



# Your Money or your ~~Life~~ Site

Leo Noman

System Engineer – F5 Security Specialist for Australia & New Zealand

[l.noman@f5.com](mailto:l.noman@f5.com)

# ATTACK TYPES AND HISTORY



# The evolution of attackers

September 1996

First high profile DDoS attack. NY ISP Panix.com that was nearly put out of business.

January 2008

Anonymous executes a series of high-profile DDoS attacks against the Church of Scientology.

December 2010

WikiLeaks supporters hit PayPal, Visa, Mastercard, and other financial sites with DDoS attacks.

April 2011

Attackers use a DDoS attack against Sony to mask the theft of millions of customer records.

April 2012

Anonymous knocks down the sites of the U.S. Dept. of Justice, the CIA, and the British Secret Intelligence Service.

September 2012

Syrian Cyber Fighters launch Operation Ababil with DDoS attacks on 13 U.S. banks to protest an anti-Muslim video.

1996 | ... | 2008 | 2009 | 2010 | 2011 | 2012 | 2013

01001  
11010  
10010

Script  
kiddies



The rise  
of hacktivism



Cyber  
war

# The evolution of attackers

December 2014

Lizard Squad strikes XBOX and Play Station Network.

March 2015

Massive github DDoS attack tied to Chinese government.

January 2016

BBC sites targeted with the largest DDoS attack in history by the group New World Hacking using the BangStresser DDoS tool.

2014

2015

2016

01001  
11010  
10010

Script  
kiddies



The rise  
of hacktivism



Cyber  
war

# Attacks

- Volumetric L3/4
- Reflection & Amplification
- 'Low and Slow' L7
- Blended
- Volumetric L7

**THE THREAT IS COMING  
FROM INSIDE YOUR BUILDING**Stop insider threats **READ THE REPORT** ▶**FORCEPOINT**

POWERED BY SnipeSystems

[Home](#) / [Security](#)

# Massive application-layer attacks could defeat hybrid DDoS protection

Unusual application-layer DDoS attacks that consume a lot of bandwidth could spell trouble for on-premise DDoS defenses



Credit: Gerd Altmann / Pixabay

## Remove Malware - Free

[free-malware-removal.sparktrust.com](http://free-malware-removal.sparktrust.com)

Quick Malware Removal in 2 minutes. Free Download (Highly Recommended)

Shop Now

amazon

**The World Is Flat**

By Thomas L. Friedman (Paperbac...

**\$5.53****Das geplante Ende der Welt (German Edition)**

By Peter Goll (Paperback - Apr 8, 2...

**\$31.99** Prime**Top Android stories**

from our new site, Greenbot



AdBlock, AdBlock Plus arrives for Windows 10 Insider users

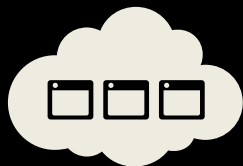


# LANDSCAPE & TRENDS



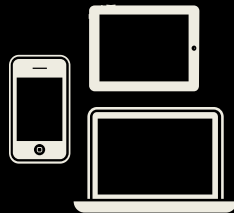
# Protecting Against DDoS is Challenging

## Webification of apps



**71%** of internet experts predict most people will do work via web or mobile by 2020

## Device proliferation



**95%** of workers use at least one personal device for work

**190 million** enterprises will use mobile apps by 2018

## Evolving security threats

**58%** of all e-theft tied to activist groups

**81%** of attacks are multi vector



## Shifting perimeter

**80%** of new apps will target the cloud.

**72%** of IT leaders have or will move applications to the cloud





# The Threat is Real

## DDoS as a Service



For as little as \$150 you can buy a week long DDoS attack

## Constant Attacks



More than 2000 daily DDoS attacks are observed

## Website Down!

1/3 of all downtime incidents are attributed to DDoS attacks



## Your Money or your Website

Hello!

All your servers are going under attack unless you pay 2 Bitcoin.

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 200-300 Gbps....



# Attack Threats: Pay up or Else!

April - May of 2015: emails sent to legitimate businesses with the threat of massive DDoS attacks

## Hong Kong Banks Hit By Bitcoin Ransom Demands

DD4BC cyber extortion gang targets key European sectors

- DD4BC claims ~400 Gbps
- Extortion demands starting at 25 Bitcoins
- Initially targeted Bitcoin, Payment providers, banks and now moving to other targets
- UDP Amplification Attacks (NTP, SSDP, DNS); TCP SYN Floods; and Layer 7 attacks

### Sample from actual email

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother. At least, don't expect cheap services like CloudFlare or Incapsula to help...but you can try. :)

The Hacker Store

uz5gs45ls3am2ikq.onion

## The Hacker Store

Contact: [hackerstore@bitmessage.ch](mailto:hackerstore@bitmessage.ch)

### Anonymous Phone Verification

**0.5 BTC**

You can use the number I gave you for 30 days since the first SMS arrives.  
All numbers are unique, I NEVER use the same for 2 or more customers.

---

### DDOS

DDOS one (1) IP address for 12, 24, 48 or as many hours as you wish, please send me an email if you want more information about it.  
**YOU CAN GET FROM 5 Gb/sec to 20Gb/sec ATTACK. If you want more just ask ;)**  
Just mail me with, how much time you want, how many Gb/sec you wish and I'll reply you with an offer. I'm open for negotiations.

---

### BTC Laundering

**DDOS**

**DDOS one (1) IP address for 12, 24, 48 or as many hours as you wish, please send me an email if you want more information about it.**  
**YOU CAN GET FROM 5 Gb/sec to 20Gb/sec ATTACK. If you want more just ask ;)**  
**Just mail me with, how much time you want, how many Gb/sec you wish and I'll reply you with an offer. I'm open for negotiations.**

#### Encrypted HDD 500Gb 2.5 inch USB 3.0 / 2.0

No Installation! No Software or Driver for security is required- it's a stand-alone hardware encryption device  
OS Free! Independent and real-time hardware Encryption compatible with any device supporting a USB host  
High-speed Transfer! No delay of data transfer even on reading or writing under security mode  
A perfect security protection with 1-8 digit PIN  
USB powered  
Dimension and gross weight of each unit in a retail box : 22.5 x 10 x 5 cm & 0.212kg  
Price: 2.5 BTC Free Shipping  
**Mail me for more details.**

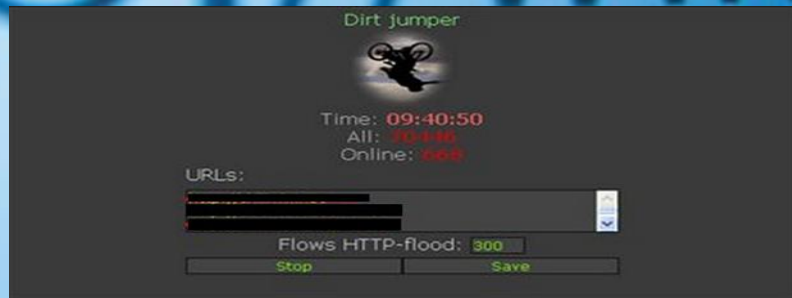
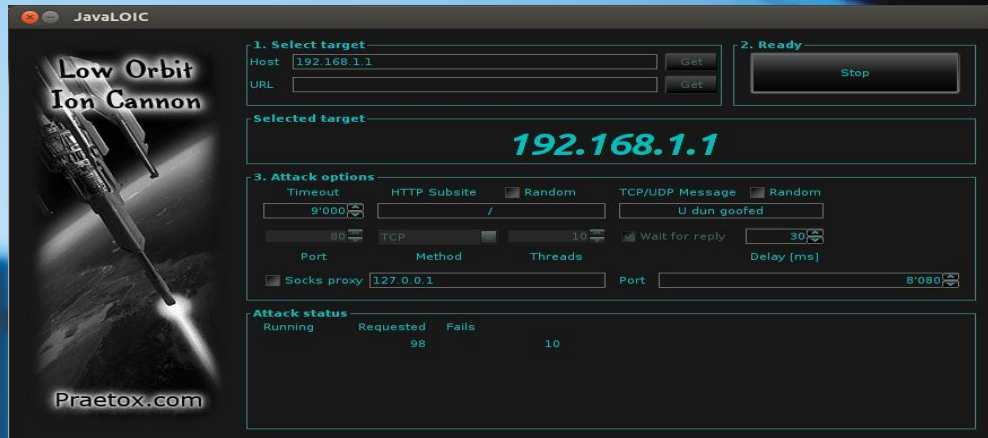
Paypal: 0.5 BTC (phone number confirmed by me) + guide  
Ebay: 0.1 BTC (phone number confirmed by me)  
- 10 positive feedbacks as a seller: 0.4 BTC (get as many as you wish)  
- 10 positive feedbacks as a buyer: 0.2 BTC (get as many as you wish)  
Ask for any other type of accounts

Once they were only a few, now  
attackers are coming out in record  
numbers

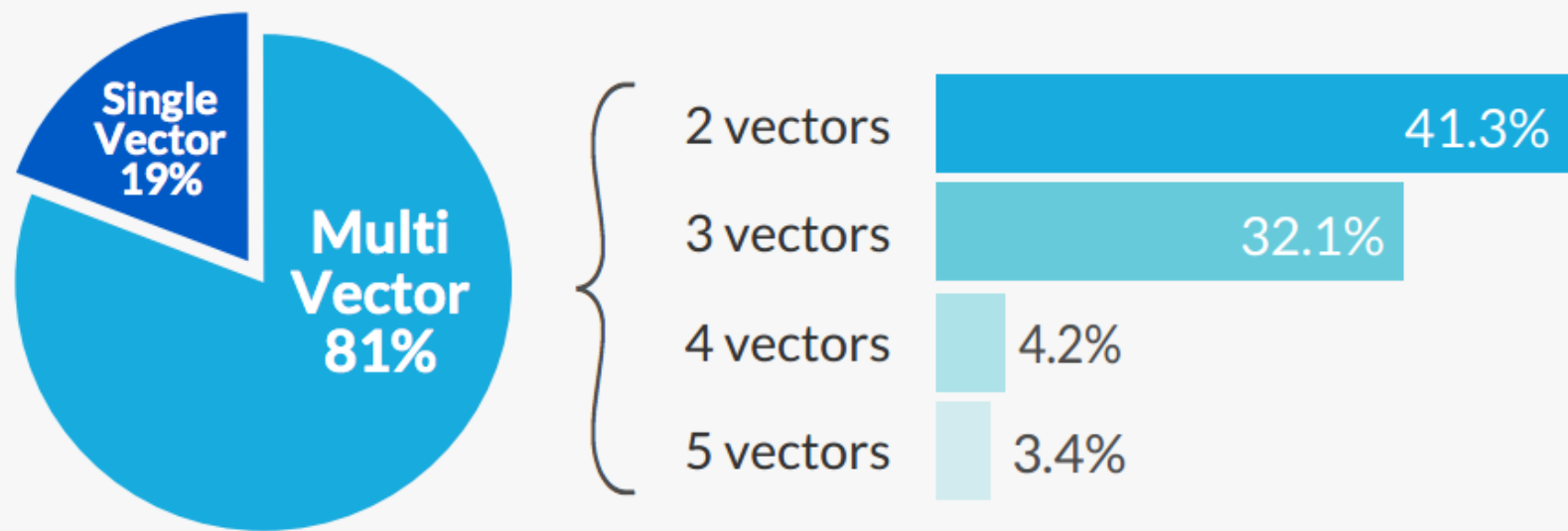


# Pre-Packaged Automated hacking tools are an Increasing Problem





## Network DDoS Attacks: Distribution by Number of Vectors





# DDoS attacks hide the Real Threat

CSO

## DDoS attacks: a perfect smoke screen for APTs and silent data breaches



Credit: Public Domain

Growing DDoS attacks more and more frequently try to distract incident response teams in order to hide much bigger security incidents.

PCI Compl  
FOR  
DUMM  
A Reference  
for the  
Rest of Us!  
Kamath Thakur  
SVP, Infosys

ComputerWeekly.com

## Most DDoS attacks hiding something more sinister, Neustar warns

Warwick Ashford  
Security Editor

15 Sep 2016 10:00

Twitter Google+ LinkedIn Email

Smaller DDoS attacks can be more dangerous than a powerful attack that knocks a company offline but does not install malware or steal data, warns Neustar

**PROJECT PLANNING SUCCESS GUIDE**  
Access this exclusive 80+ page guide to cloud migration

Explore the pros and cons of migrating, tips for evaluating cloud providers, tactics for staff training and more.

[Download Now](#)

http://www.nj.com/middlesex/index.ssf/2015/12/h... Cyber attack shuts down Rutgers online classroom site

2

Facebook Twitter Email 54 shares

**Cyber attack shuts down Rutgers online classroom site**


Hacked:

Sponsored by: SOURCE

Universities suffer cyber-at... x +

www.bbc.com/news/educa

8 December 2015 | Education & Family



The UK's main academic computer network came under sustained attack

**University students across the UK have been unable to submit work, after the academic computer network known as Janet came under cyber-attack.**

Distributed denial of service (DDoS) attacks began on Monday and are continuing, according to the network's operator, Jisc.

High schooler allegedly hir... x +

https://nakedsecurity.sophos.com/2015

naked security by SOPS

SOPHOS.COM FREE TOOLS

Award-winning computer security news

**High schooler allegedly hired third party to DDoS his school district**

22 MAY 2015 1

Connecting to stats.wp.com...

Universities across the cou... x +

www.telegraph.co.uk/technology/internet-security/12

Privacy and cookies | Jobs | Dating | Offers | Shop | Puzzles | Investor | Log in | Register | Subscribe

**The Telegraph**

Tuesday 19 April 2016

Home Video News World Sport Business Money Comment Culture Travel Life Women Fashion Luxury Tech Film

Apple iPhone Technology News Technology Companies Technology Reviews Video Games Technology Video Mobile Apps

HOME » TECHNOLOGY » INTERNET SECURITY

**Universities across the country lose internet connections following cyber attack**

An cyber attack is behind universities and fire services across the country losing their internet connections

Top Technology Videos

 Rise of a tech giant: the history of Google

 The history of Uber

Facebook 0 Twitter 0 Pinterest 0 LinkedIn 0 Email

# So what about right now?

I only see DDoS in the news a few times a year!  
How much of it could really be happening right now?

Lets take a look...

<http://www.digitalattackmap.com/>

June 14

2014

Philippines

Show All

Show Attacks



Large

Unusual

Combined

Large attacks on Philippines, United States, United Kingdom, + 10 others

Color Attacks By

Type

Source Port

Duration

Dest. Port

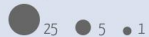
TCP Connection

Volumetric

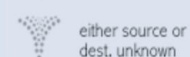
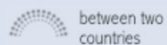
Fragmentation

Application

Size (Bandwidth, in Gbps)



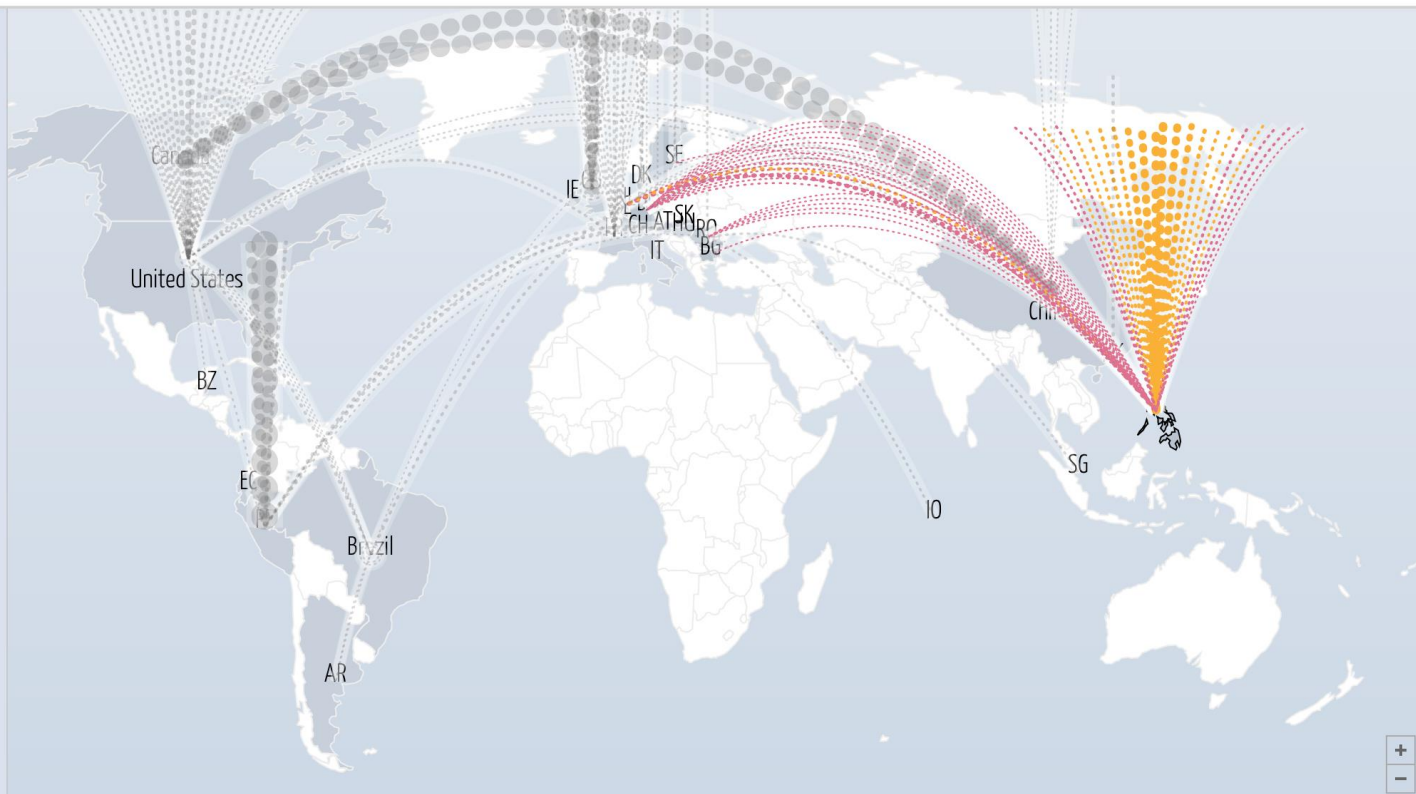
Shape (source + destination)



<Get Embed Code>

Map

Table



Attack Bandwidth (Philippines), Gbps

Dates are shown in GMT

Data shown represents the top ~2% of reported attacks





Please visit [f5.com/security](https://f5.com/security)  
for more information



**SOLUTIONS FOR AN APPLICATION WORLD**