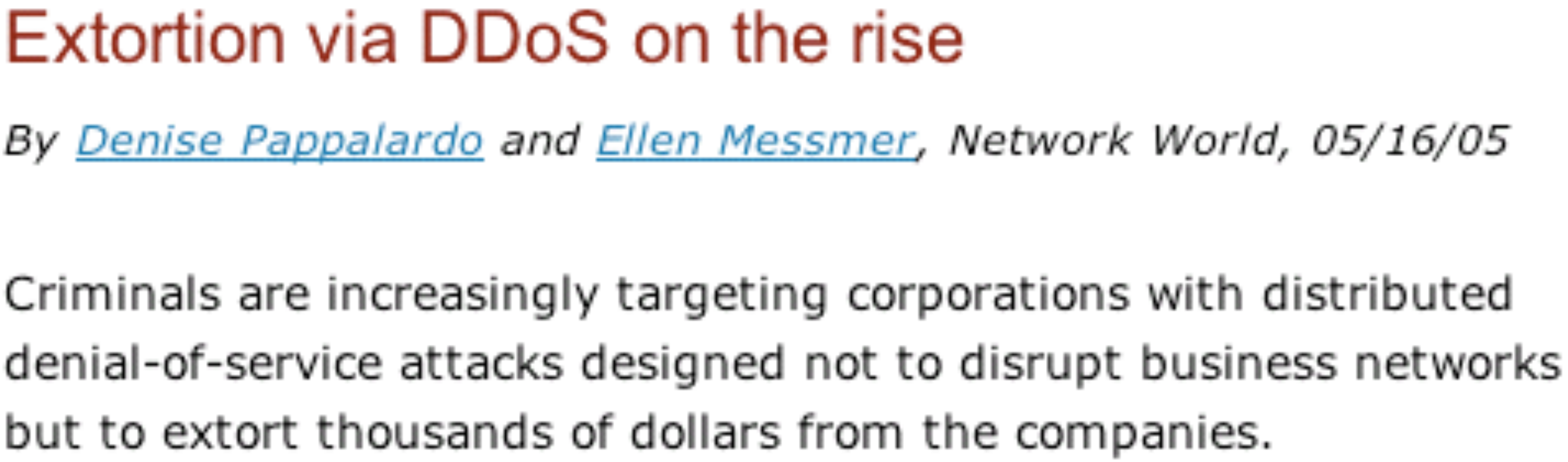
IP Tools

- Geolocation
- IP Logger
- Host to IP

MAX BOOT TIME OF

3600

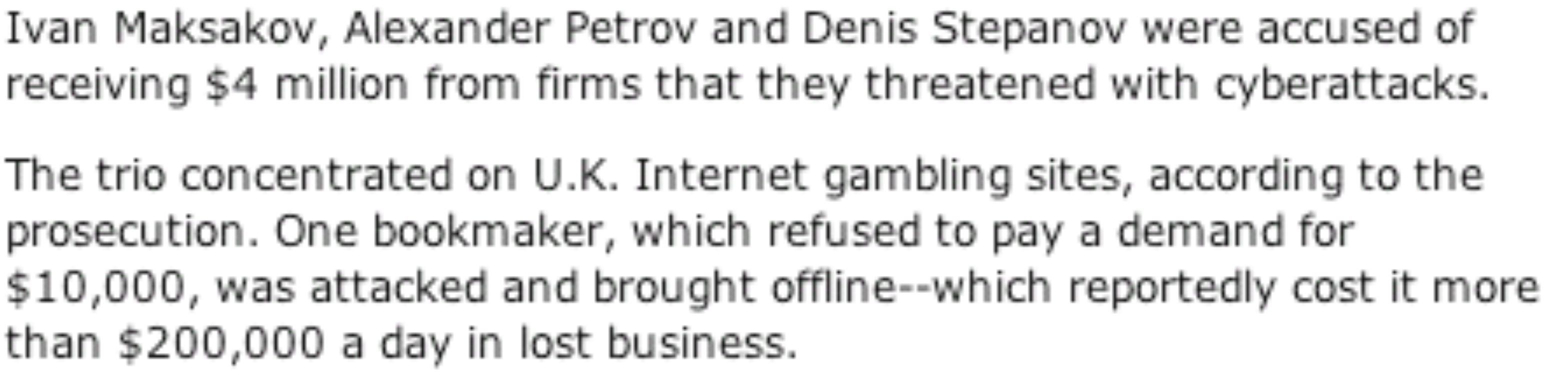
UDP, SSYN, RUDY, UDP-LAG, ARME, GET, POST



Extortion via DDoS on the rise

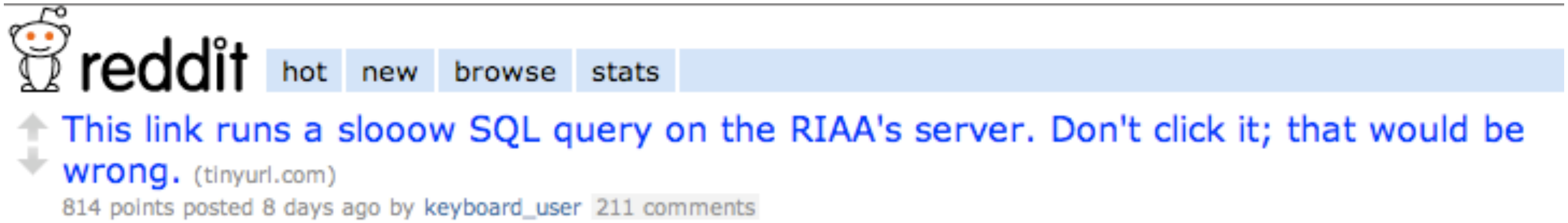
By Denise Pappalardo and Ellen Messmer, Network World, 05/16/05

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.



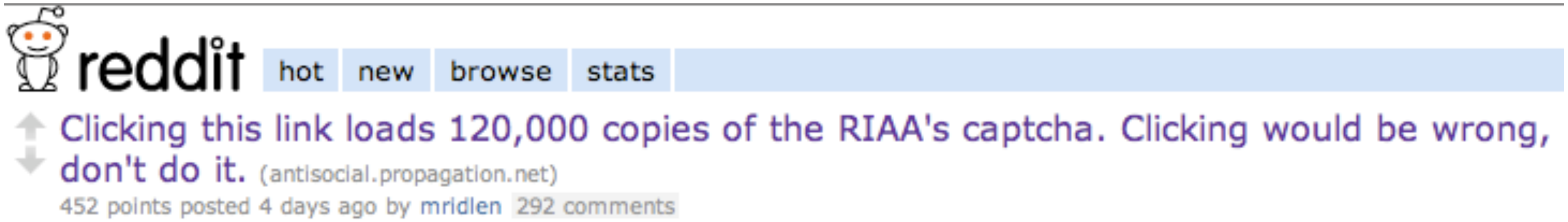
Ivan Maksakov, Alexander Petrov and Denis Stepanov were accused of receiving $4 million from firms that they threatened with cyberattacks.

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.



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



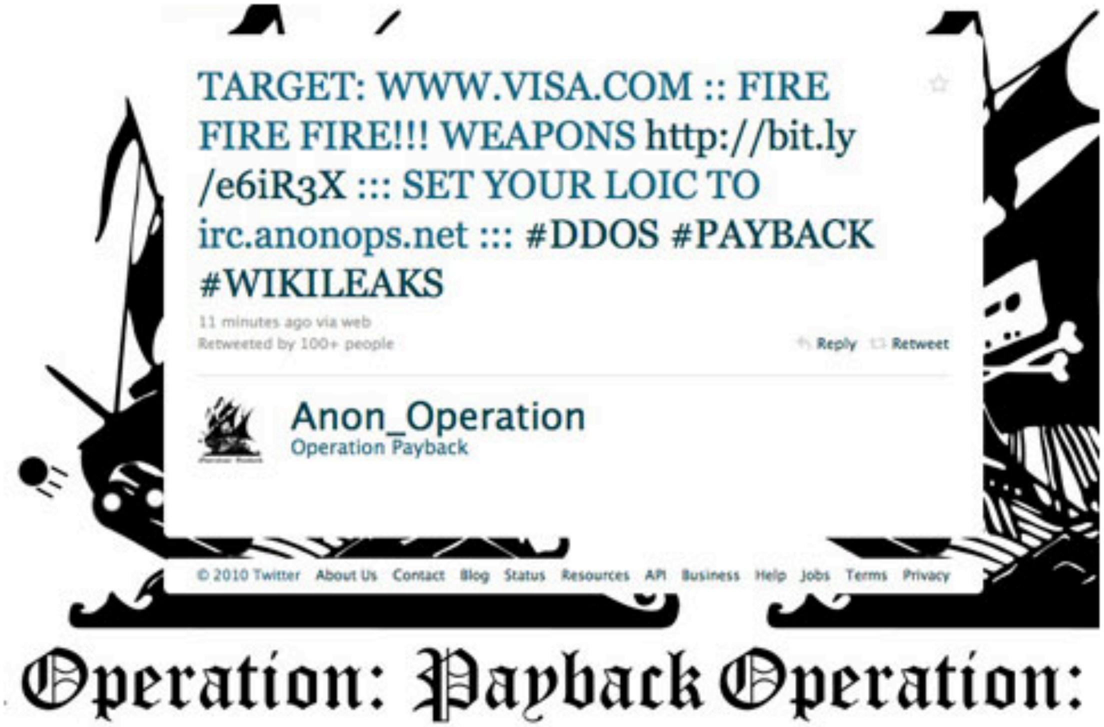
Clicking this link loads 120,000 copies of the RIAA's captcha. Clicking would be wrong, don't do it. (antisocial.propagation.net)

452 points posted 4 days ago by mridlen 292 comments

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

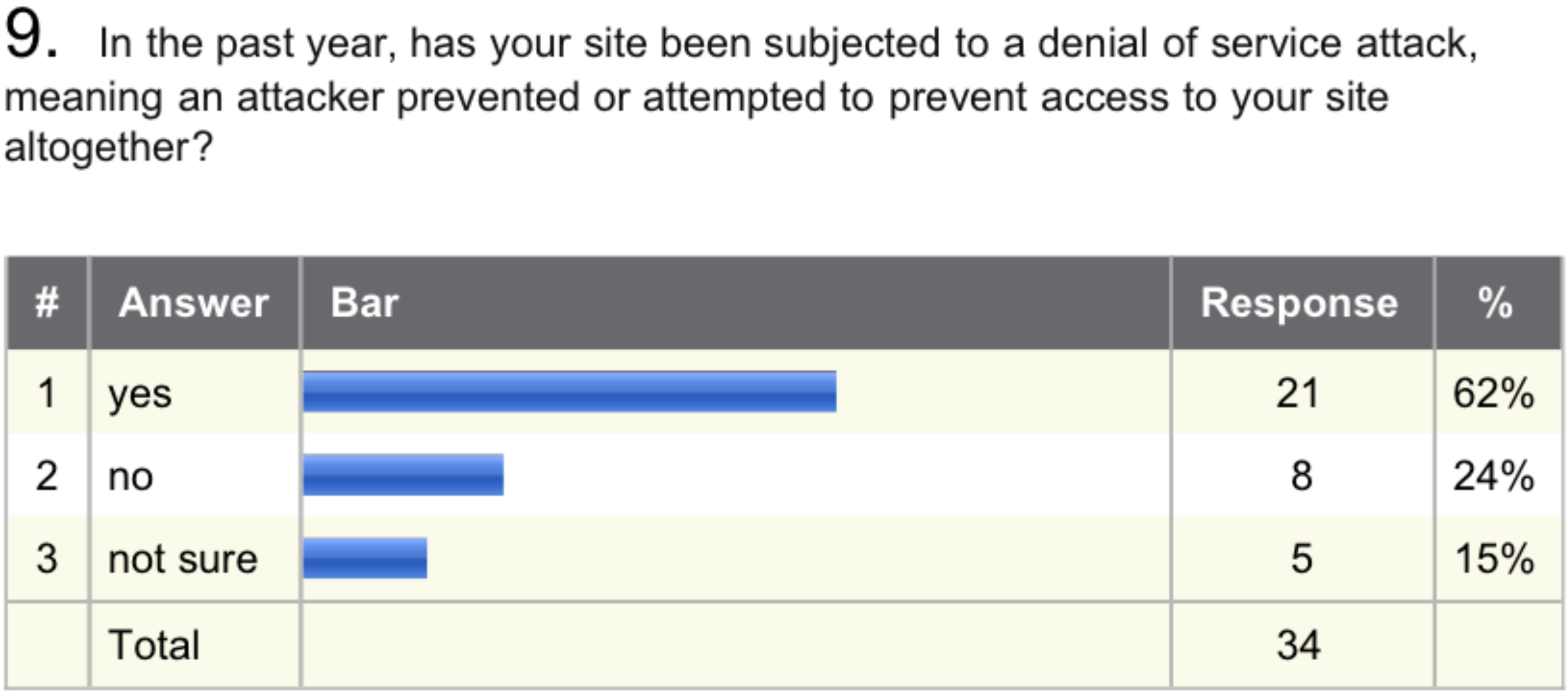
Anon_Operation
Operation Payback

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.

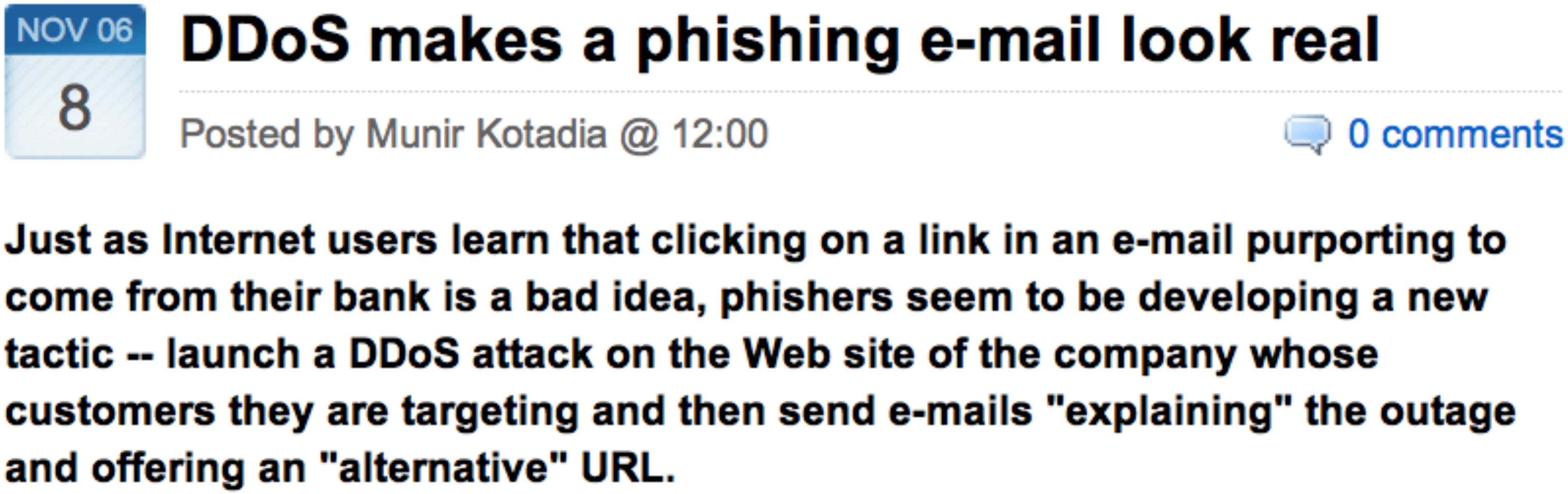
Last Updated | 6:54 p.m. A group of Internet activists took credit for crashing the Visa.com Web site on Wednesday afternoon, hours after they launched a similar attack on MasterCard. The cyber attacks, by activists who call themselves Anonymous, are aimed at punishing companies that have acted to stop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



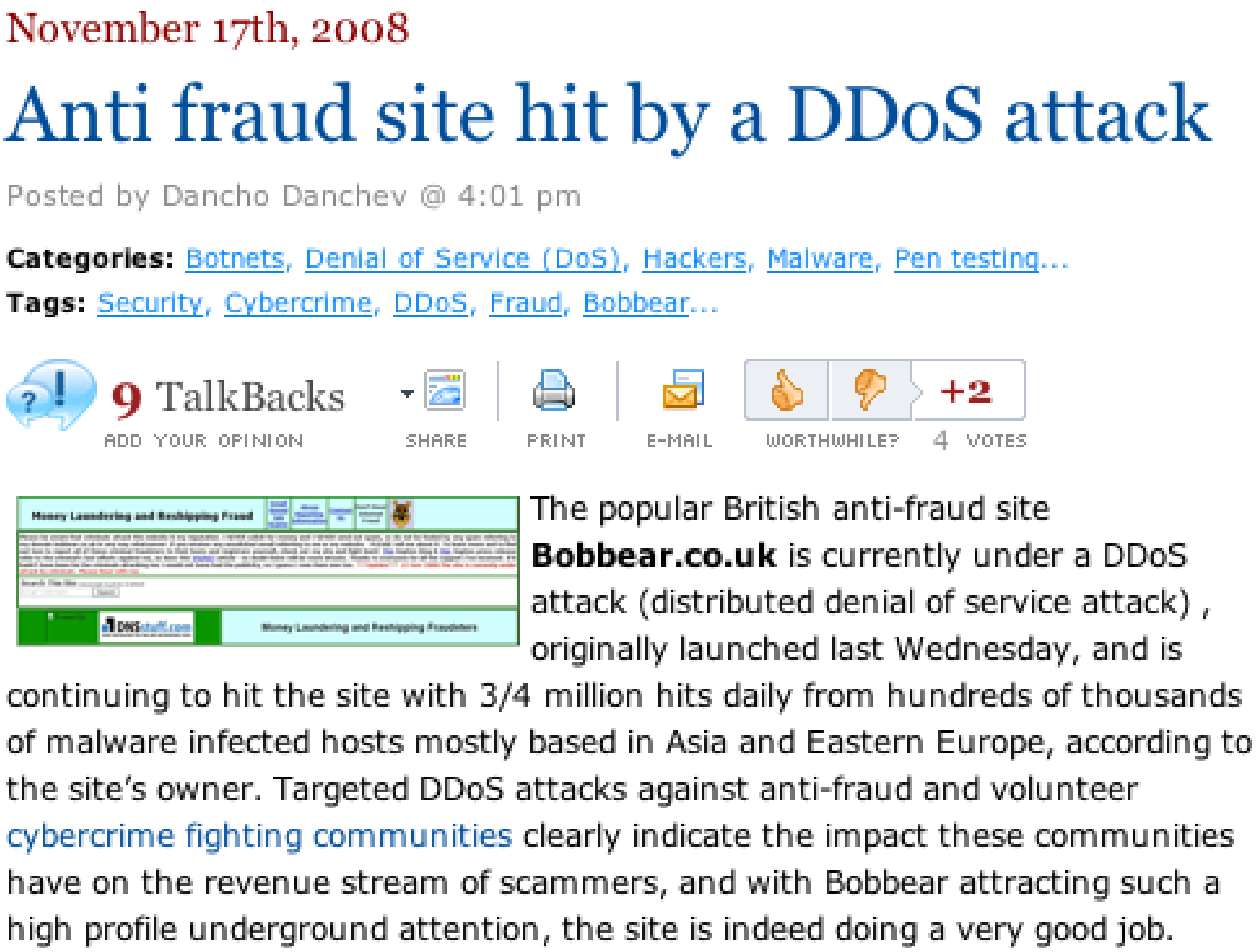
NOV 06
8

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.



Money Laundering and Reshipping Fraud
DNSstuff.com
Money Laundering and Reshipping Fraudsters
SHARE
PRINT
E-MAIL
WORTHWHILE?

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

+2
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 in 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.

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

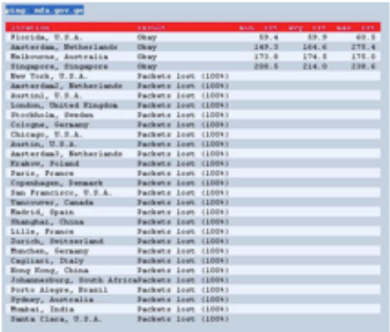
Coordinated Russia vs Georgia cyber attack in progress

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...

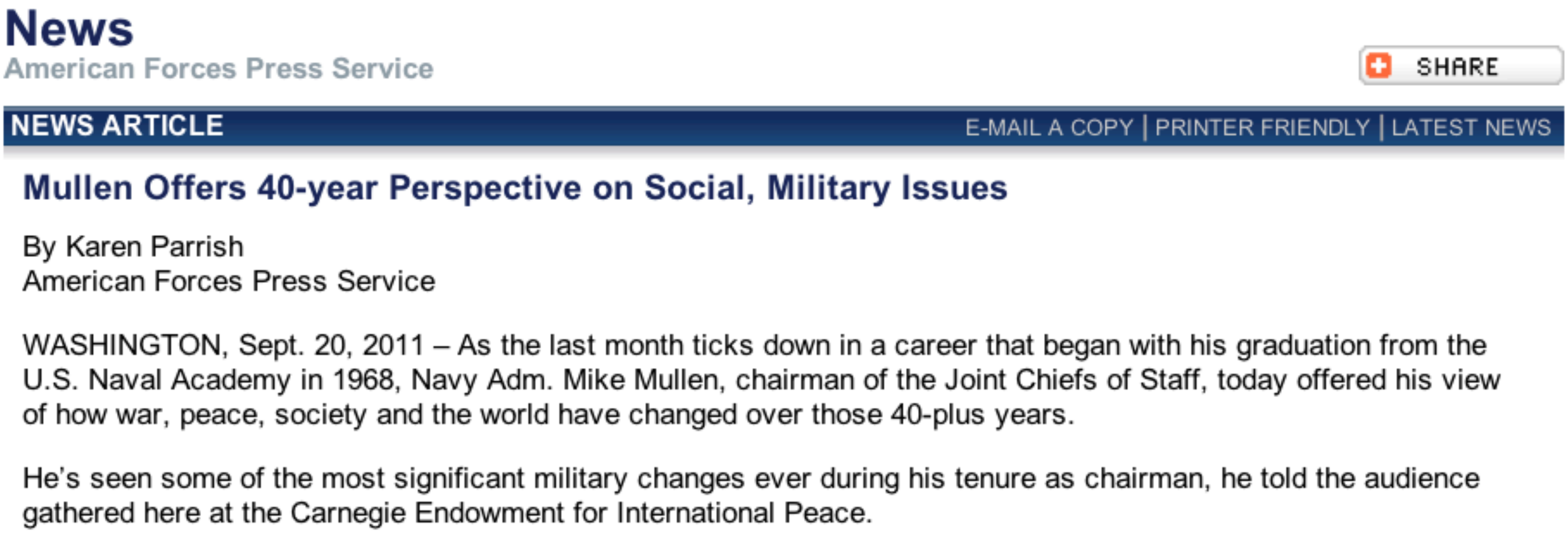
62 TalkBacks ADD YOUR OPINION · SHARE · PRINT · E-MAIL · WORTHWHILE? +18 24 VOTES

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	176.0
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%)			



News
American Forces Press Service

NEWS ARTICLE

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.

Kids responsible for Estonia attack

Author: Ian Grant

Posted: 15:25 13 Mar 2009
Topics: Security

BOOKMARK

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

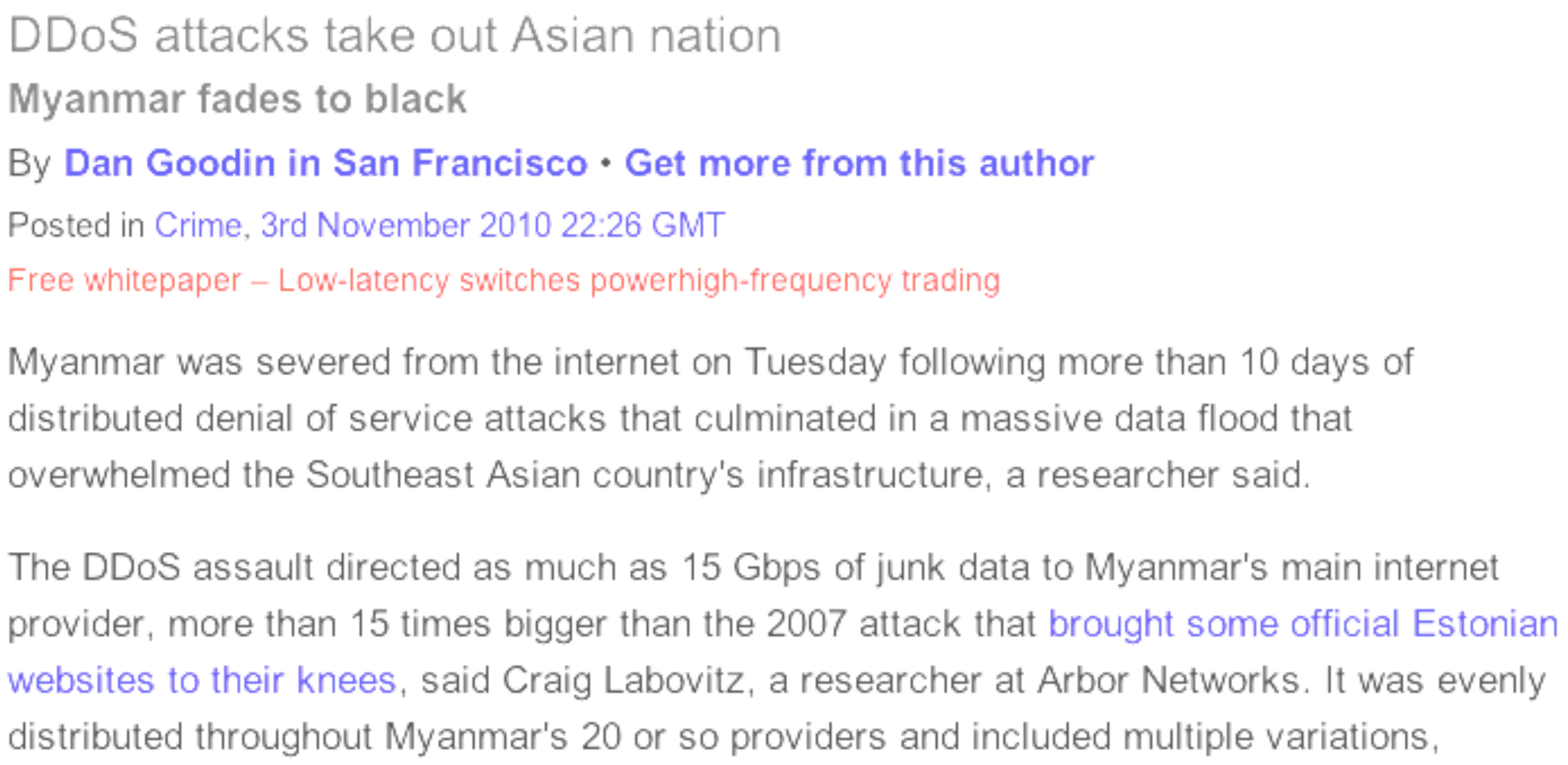
Myanmar fades to black

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

Posted in Crime, 3rd November 2010 22:26 GMT

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

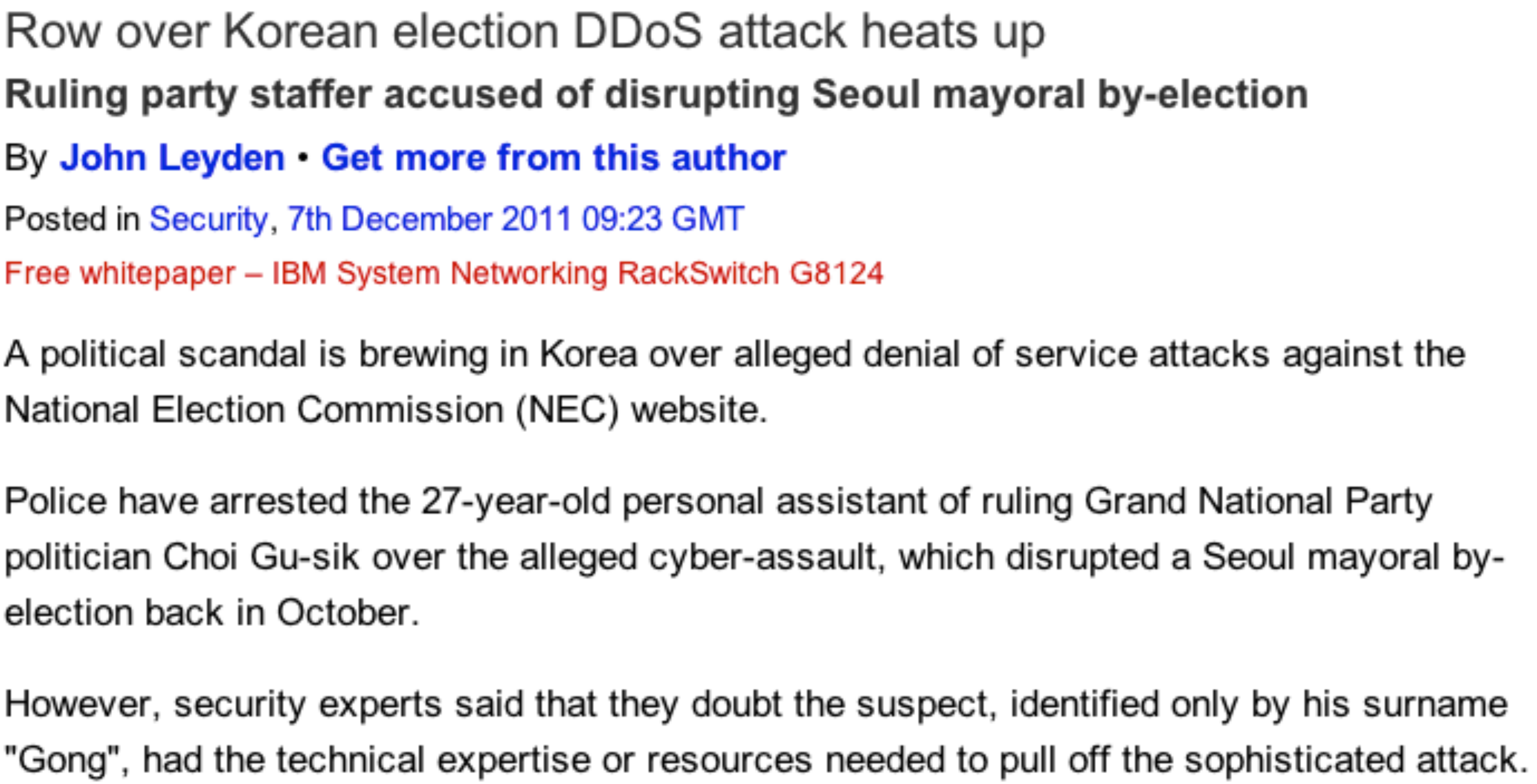
By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Crime, 3rd November 2010 22:26 GMT

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

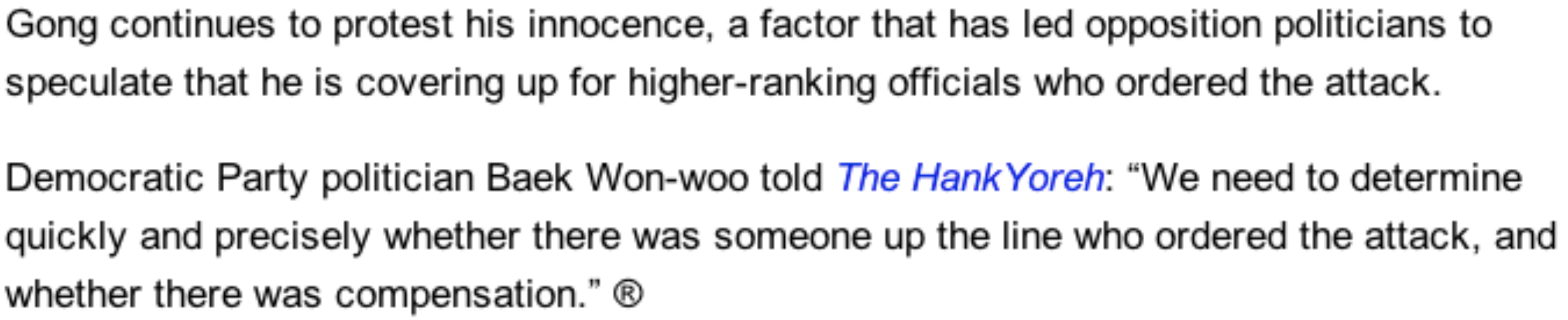
By John Leyden • Get more from this author

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

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.” ®

DDoS Attack Motivations

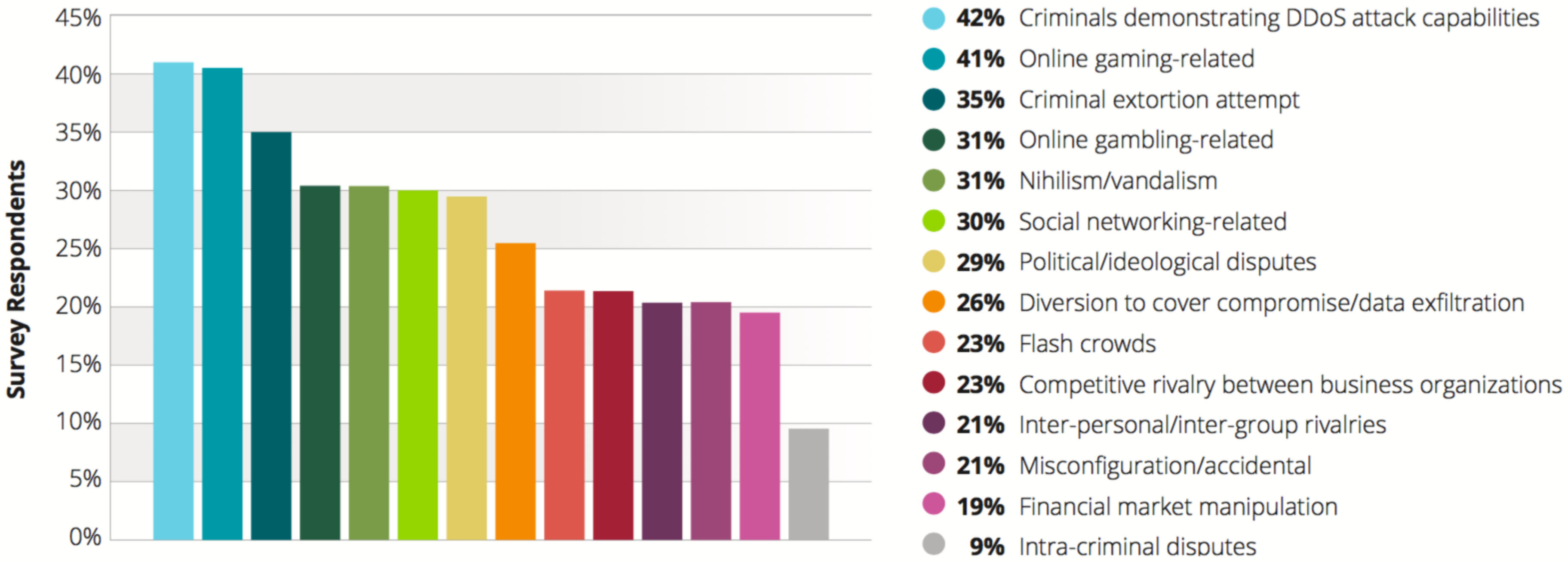


Figure 25 *Source: Arbor Networks, Inc.*

DDoS Attack Frequency

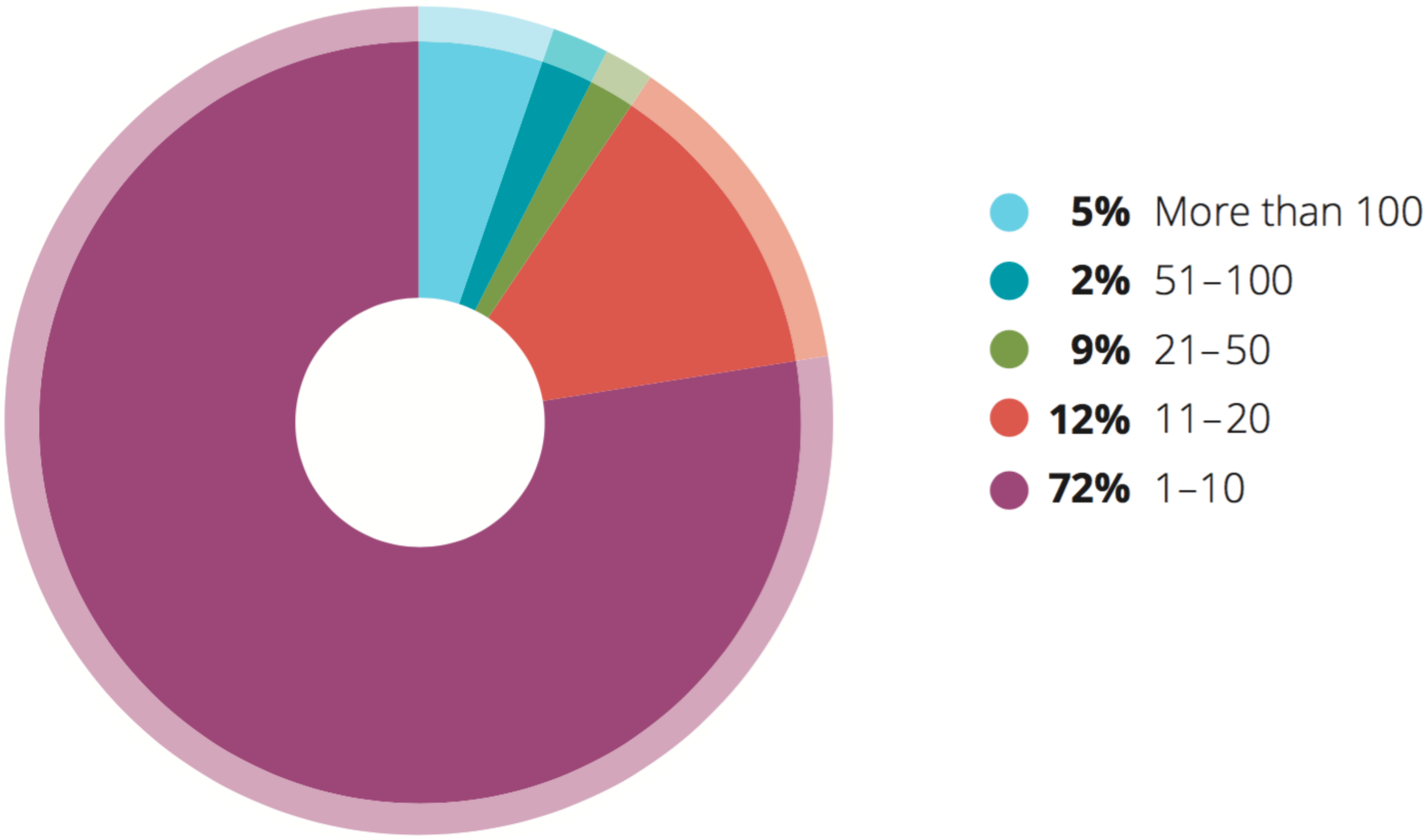


Figure 97 *Source: Arbor Networks, Inc.*

DDoS Attack Frequency

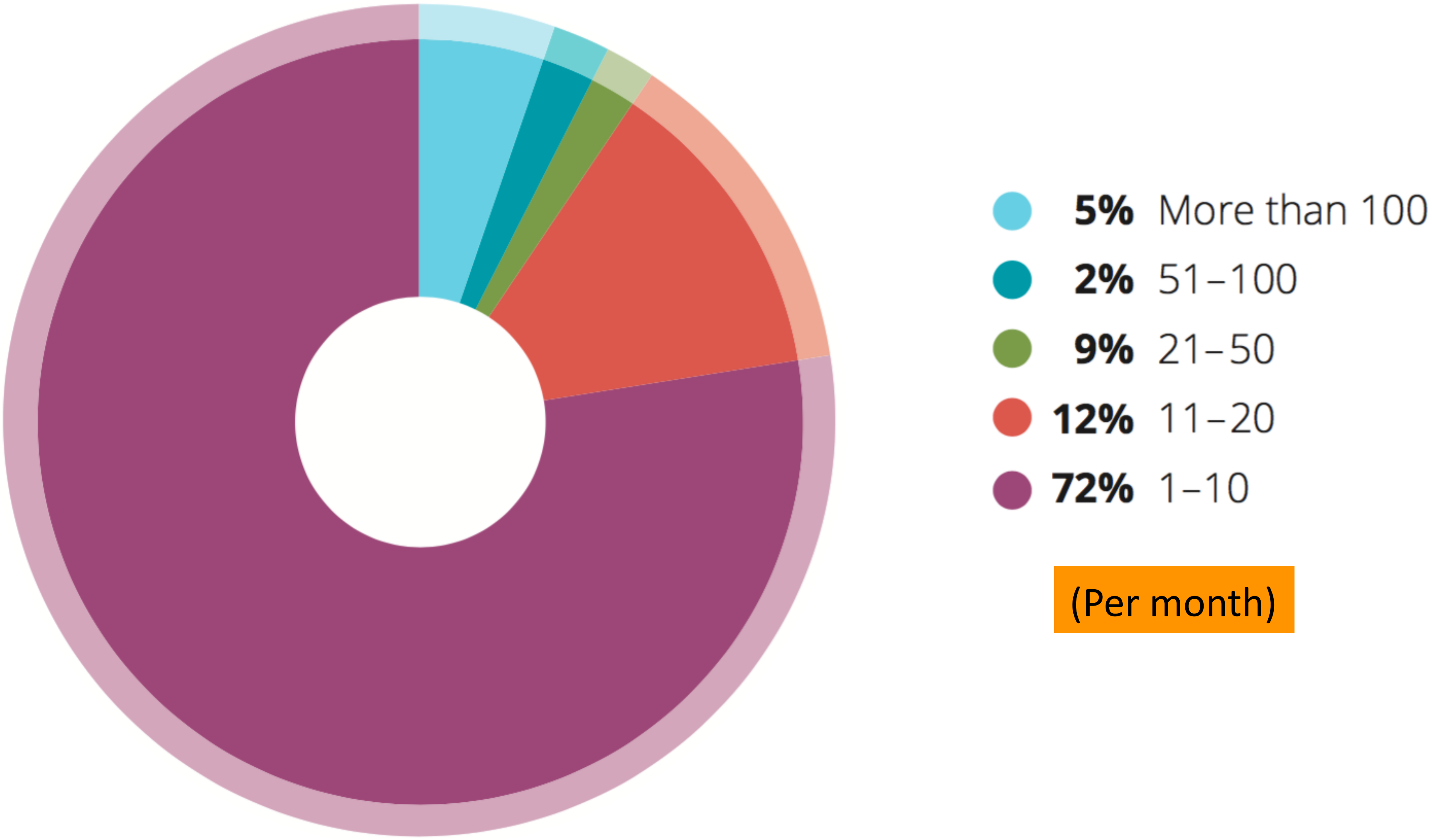
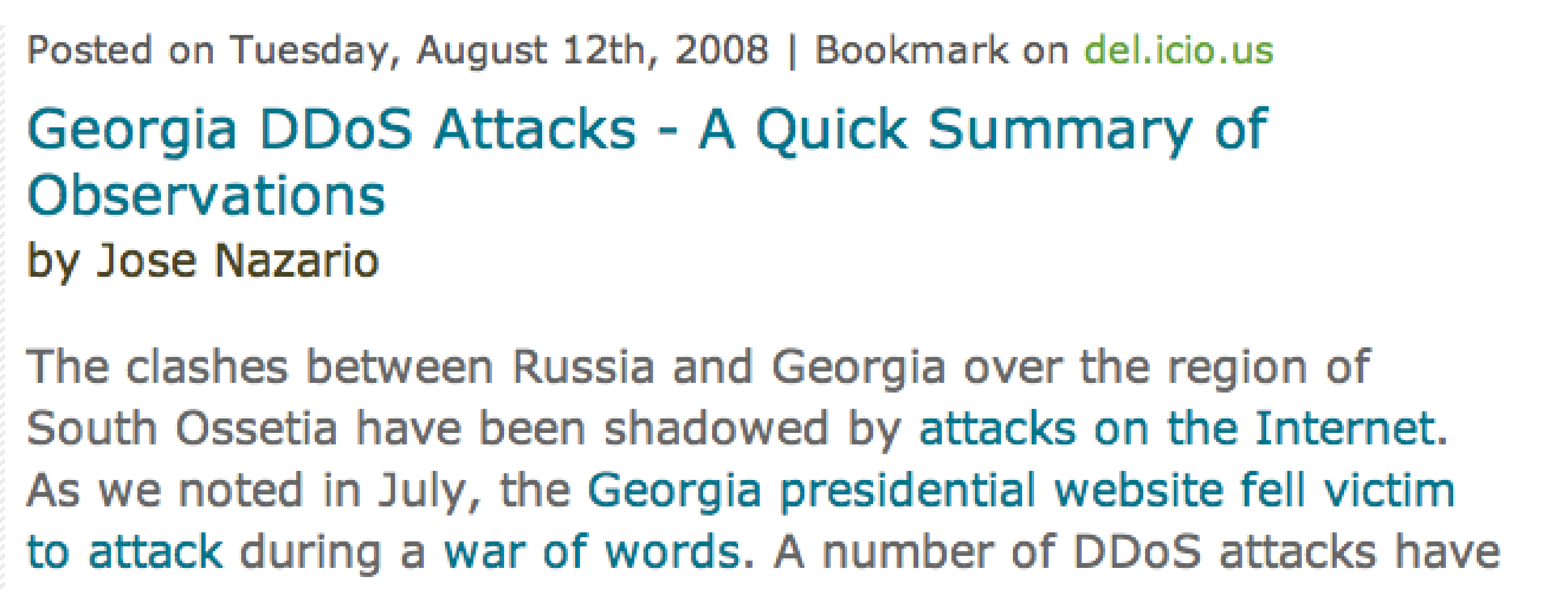


Figure 97 *Source: Arbor Networks, Inc.*

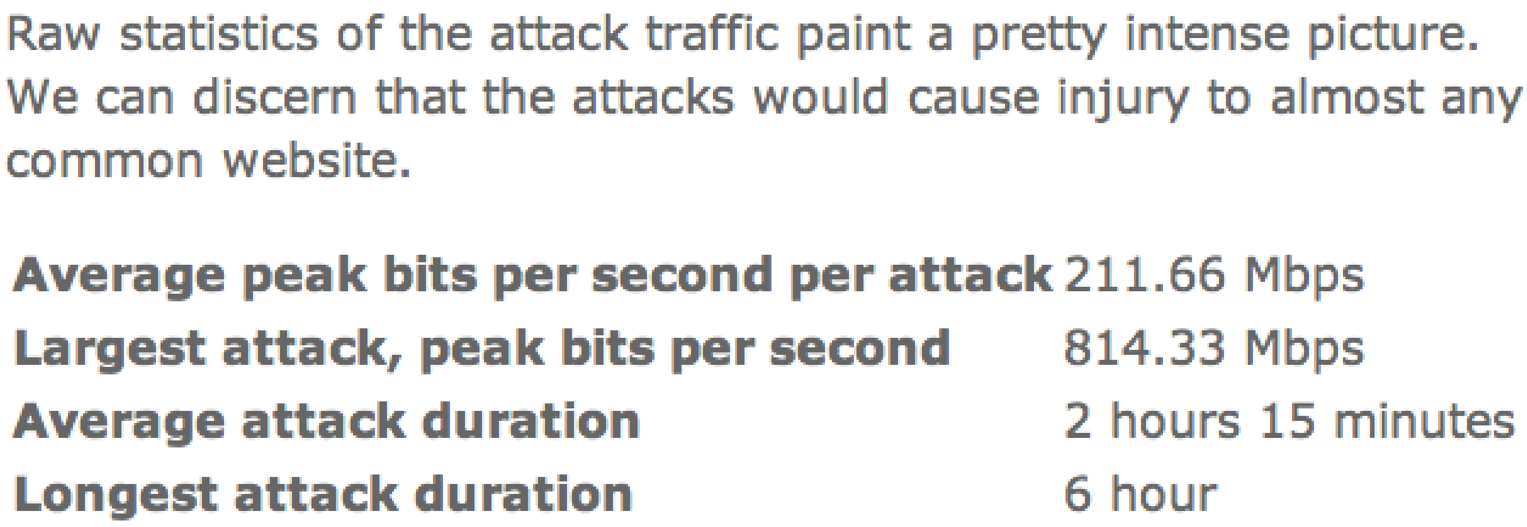


Posted on Tuesday, August 12th, 2008 | Bookmark on del.icio.us

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

Size of Largest Reported DDoS Attack (Gbps)

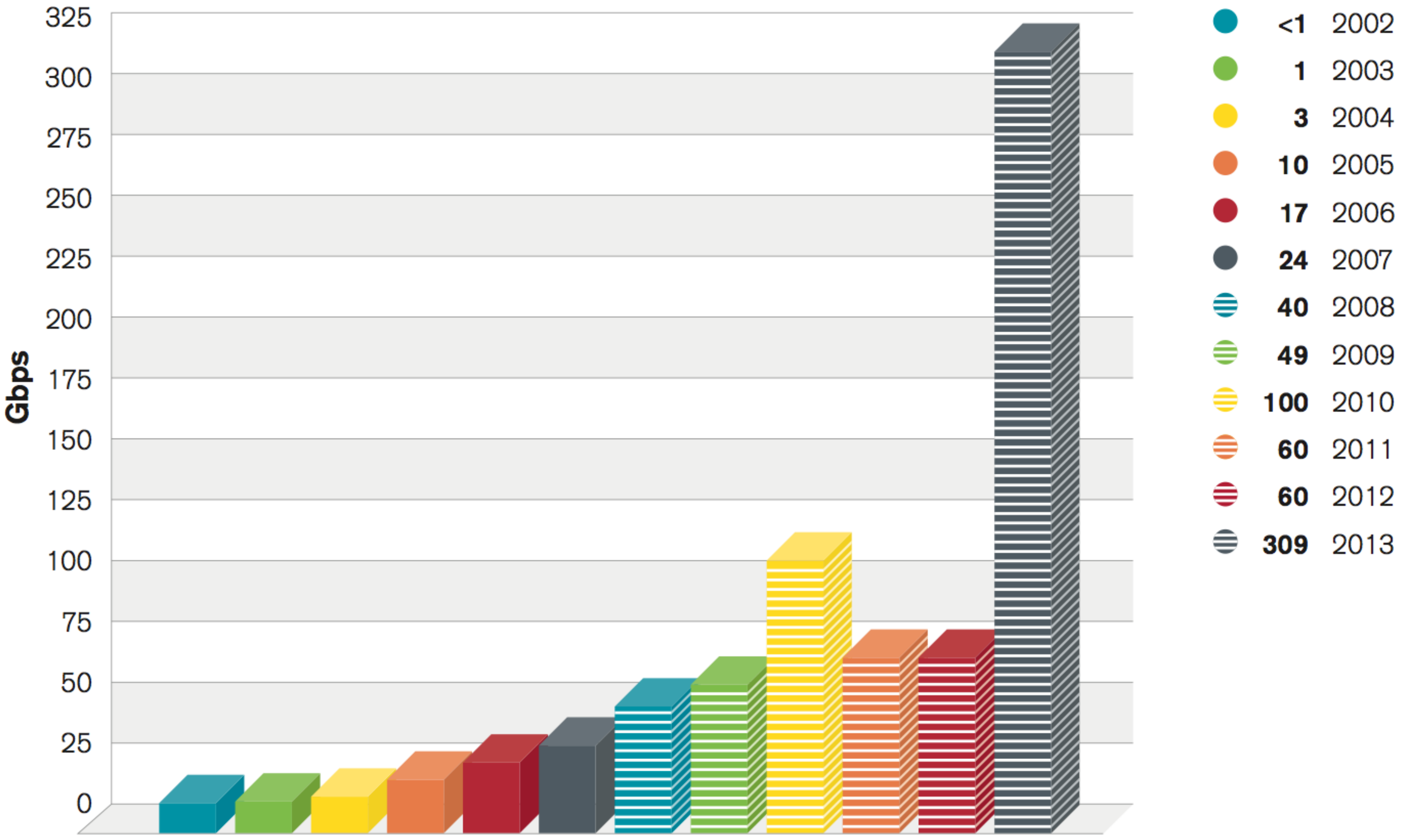


Figure 14 *Source: Arbor Networks, Inc.*

2014 Report

Survey Peak Attack Size Year Over Year

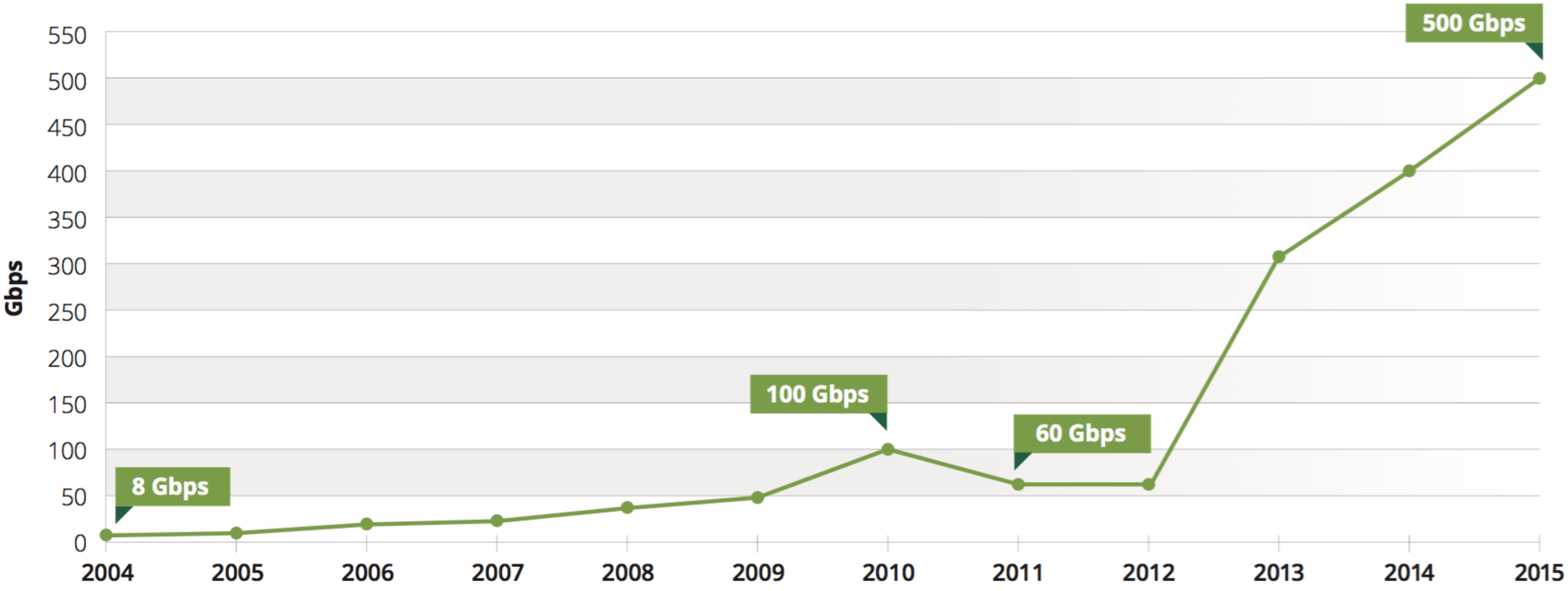
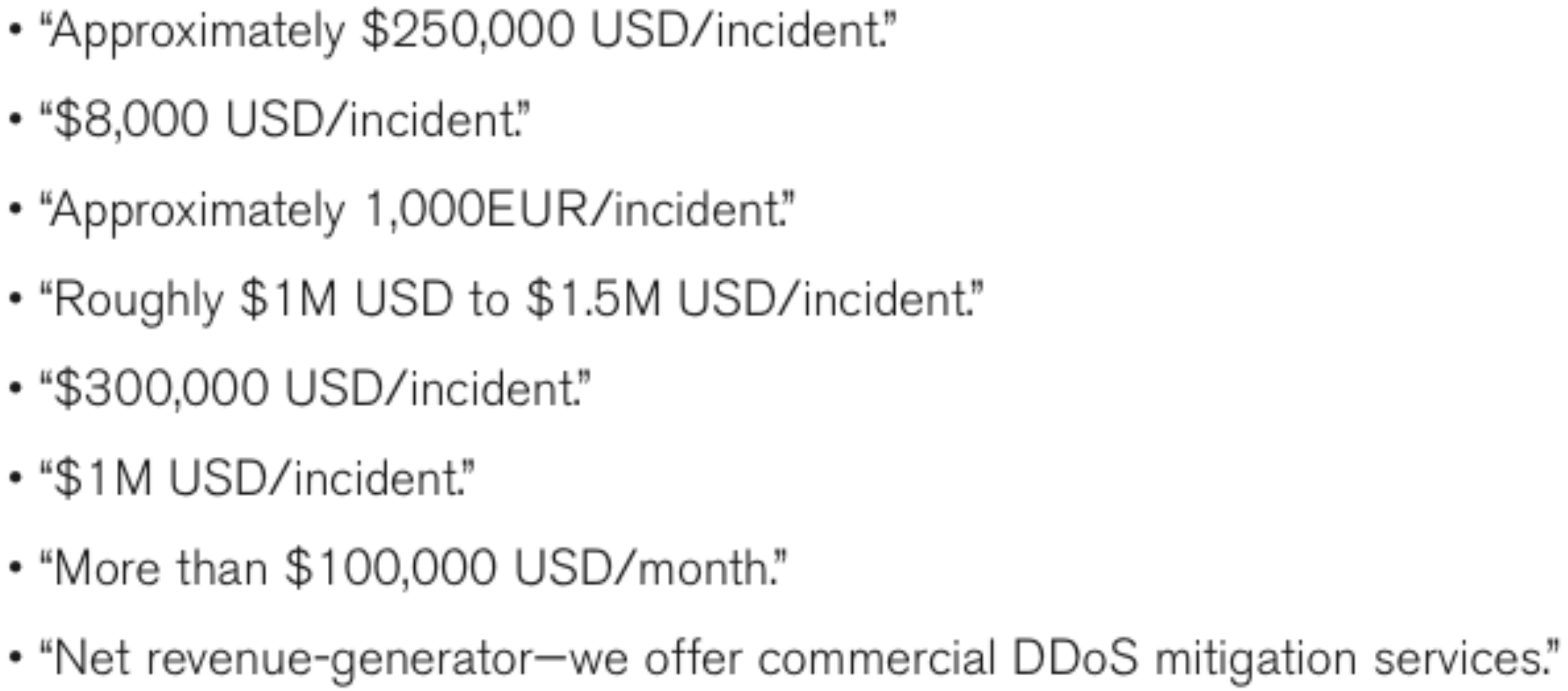


Figure 14 *Source: Arbor Networks, Inc.*

2016 Report

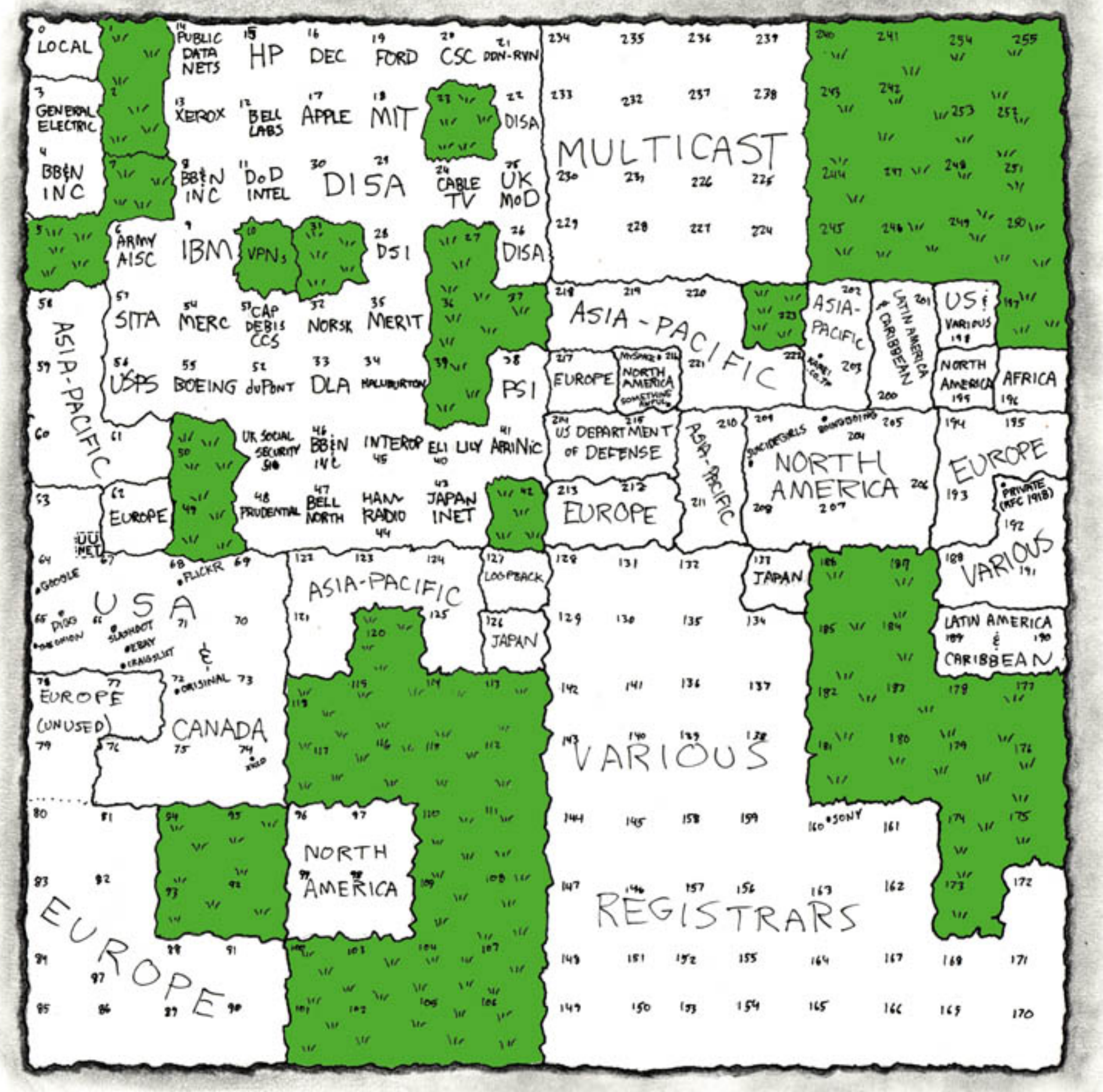


- “Approximately $250,000 USD/incident.”
- “$8,000 USD/incident.”
- “Approximately 1,000EUR/incident.”
- “Roughly $1M USD to $1.5M USD/incident.”
- “$300,000 USD/incident.”
- “$1M USD/incident.”
- “More than $100,000 USD/month.”
- “Net revenue-generator—we offer commercial DDoS mitigation services.”

2011 Report

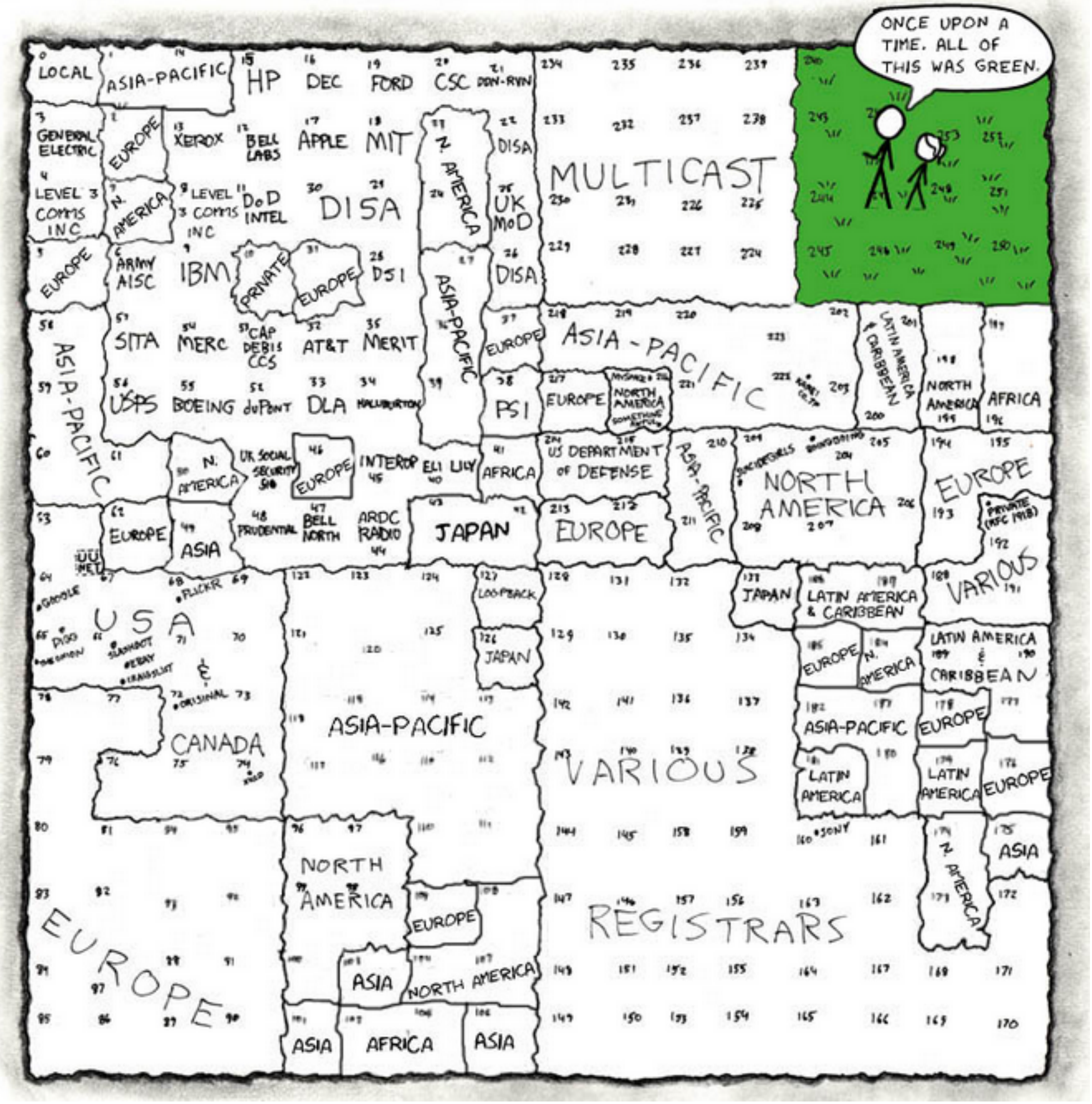
MAP OF THE INTERNET

THE IPv4 SPACE, 2006



MAP OF THE INTERNET

THE IPv4 SPACE, 2011



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.

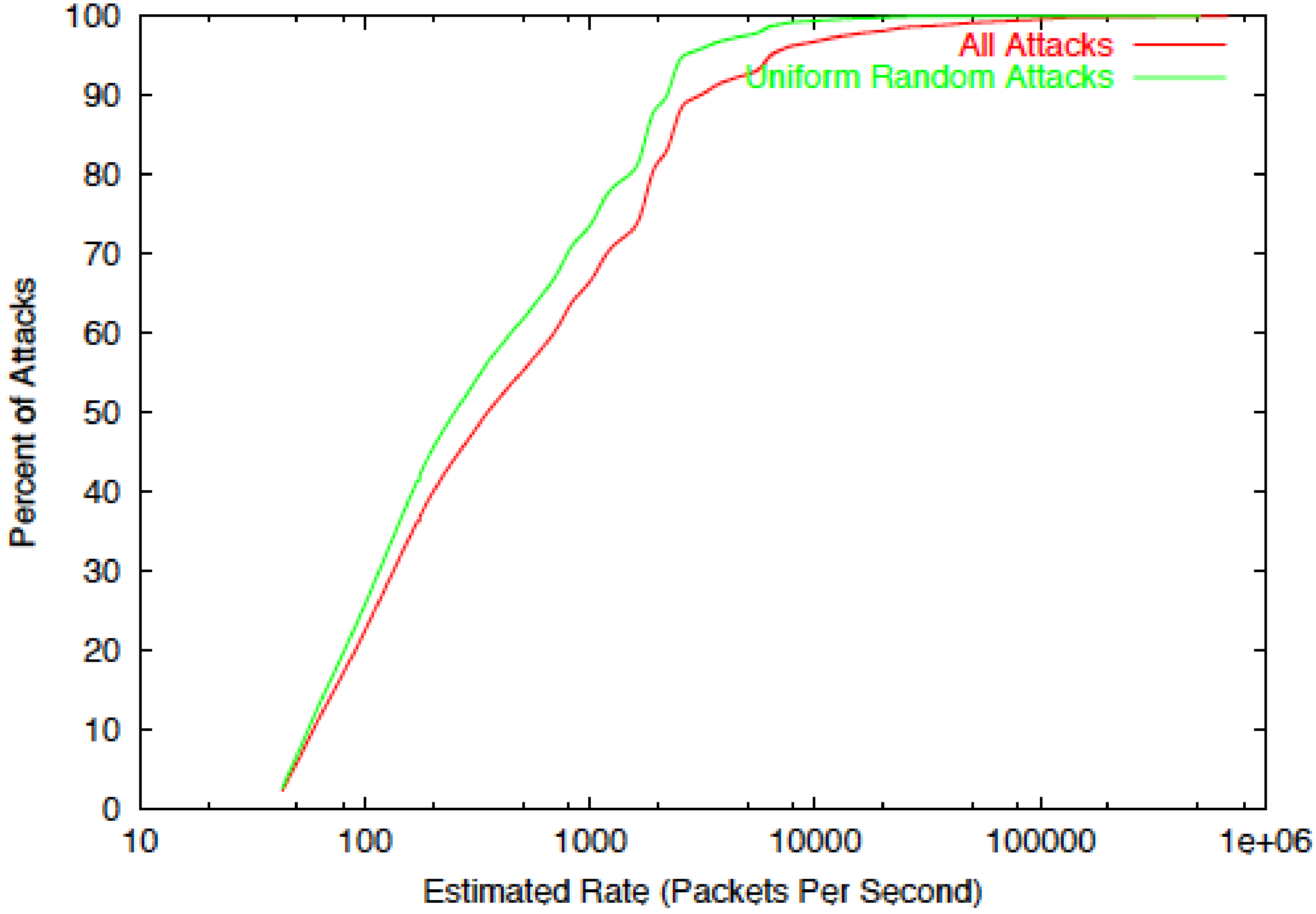


Figure 4: Cumulative distributions of estimated attack rates in packets per second.

Kind	Trace-1				Trace-2				Trace-3			
	Attacks		Packets (k)		Attacks		Packets (k)		Attacks		Packets (k)	
Other	1,917	(46)	19,118	(38)	1,985	(51)	25,305	(32)	2,308	(49)	17,192	(28)
In-Addr Arpa	1,230	(29)	16,716	(33)	1,105	(28)	24,645	(32)	1,307	(27)	26,880	(43)
Broadband	394	(9.4)	9,869	(19)	275	(7.1)	13,054	(17)	375	(7.9)	8,513	(14)
Dial-Up	239	(5.7)	956	(1.9)	163	(4.2)	343	(0.44)	276	(5.8)	1,018	(1.6)
IRC Server	110	(2.6)	461	(0.91)	88	(2.3)	2,289	(2.9)	111	(2.3)	6,476	(10)
Nameserver	124	(3.0)	453	(0.89)	84	(2.2)	2,796	(3.6)	90	(1.9)	451	(0.72)
Router	58	(1.4)	2,698	(5.3)	76	(2.0)	4,055	(5.2)	125	(2.6)	682	(1.1)
Web Server	54	(1.3)	393	(0.77)	64	(1.7)	5,674	(7.3)	134	(2.8)	730	(1.2)
Mail Server	38	(0.91)	156	(0.31)	35	(0.90)	71	(0.09)	26	(0.55)	292	(0.47)
Firewall	9	(0.22)	7	(0.01)	3	(0.08)	3	(0.00)	2	(0.04)	1	(0.00)

Table 6: Breakdown of victim hostnames.

The majority of attacks are not classified by this scheme, either because they are not matched by our criteria (shown by "other"), or more likely, because there was no valid reverse DNS mapping (shown by "In-Addr Arpa").