

Lecture 15 – Networking Attacks in Practice

Michael Bailey

University of Illinois

ECE 422/CS 461 – Spring 2018

Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks

Jakub (Jake) Czyz, University of Michigan

Michael Kallitsis, Merit Network, Inc.

Manaf Gharaibeh, Colorado State University

Christos Papadopoulos, Colorado State University

Michael Bailey, University of Michigan and University of Illinois

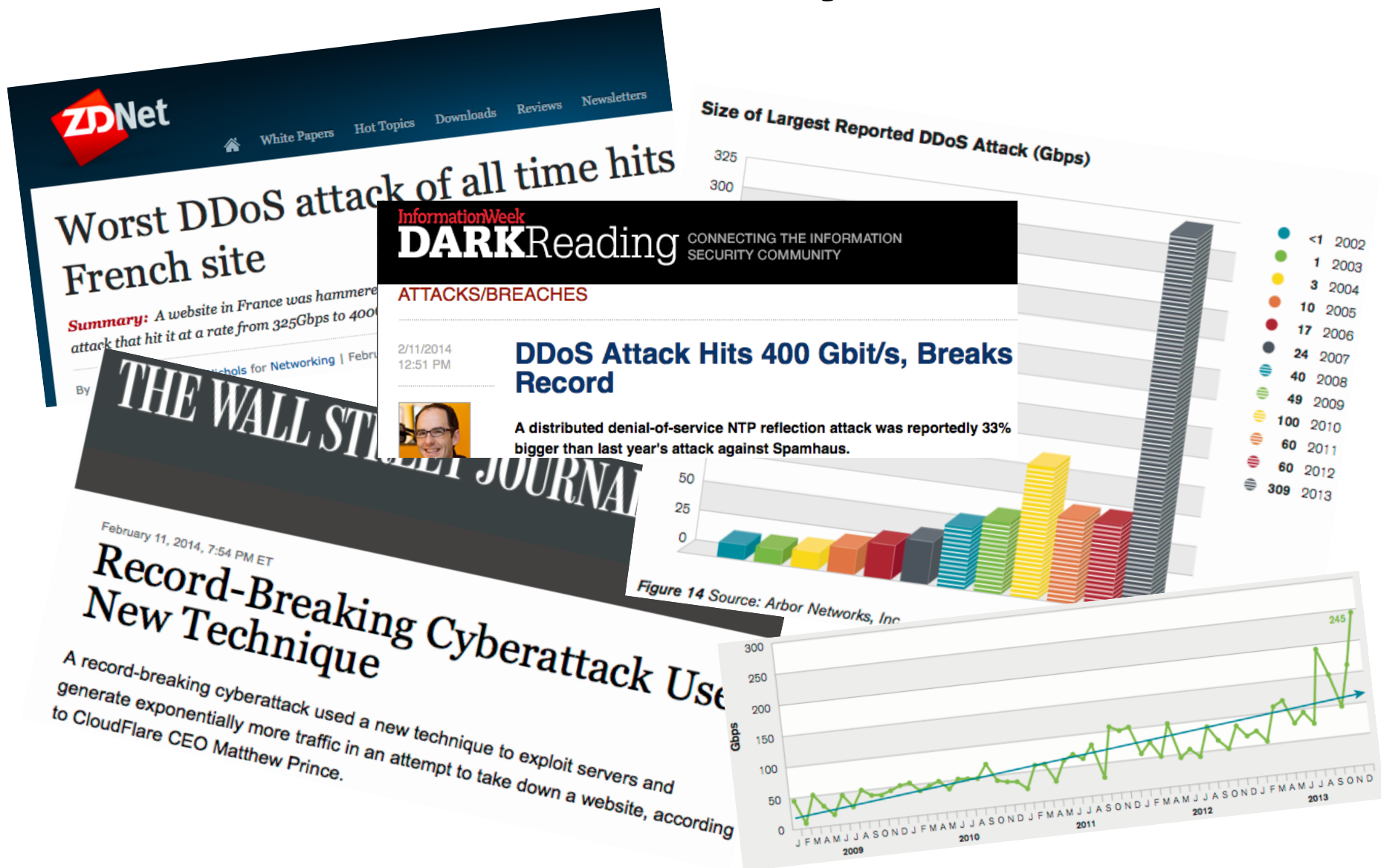
Manish Karir, Merit Network, Inc.

Internet Measurement Conference

Vancouver, BC, Canada

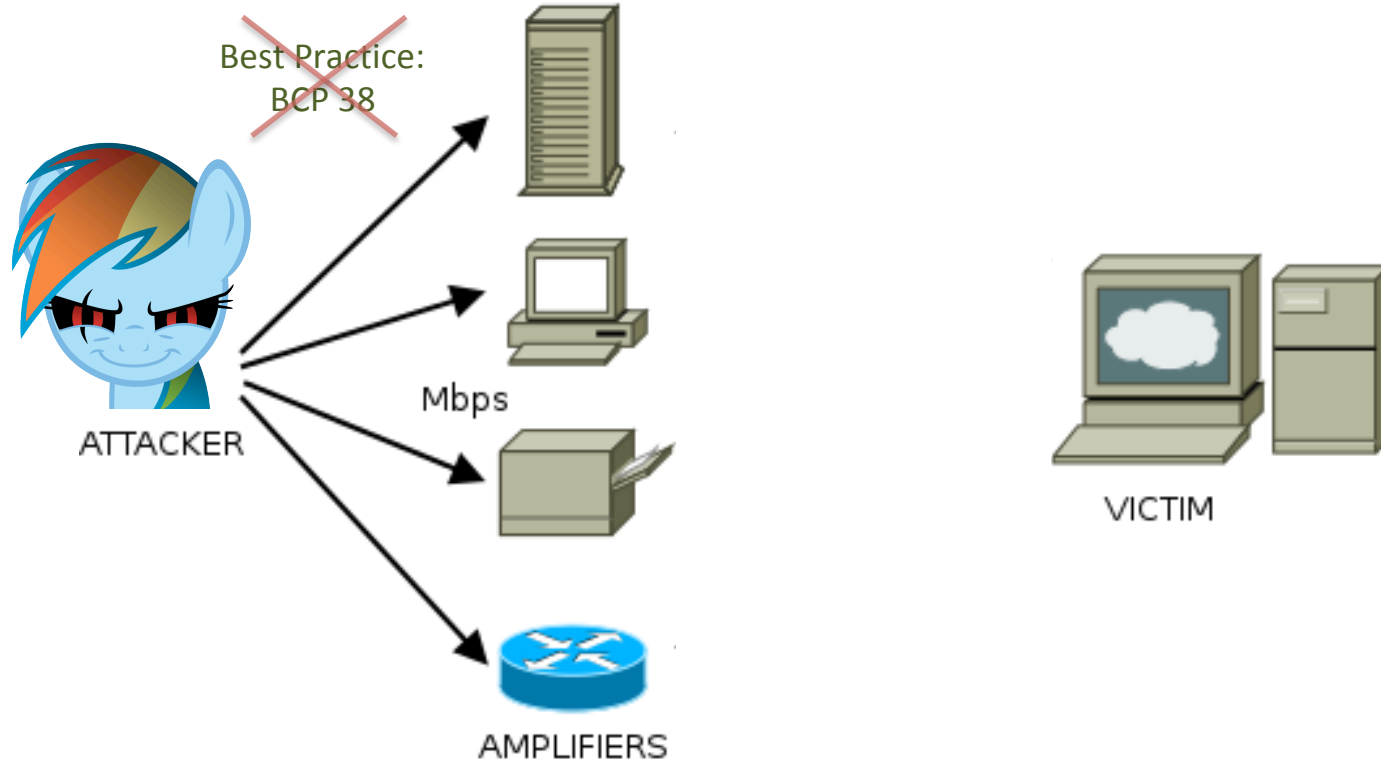
November 5-7, 2014

The DDoS “Hockey Stick Era”



Reflected & Amplified DDoS Attacks

- **Volumetric** attacks that seek to overwhelm victim with traffic
- Often rely on properties of several **UDP**-based protocols:
 - **Spoofability, broad deployment, and large responses** to small requests

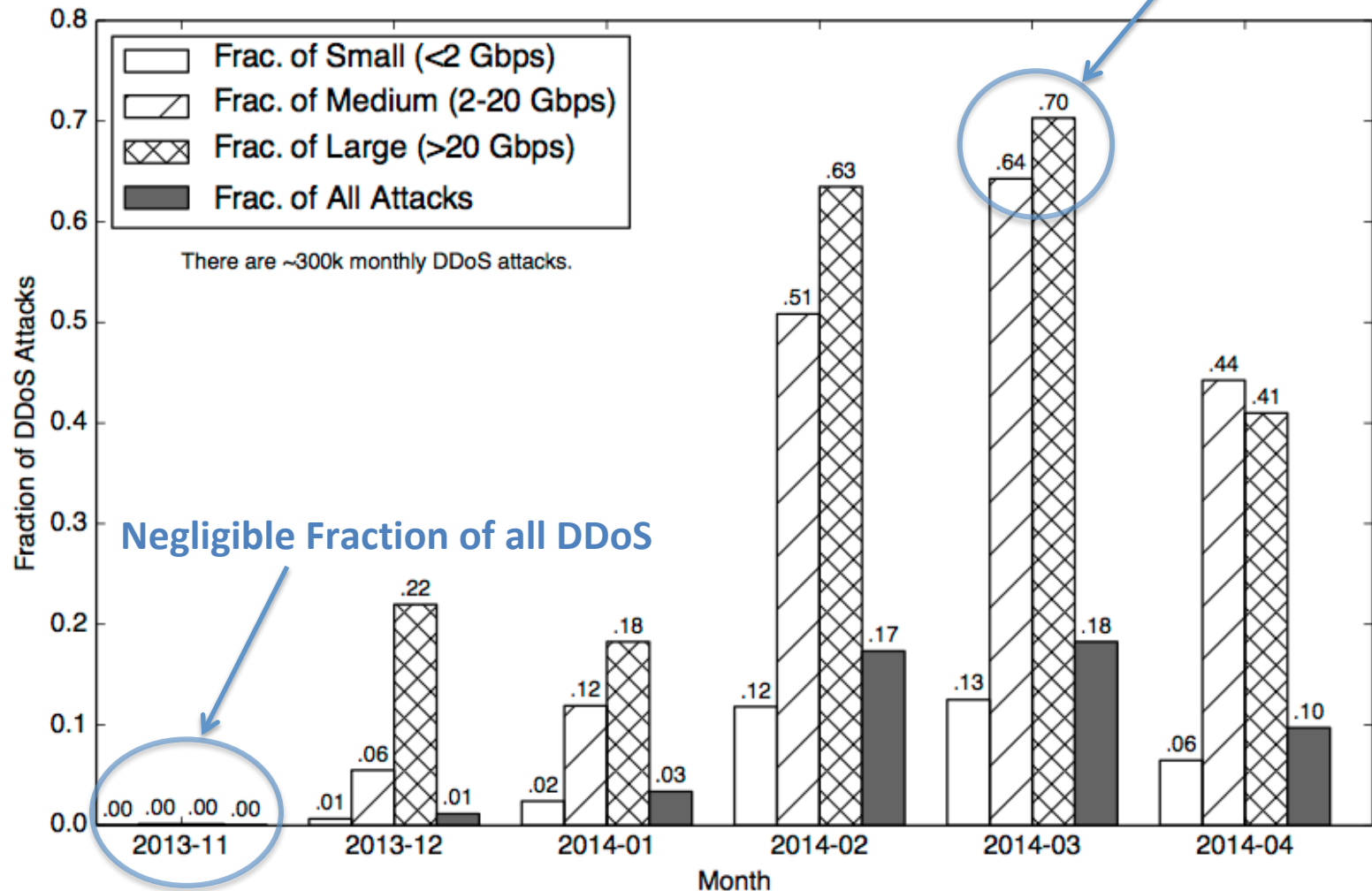


NTP DDoS Attack Mechanics

- Network Time Protocol: for synchronizing system clocks
 - Widely deployed on servers, workstations, and network gear
- **Normal Use:**
 - small client and small server packets (symmetric)
 - typically one exchange every 1 to 12 minutes
 - NTP protocol normal modes (mode 3 or 4)
- **Attacks:**
 - small requests, large responses (asymmetric)
 - typically many times per second
 - NTP protocol special diagnostic modes (6 or 7); most egregiously: “**monlist**” command (out of several):
 - Request: 1pkt, ~100B
 - Response: up to 40pkt, ~20,000B; **~200x amplification**

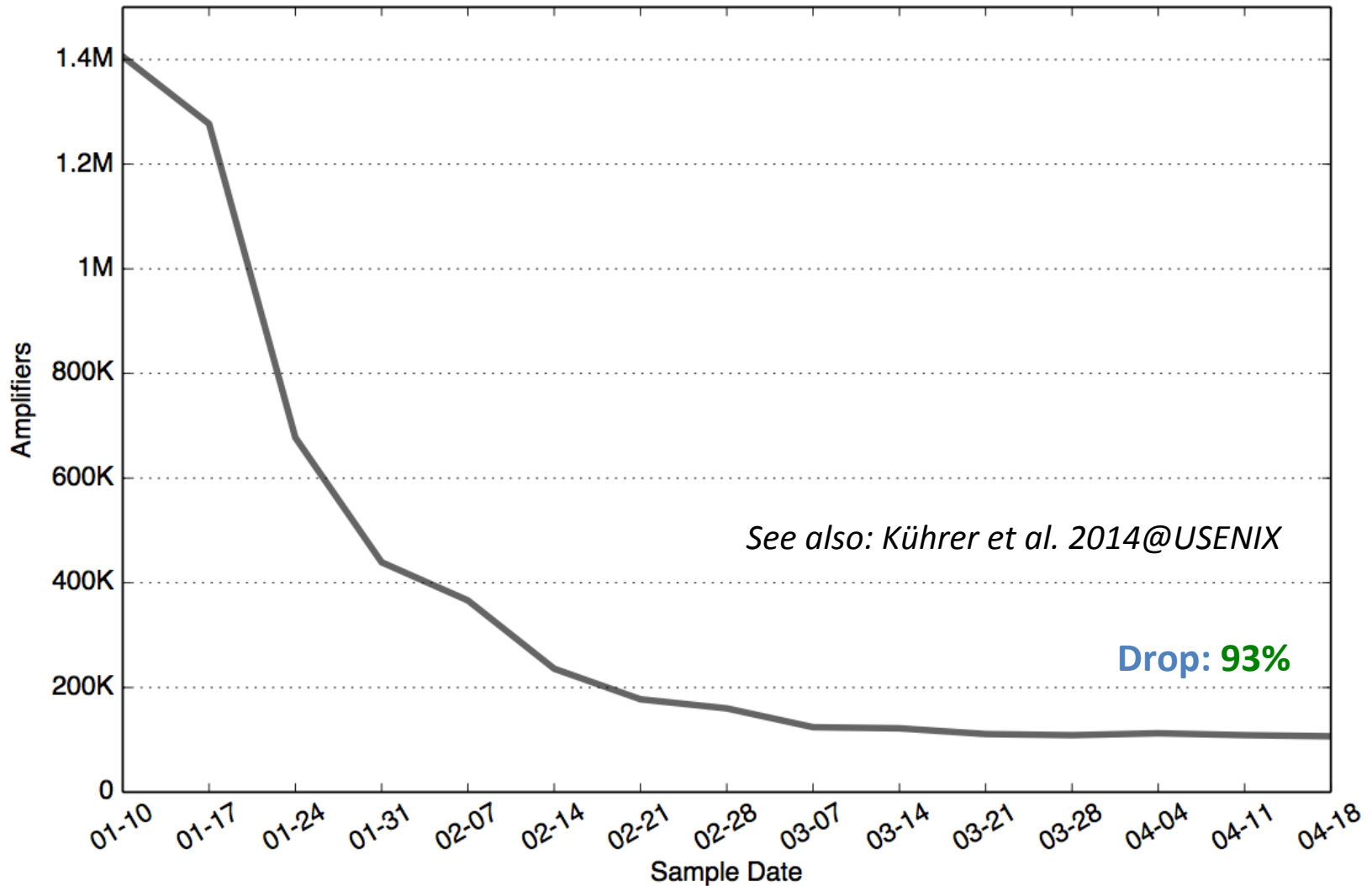
NTP Attacks

Majority of Large Attacks

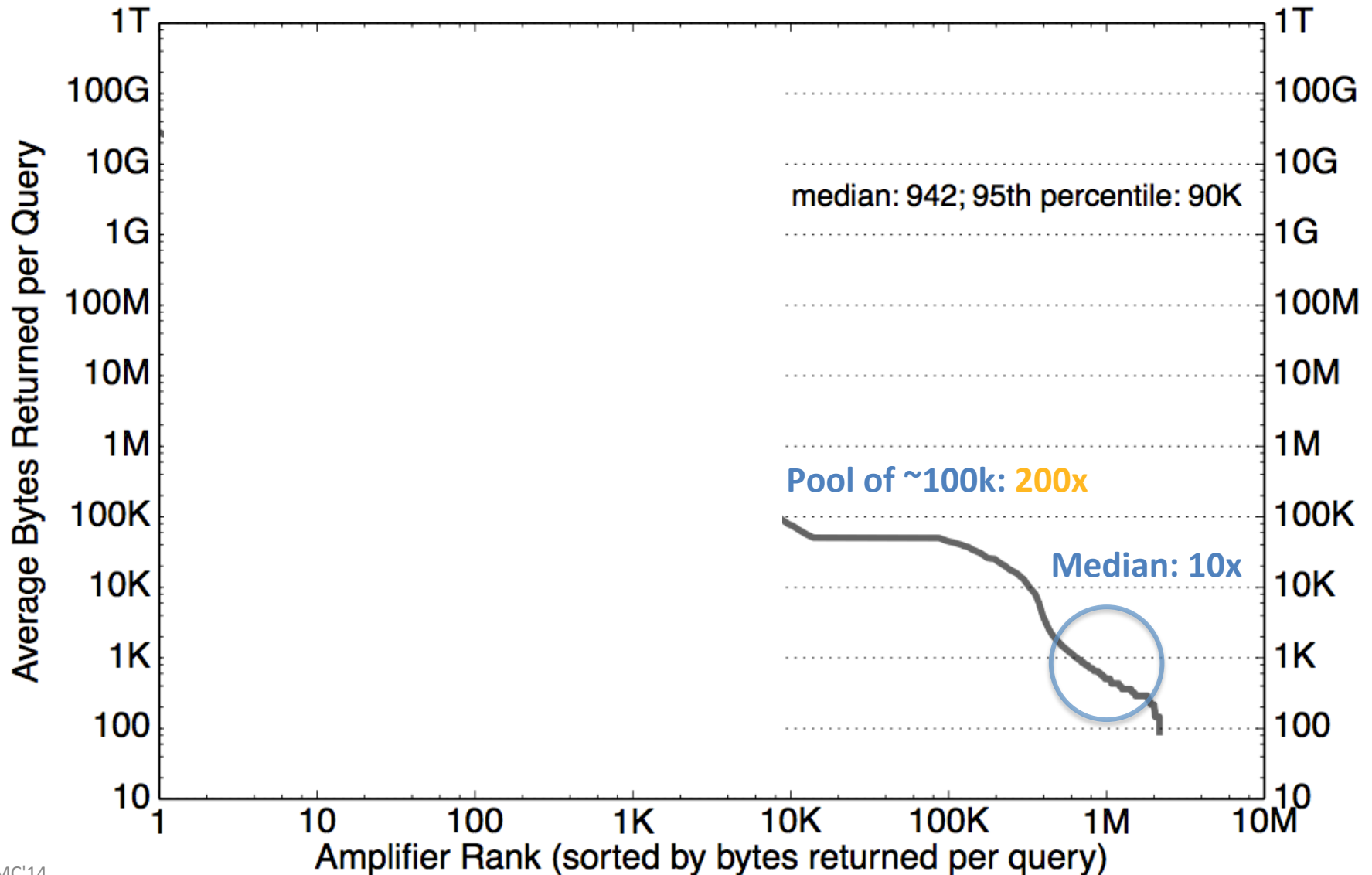


Negligible Fraction of all DDoS

NTP monlist Amplifier Population



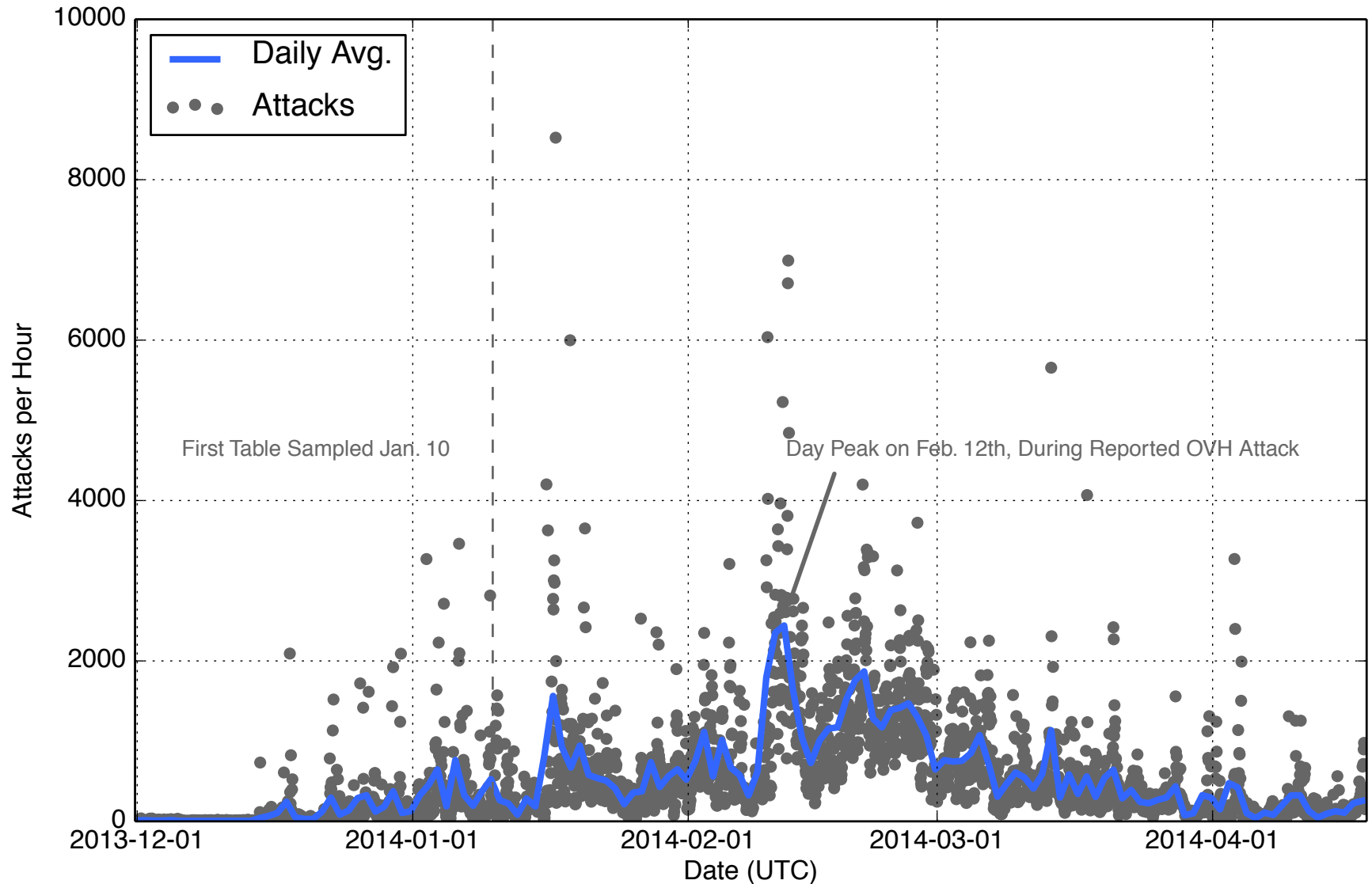
Amplifier Power



The monlist Table

remote address	port	local address	count	m	ver	rstr	avgint	lstint
204.	37164	0.0.0.0	5	7	2	0	3835	0
217.	123	0.0.0.0	1041759	7	2	0	0	0
204.	80	0.0.0.0	135	7	2	0	1	0
31.	27	0.0.0.0	35843	7	2	0	0	0
192.	8088	0.0.0.0	52071	7	2	0	0	0
198.	27016	0.0.0.0	21282	7	2	0	0	0
75.	3074	0.0.0.0	1	7	2	0	0	1
128.	43009	0.0.0.0	29430	3	3	0	63	2
75.	80	0.0.0.0	10	7	2	0	9	2
174.	9987	0.0.0.0	281	7	2	0	11	3
101.	3074	0.0.0.0	2	7	2	0	6	4
98.	53	0.0.0.0	2	7	2	0	6	4
5.	25565	0.0.0.0	1163	7	2	0	5	4
108.	3074	0.0.0.0	2	7	2	0	12	4
198.	3074	0.0.0.0	11	7	2	0	11	5

Attack Time Series



Top Attacked Ports

Rank	Attacked Port	Fraction	Common UDP Use
1	80	0.362	None. via TCP:HTTP (<i>g</i>)
2	123	0.238	NTP server port
3	3074	0.079	XBox Live (<i>g</i>)
4	50557	0.062	Unknown
5	53	0.025	DNS; XBox Live (<i>g</i>)
6	25565	0.021	Minecraft (<i>g</i>)
7	19	0.012	chargen protocol
8	22	0.011	None. via TCP:SSH
9	5223	0.007	Playstation (<i>g</i>); other
10	27015	0.006	Steam/e.g. Half-Life (<i>g</i>)
11	43594	0.004	Runescape (<i>g</i>)
12	9987	0.004	TeamSpeak3 (<i>g</i>)
13	8080	0.004	None. via TCP:HTTP alt.
14	6005	0.003	Unknown
15	7777	0.003	Several games (<i>g</i>); other
16	2052	0.003	Star Wars (<i>g</i>)
17	1025	0.002	Win RPC; other
18	1026	0.002	Win RPC; other
19	88	0.002	XBox Live (<i>g</i>)
20	90	0.002	DNSIX (military)

10+ of Top-20 Ports are
Gaming-related



Understanding the Emerging Threat of DDoS-as-a-Service

Mohammad Karami and Damon McCoy

George Mason University

What this Talk is About

- Booter services are **commoditizing** DDoS
- DDoS as subscription based service
 - Tiered pricing (Payment via PayPal)
 - Easy to use website interface
 - Ability to DDoS medium-end webserver
- Use leaked backend data from TWBooter to gain insight

[Quantum Booter - Stress Testing Service](#)

[quantumbooter.net/](#) ▼

Quantum **Booter** utilizes high powered dedicated servers to **stress test**. We are constantly upgrading our servers to fulfill the power needs of our clients. We only ...

[Grim Booter](#)

[grimboot.com/tos.php](#) ▼

Permission is granted to **stress test** dedicated servers and networks owned by you. ...
You are liable for what you do at <http://grimbooter.com>, if you break any of ...

[DESTRESS BOOTER Home](#)

[destressbooter.com/](#) ▼

THE BEST **BOOTER**. ... Protected. Destress **Booter** is powered by quick, strong, and DDoS protected servers to guarantee uptime and stability. With the ...

[Orion Booter - Powered by InfernoAPI](#)

[www.orionbooter.com/](#) ▼

We are not responsible how you use this **booter**, the website was meant to be used as a **stress network tester**. 4. Sharing your account will result in suspension ...

[ToxicBoot | Login](#)

[toxicboot.net/](#) ▼

Login. Username: Password: By Logging in you agree to all Terms of service.

[Opaque Booter - Home](#)

[opaquebooter.weebly.com/](#) ▼

Create a free website with Weebly. Quantum **Booter**. Affordable and professional stress testing service. Main · **Stress Test** · User CP · Forums · Tools · Logout ...









[\[FREE\] JabXBooter | Stress Tester | UDP | 250+ Shells *Powerful ...](#)

[www.hackcommunity.com](#) › ... › [Hacking Tools and Similar Applications](#) ▼



Sep 28, 2011 - 10 posts - 4 authors

RE: [FREE] JabXBooter | **Stress Tester** | UDP | 250+ Shells *Powerful. **Booters** are worthless, but that's my opinion. RAT servers 4ever lol ...

Important Threads

	#1 Big Bang Booter [>TAKES EVERYTHING DOWN<] Skype BETA 10800 Seconds DDoS Attacks (Pages: 1 2 3 4 ... 57) Prime	5
	REBOOT \$1.99 20+ GBPS 100% UPTIME LAYER 4&7 BETA SKYPE RESOLVER STOP BTN (Pages: 1 2 3 4 ... 35) Joey	3
	OLYMPUS STRESSER 12 ATTACK METHODS UNTRACEABLE CUSTOM SOURCE UNIQUE FEATURES (Pages: 1 2 3 4 ... 59) MineSQL	5
	DDoS Em SKYPE RESOLVER HOUR BOOTS WITH 25+GPBS EXTREMELY POWERFUL BEST ON HF (Pages: 1 2 3 4 ... 13) Platinum	1
	MASTER BOOT 40+GBPS AUTO BUY STOP ATTACK Ran by adults no BS. (Pages: 1 2 3 4 ... 20) iNviZ	1
	NetStress 12GBPS 3600 SECONDS SKYPE BETA RESOLVER CUSTOM SOURCE STOP BUTTON (Pages: 1 2 3) Lani	
	xBOOT Drops it like it's hot 12 Attack Methods 65Gbps+ Capacity BEST ON HF! (Pages: 1 2 3 4 ... 24) DaL33T	2
	THBOOT (Pages: 1 2 3) Dan.	

Normal Threads

	Venom Stresser 7200 Seconds Max Boot 30GBPS Resolvers Takes Shit Down (Pages: 1 2 3) Perfect	5
	#1 Maximboot - Unlimited boot time 65Gbps+ More Features Stop Button BuyNow! (Pages: 1 2 3 4 ... 13) ...	1



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

You can upgrade to paid version by completing survey, start now by clicking [here](#)

Global Message: Server replaced

Domain/Skype Resolver:

Host

Resolve

IP Address: 1.1.1.1

80

Time: 54 seconds(s)

Power: 50%

Start Attack

- Layer4
 - ✓ UDP
 - ESSYN
 - SkypeCloud
 - TCP Amp
 - UDP-Lag
- Layer-7
 - Source
 - MIME
 - RUDY
 - ARME
 - GET
 - HEAD
 - POST
 - Slowloris

Booter Statistics

Status: **Online**

Total Users: 1203

Users Online: 11

Attacks Running: 2/3

User Statistics

Boots Initiated: 0

Current IP: 5.254.149.156

Subscription Ends: Free

Concurrent Attacks: 1 attacks

Max Boot time: 300 sec

Server Status

Server Alpha [?]: **Available**

Question?

Click here to chat with us!

How to Setup Booter Service

- Step 1: Website code
 - Asylumbooter source code is available at:
<http://softwaretopic.informer.com/asylum-booter-source/>
- Step 2: Attack Infrastructure
 - Rent or use compromised servers
- Step 3: Establish payment via PayPal
- Step 4: Advertise on Hackforums and Gamer sites
- Step 5: Profit \$\$\$

Dataset

- Publicly post backend data from TWBooter2

Duration	Users	Victims	Attacks
Jan. 2013 - Mar. 2013	312	11,174	48,844

- Includes information on all attacks
 - IP/Domain targeted, type, duration, client
 - Confirmed details of attacks with one victim
- Provides insight into infrastructure, users, and victims

Attack Infrastructure

- 15 servers total servers
 - 3 active the entire two months
 - Most hosted at a Netherlands ISP
 - 9 active at the time of data leak
- Offered SYN flood, UDP flood and amplification attacks, HTTP-based attacks including HTTP POST/GET/HEAD and RUDY (R-U-Dead-Yet)

Attack Capacity

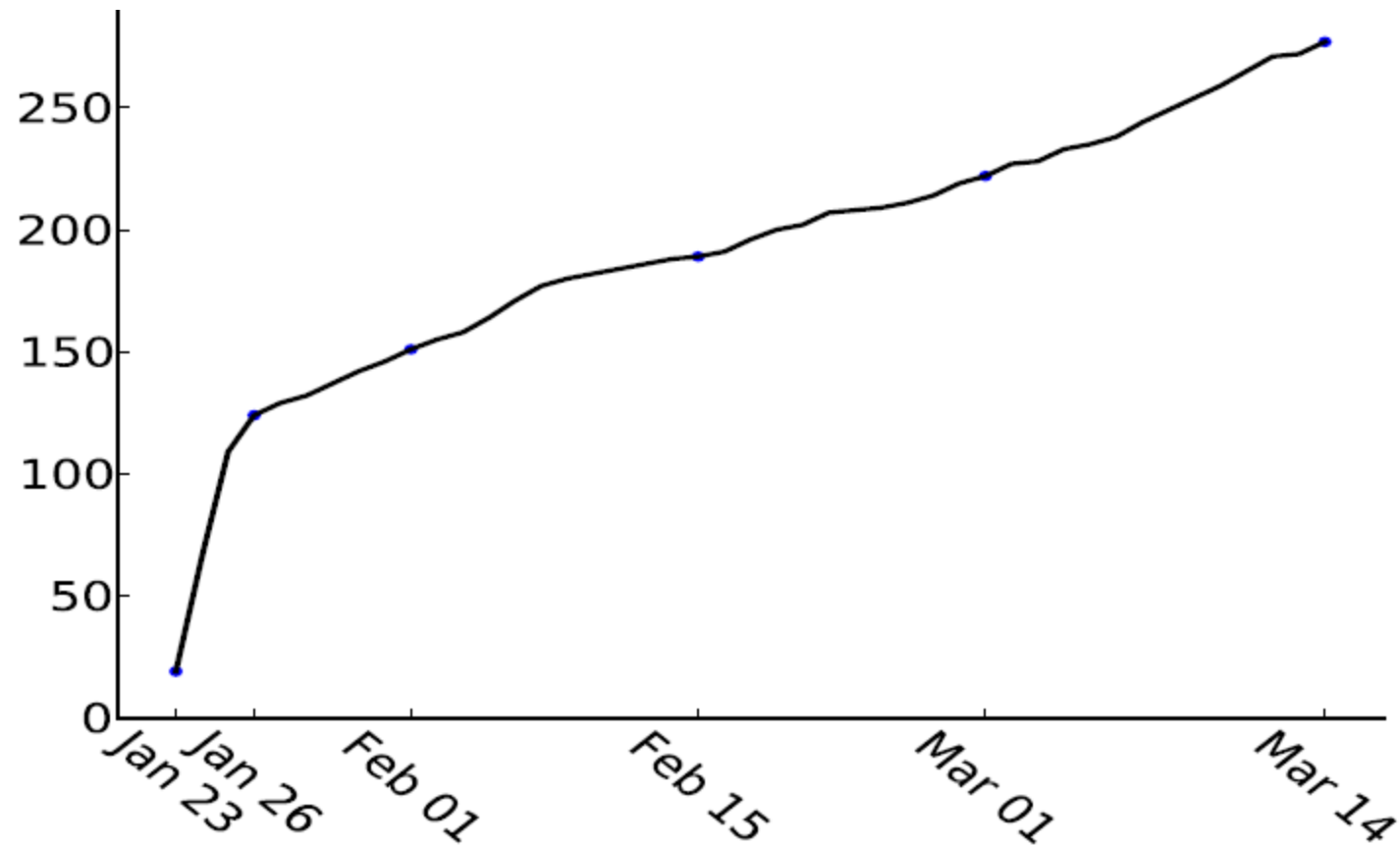
- Subscribed to service to measure capacity.
- SYN Floods spoof IP
- UDP Flood uses DNS amplification

Attack Type	# of packets	Avg. packet size	Volume
UDP Flood	4,552,899	1,363 bytes	827 MBit/sec
SYN Flood	5,625,086	54 bytes	40 MBit/sec

- HTTP used 26,296 proxy servers over 5 mins
 - Some of these leaked original attack servers IPs

User Growth Rate

- After initial burst growth rate of 3.2 Users



User Subscriptions

- Categorized users based on subscription type
 - Gamers \leq 10 Min attacks (65%)
 - Website \geq 1 hour attacks (32%)
 - Privileged unlimited attacks (3%)
- TwBooter earned \$7,727/month based on subscription type

Victims

- 10,485 unique IP addresses attacked
- 689 identified as websites
 - Most are either game servers or game forums
 - Other booters and bloggers also targeted
- Two users attacked government sites for 142 hours
 - Two Indian government
 - Los Angeles police department

