

A 3D network diagram with a dark background. It consists of numerous black and orange spheres representing nodes, connected by a web of white lines. The orange nodes are concentrated in the center-right area, while the black nodes are more widely distributed. The nodes have a glossy, reflective surface.

# DDoS – Yesterday, Today and tomorrow

Frank Tse, William Guo

Nexusguard

# Agenda

- 1 DDoS Introduction
- 2 DDoS Attack Analysis
- 3 DDoS Detection and Mitigation
- 4 Fighting DDoS in Mobile Era
- 5 FAQ

## About us

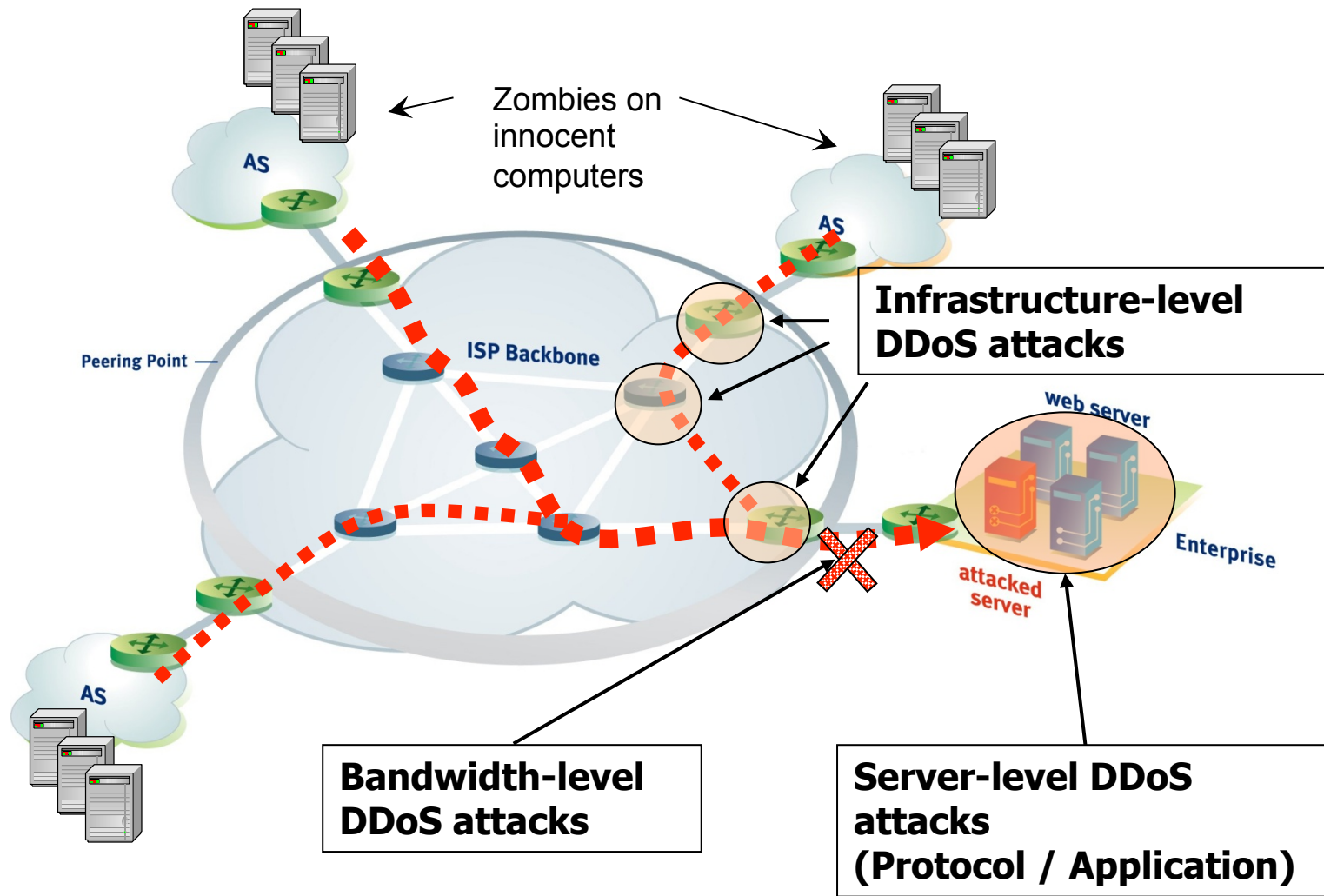
Nexusguard, incorporated in 2008, is a premium provider of end-to-end, in-the-cloud Internet Security Solutions. Nexusguard delivers solutions over the internet to ensure that our clients enjoy uninterrupted web-service delivery to their users, by protecting them against the ever-increasing and evolving multitude of internet threats, particularly Denial-of-Service (DDoS) attacks, and other attacks directed at web application software.

Re:SEARCH 

We Take Quality Seriously

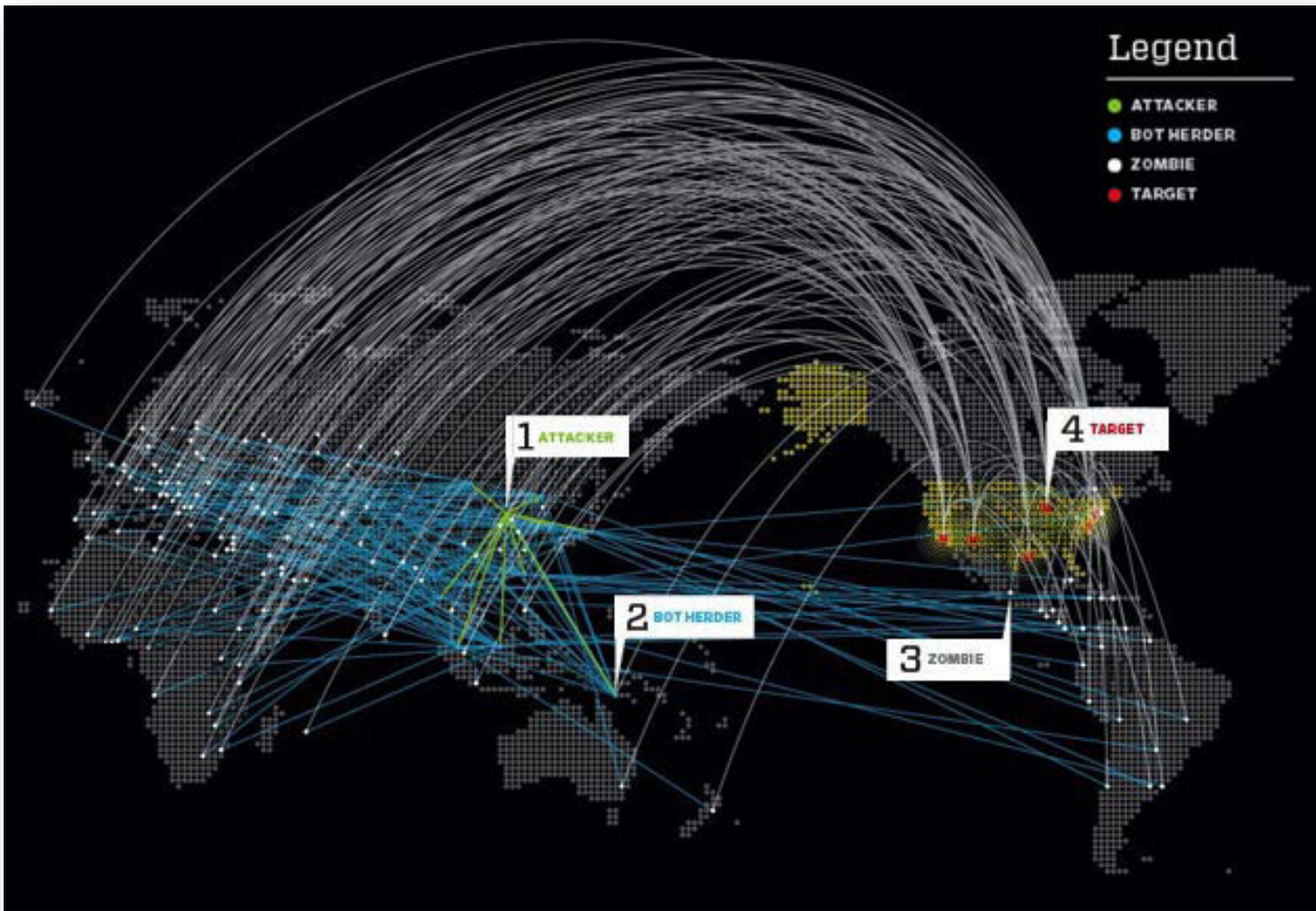


# What is DDoS





# What is DDoS



Credit [http://www.wired.com/politics/security/magazine/15-09/ff\\_estonia\\_bots](http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots)

# DDoS in the news



## Operation: Payback

<irc://irc.anonops.net/operationpayback> est. 2010



Target:



We will attack any organization which seeks to remove WikiLeaks from the internet or promote the censorship of the masses. *Join us.*

TARGET THESE IP's

208.73.210.29

204.152.204.166

209.85.51.151

195.74.38.17

89.18.176.148

# facebook

Account temporarily unavailable

Your account is currently unavailable due to a site issue. We expect this to be resolved shortly. Please [try again](#) in a few minutes.

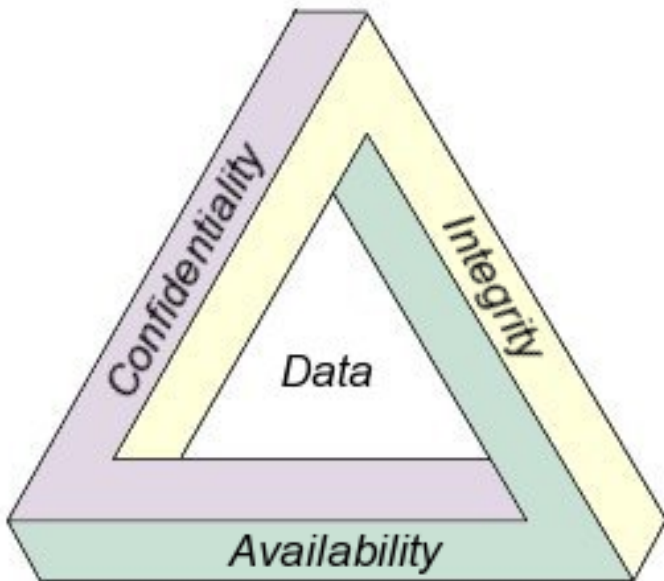
# Motivation of Cyber Attack





# DDoS vs. Hacking

## Hacking



## DDoS

```
If (Avalible) {  
    try  
  
    {  
        SQLi, XSS, CSRF  
        MITM, Brute Force, Reverse  
        Engineering, Buffer Overflow, RFI,  
        Session Hijacking, Information  
        Leakage, Defacement,  
        something cool  
    } catch (data)  
    finally  
    { DDoS }
```

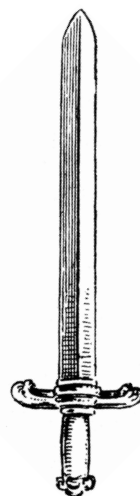
```
while (Available) {  
    try  
  
        { DDoS () }  
    finally  
    { Give_up () }
```



# DDoS Attack – Brief History



**Packet Generator**



**Packet Crafter**



**Creative Attacks**

# DDoS - Yesterday

## 2002 root DNS attack

All thirteen (13) DNS root name servers were targeted simultaneously. Attack volume was approximately 50 to 100 Mbits/sec (100 to 200 Kpkts/sec) per root name server, yielding a total attack volume was approximately **900 Mbits/sec** (1.8 Mpkts/sec).

Attack traffic contained ICMP, TCP SYN, fragmented TCP, and UDP.

## Some attack types you might heard of

ICMP flood, Ping flood, UDP flood, IP Fragment, SYN flood, Teardrop, ACK flood, RST flood, Land attack, smurf attack, Ping to death, Nuke, ARP Poison, Reflex attack, TCP NULL, XMAS, Malformed TCP flags, PUSH ACK flood, DNS query flood, GET flood, POST flood, authentication flood, de-authentication flood, SIP flood





# DDoS - Yesterday

**Tools (comes with your OS)**

**Ping, telnet, wget**

**Tools ( can easily get from internet)**

**hping, scapy, cURL,**

**Library:**

**Libpcap-dev, libthread, libnet-dev, netinet/\*.h,  
string.h**



Simple GET flood in 1 line

```
for ((i=0;i<100;i++)) do `wget target.com &`; done
```

# DDoS - Today

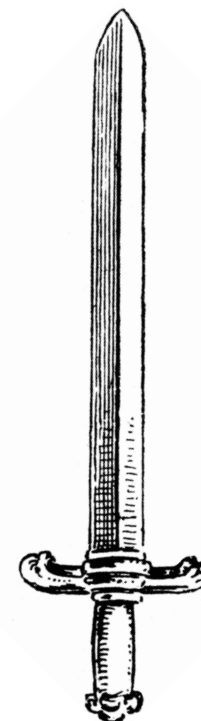
- **Open source,**
- **Cross platform,**
- **More in flow control,**
- **More in application layer**

**Tools ( can be easily get from internet)**

**apache-killer.pl, slowloris.pl, slowhttpstest,  
LOIC, HOIC, via IRC channel**

**Library:**

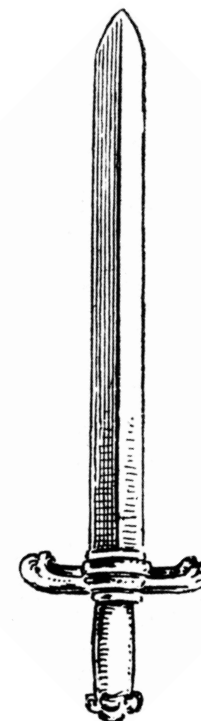
**Libpcap-dev, libthread, libnet-dev,  
urllib, libpcap-dev, libdnet-dev, socket**



# DDoS - Today

apache-killer.pl

```
$p = "";  
for ($k=0;$k<1300;$k++) {  
    $p .= ",5-$k";  
}  
  
$p = "HEAD / HTTP/1.1\r\nHost: $ARGV[0]\r\n\r\nRange:bytes=0-$p\r\nAccept-Encoding:  
gzip\r\nConnection: close\r\n\r\n\r\n";
```



# DDoS - Today

## Slowhttp 'test'

`-w bytes`

start of the range **advertised window size** would be picked from.

Effective in slow read (-X) mode only, min: 1, default: 1

`-y bytes,`

end of the range **advertised window size** would be picked from.

Effective in slow read (-X) mode only, min: 1, default: 512

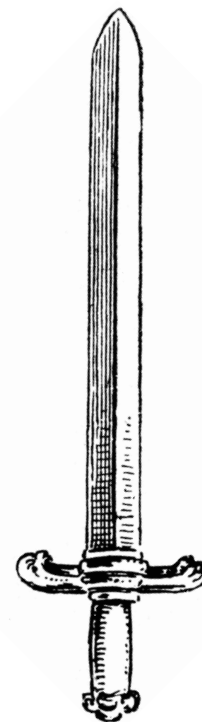
`-x bytes,`

max length of each **randomized name/value pair** of follow up data per tick, e.g. `-x 2` generates `X-xx: xx` for header or `&xx=xx` for body, where `x` is random character, default: 32

`-z bytes`

bytes to **slow read from receive buffer** with single `read()` call.

Effective in slow read (-X) mode only, default: 5





# DDoS – Tomorrow

- **0-day focused**
- **Standardized – part of worms and bots**
- **DDoS as a project, in a team**
- **Focus on target application**

## Tools:

**HashDDoS – DJB33X, protocol fuzzer, iFrame bot, js bot, Unicornscan (2007), plug-in for worms, mobile bots**

## DDoS as a Service:

**DDoS attack repository, open DDoS ‘testing’ server, RFC for DDoS, “Like” this attack, DDoS ‘app’ market, auto CAPTCHA breaking**



# DDoS – Tomorrow

Internet is

designed for inter-connect,  
goodwill in self-discipline

Internet is NOT

designed for **security**.

TCP is :

designed for state-ful,  
connection-oriented connection,

TCP is NOT:

temper proof

**synchronized**

source **authenticate**

sensitive to intercept (MITM)



# DDoS – Tomorrow

Unicronscan (<http://www.unicronscan.org/> )

Unicrons are fast!

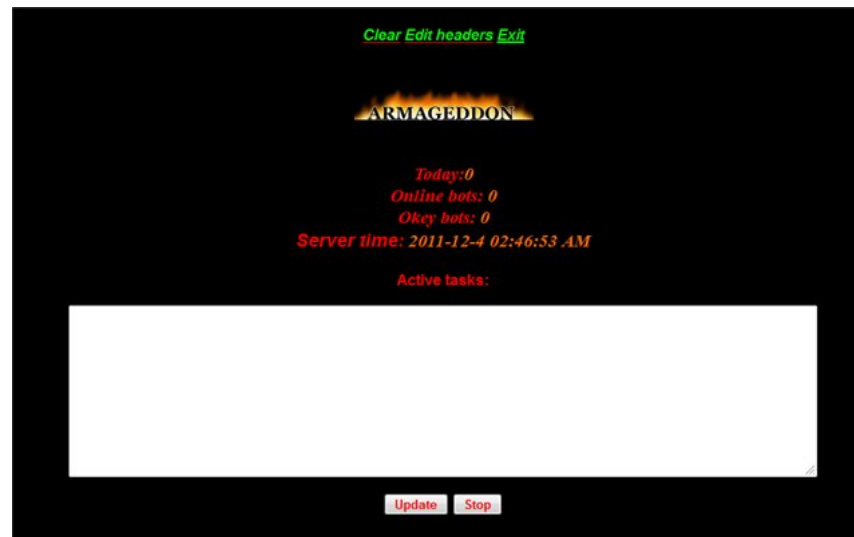
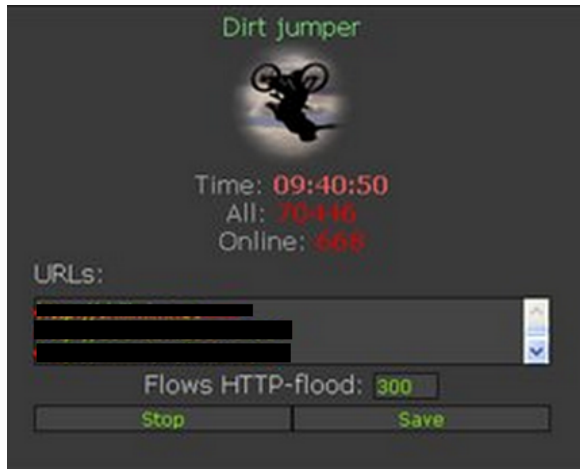
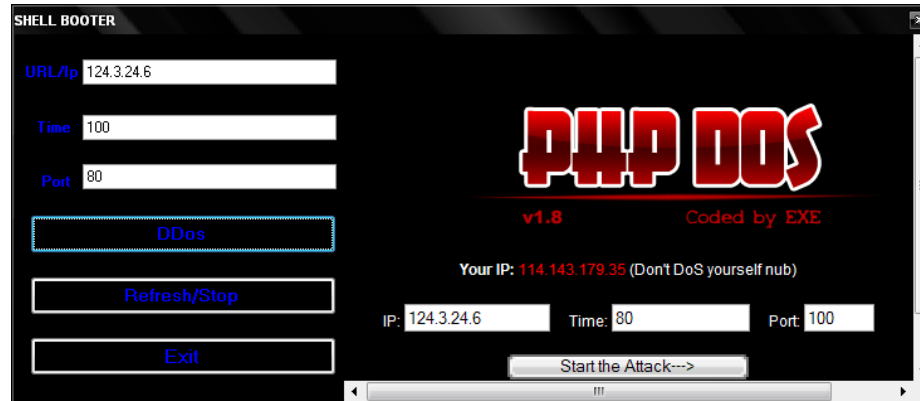


**Asynchronous** stateless TCP scanning with all variations of TCP Flags.  
**Asynchronous** stateless TCP banner grabbing  
**Asynchronous** protocol specific UDP Scanning



# DDoS – Tomorrow

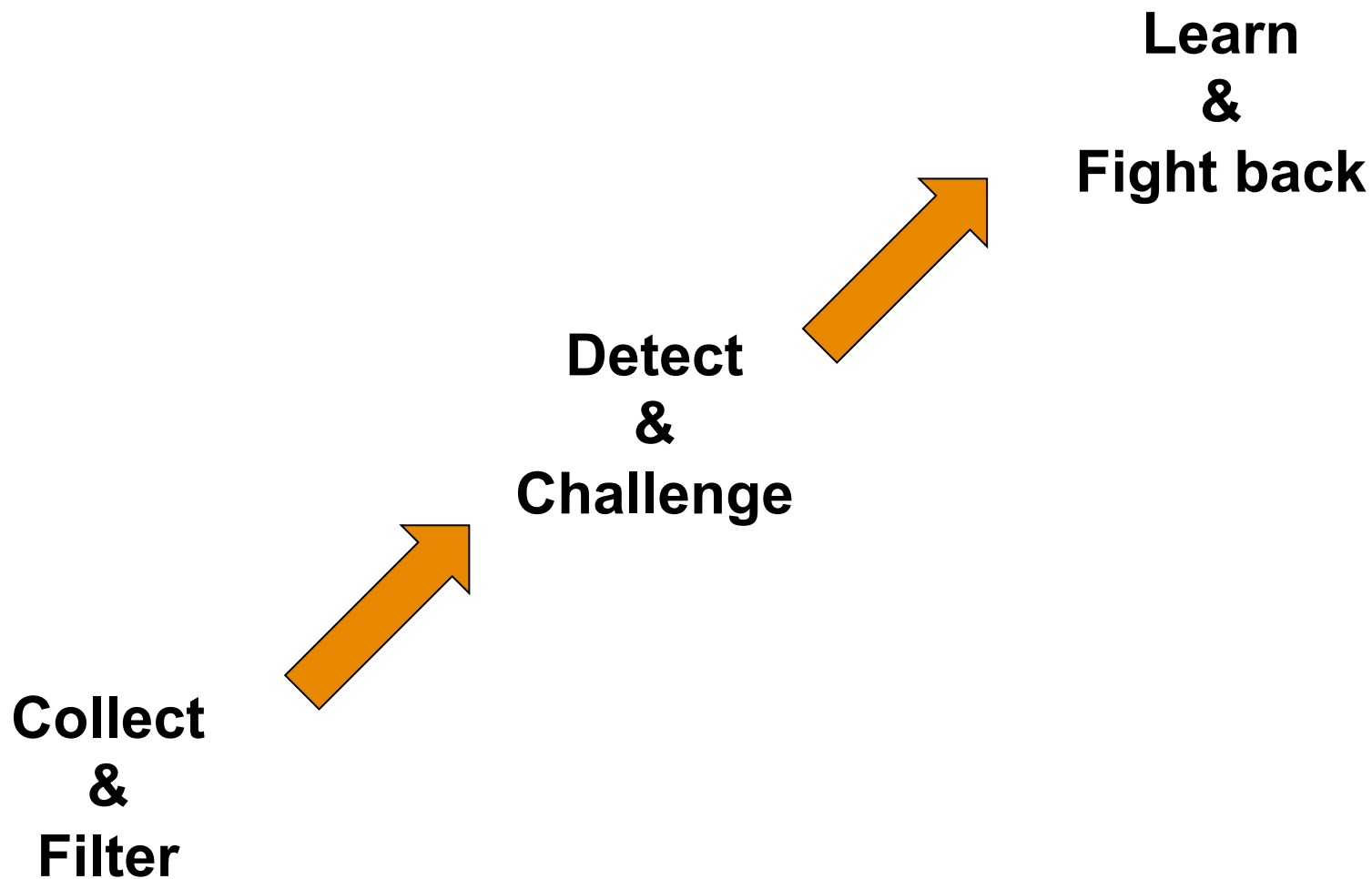
## Web Shell



Credit <http://ddos.arbornetworks.com/2012/02/ddos-tools/>

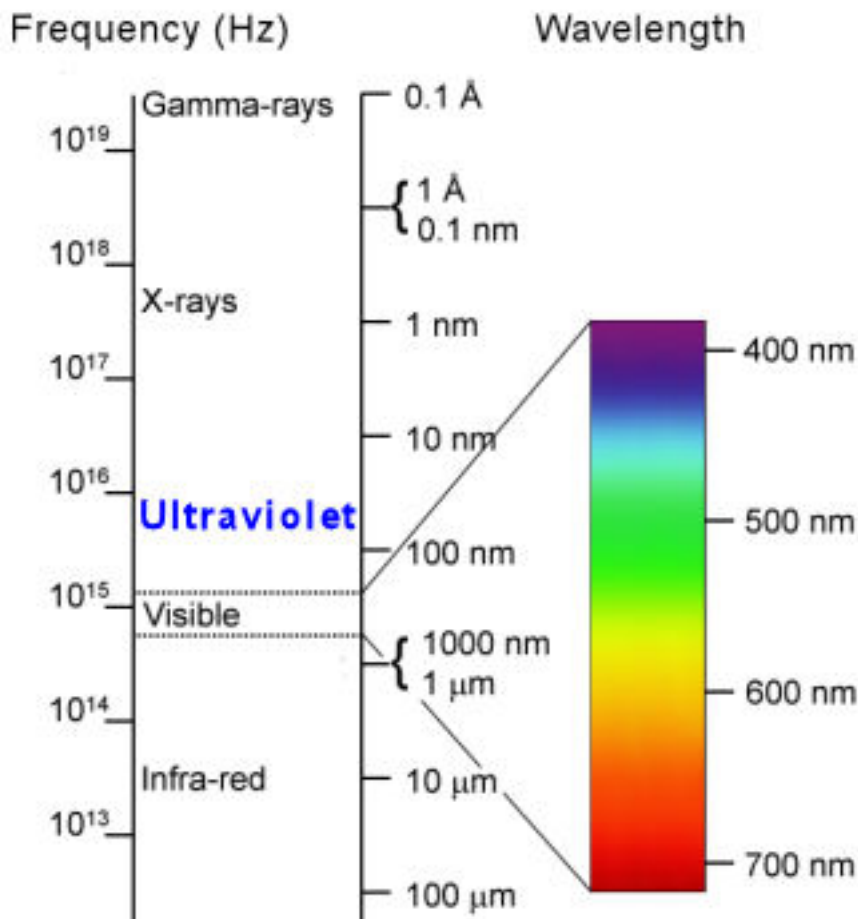


# DDoS Detection and mitigation– Brief History



# DDoS Detection and mitigation – Yesterday

- **Blackhole**
- **Rate-limiting**
- **ACL**
- **iptables**
- **CoPP**
- **SYN-cookie**
- **IDS**
- **IPS**
- **Load balancing**
- **Port-security**
  
- **Detection: SNMP, netflow**



# DDoS Detection and mitigation – Today

- **DNS poisoning**
  - **CDN**
  - **WAF**
  - **Hot-link protection**
  - **CAPTCHA**
  - **Source authentication**
- 
- **Detection: SNMP, Netflow, PCAP**



# DDoS Detection and mitigation – Tomorrow

- **Browser authentication**
- **User behavior validation**
- **Application learning**
- **User-id correlation**
- **Differentiate mitigation**
- **Bot / tools identification**
- **(Friendly) Attack back**

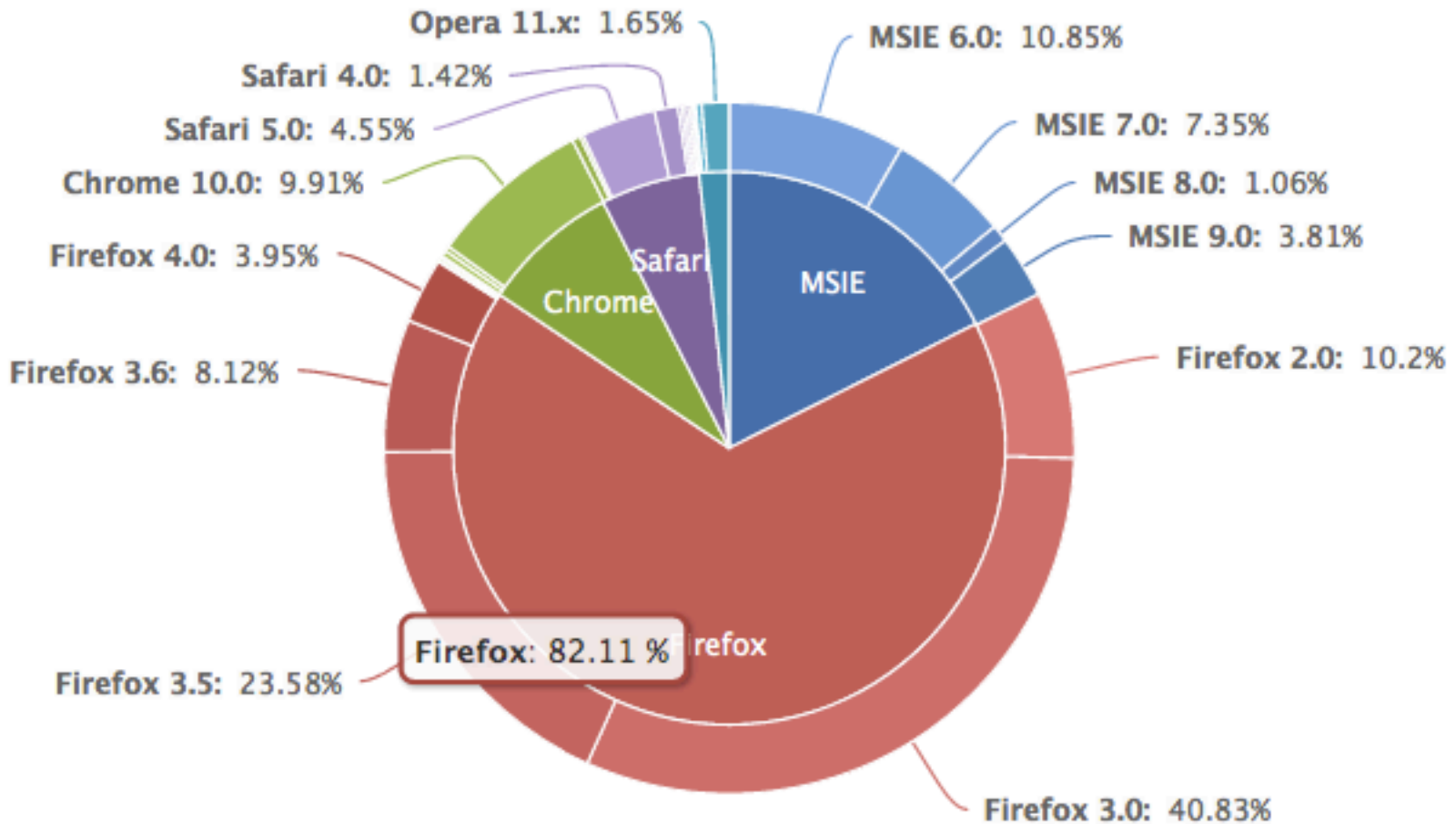
*"Apparently the war is over and you are ordered to cease firing; so, if you see any Jap planes in the air, you will just have to **shoot them down** in a **friendly** manner."*

- Admiral Halsey, 1945

- **Detection: SNMP, Netflow, PCAP, logs + big data**



# Next Generation Detection---Profiling and Data Mining



# A HTTP Get Flood Attack Analysis

```
sh-3.2$ cat httpget.log | more
```

```
1.0.0.4  
1.113.1  
1.113.5  
1.115.1  
1.160.1  
1.160.2  
1.160.2  
1.160.2  
1.162.1  
1.162.4  
1.162.5  
1.162.5  
1.168.7  
1.169.1  
1.169.4  
1.170.1  
1.170.1  
1.171.1  
1.171.1  
1.171.2  
1.171.2
```

```
sh-3.2$ tail -n 20 httpget.log
```

```
99.225.1  
99.225.3  
99.225.9  
99.226.1  
99.226.1  
99.226.2  
99.226.3  
99.230.3  
99.236.1  
99.237.1  
99.241.1  
99.243.1  
99.243.1  
99.243.2  
99.244.1  
99.247.8  
99.249.1  
99.250.4  
99.251.8  
99.255.1
```

# A HTTP Get Flood Attack Analysis

```
{'city': u'Moscow', 'region_name': u'48', 'time_zone': 'Europe/Moscow', 'longitude': 37.6156, 'metro_code': '', 'country_code3': 'RUS', 'latitude': 55.752199999999999, 'postal_code': None, 'country_code': 'RU', 'country_name': 'Russian Federation'}
```

```
{'city': u'Novosibirsk', 'region_name': u'53', 'time_zone': 'Asia/Novosibirsk', 'longitude': 82.934399999999998, 'metro_code': '', 'country_code3': 'RUS', 'latitude': 55.0411, 'postal_code': None, 'country_code': 'RU', 'country_name': 'Russian Federation'}
```

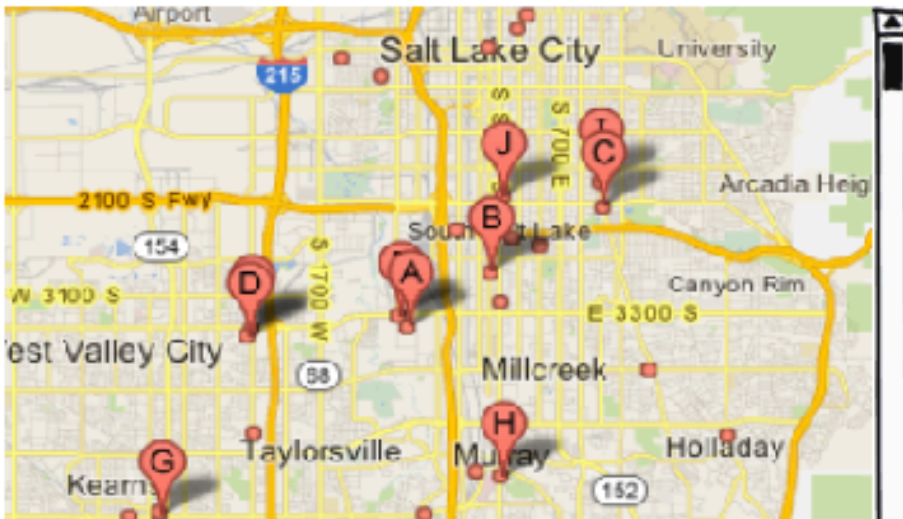
```
{'city': u'Chelyabinsk', 'region_name': u'13', 'time_zone': 'Asia/Yekaterinburg', 'longitude': 61.4297, 'metro_code': '', 'country_code3': 'RUS', 'latitude': 55.154400000000001, 'postal_code': None, 'country_code': 'RU', 'country_name': 'Russian Federation'}
```

# Next Generation Detection---With Google API ?

DDoS GeolP Trace System

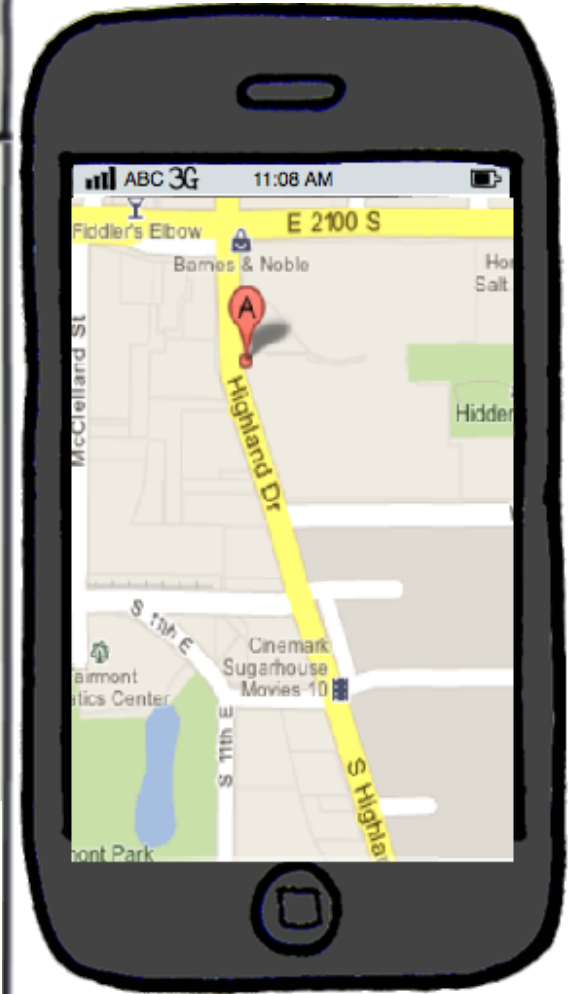
← → × 🏠  🔍

[Home](#) | [Alerts](#) | [GeolP](#) |



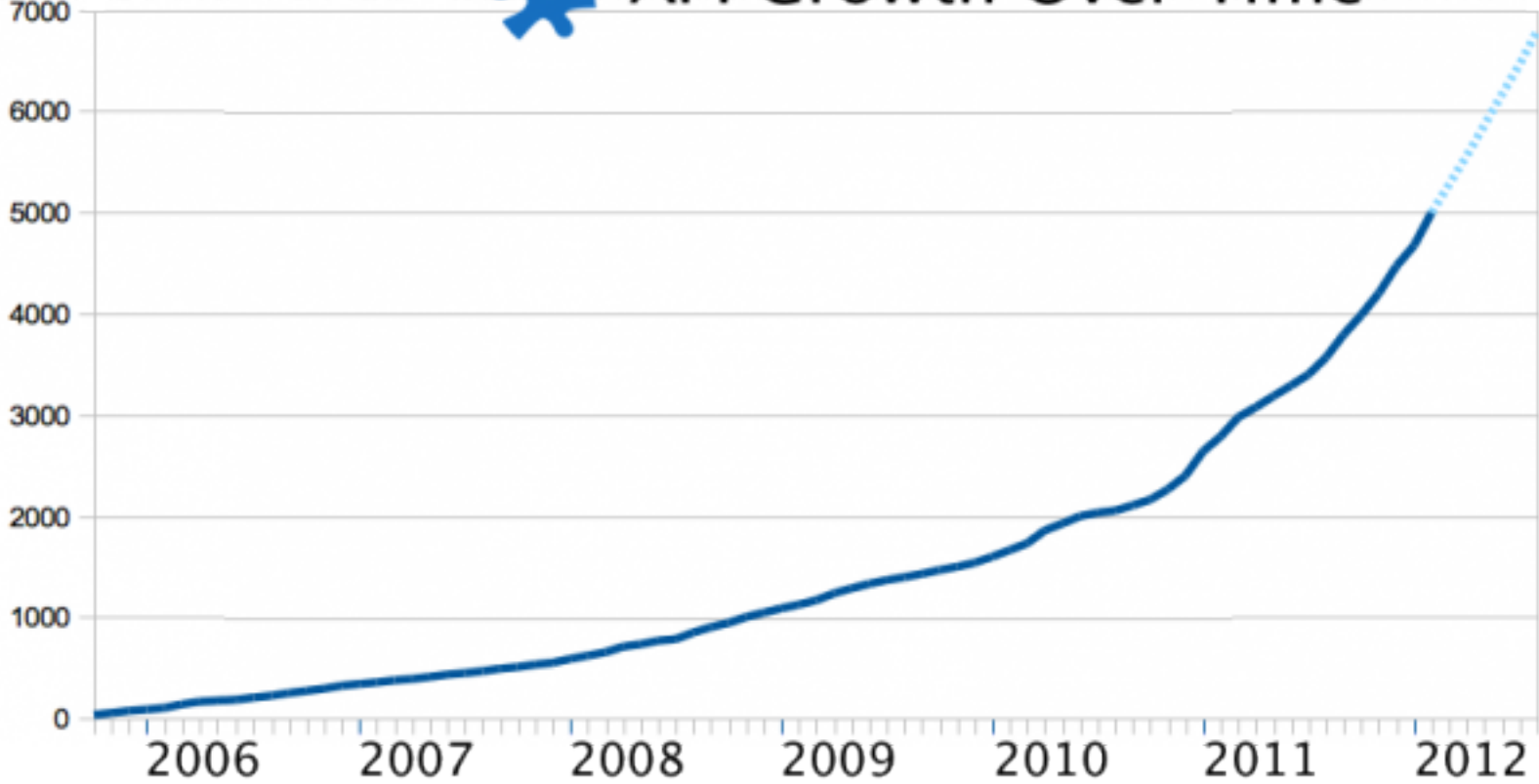
**Google slashes price 88% for using Google Maps API**

Shortly after Apple dumped Google Maps for iOS, Google announces it's time to dramatically cut the price for others using the online service. Google also gives a plug for its map-based ad service.



# Mobile Internet & Web API

programmableweb  API Growth Over Time





# API Request Load

## API Billionaires Club, 2011 edition



13 billion API calls / day *(May 2011)*



5 billion API calls / day *(April 2010)*



5 billion API calls / day *(October 2009)*



10 billion API calls / month *(January 2011)*



8 billion API calls / month *(Q3 2009)*



3 billion API calls / month *(March 2009)*



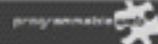
1.1 billion API-delivered stories / month *(March 2010)*



Over 50% of all traffic via API *(March 2008)*



Over 260 billion objects stored in S3 *(January 2011)*



Web

# Flipboard / Instagram Down?



**Flipboard** @Flipboard  
 Our service is currently down. Thank you for your patience.  
 Expand ← Reply ↻ Retweet



**Flipboard** @Flipboard  
 We are currently experiencing issues. We will be back up as soon as possible.  
 Expand



**Instagram Support** @Instagram  
 We're currently experiencing issues. We're working to correct the issues. Thank you for your patience.  
 Retweeted by Instagram  
 Expand



Popular Science  
 No content

Cool  
 No content

The New Yorker  
 No content

Vanity Fair  
 No content

Guardian Film  
 No content

Photos  
 No content

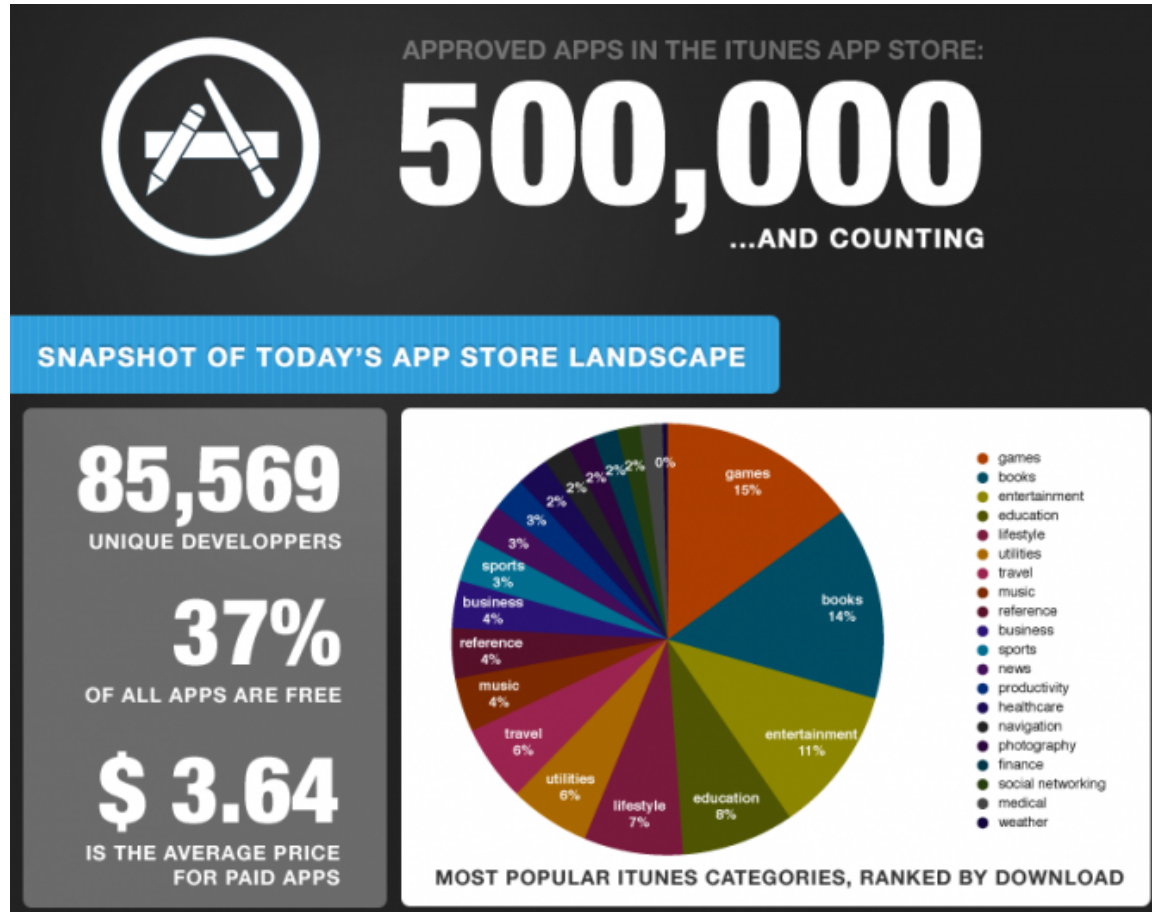
The Craft of Photography  
 No content



**Flipboard**

Browse your own personal sports magazine with ESPN content in Flipboard.  
 Leverages: **Headlines API**

# Know it before you hack it



# API Abused DDoS

## ■ API Security Threats

- API Key spoofing
- API Throttling bypass
- Quota System bypass
- API ACL (Private API accessed by Public)

## ■ API Request DDoS

- HTTP/HTTPS GET flood
- HTTP/HTTPS POST flood
- PUT/DELETE/HEAD ?

# What if it's not abuse?

100,000 Users Have Downloaded Malware From Google Play



# Google/ Alternative Android Markets and the Audit Policy





# Mobile Device Botnet---Existing Apps

## Android DDoS Tool

### Available in Google Play

1. Requires Internet access to send the http post data
2. Requires phone state to access the IMEI

Pretty common requirement for Apps.



# Mobile Device Botnet--- Free App Generator


Home / Create

## Step 1 of 2

Website URL:  valid name

App name :

Description :

Icon :  Default icon   Custom icon

Screen Orientation :  Auto  Vertical  Horizontal

Category :

**CREATE**

## App Statistics

Installs: 0  
Uninstalls: 0  
Downloads: 0  
Usages: 0

ALL STATS

## What next?

### 1. Download your App

Download your App to your Android device to test it



Your users can download your app from:

<http://www.appsgeyser.com/getwidget/Android%20DDoS%20for%20HIT%20>

Short url: <http://www.appsgeyser.com/199699>

### 2. Publish Android DDoS for HIT to Google Play

PUBLISH

Read [our blog](#) to learn why it is important or see [how to video](#).

### 3. Monetize

Start earning money from your app.

MONETIZE

# Next Generation Detection---Profiling and Data Mining

## ■ Traffic Baseline

- HTTP Field Pattern
- HTTP Traffic Volume
- TCP Connections

## ■ IP Ranking

- Geo IP
- 80 / 20
- Open API Data Comparison---e.g. Google Safe Browsing API
- Seculert API(expensive!).



# Do You Have Any Questions?

Contact us at:  
[research@nexusguard.com](mailto:research@nexusguard.com)