ARBOR® NETWORKS

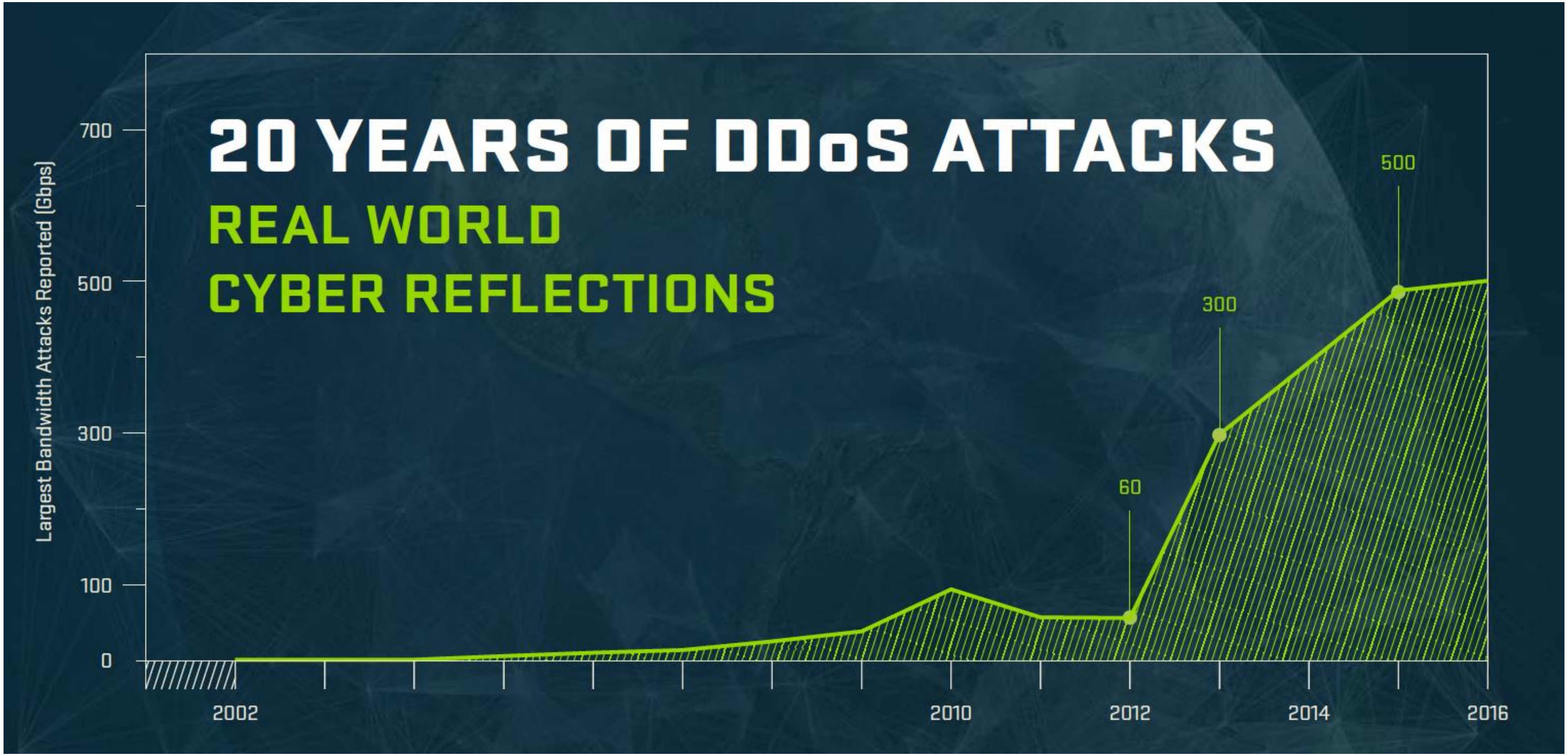
The Security Division of NETSCOUT

THE STAKES HAVE CHANGED

The Changing Security Landscape

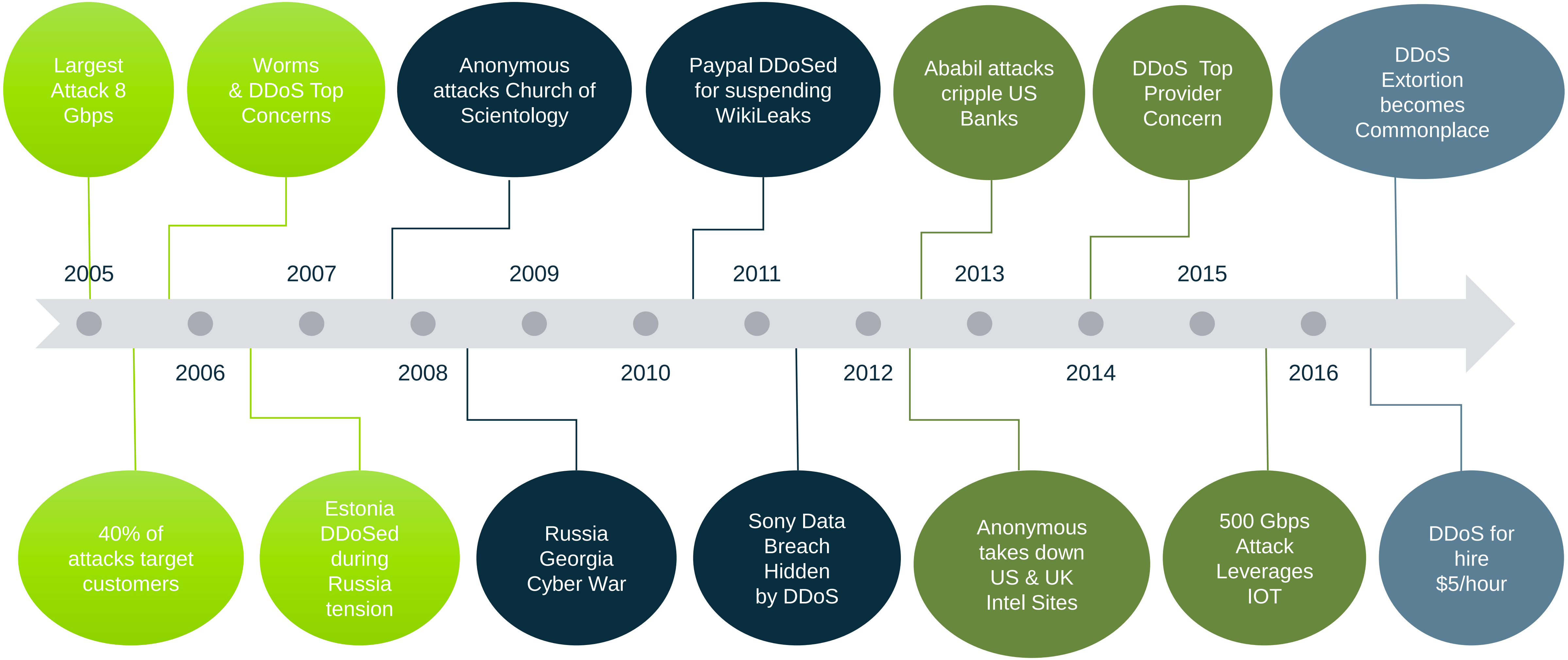
C F Chui,
Principal Security Technologist

20 Years of DDoS Attacks



©2017 ARBOR® CONFIDENTIAL & PROPRIETARY

The Long History of DDoS…



Largest Attack 8 Gbps

40% of attacks target customers

Worms & DDoS Top Concerns

Estonia DDoSed during Russia tension

Anonymous attacks Church of Scientology

Russia Georgia Cyber War

Paypal DDoSed for suspending WikiLeaks

Sony Data Breach Hidden by DDoS

Ababil attacks cripple US Banks

Anonymous takes down US & UK Intel Sites

DDoS Top Provider Concern

500 Gbps Attack Leverages IOT

DDoS Extortion becomes Commonplace

DDoS for hire $5/hour

ARBOR NETWORKS

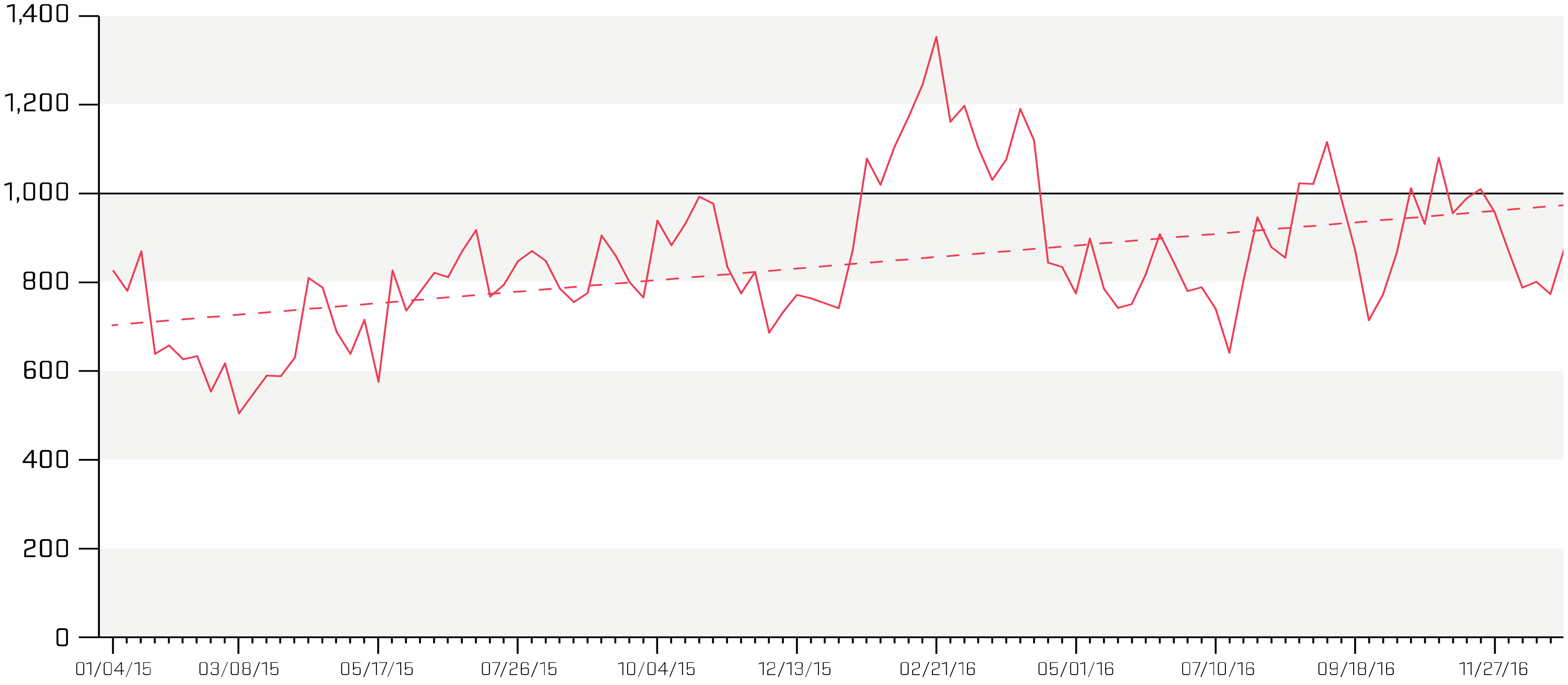
DDoS: Size

558 attacks over 100 Gbps, as opposed to 223 in 2015

87 attacks over 200 Gbps, as opposed to 16 in 2015

Average attack size increased by 23%, trending towards 1.2 Gbps

Average Attack Size (Mbps), 2015–2016

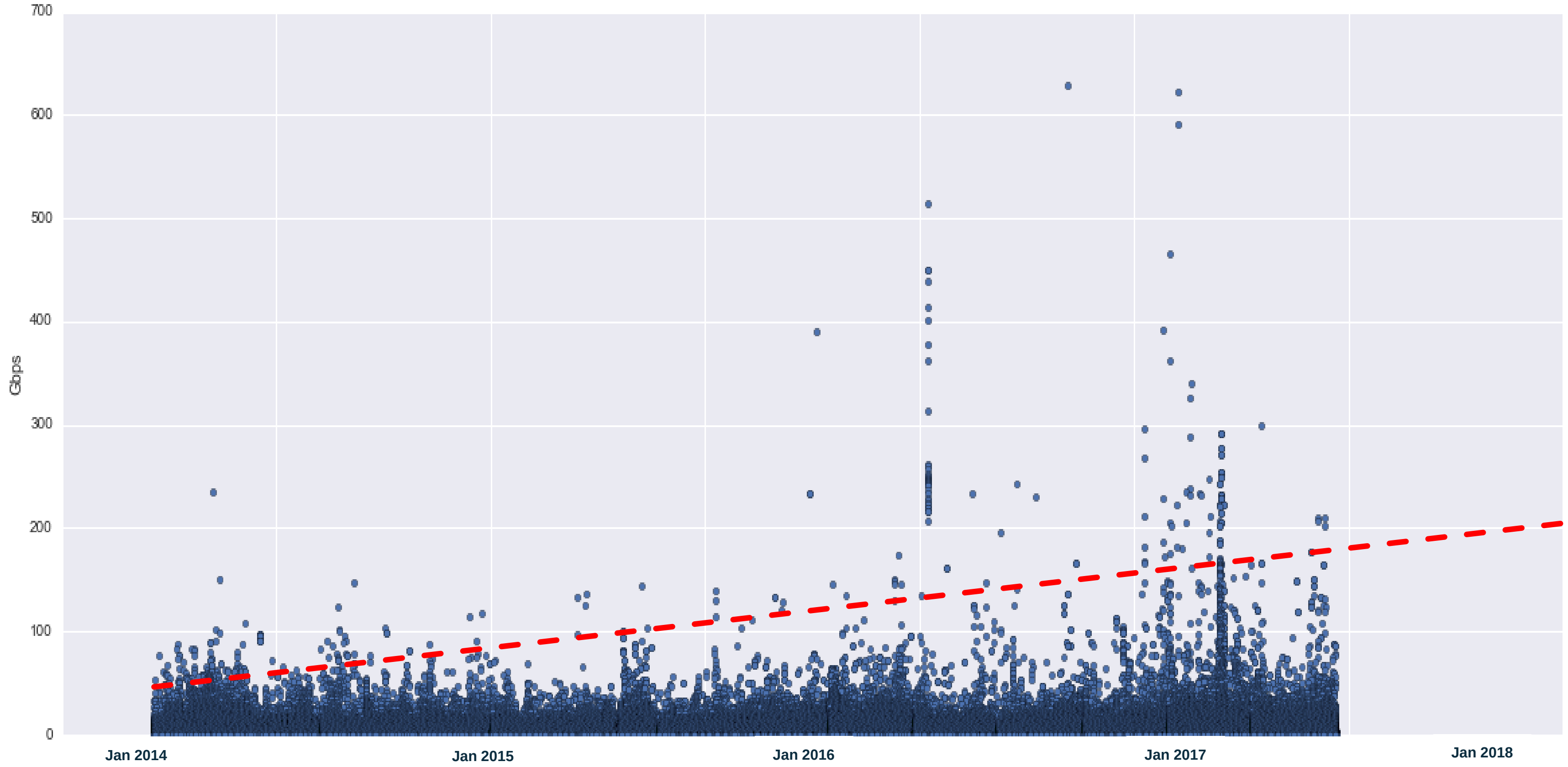


Source: Arbor Networks, Inc.

DDoS: Size

APAC attacks between 2014 to 2017

Lot more attacks over 200 Gbps



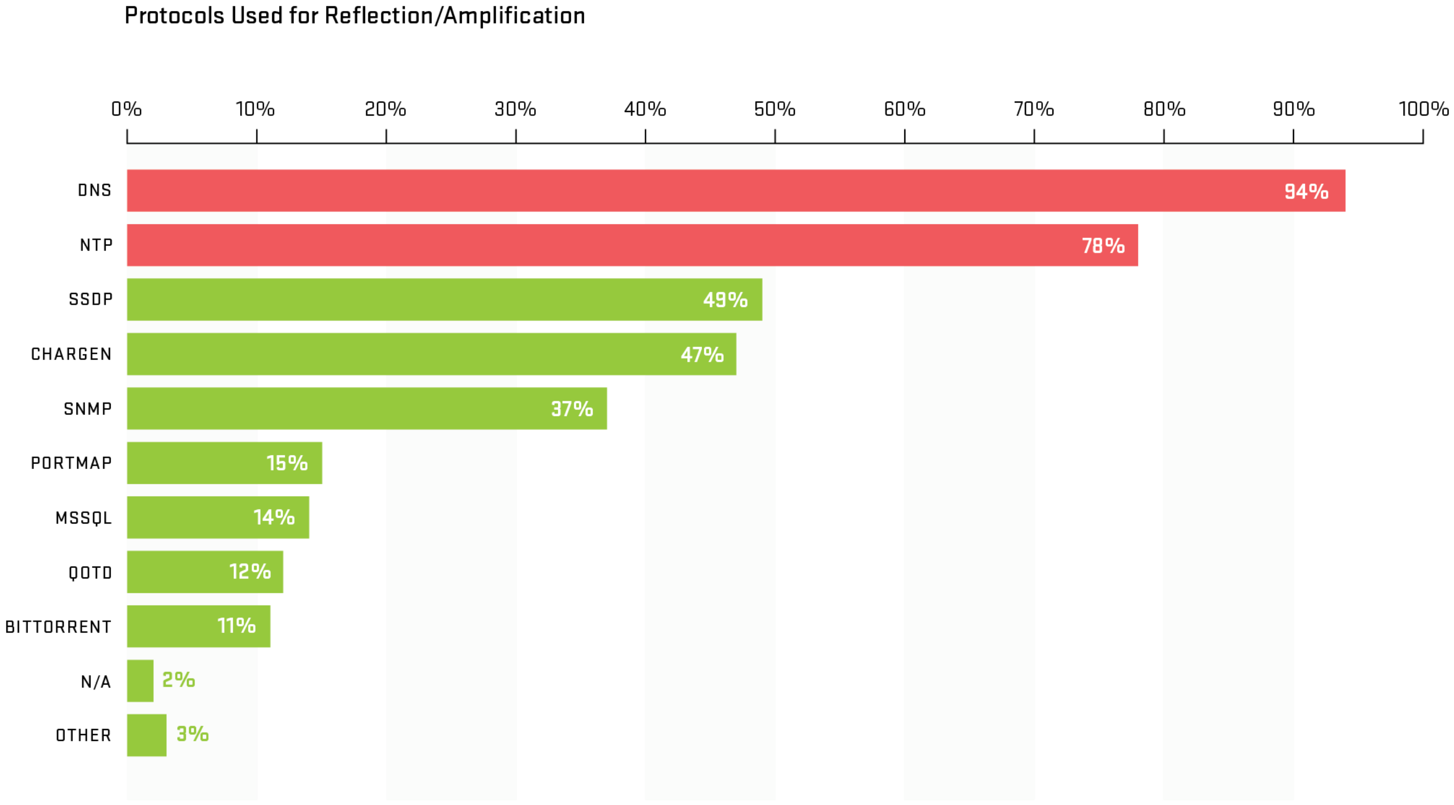
DDoS : The Reflection Problem

NOT gone away

18,500 DNS attacks / Week

498Gbps Attack using NTP

Multiple > 400Gbps



Source: Arbor Networks, Inc.

DDoS : Frequency

21% of Data-Centers see more than 50 Attacks per month

45% of Enterprise see more than 10 attacks per month

33% of Mobile Operators see more than 20 attacks per month at SGi

ARBOR® NETWORKS

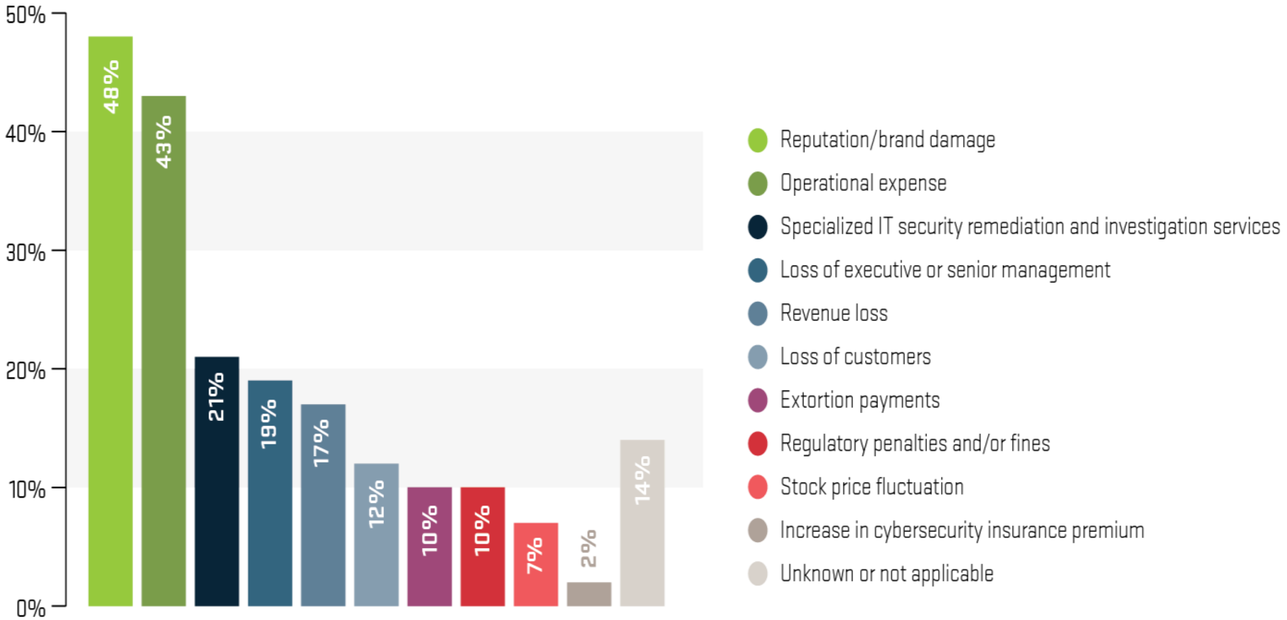
DDoS : Frequency

23% of Data-Centers estimate cost of DDOS attack > $100K

59% of Enterprises estimate downtime cost > $500/min

Two-Thirds of Enterprises factor DDoS into risk assessment process

Business Impacts of DDoS Attacks



Source: Arbor Networks, Inc.

DDoS : Complexity

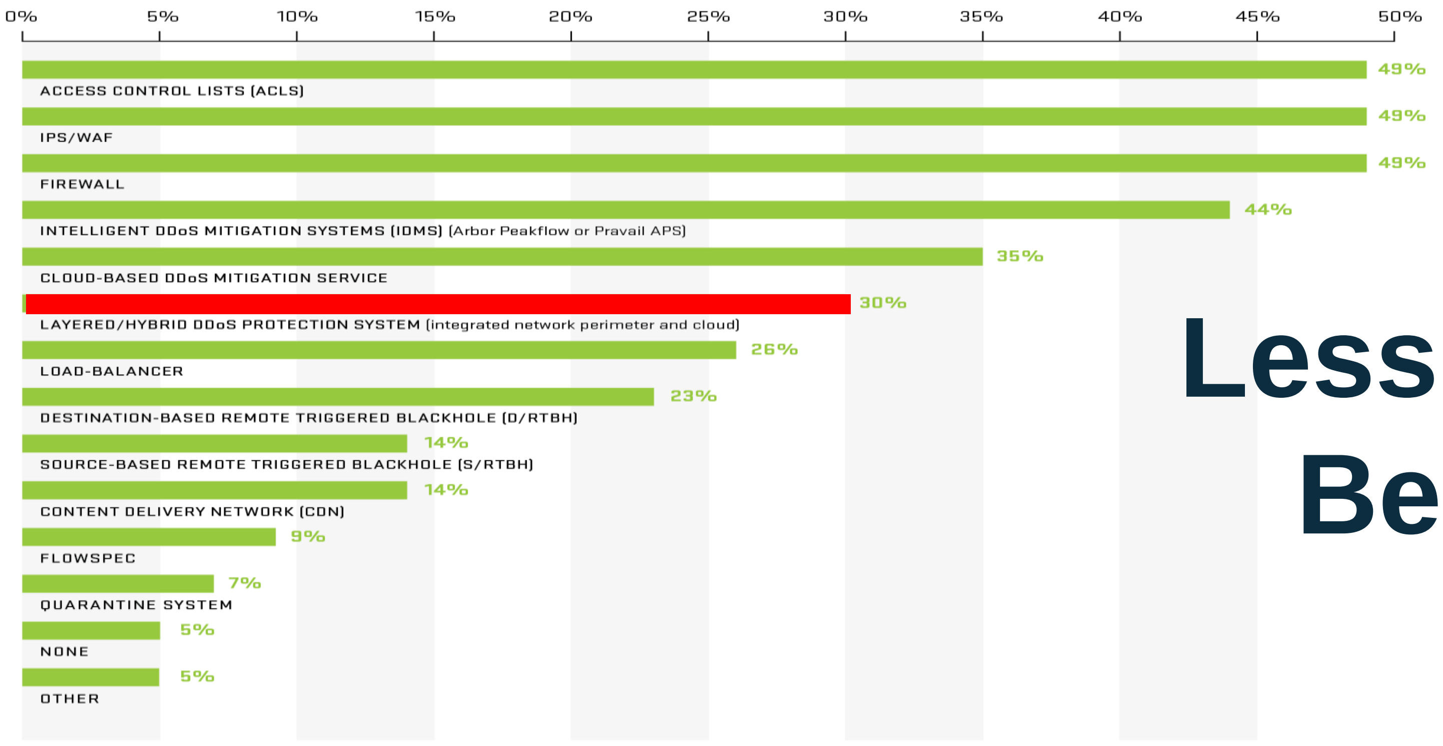
95%

67%

Application-Layer Attacks

Multi-Vector Attacks

DDoS : Dealing With It

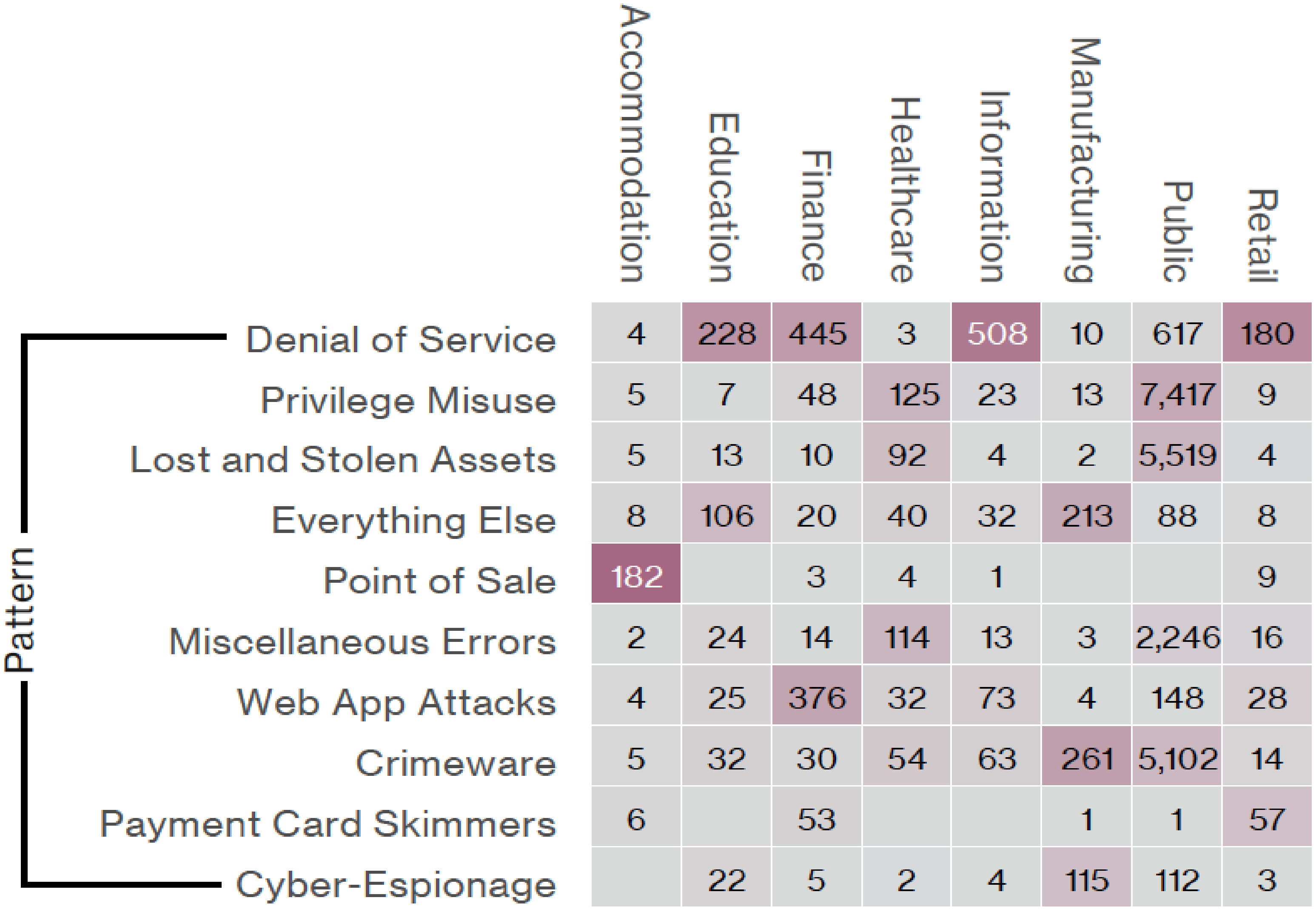


DDoS Mitigation Techniques

Source: Arbor Networks, Inc.

Less than 1/3 Use Best-Practice

Uptick in DDoS attacks



Pattern	Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
Denial of Service	4	228	445	3	508	10	617	180
Privilege Misuse	5	7	48	125	23	13	7,417	9
Lost and Stolen Assets	5	13	10	92	4	2	5,519	4
Everything Else	8	106	20	40	32	213	88	8
Point of Sale	182		3	4	1			9
Miscellaneous Errors	2	24	14	114	13	3	2,246	16
Web App Attacks	4	25	376	32	73	4	148	28
Crimeware	5	32	30	54	63	261	5,102	14
Payment Card Skimmers	6		53			1	1	57
Cyber-Espionage		22	5	2	4	115	112	3

Verizon: 2017 Data Breach Investigations Report

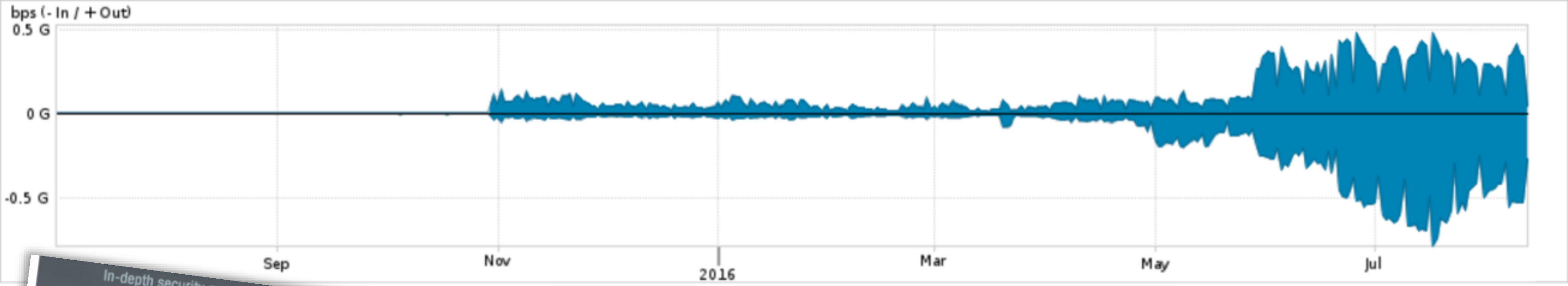
…and its only. JUST. BEGINNING.

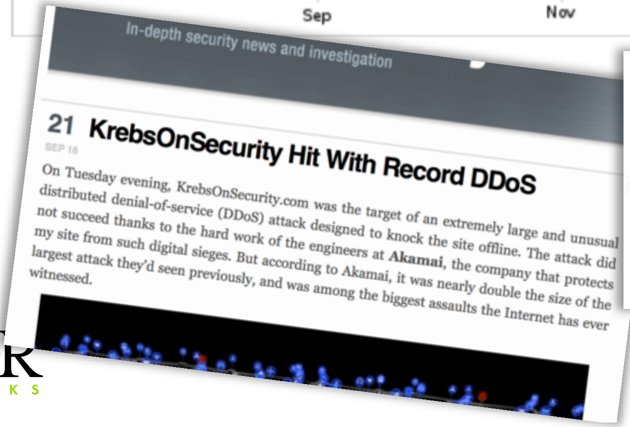
Example of malware infection method: Cameras and DVRs logging data using hard-coded Telnet passwords. **A 20+ year old problem…**

Most of the devices are embedded with Linux BusyBox, there's no easy fix other than disconnecting the devices. **GOOD LUCK!**

2015 | 2016 ARBOR

TELNET traffic monitored by Arbor since last year

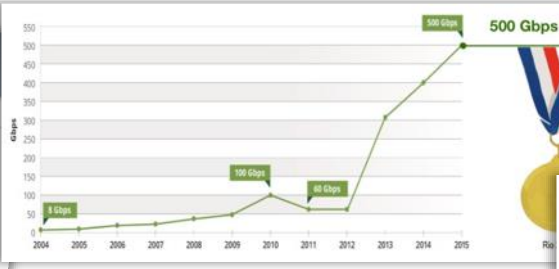


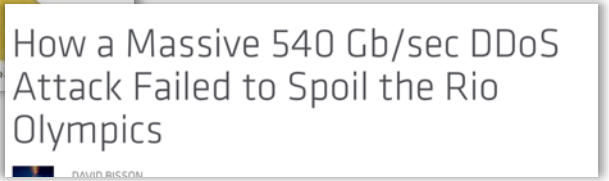


In-depth security news and investigation

21 SEP 16 **KrebsOnSecurity Hit With Record DDoS**

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

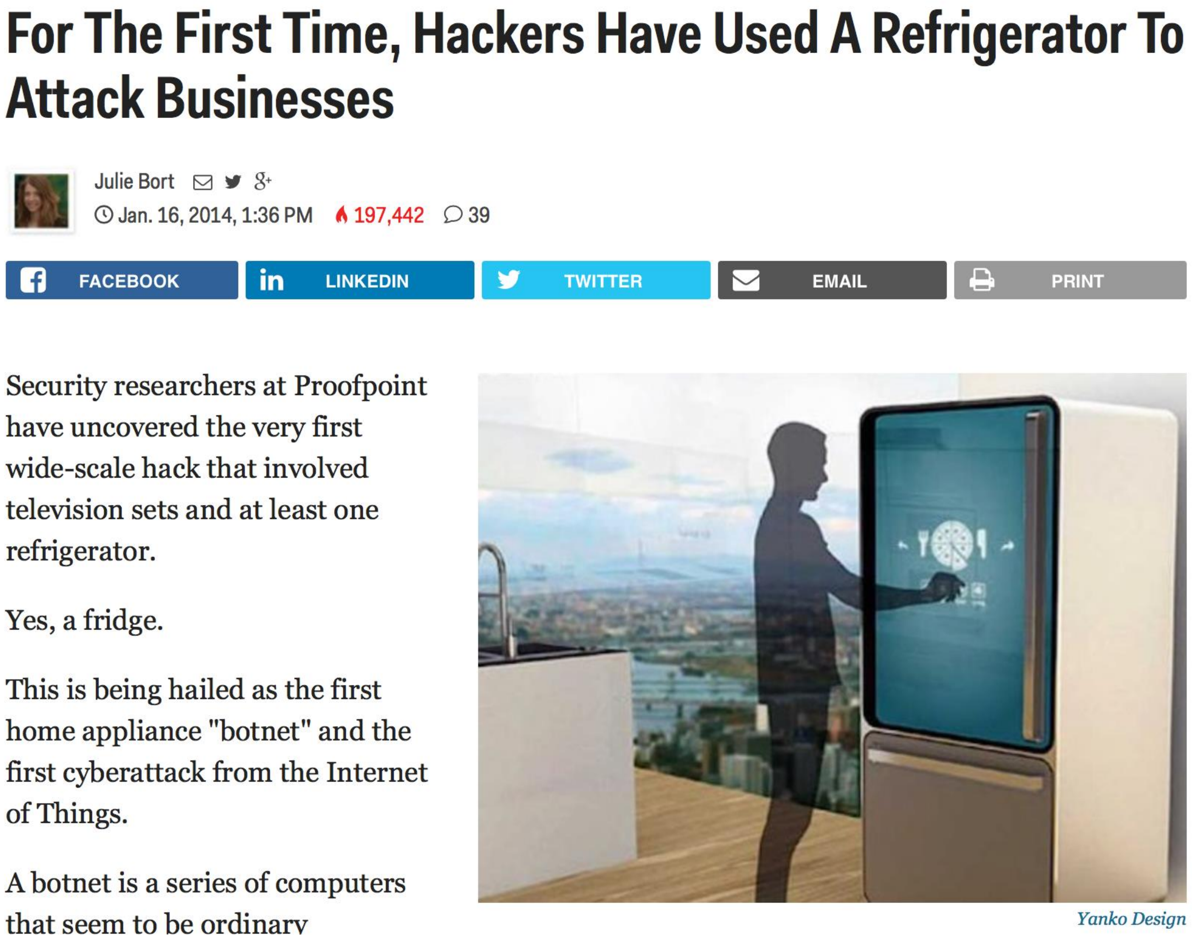




How a Massive 540 Gb/sec DDoS Attack Failed to Spoil the Rio Olympics

DAVID BISSON

Internet of Things



For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

Julie Bort

Jan. 16, 2014, 1:36 PM 197,442 39

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

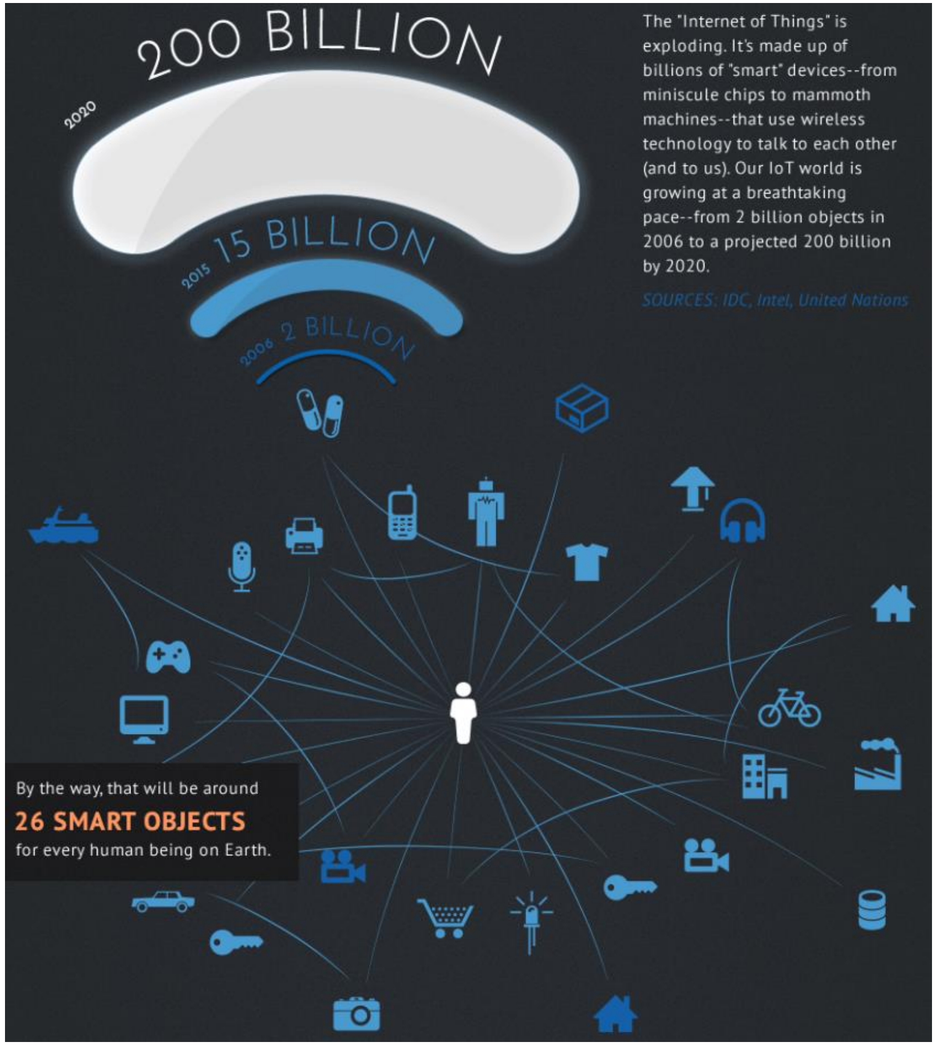
Security researchers at Proofpoint have uncovered the very first wide-scale hack that involved television sets and at least one refrigerator.

Yes, a fridge.

This is being hailed as the first home appliance "botnet" and the first cyberattack from the Internet of Things.

A botnet is a series of computers that seem to be ordinary

Yanko Design



The "Internet of Things" is exploding. It's made up of billions of "smart" devices--from miniscule chips to mammoth machines--that use wireless technology to talk to each other (and to us). Our IoT world is growing at a breathtaking pace--from 2 billion objects in 2006 to a projected 200 billion by 2020.

SOURCES: IDC, Intel, United Nations

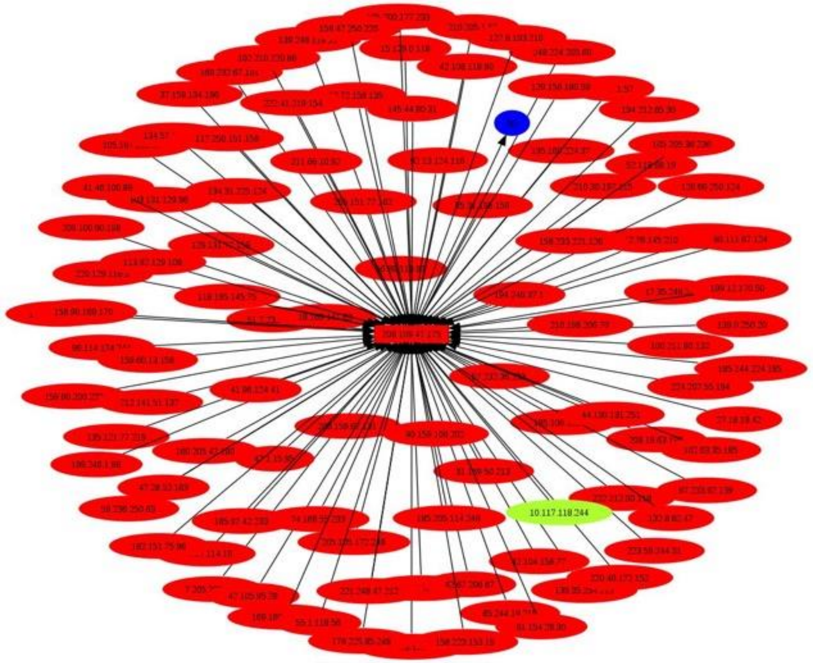
By the way, that will be around **26 SMART OBJECTS** for every human being on Earth.

Internet of Things

- More and more low-cost devices being pushed to the web.
- Safety and security taking a back seat.
- Devices that won’t or can’t be patched.
- Enslaved in bot armies through password guessing.
- We need to think about these devices as populations with yield.
- LizardStressor is sourced predominately from web cams.

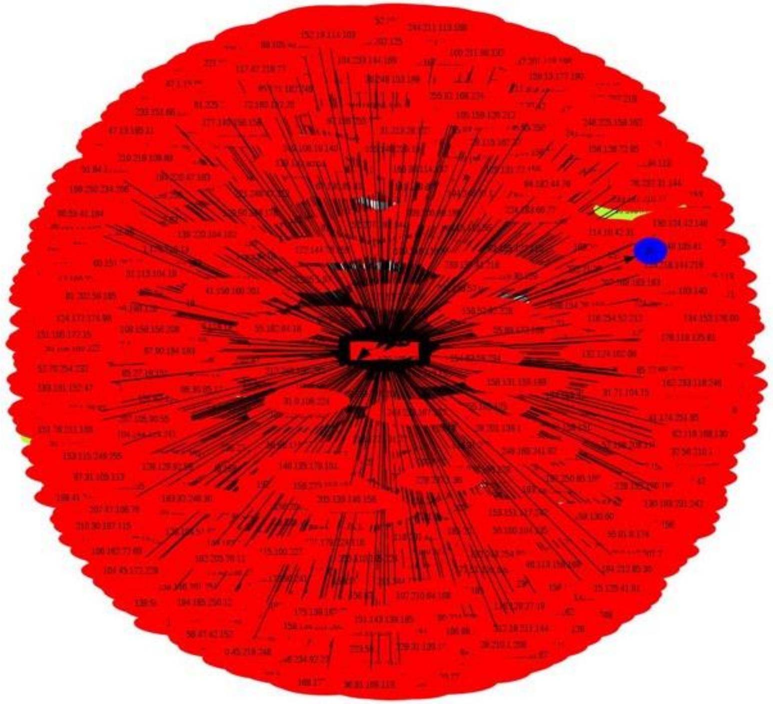
DDoS Scale Like Never Before...

LEGACY BOTNET
10’S OF THOUSANDS
OF HOSTS



AfterGlow 1.6.2 - Property File: color.properties

IoT BOTNET
100’S OF THOUSANDS
TO MILLIONS OF HOSTS



AfterGlow 1.6.2 - Property File: color.properties

Ability

Fact: It's Never Been Easier to Launch a DDoS Attack. DDoS attack tools and DDoS for Hire Services add to the weaponization of DDoS.

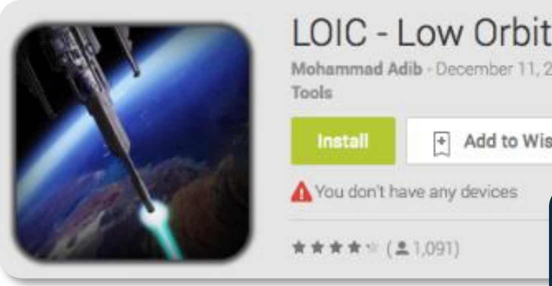
$5:$100sK

$\underbrace{\text{\$5}}_{\text{Cost of DDoS Service}}:\underbrace{\text{\$100sK}}_{\text{Impact to Victim}}$

Cost of DDoS Service

Impact to Victim

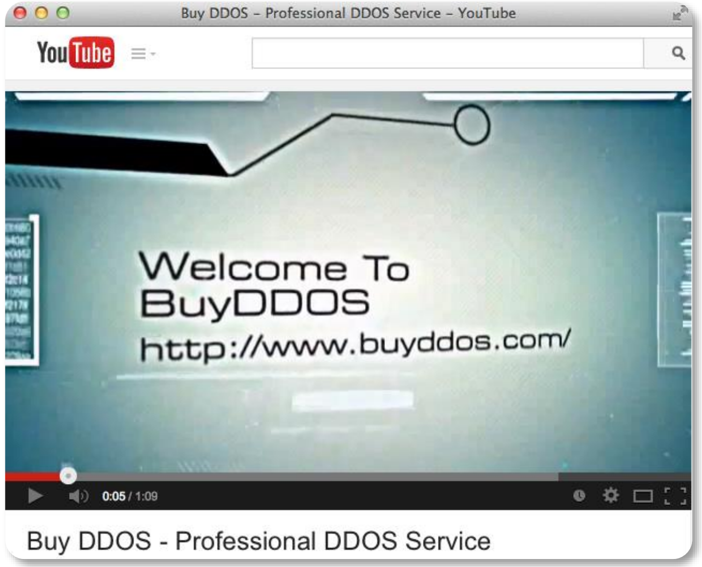
DDoS Attacks Are The Great Equalizer…



LOIC - Low Orbit Ion Cannon

Mohammad Adib - December 11, 2013

Tools



Buy DDOS - Professional DDOS Service

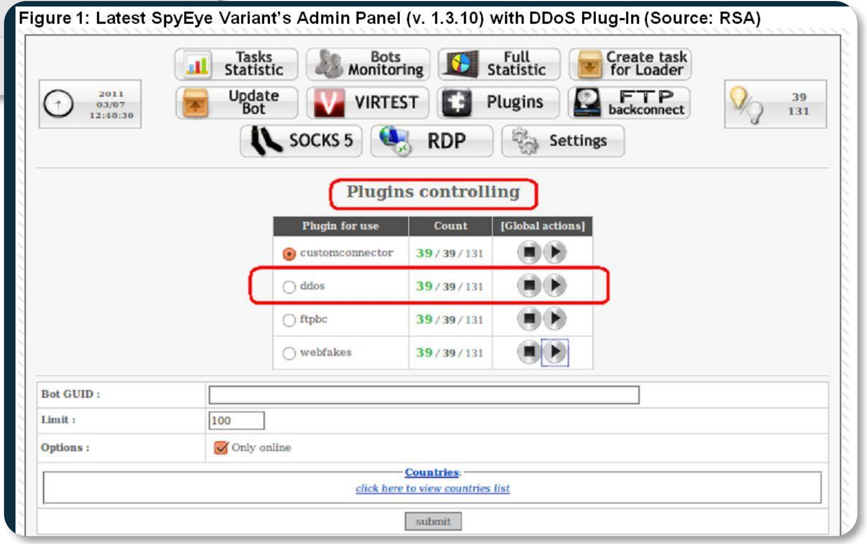


Figure 1: Latest SpyEye Variant's Admin Panel (v. 1.3.10) with DDoS Plug-In (Source: RSA)

Plugins controlling

Plugin for use	Count	[Global actions]
● customconnector	39 / 39 / 131	■ ▶
○ ddos	39 / 39 / 131	■ ▶
○ ftpbc	39 / 39 / 131	■ ▶
○ webfakes	39 / 39 / 131	■ ▶

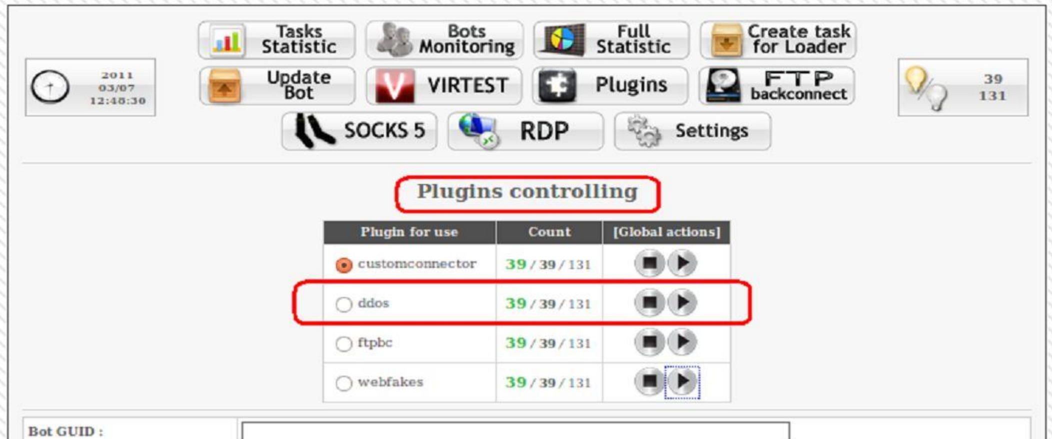
Bot GUID :	
Limit :	100
Options :	☑ Only online

Countries:
click here to view countries list

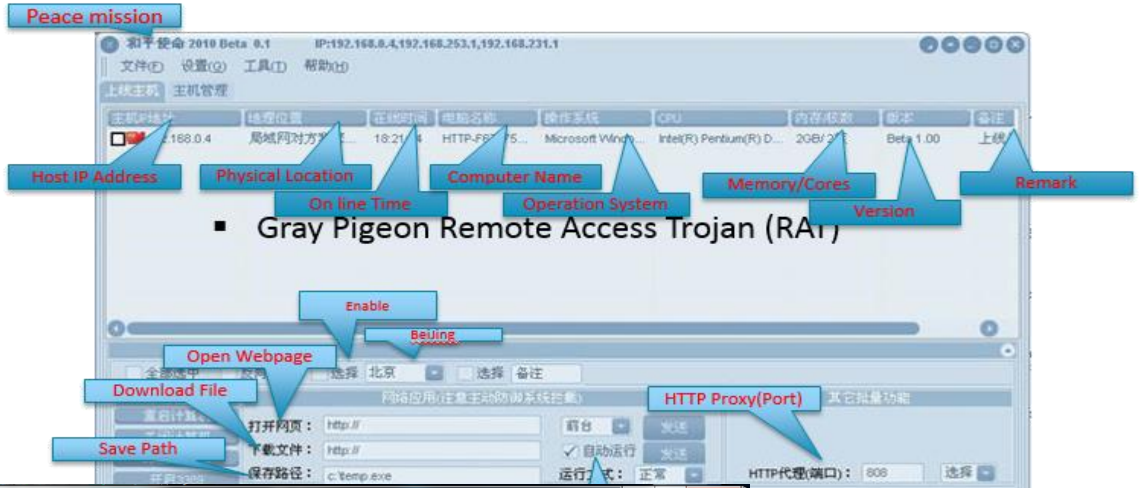
submit

Examples of Combo DDoS & Advanced Threat Tools

Figure 1: Latest SpyEye Variant's Admin Panel (v. 1.3.10) with DDoS Plug-In (Source: RSA)



Plugin for use	Count	[Global actions]
● customconnector	39 / 39 / 131	■ ▶
○ ddos	39 / 39 / 131	■ ▶
○ ftpbc	39 / 39 / 131	■ ▶
○ webfakes	39 / 39 / 131	■ ▶



.168.0.4 局域网对方 18:21 HTTP-F6 Microsoft Windo... Intel(R) Pentium(R) D... 2GB/2 Beta 1.00 上线

选择 北京 选择 备注

打开网页： http://

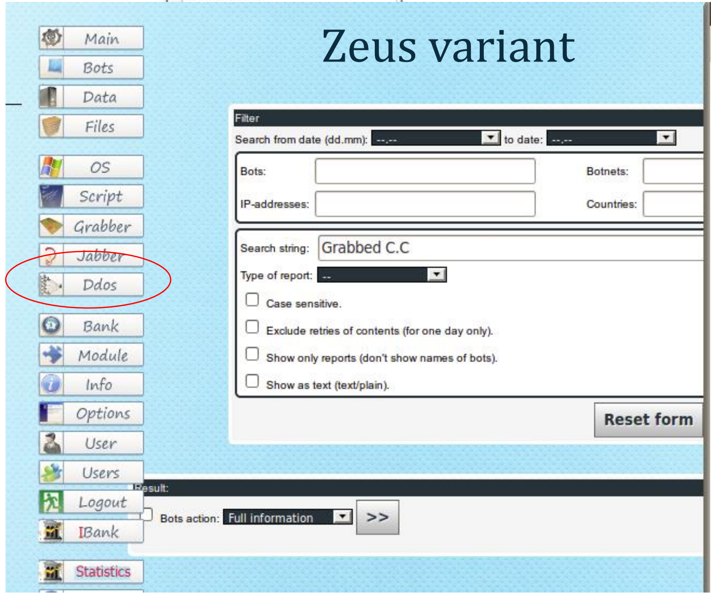
下载文件： http://

保存路径： c:\temp.exe

自动运行

HTTP代理(端口)： 808

- Gray Pigeon Remote Access Trojan (RAT)



Zeus variant

Filter

Search from date (dd.mm): --.-- to date: --.--

Bots: Botnets:

IP-addresses: Countries:

Search string: Grabbed C.C

Type of report: --

□ Case sensitive.

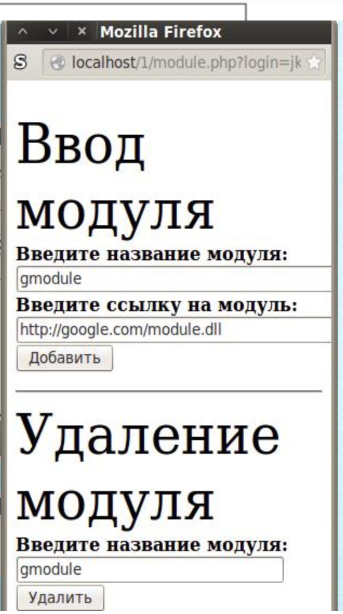
□ Exclude retries of contents (for one day only).

□ Show only reports (don't show names of bots).

□ Show as text (text/plain).

Result:

Bots action: Full information



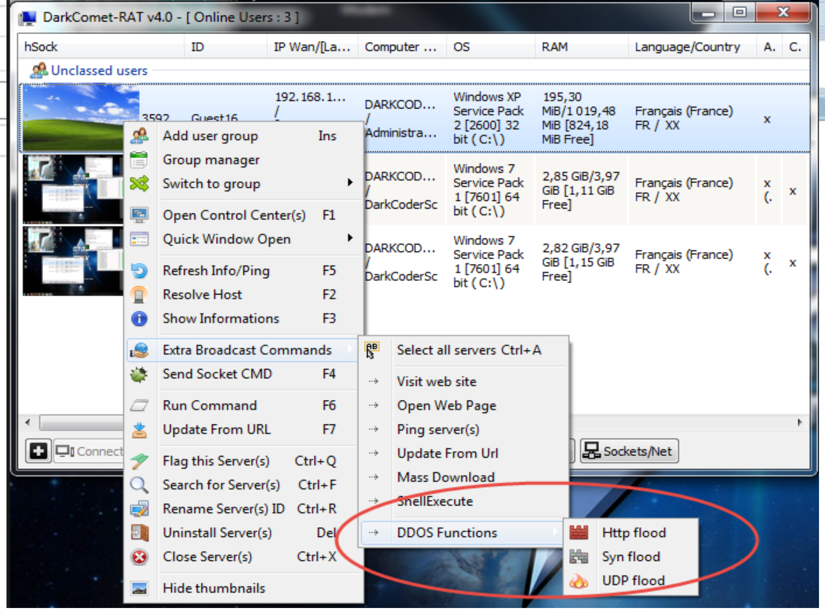
Ввод модуля

Введите название модуля: gmodule

Введите ссылку на модуль: http://google.com/module.dll

Удаление модуля

Введите название модуля: gmodule

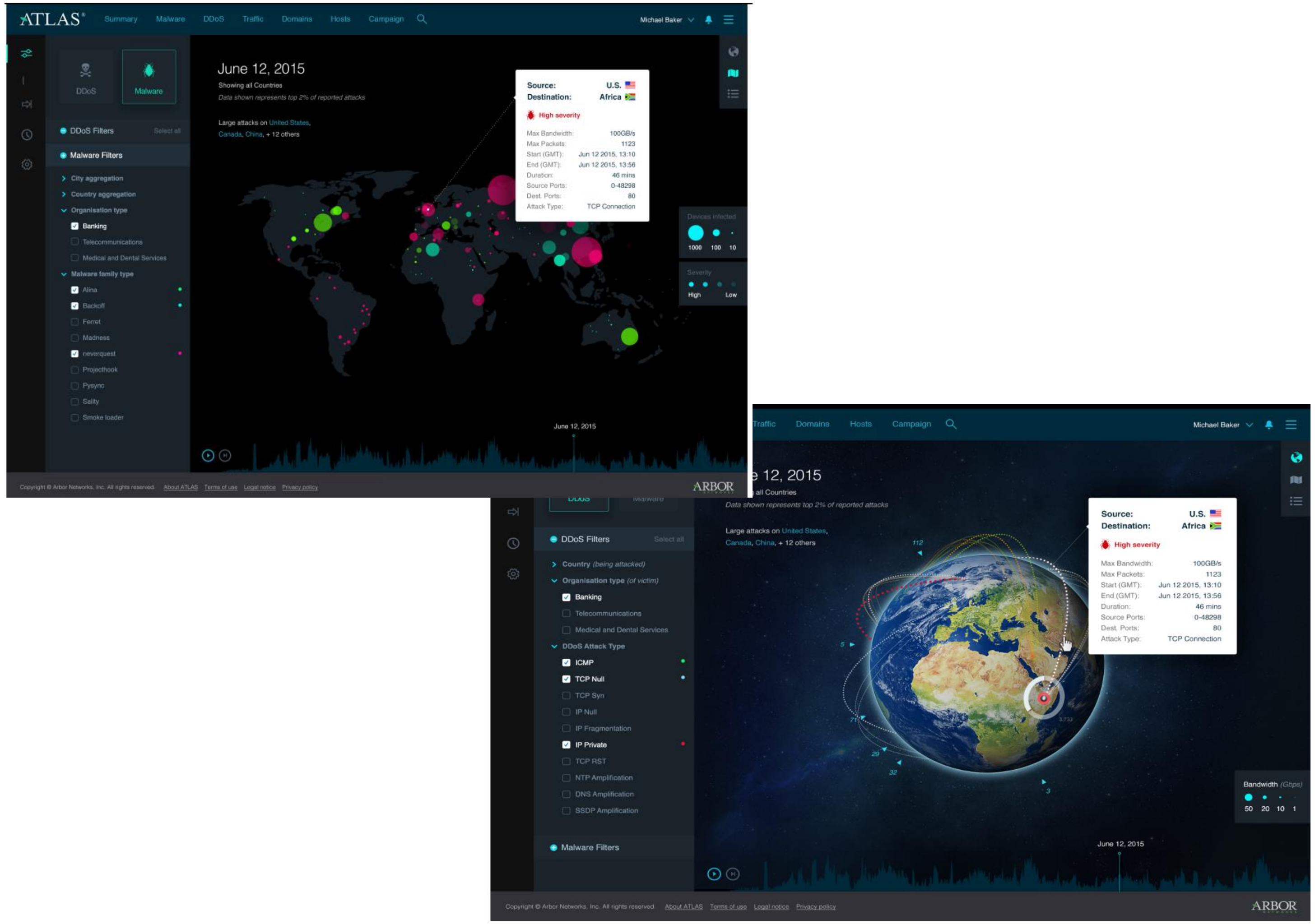


3592 Guest16 192.168.1... / DARKCOD... / Administra... Windows XP Service Pack 2 [2600] 32 bit (C:\ ) 195,30 MiB/1 019,48 MiB [824,18 MiB Free] Français (France) FR / XX x

DARKCOD... / DarkCoderSc Windows 7 Service Pack 1 [7601] 64 bit (C:\ ) 2,85 GiB/3,97 GiB [1,11 GiB Free] Français (France) FR / XX x x

DARKCOD... / DarkCoderSc Windows 7 Service Pack 1 [7601] 64 bit (C:\ ) 2,82 GiB/3,97 GiB [1,15 GiB Free] Français (France) FR / XX x x

Arbor DAM (Digital Attack Map)



Source: U.S.
Destination: Africa
High severity

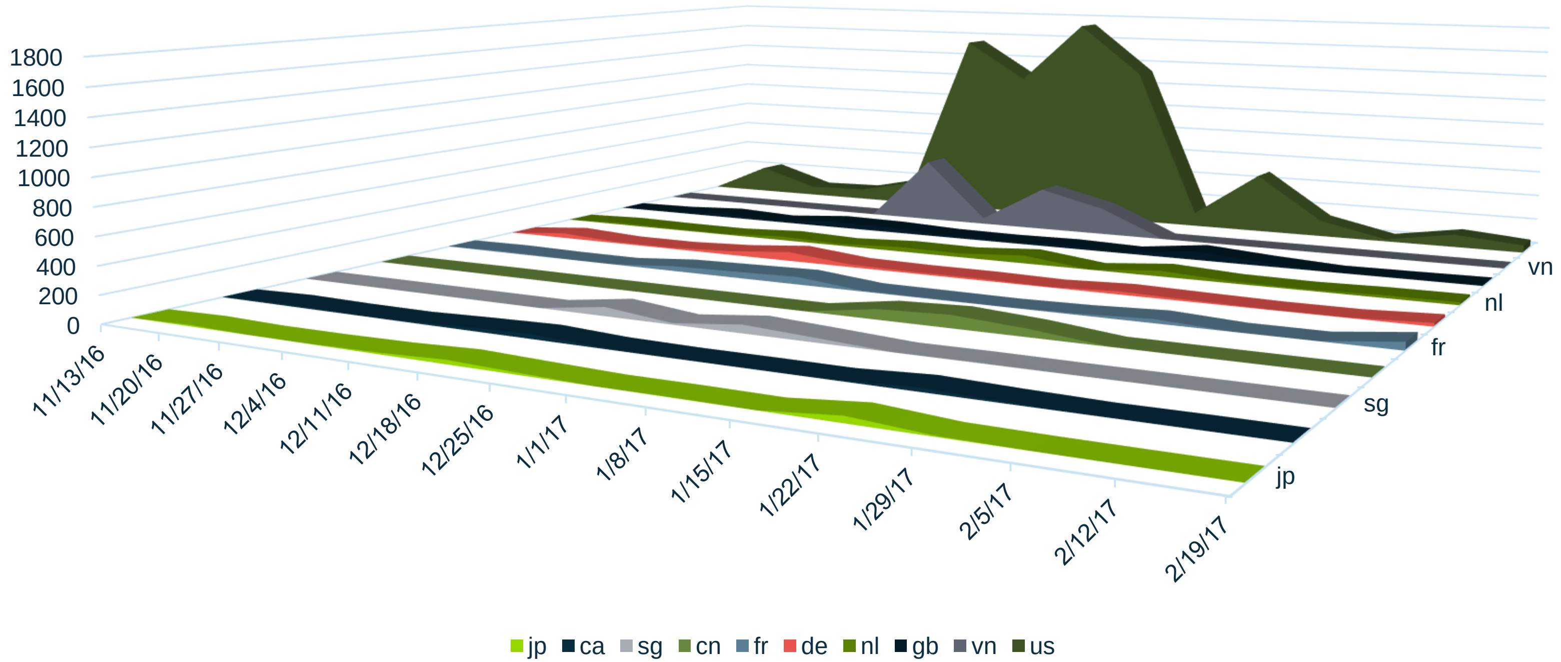
Max Bandwidth:	100GB/s
Max Packets:	1123
Start (GMT):	Jun 12 2015, 13:10
End (GMT):	Jun 12 2015, 13:56
Duration:	46 mins
Source Ports:	0-48298
Dest. Ports:	80
Attack Type:	TCP Connection

Source: U.S.
Destination: Africa
High severity
Max Bandwidth: 100GB/s
Max Packets: 1123
Start (GMT): Jun 12 2015, 13:10
End (GMT): Jun 12 2015, 13:56
Duration: 46 mins
Source Ports: 0-48298
Dest. Ports: 80
Attack Type: TCP Connection

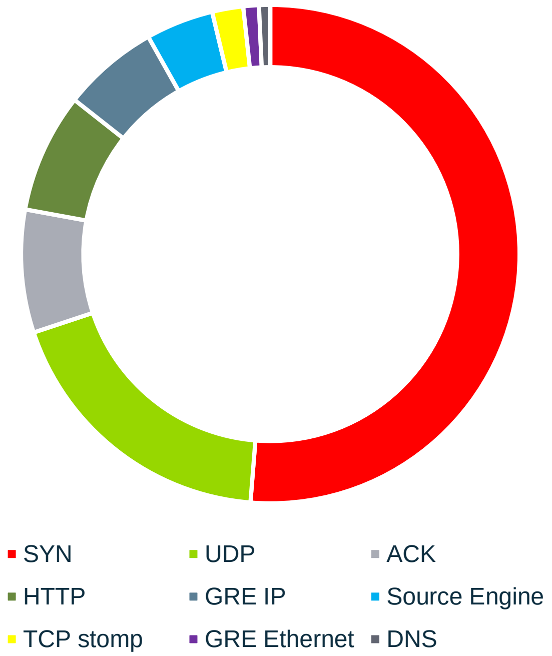
- New Arbor DAM
- More visualisation options
- Additional datasets within ATLAS

Unique IoT Insight

- Not one but two networks of honeypots looking at IoT threats!
  - Can see new behaviors, sources, reverse binaries, etc.
- Infiltration of multiple IoT Botnets for DDoS monitoring
  - Monitored 11412 attacks over 3 month period



Attack Destinations Over Time



Mirai Attack Types

ARBOR® NETWORKS

Knowledge & Preparation Are the Keys to Protection

Without the proper knowledge of…

1. DDoS Attack Trends (i.e. Ease, motivations, attack types, relationship with data breach)
2. Best Practices in DDoS Mitigation (i.e. Products, People and Processes)
3. Impact to Your Business (i.e. Downtime, loss revenue, mitigation costs etc.)

…You cannot accurately calculate the risk of a DDoS Attack.

10 Best Practices in DDoS Defense

1

- Factor network availability into the design of online services or applications; continuously stress-test.

2

- Develop a DDoS Attack Mitigation Process
- Continuously stress-test & refine.

3

- Utilize flow telemetry (e.g. NetFlow) collection & analysis for attack detection, classification & trace back.

4

Deploy multi-layered DDoS protection which includes:

- On-premises Intelligent DDoS Mitigation Systems (e.g. Arbor APS / TMS products)
- Overlay cloud-based DDoS protection services (i.e. Arbor Cloud or ISP/MSSP)
- Network infrastructure-based techniques such as S/RTBH & Flowspec at all network edges

5

- Scan for misconfigured, abusable services running on servers, routers, switches, home CPE devices, etc. (i.e. TCP 23/2323). Alert users running abusable services – possibly blocking until they are remediated.

10 Best Practices in DDoS Defense *(cont'd)*

6 NTP Services

- Check Open NTP Project for abusable NTP services on your networks.
- Disallow Level 6/7 NTP queries from the Internet.

7 DNS Recursors

- Check Open Resolve Project for abusable open DNS recursors on your networks. Ensure only authorized users can query recursive DNS servers.

8

- Ensure SNMP is blocked on public-facing infrastructure/ servers.

9

- Employ Anti-spoofing mechanisms such as Unicast Reverse-Path Forwarding, ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, etc. on all edges of ISP and enterprise networks.

10

- Participate in the global operational security community and share threat intelligence and defense best practices.

Q&A / Thank You

For more info, please contact:

CF Chui
Principal Security Technologist
cfchui@arbor.net

ARBOR® NETWORKS
The Security Division of NETSCOUT

NETSCOUT®

Guardians of the Connected World