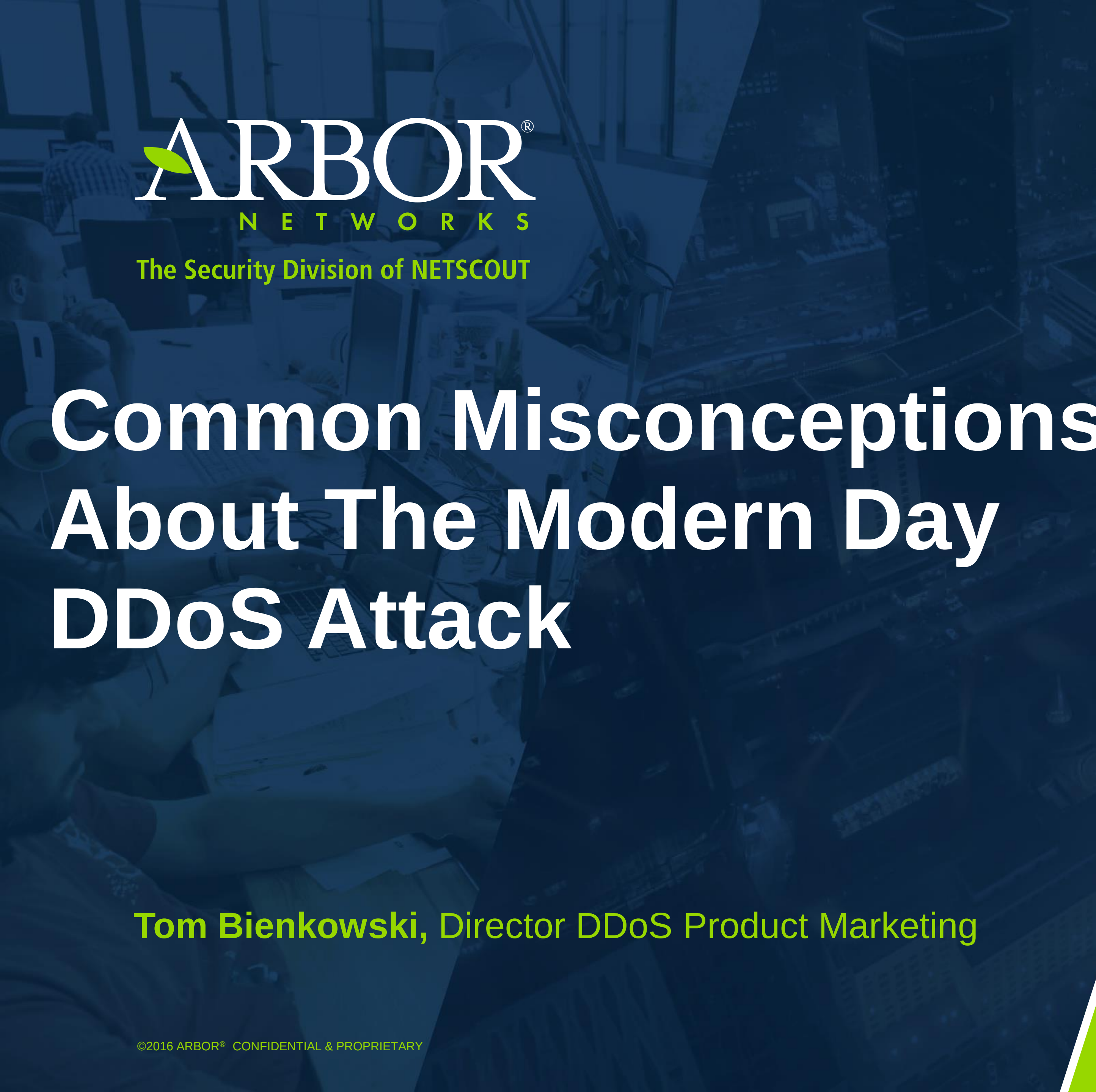


ARBOR® NETWORKS

The Security Division of NETSCOUT

Common Misconceptions About The Modern Day DDoS Attack

Tom Bienkowski, Director DDoS Product Marketing

Black Hat Webinar
October 20, 2016

Arbor Networks *The Security Division of* NETSCOUT™

16

Number of years Arbor has been delivering innovative security and network visibility technologies & products

#1

Arbor market position in Carrier, Enterprise and Mobile DDoS equipment market segments – [Infonetics Research Dec, 2015]

100%

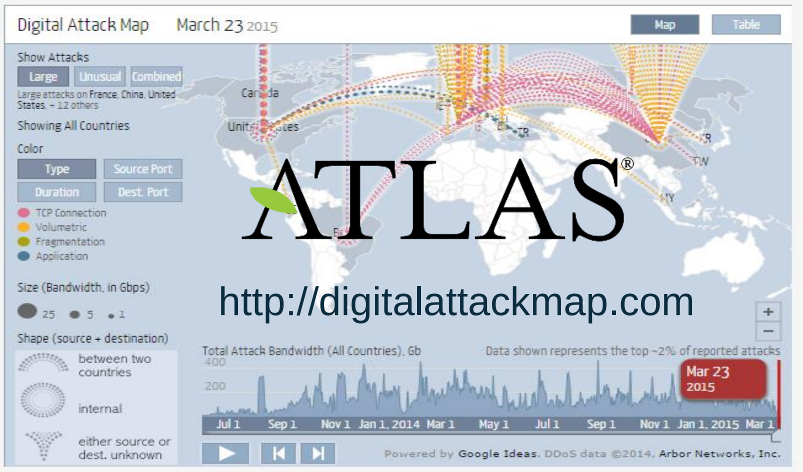
Percentage of world's Tier 1 service providers who are Arbor customers

NTT · at&t · TATA · verizon

中国电信 CHINA TELECOM · T-Com · Telefonica

vodafone · BT · france telecom

120 Tbps = Amount of global traffic monitored by the ATLAS



Digital Attack Map March 23 2015

Map Table

Show Attacks

Large Unusual Combined

Large attacks on France, China, United States, + 12 others

Showing All Countries

Color

Type Source Port

Duration Dest. Port

- ● TCP Connection
- ● Volumetric
- ● Fragmentation
- ● Application

Size (Bandwidth, in Gbps)

● 25 ● 5 ● 1

Shape (source + destination)

- between two countries
- internal
- either source or dest. unknown

Total Attack Bandwidth (All Countries), Gb

Data shown represents the top ~2% of reported attacks

Powered by Google Ideas. DDoS data ©2014, Arbor Networks, Inc.

ATLAS®

http://digitalattackmap.com

Common Misconceptions About DDoS Attacks

I have adequate DDoS protection solutions in place.
(My firewall, IPS, ISP)

Impact does not justify the cost of protection.

The odds are we will NOT be attacked.

DDoS is “old news” …I’m more concerned with Advanced Threats.

Common Misconceptions About DDoS Attacks

I have adequate DDoS protection solutions in place.
(My firewall, IPS, ISP)

Impact does not justify the cost of protection.

The odds are we will NOT be attacked.

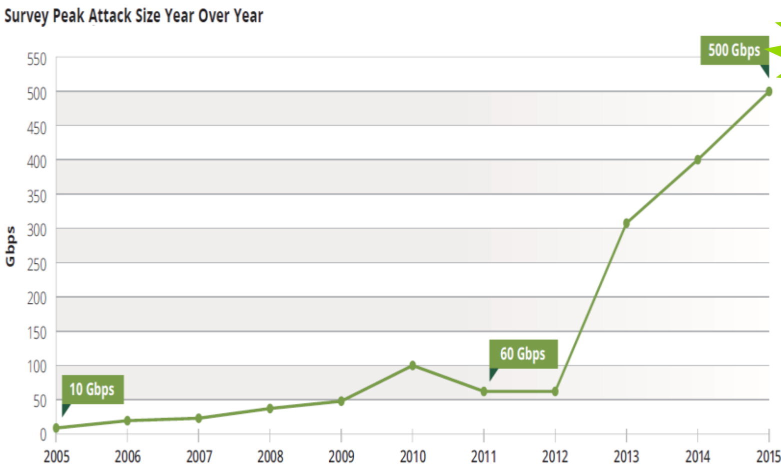
DDoS is “old news” …I’m more concerned with Advanced Threats.

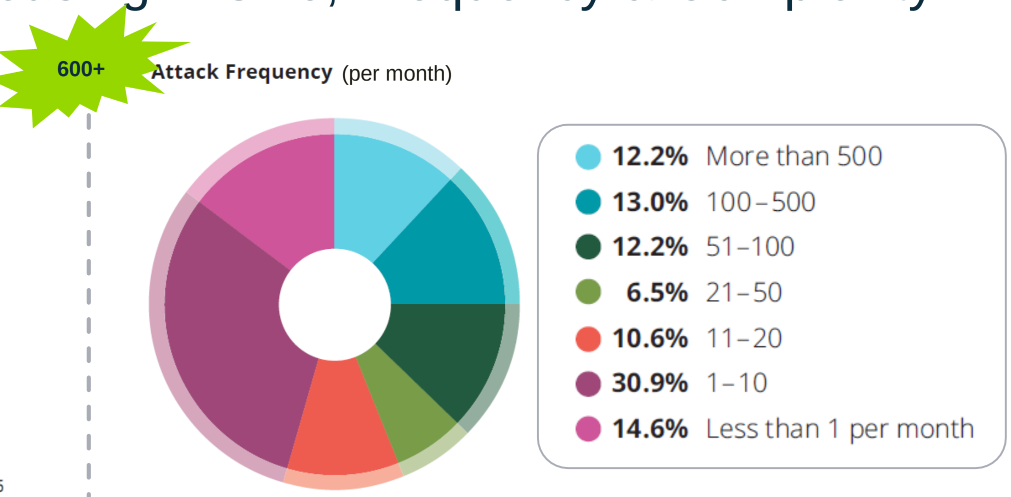
The Cyber Reflection

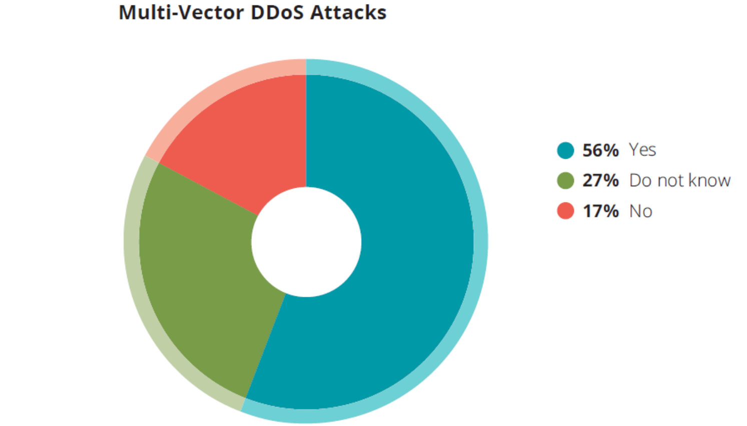
Every Physical Geo-Political Event…

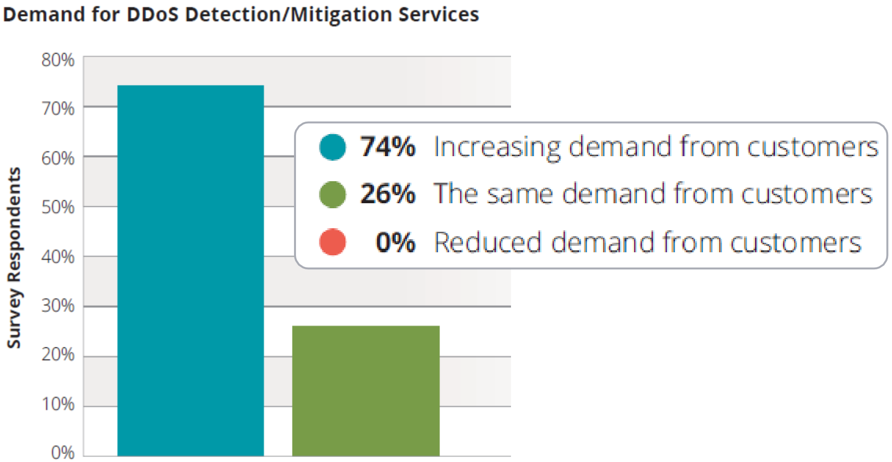
DDoS Attack Trends

Fact: DDoS Attacks Increasing in Size, Frequency & Complexity









*Source: Arbor Networks 11th Annual Worldwide Infrastructure Security Report

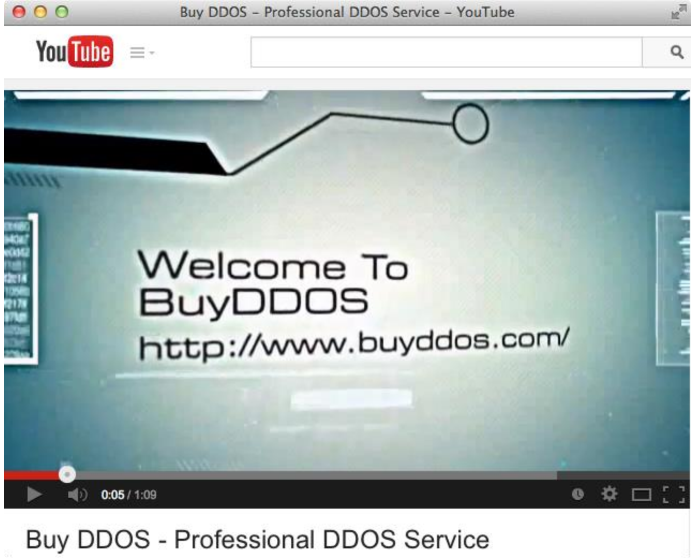
Ability & Motivations

Fact: It’s never been easier to launch a DDoS attack

$5:$100sK

Cost of DDoS Service

Impact to Victim

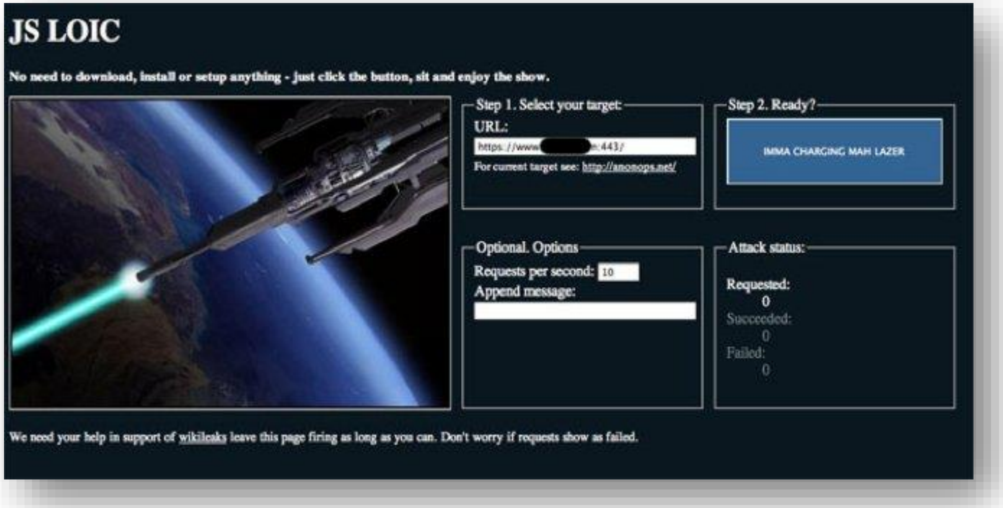


Buy DDOS – Professional DDOS Service – YouTube

Welcome To BuyDDOS
http://www.buyddos.com/

0:05 / 1:09

Buy DDOS - Professional DDOS Service



JS LOIC

No need to download, install or setup anything - just click the button, sit and enjoy the show.

Step 1. Select your target:

URL: https://www[redacted]:443/

For current target see: http://anonops.net/

Step 2. Ready?

IMMA CHARGING MAH LAZER

Optional. Options

Requests per second: 10

Append message:

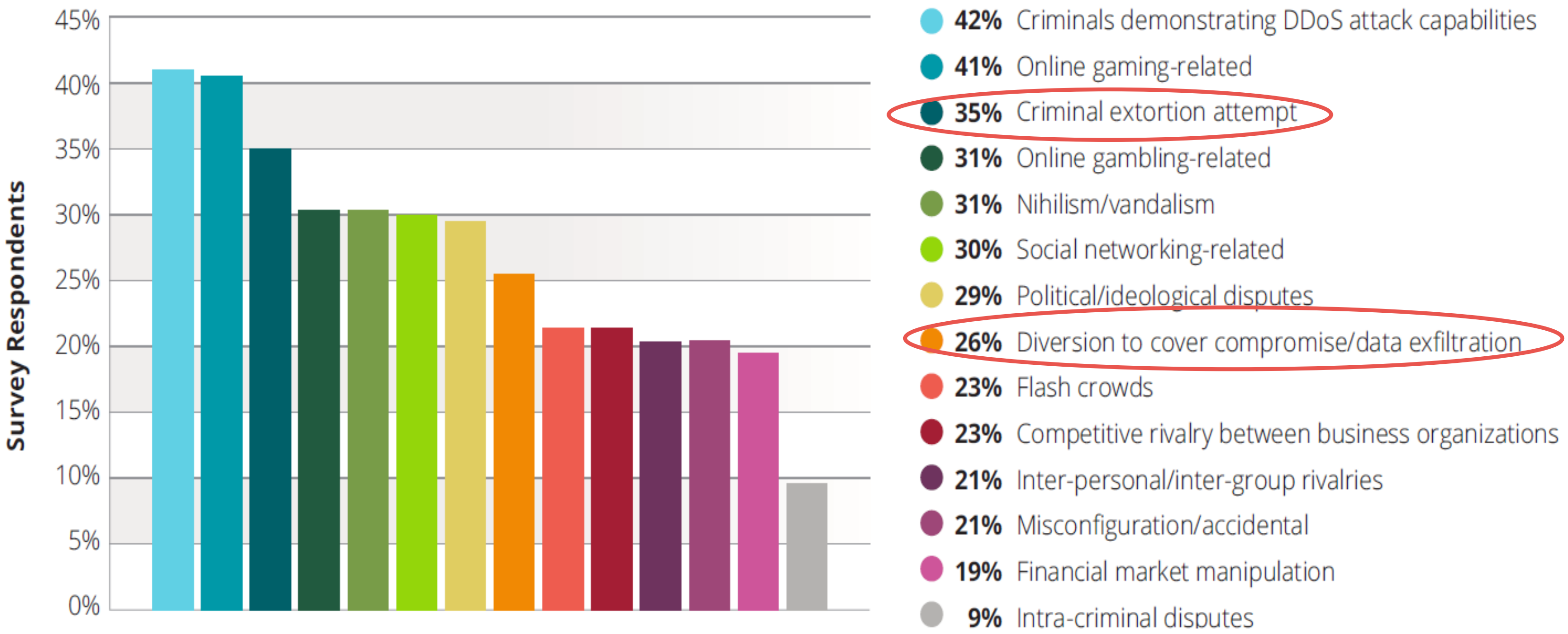
Attack status:

Requested:
0
Succeeded:
0
Failed:
0

We need your help in support of wikileaks leave this page firing as long as you can. Don't worry if requests show as failed.

Ability & Motivations

Fact: Many motivations behinds DDoS attacks



DDoS Attack Motivations

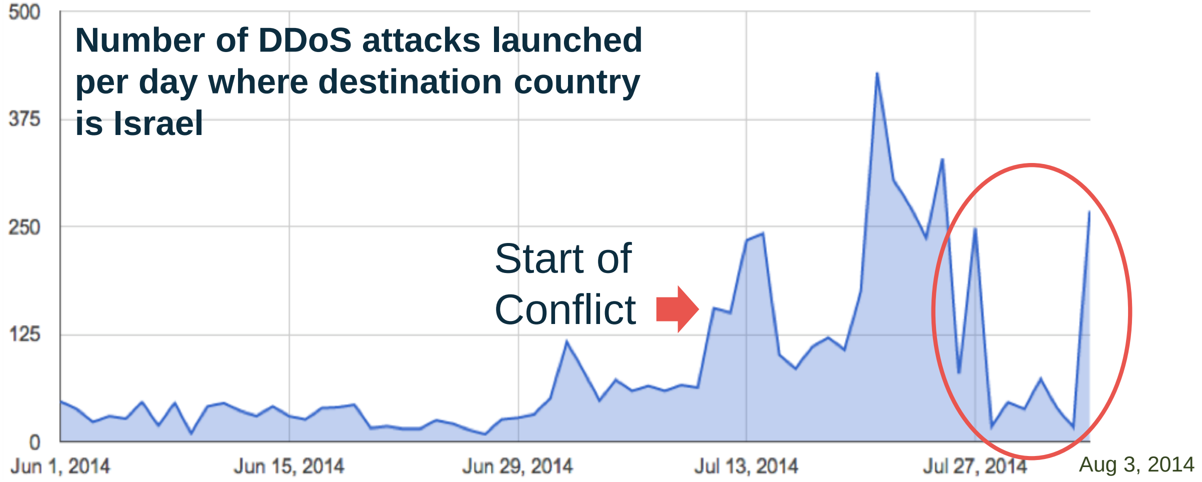
*Source: Arbor Networks 11th Annual Worldwide Infrastructure Security Report

Examples of The Cyber Reflection

Every Physical Geo-Political Event…

Has a Cyber Reflection…

The Gaza Strip Conflict



- **July 27th:** [Reuters] “UN Security Council Calls For Cease-Fire As Muslims Start Celebrating Eid al-Fitr” – there is a noticeable reduction in physical and DDoS attacks.
- **July 29th:** [Jewish Daily Forward] “The Palestinian Authority announced that it had brokered a 24-hour humanitarian cease-fire with all Palestinian factions with the possibility of extending it an additional 48 hours.”
- **August 1st:** [NY Times] “Gaza fighting intensifies as cease fire falls apart”
- **August 3rd:** Notice that the number of attacks rises again sharply. From July 28th through August 2nd, there were a total of **192** attacks. On August 3rd there were **268**.

Flint, Michigan Water Contamination

- Michigan.gov website was attacked on Saturday, Jan. 16
- Hurley Medical Center confirmed on Thursday, Jan 21 it was the victim of a "cyber attack" a day after Anonymous hacktivists threatened action over Flint's water crisis.

Ferguson, MO & Cleveland, OH 2014

WE ARE LEGION • WE DO NOT FORGIVE • WE DO NOT FORGET • EXPECT US • WE ARE ANONYMOUS •

Anonymous - #OpFerguson

- Attack and threats against Ferguson law enforcement and town government websites.

Tamir Rice shooting

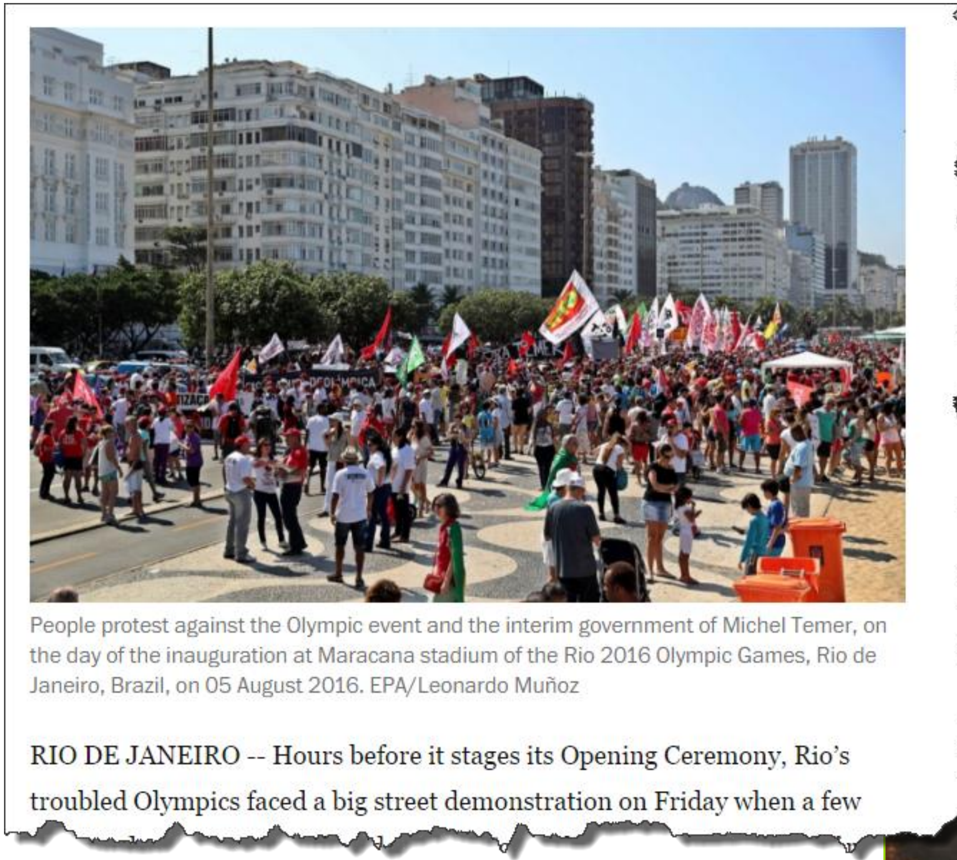
- Madness C2 started ordering attacks against Cleveland city websites
  - C2 appears to be associated with Anonymous
- ATLAS also reported NTP amplification attack (Peaked at 5Gbps)

FIFA World Cup Brazil

- Over 60 World Cup related websites were attacked.

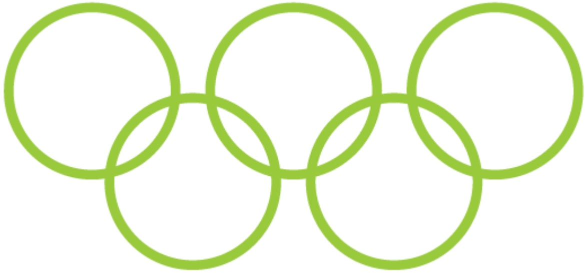
- Also threatened to take down sponsor sites.

2016 Rio Summer Olympics

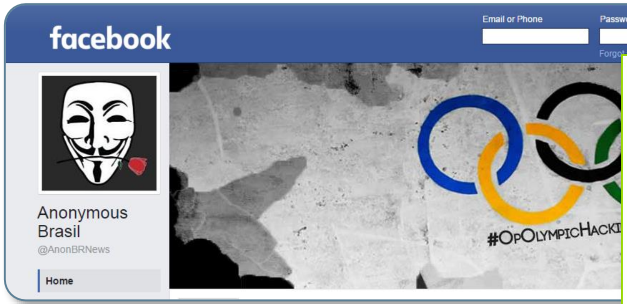


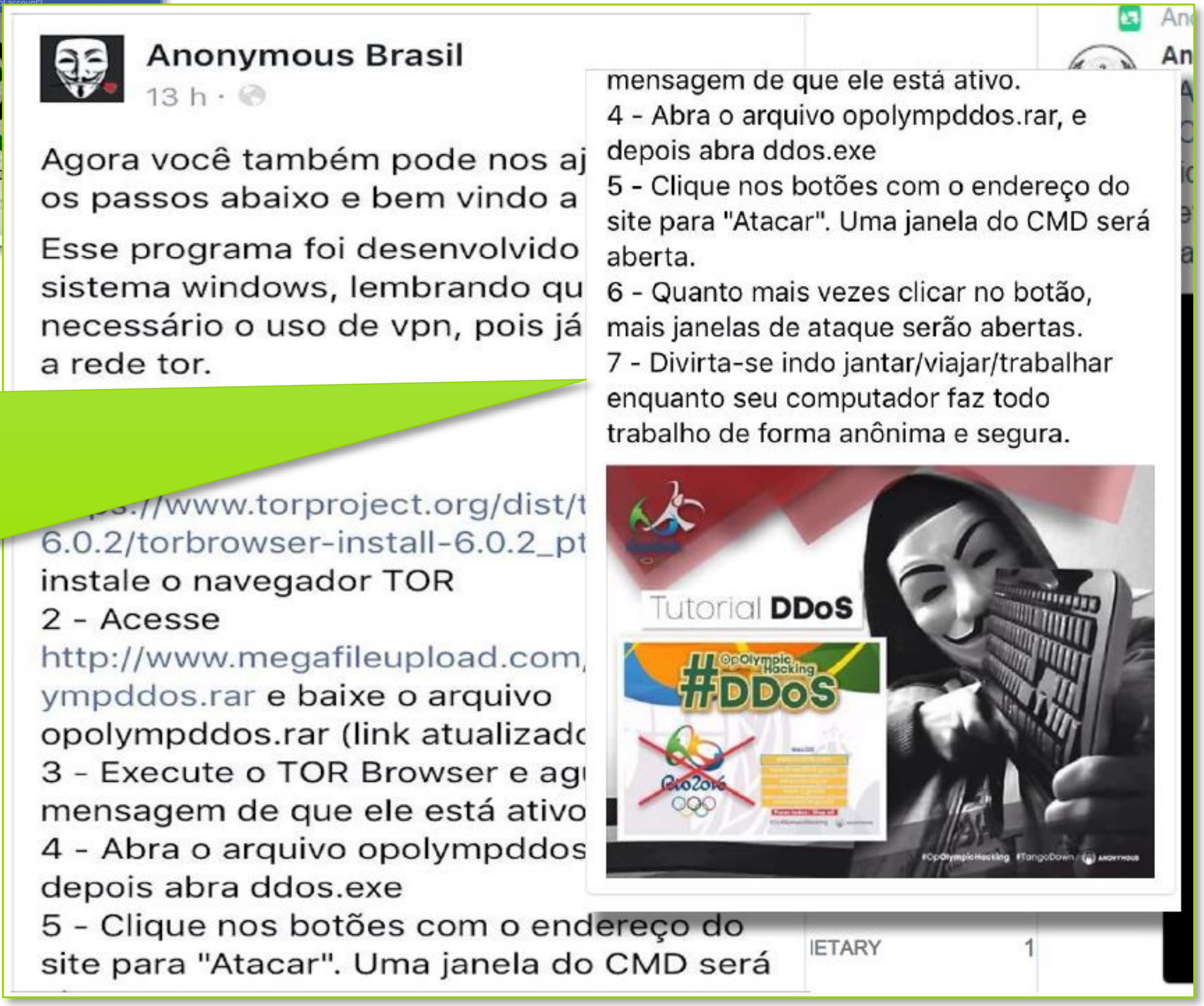
People protest against the Olympic event and the interim government of Michel Temer, on the day of the inauguration at Maracana stadium of the Rio 2016 Olympic Games, Rio de Janeiro, Brazil, on 05 August 2016. EPA/Leonardo Muñoz

RIO DE JANEIRO -- Hours before it stages its Opening Ceremony, Rio's troubled Olympics faced a big street demonstration on Friday when a few



2016 Rio Summer Olympics





Anonymous Brasil
13 h ·

Agora você também pode nos aj
os passos abaixo e bem vindo a

Esse programa foi desenvolvido
sistema windows, lembrando qu
necessário o uso de vpn, pois já
a rede tor.

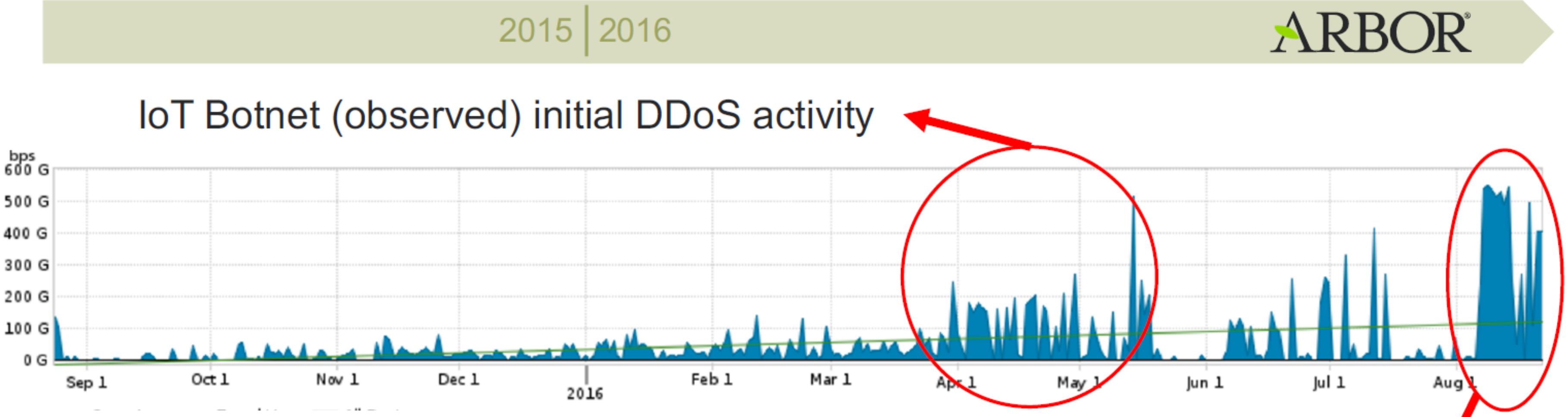
...://www.torproject.org/dist/t
6.0.2/torbrowser-install-6.0.2_pt
instale o navegador TOR
2 - Acesse
http://www.megafileupload.com/
ympddos.rar e baixe o arquivo
opolympddos.rar (link atualizado
3 - Execute o TOR Browser e agu
mensagem de que ele está ativo
4 - Abra o arquivo opolympddos
depois abra ddos.exe
5 - Clique nos botões com o endereço do
site para "Atacar". Uma janela do CMD será

mensagem de que ele está ativo.
4 - Abra o arquivo opolympddos.rar, e depois abra ddos.exe
5 - Clique nos botões com o endereço do site para "Atacar". Uma janela do CMD será aberta.
6 - Quanto mais vezes clicar no botão, mais janelas de ataque serão abertas.
7 - Divirta-se indo jantar/viajar/trabalhar enquanto seu computador faz todo trabalho de forma anônima e segura.

"the more you click on the button, the more attack windows will be launched..." "have fun going to dinner, travel, work while your computer does all the work safely and anonymously..."

2016 Rio Summer Olympics

Attack Volume



IoT Botnet (observed) initial DDoS activity

Rio 2016 Olympic Games

- Pre-Olympics probing attacks using IoT botnet (200 Gbps)
- Sustained 500+Gbps attack from Opening to Closing Ceremonies (GRE, non reflection/amplification)
- Targets include Brazilian ISPs, banks, government institutions and sponsors

Common Misconceptions About DDoS Attacks

I have adequate DDoS protection solutions in place.
(My firewall, IPS, ISP)

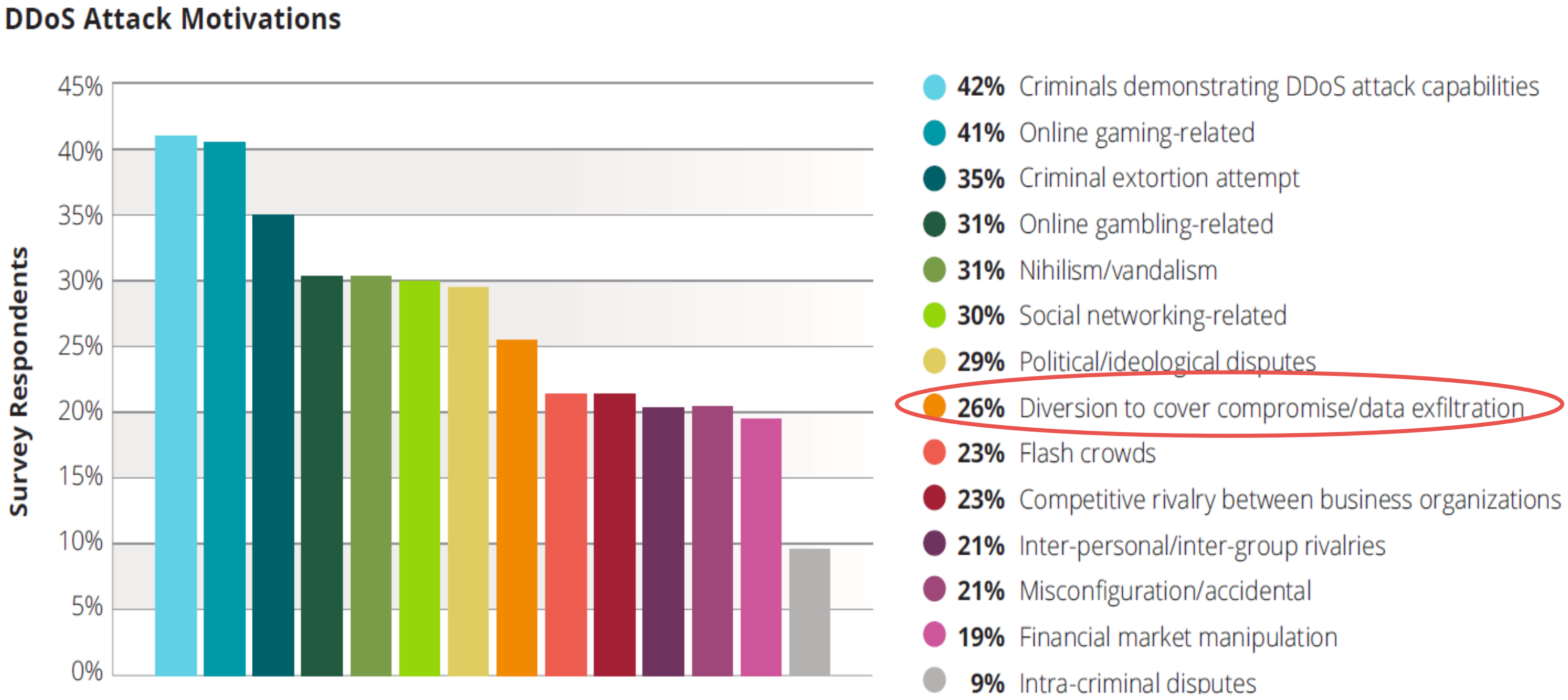
Impact does not justify the cost of protection.

The odds are we will NOT be attacked.

DDoS is “old news” …I’m more concerned with Advanced Threats.

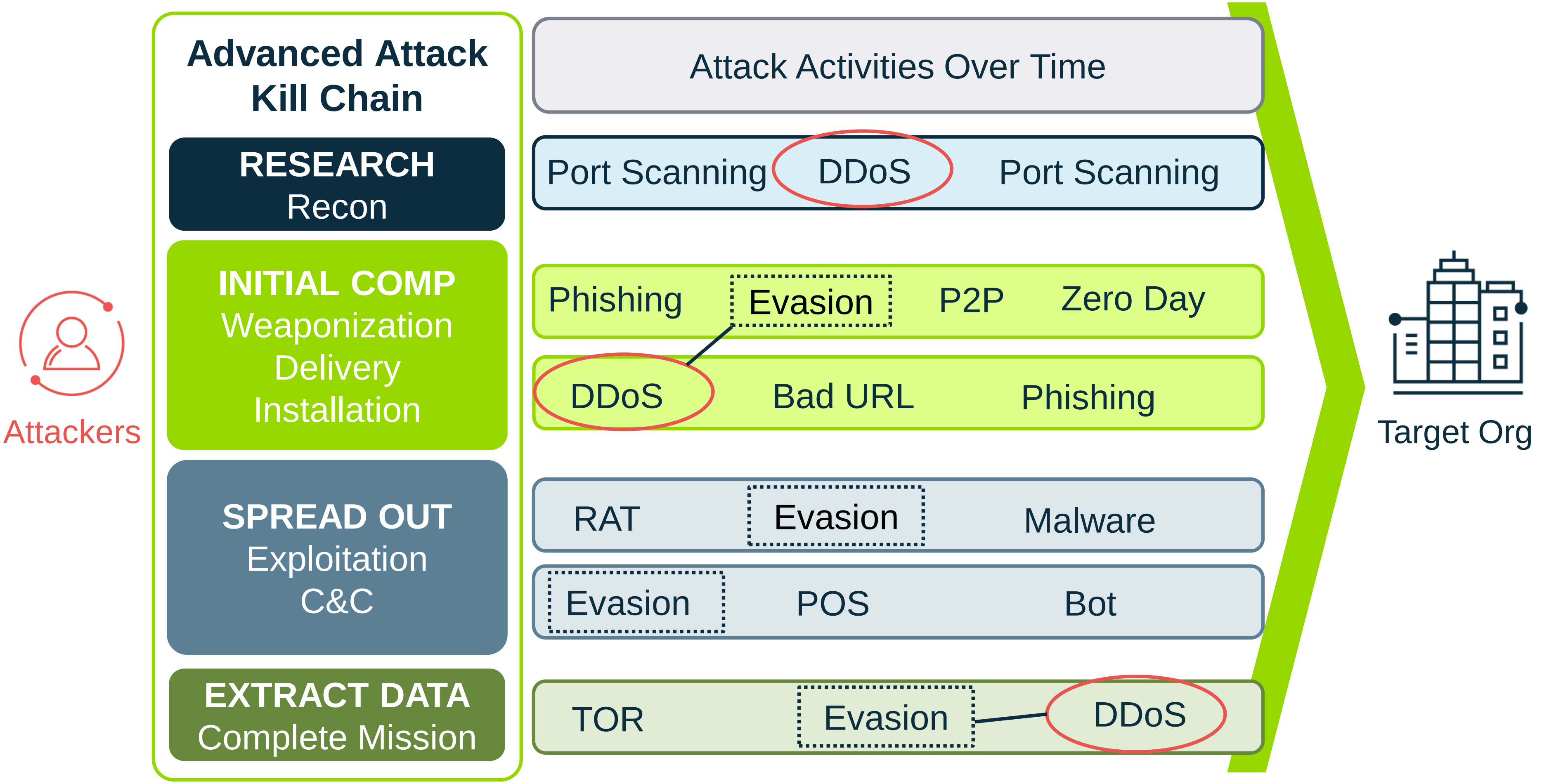
Motivations

Fact: Many motivations behinds DDoS attacks



*Source: Arbor Networks 11th Annual Worldwide Infrastructure Security Report

DDoS Used in Multiple Stages of Kill Chain



Attackers

Advanced Attack Kill Chain

RESEARCH
Recon

INITIAL COMP
Weaponization
Delivery
Installation

SPREAD OUT
Exploitation
C&C

EXTRACT DATA
Complete Mission

Attack Activities Over Time

Port Scanning DDoS Port Scanning

Phishing Evasion P2P Zero Day

DDoS Bad URL Phishing

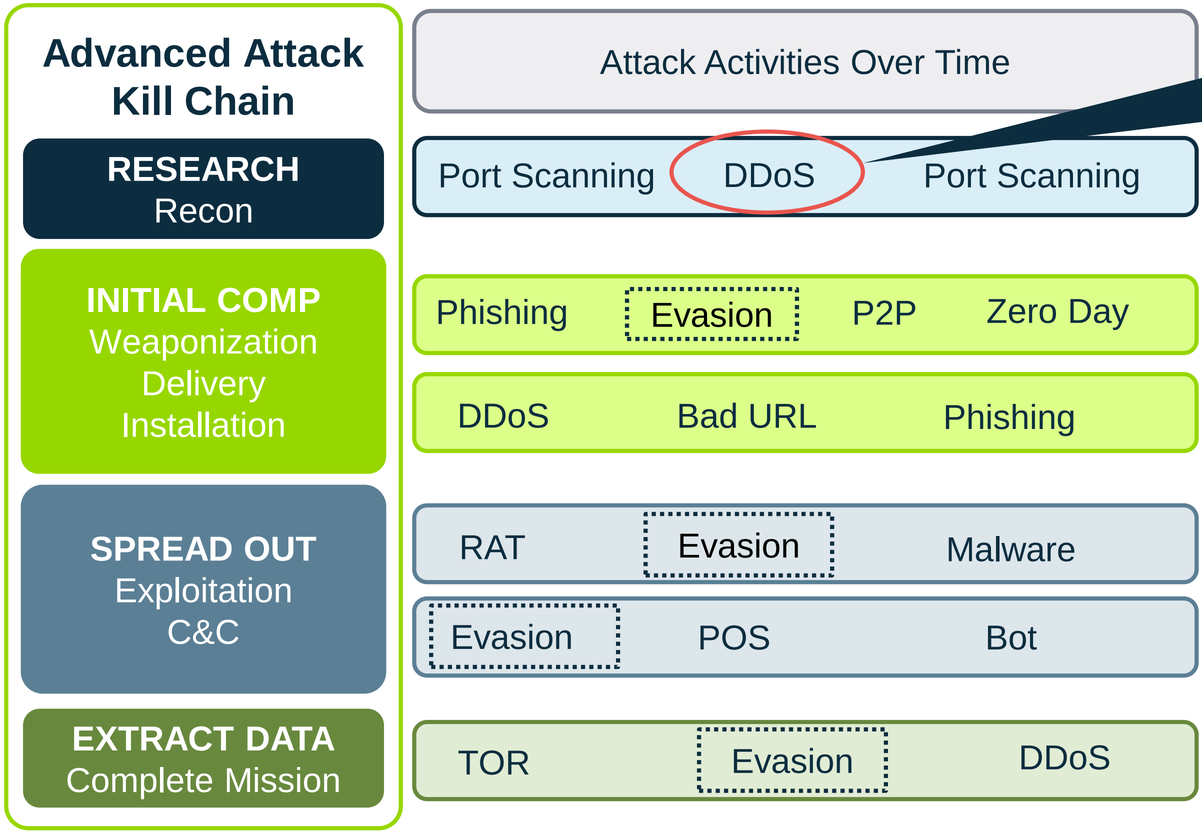
RAT Evasion Malware

Evasion POS Bot

TOR Evasion DDoS

Target Org

DDoS Used in Multiple Stages of Kill Chain



Advanced Attack Kill Chain	Attack Activities Over Time
RESEARCH Recon	Port Scanning · DDoS · Port Scanning
INITIAL COMP Weaponization Delivery Installation	Phishing · Evasion · P2P · Zero Day DDoS · Bad URL · Phishing
SPREAD OUT Exploitation C&C	RAT · Evasion · Malware Evasion · POS · Bot
EXTRACT DATA Complete Mission	TOR · Evasion · DDoS

Sizing up your security posture...in preparation for later weaponization/data exfiltration stage

DDoS Used in Multiple Stages of Kill Chain

Advanced Attack Kill Chain

RESEARCH
Recon

INITIAL COMP
Weaponization
Delivery
Installation

SPREAD OUT
Exploitation
C&C

EXTRACT DATA
Complete Mission

Attack Activities Over Time

Port Scanning DDoS Port Scanning

Phishing Evasion P2P Zero Day

DDoS Bad URL Phishing

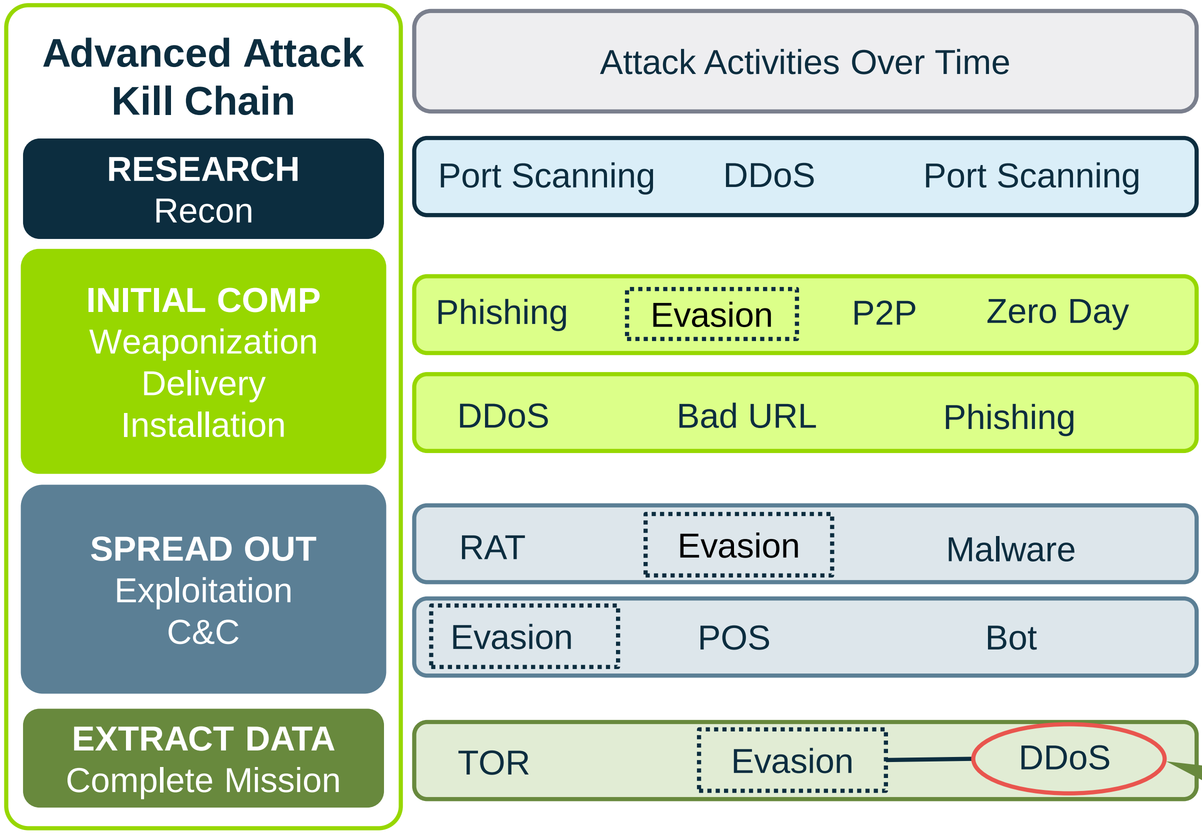
RAT Evasion Malware

Evasion POS Bot

TOR Evasion DDoS

Evasion / Diversion Tactic: Overwhelming your security forensics making it harder to find indicators of compromise / breach

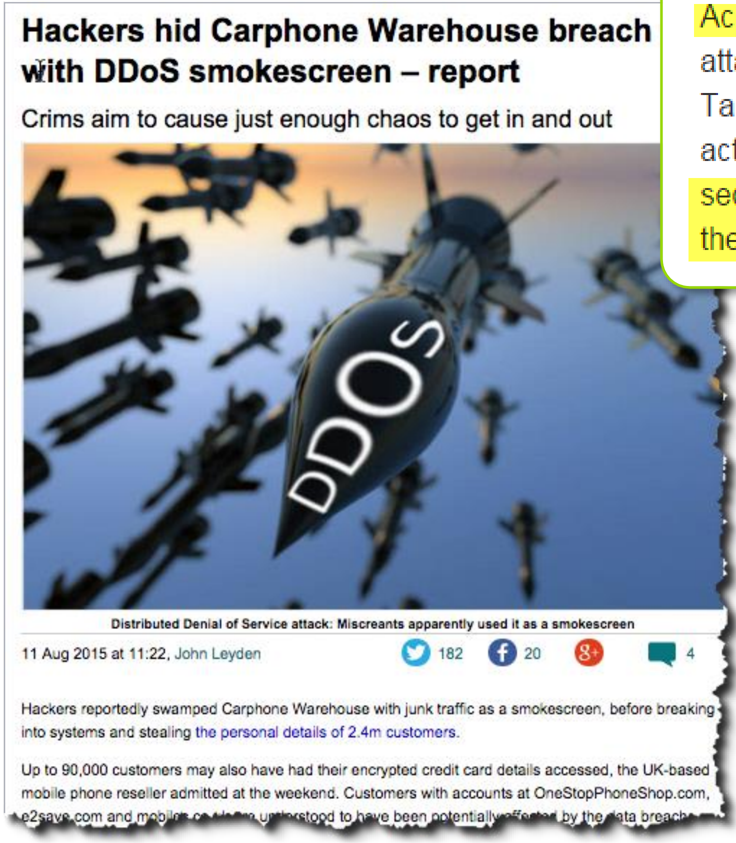
DDoS Used in Multiple Stages of Kill Chain



Advanced Attack Kill Chain	Attack Activities Over Time			
RESEARCH Recon	Port Scanning	DDoS	Port Scanning	
INITIAL COMP Weaponization Delivery Installation	Phishing	Evasion	P2P	Zero Day
	DDoS	Bad URL	Phishing	
SPREAD OUT Exploitation C&C	RAT	Evasion	Malware	
	Evasion	POS	Bot	
EXTRACT DATA Complete Mission	TOR	Evasion	DDoS	

Diversion: Analogous to setting alarms off at one end of building while thief slips out the other with all the loot.

DDoS as Smokescreen



Hackers hid Carphone Warehouse breach with DDoS smokescreen – report

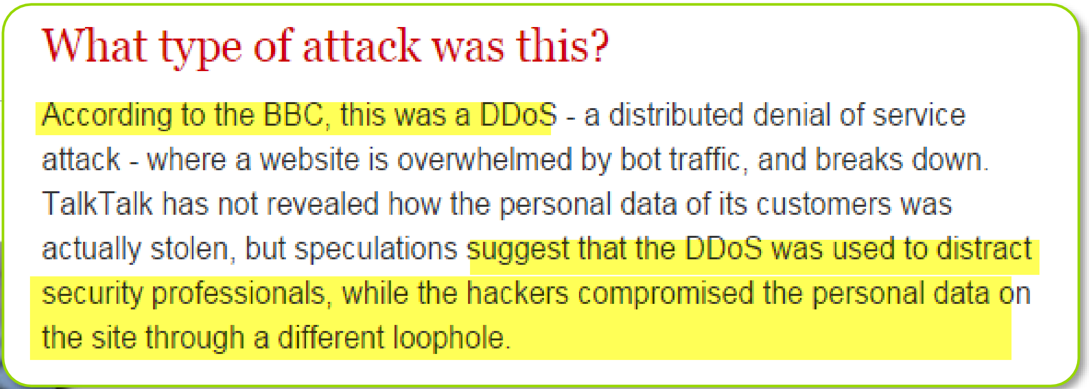
Crims aim to cause just enough chaos to get in and out

Distributed Denial of Service attack: Miscreants apparently used it as a smokescreen

11 Aug 2015 at 11:22, John Leyden 182 20 4

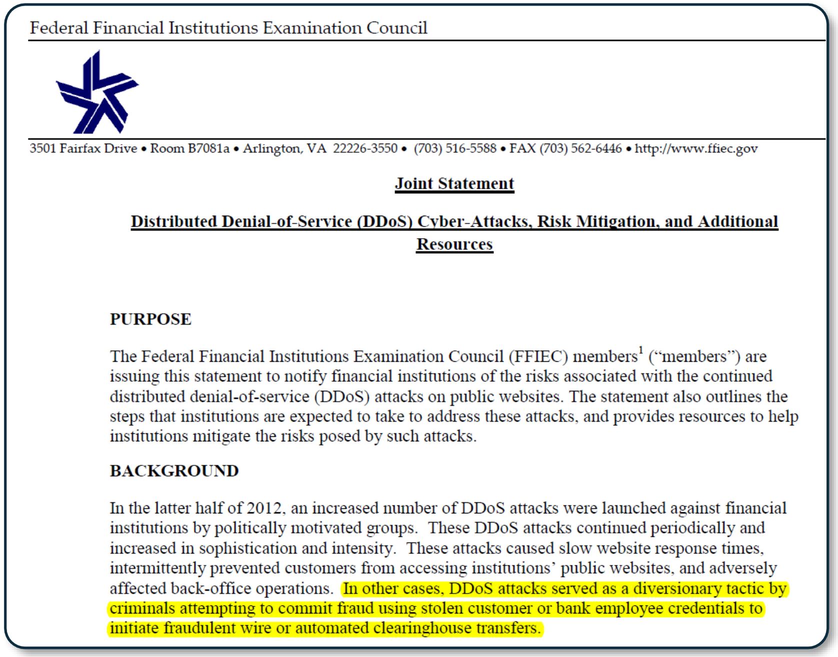
Hackers reportedly swamped Carphone Warehouse with junk traffic as a smokescreen, before breaking into systems and stealing the personal details of 2.4m customers.

Up to 90,000 customers may also have had their encrypted credit card details accessed, the UK-based mobile phone reseller admitted at the weekend. Customers with accounts at OneStopPhoneShop.com, e2save.com and mobiles.co.uk are understood to have been potentially affected by the data breach.



What type of attack was this?

According to the BBC, this was a DDoS - a distributed denial of service attack - where a website is overwhelmed by bot traffic, and breaks down. TalkTalk has not revealed how the personal data of its customers was actually stolen, but speculations suggest that the DDoS was used to distract security professionals, while the hackers compromised the personal data on the site through a different loophole.



Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Joint Statement

Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources

PURPOSE

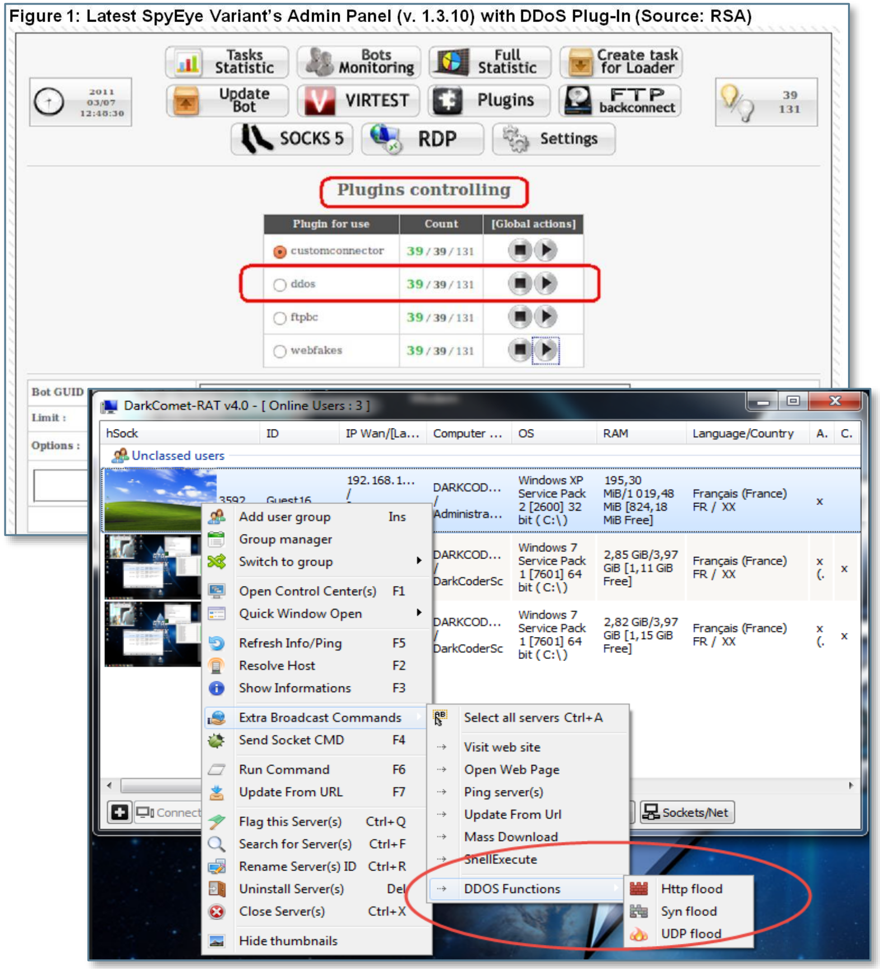
The Federal Financial Institutions Examination Council (FFIEC) members[1] ("members") are issuing this statement to notify financial institutions of the risks associated with the continued distributed denial-of-service (DDoS) attacks on public websites. The statement also outlines the steps that institutions are expected to take to address these attacks, and provides resources to help institutions mitigate the risks posed by such attacks.

BACKGROUND

In the latter half of 2012, an increased number of DDoS attacks were launched against financial institutions by politically motivated groups. These DDoS attacks continued periodically and increased in sophistication and intensity. These attacks caused slow website response times, intermittently prevented customers from accessing institutions' public websites, and adversely affected back-office operations. In other cases, DDoS attacks served as a diversionary tactic by criminals attempting to commit fraud using stolen customer or bank employee credentials to initiate fraudulent wire or automated clearinghouse transfers.

Examples of Combo DDoS & Advanced Threats Tools in the Wild

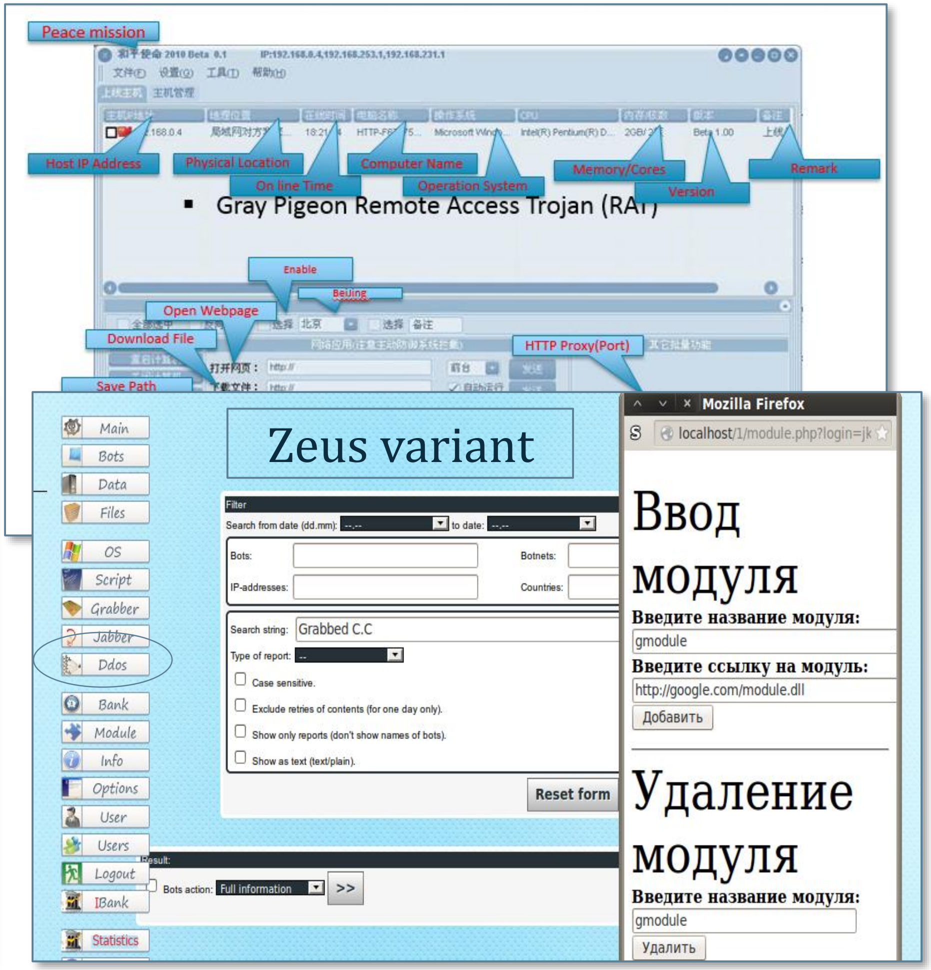
Figure 1: Latest SpyEye Variant's Admin Panel (v. 1.3.10) with DDoS Plug-In (Source: RSA)



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

DarkComet-RAT v4.0 - [Online Users : 3]

hSock	ID	IP Wan/[La...	Computer ...	OS	RAM	Language/Country	A.	C.
Unclassed users								
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



- 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).

Reset form

Result:

Bots action: Full information >>

Ввод модуля

Введите название модуля: gmodule

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

Добавить

Удаление модуля

Введите название модуля: gmodule

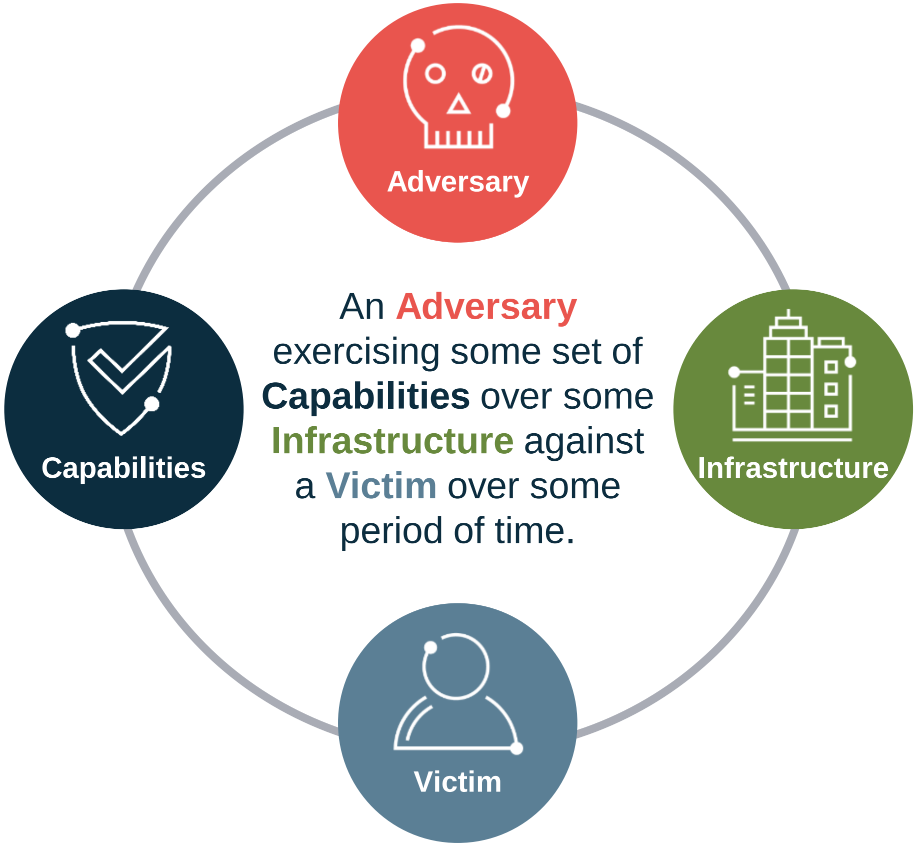
Удалить

©2016 ARBOR® CONFIDENTIAL & PROPRIETARY

The Game Has Changed

Fact:

- Advanced threats have evolved from independent DDoS attacks and malware to **attack campaigns.**
- Attack campaigns are organized human to human campaigns, using multiple tools and techniques - DDoS is a common attack tool.



An **Adversary** exercising some set of **Capabilities** over some **Infrastructure** against a **Victim** over some period of time.

Common Misconceptions About DDoS Attacks

I have adequate DDoS protection solutions in place.
(My firewall, IPS, ISP)

Impact does not justify the cost of protection.

The odds are we will NOT be attacked.

DDoS is “old news” …I’m more concerned with Advanced Threats.

Misconception: Firewall / IPS Will Stop DDoS Attacks

Fact: Firewalls and IPS (load balancers, WAF etc.) are not designed to stop DDoS attacks.

- DDoS attacks use legitimate packets and do not violate protocols rules – thus many go undetected by firewalls and IPS.
- Because firewalls and IPS (load balancers, WAF) are required to track state, they are vulnerable to some DDoS attacks (e.g. HTTP/TCP SYN floods) – and routinely fail during attacks.

Firewalls and IPS Affected by DDoS Attacks

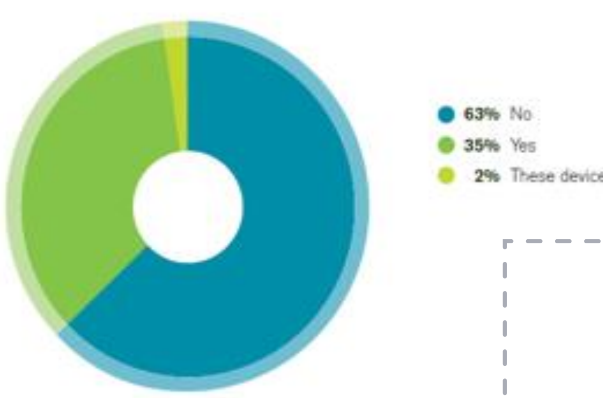
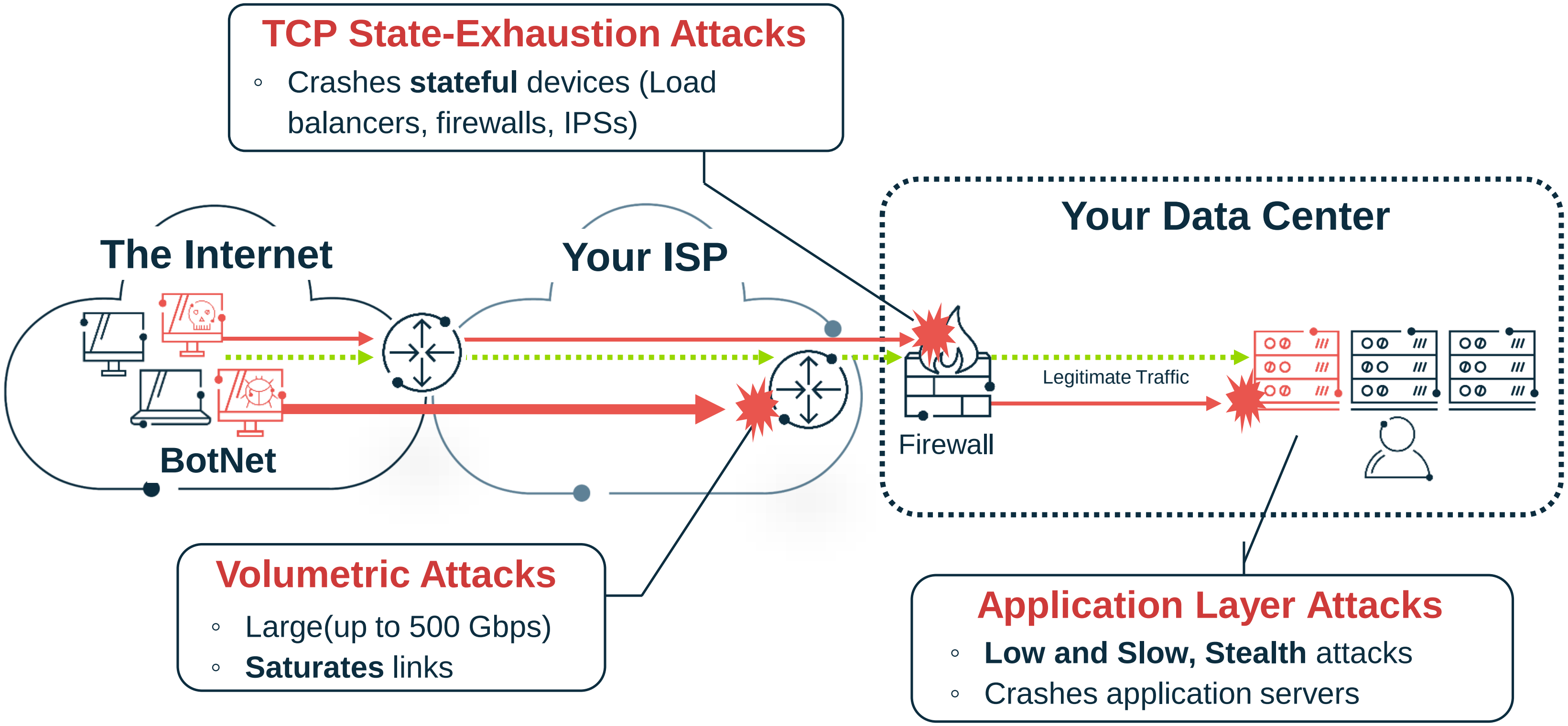


Figure 92 Source: Arbor Networks, Inc.

Completing the Security Triad:

The Modern Day DDoS Attack Is Complex

Dynamic, multi-vector combination



TCP State-Exhaustion Attacks

- Crashes **stateful** devices (Load balancers, firewalls, IPSs)

Volumetric Attacks

- Large(up to 500 Gbps)
- **Saturates** links

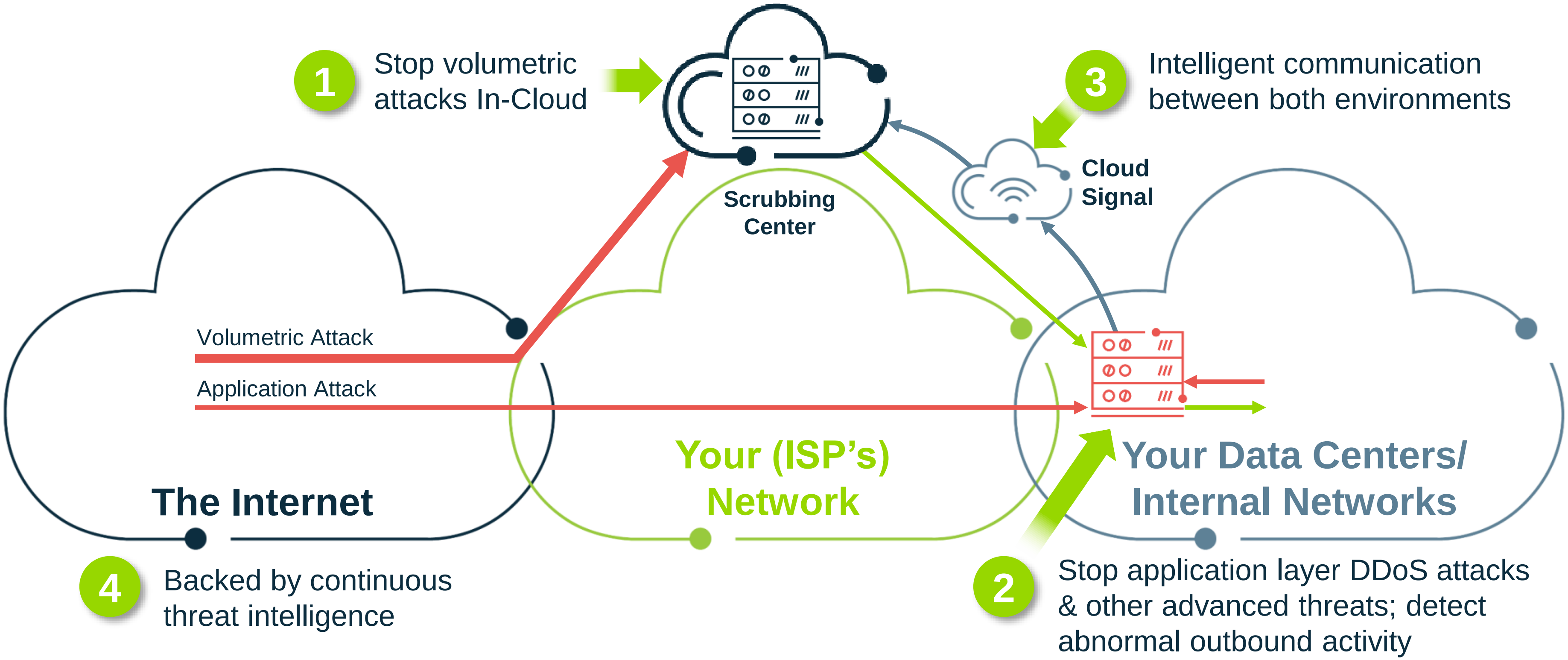
Application Layer Attacks

- **Low and Slow, Stealth** attacks
- Crashes application servers

Industry Best Practices exist to stop **all** of these attacks

Stopping Modern Day DDoS Attacks

Layered DDoS Attack Protection


1
Stop volumetric attacks In-Cloud
3
Intelligent communication between both environments
Cloud Signal
Scrubbing Center
Volumetric Attack
Application Attack
The Internet
Your (ISP's) Network
Your Data Centers/ Internal Networks
4
Backed by continuous threat intelligence
2
Stop application layer DDoS attacks & other advanced threats; detect abnormal outbound activity

Backed by Continuous Threat Intelligence

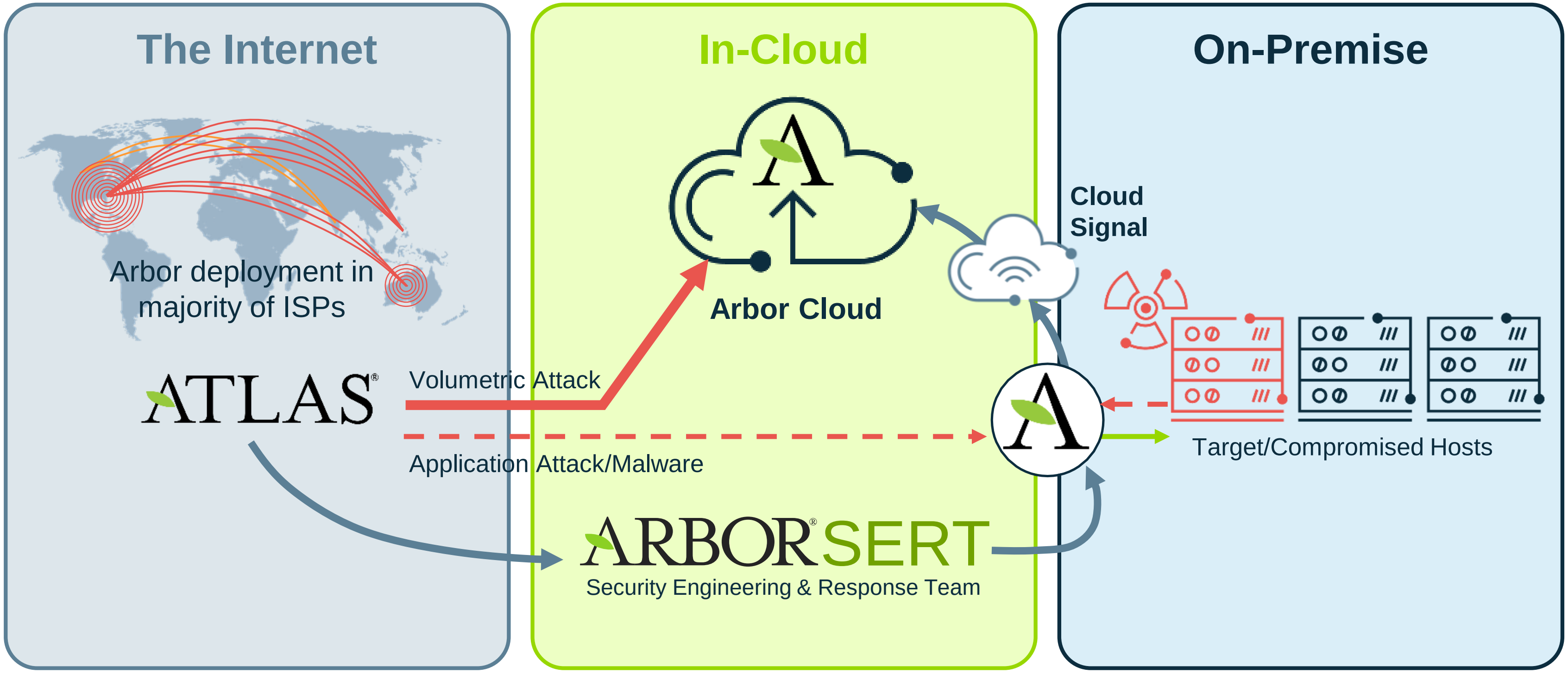
A Recommended Industry Best Practice:

FORRESTER® IDC FROST & SULLIVAN Infonetics RESEARCH Securosis ovum

ARBOR® NETWORKS

Arbor's DDoS Protection Solution

Comprehensive DDoS Protection Products & Services



Armed with Global Visibility & Actionable Threat Intelligence

Closing Statements

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 to your organization and put the proper business continuity plans in place.

Q&A / Thank You

For more info, please contact:

Tom Bienkowski
Director DDoS Product Marketing
tbienkowski@arbor.net

ARBOR®
NETWORKS
The Security Division of NETSCOUT