SECURITY CASE STUDY 2014

Real Life DoS/DDOS Threats and Benefits of Deep DDOS Inspection

Oğuz YILMAZ CTO

Labris Networks

Today

- Labris Networks
- L7 Attacks
- L7 HTTP DDoS Detection Problems
- Case Study: Deep DDOS Inspection (DDI™) for HTTP
- Case Study: L7 NTP Attacks
- Case Study: L7 Gaming World
- Future DDOS Predictions
- DDOS CERT

Labris
NETWORKS

Deloitte.
Technology Fast
500 EMEA 2013

WINNER

Industry	NETWORK SECURITY
Founded	2002
Customers	3500+
Verticals Served	ALL VERTICAL MARKETS From 5 users to 1 Million users
Area Served	EMEA (20+ countries)
Products	NETWORK SECURITY SOFTWARE UTM APPLIANCES DDOS MITIGATION APPLIANCES

EAL4+
Common Criteria
CERTIFIED

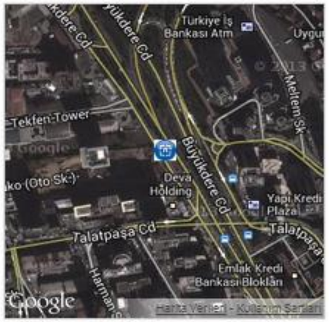
Our Current Offices

ODTÜ Kampüsü
Odtu Teknokent Gümüş Bloklar
Emrah YILMAZ
Odtu Eğitim Fakultesi
Odtu Teknokent Galyum Bloklar
ODTÜ Kampüsü
Google
Harita Verileri - Kullanım Şartları

R&D Headquarter

Silicon Block, METU Technopolis
ANKARA

Phone: (+90) 312 210 1490 (PBX)



International Export Office

Levent Loft,
ISTANBUL

Phone: (+90) 212 264 2200 (PBX)

Turkey

EU Coordination Office, UK

Rosemead House, Willington, Bedfordshire
UNITED KINGDOM

Phone: (+44) 770 350 3242
uksales@labris.eu

Eastern Europe Office, Czech Rep.

Pocernicka Praha, Prague
CZECH REPUBLIC

Phone: (+44) 770 3 50 3242

United Kingdom

Czech Republic

HARPP

ddos mitigator

Labris

NETWORKS

Product & Services

Labris UTM

MNG

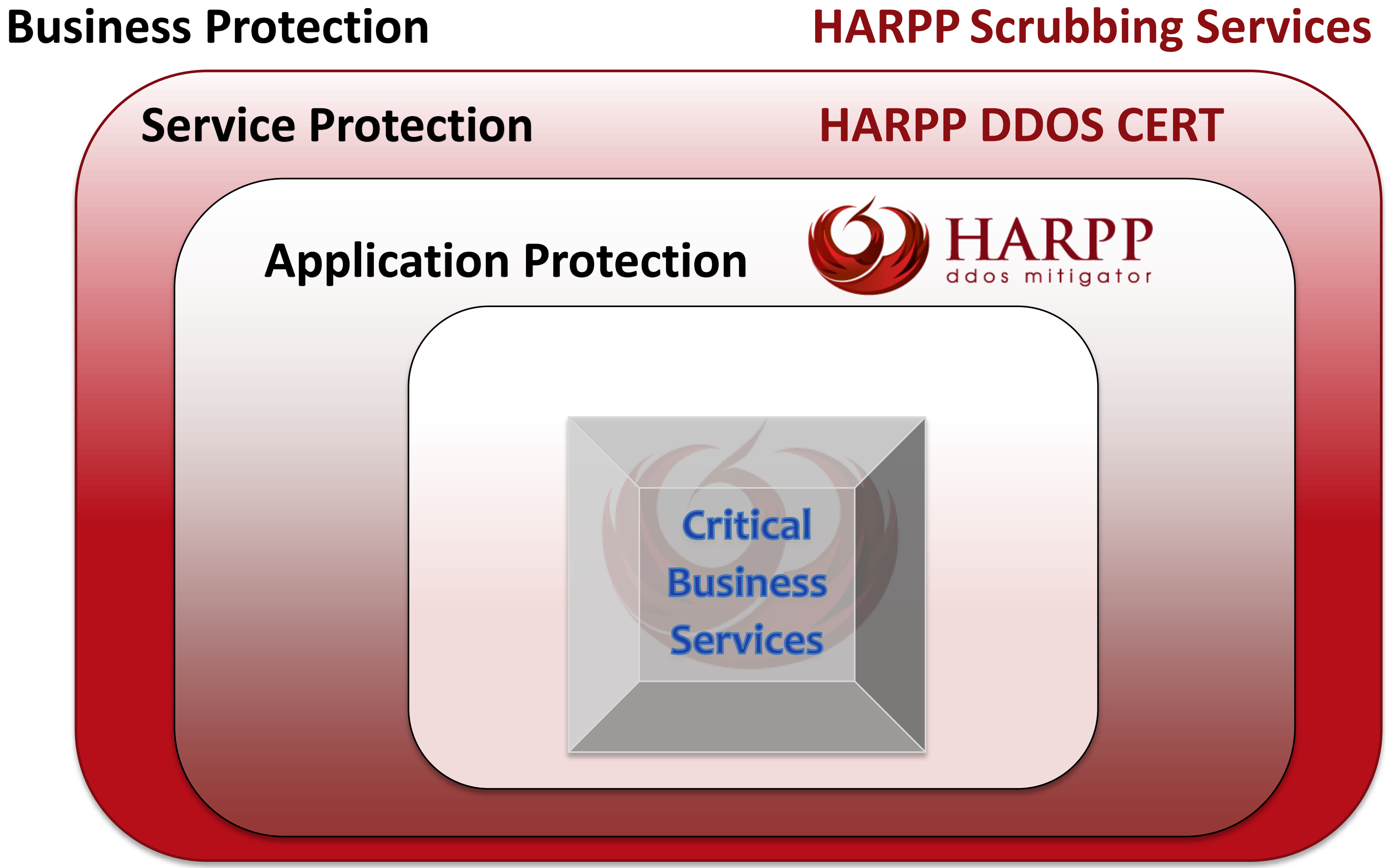
LOG

Database Updates
Firmware Updates
Technical Support
Network Security Trainings

HARPP
ddos mitigator

Database Updates
Firmware Updates
Technical Support
Specific DDoS Trainings
DDoS Mitigation Consultancy
DDoS CERT Service

HARPP DDOS Protection Model



Business Protection

HARPP Scrubbing Services

Service Protection

HARPP DDOS CERT

Application Protection

HARPP ddos mitigator

Critical Business Services

HARPP
ddos mitigator

CPE in front of conventional network security equipment

+ DDoS Specific High Performance Hardware
+ Anomaly Detection with Artificial Intelligence (CW AI)
+ Application specific protection with plugins
+ DoS/DDoS specific IPS
+ IP Reputation Networks
+ Evidence collection and timestamping

HARPP
ddos mitigator

L7 DDoS Attacks

L7 DDoS Attacks

About TCP;

- Established TCP is real IP traffic
- Amplification is possible
- If the attacker is detected, blocking is easy

- Today, %60 of DoS/DDoS attacks is on L7.
- This rate is increasing.

L7 DDoS Attacks

- Common attacks types
  - HTTP GET/POST Floods
  - Application Exploit attacks
  - DNS Floods
  - NTP Floods
  - HTTP Slow Post
  - HTTP Slowloris

HARPP
ddos mitigator

Case Study

Customer Type: E-commerce

Mobile apps and L7 HTTP DDoS Detection Problems

L7 HTTP DDoS Detection Problems

- At L3, there is shadows of L7 attacks. It is possible to try to prevent an attack via L3 information. However, with high false positives.
- Shallow looking at L7 also has high number of false positives.

One of our ecommerce customer:

```
"www.test.com": {
                "count": 8,
                "rate": 0.8,
                "uri": {

"/ProductHandler.ashx?hCase=CampaignProducts&CampaignID=11237&GenderCategoryID=undefi
ned&CCId=-1&CategoryID=-1&Size=-1&MainCategory=-1&OrderBy=like": 1,

"/ProductHandler.ashx?hCase=CampaignProducts&CampaignID=11237&GenderCategoryID=-
1&CCId=-1&CategoryID=-1&Size=-1&MainCategory=-1&OrderBy=like": 7
                }
            }
```

Totally innocent request. Only requests different ecommerce products in a page through a mobile application.

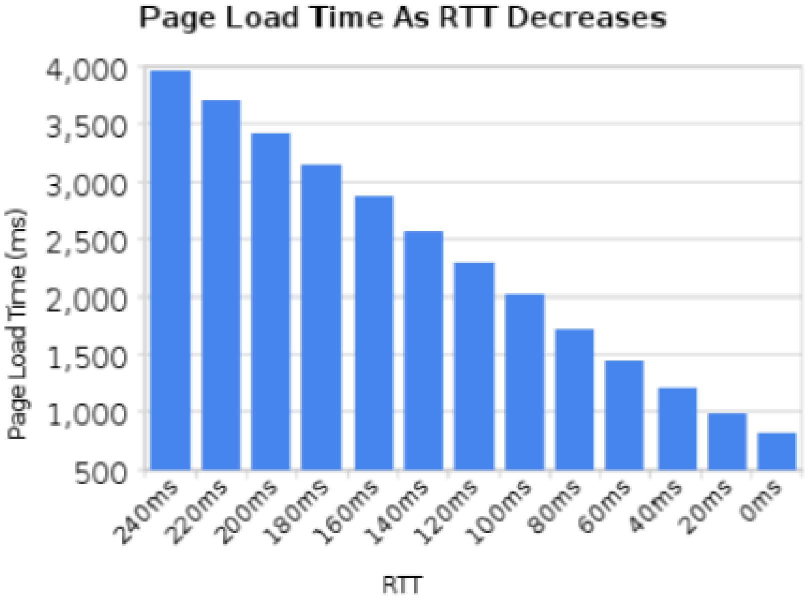
Mobile applications has limited caching and increase number of requests.

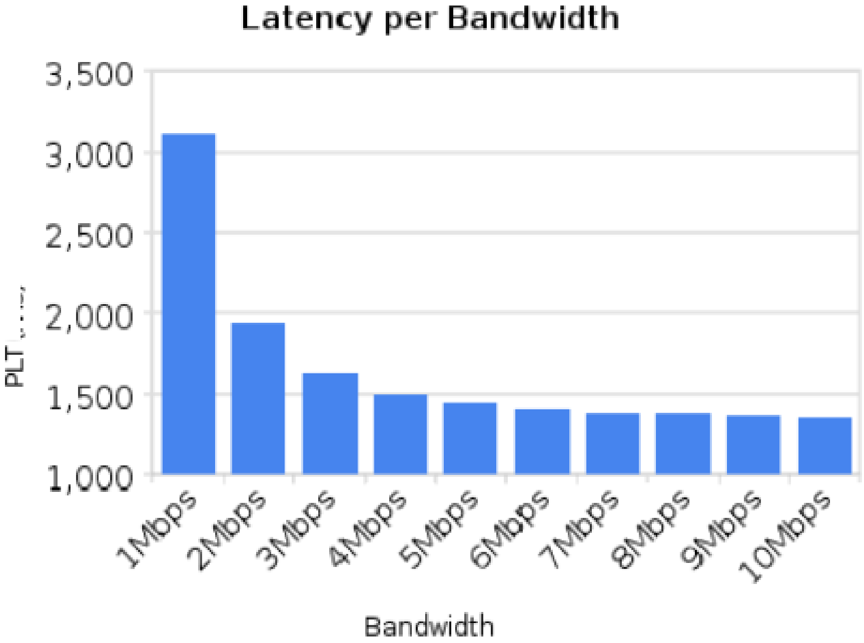
L7 HTTP DDoS Detection Problems

- Today, HTTP is changing.
- Programs and applications are becoming to work on cloud data, not local data.
- Web technologies promise high interactivity. Not «Request and wait to come», «already coming». Not Request/Response, but Stream.
- APIs and technologies are designed for this.
  - REST & AJAX
- However, All this content is carried by HTTP.

L7 HTTP DDoS Detection Problems

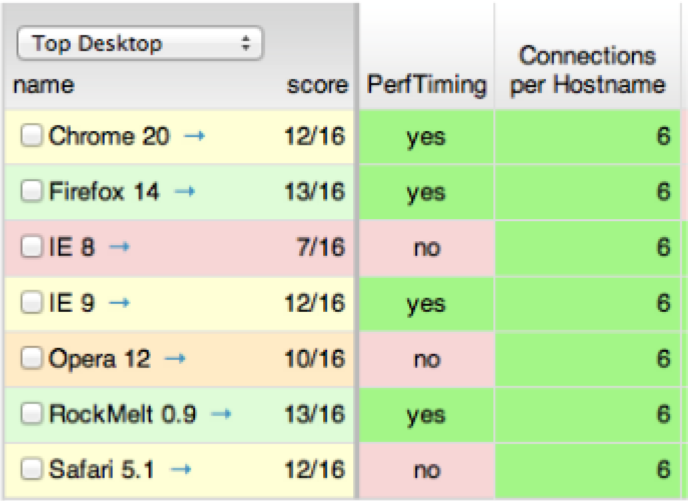
Each http request involves latency in itself





L7 HTTP DDoS Detection Problems

- Average number of contents in a web page : 50
- Browsers requests in parallel.



Top Desktop

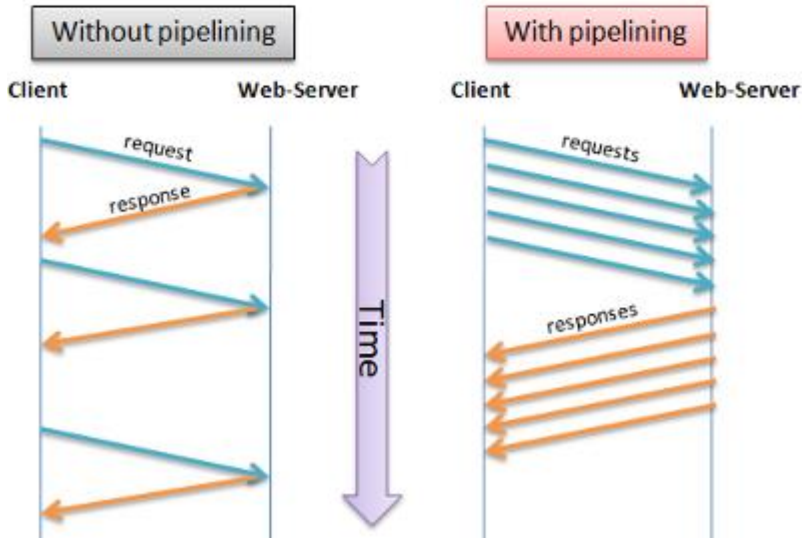
name	score	PerfTiming	Connections per Hostname
□ Chrome 20 →	12/16	yes	6
□ Firefox 14 →	13/16	yes	6
□ IE 8 →	7/16	no	6
□ IE 9 →	12/16	yes	6
□ Opera 12 →	10/16	no	6
□ RockMelt 0.9 →	13/16	yes	6
□ Safari 5.1 →	12/16	no	6

- RTT in each connection increase loading time.

L7 HTTP DDoS Detection Problems

Some solutions have been found and used:

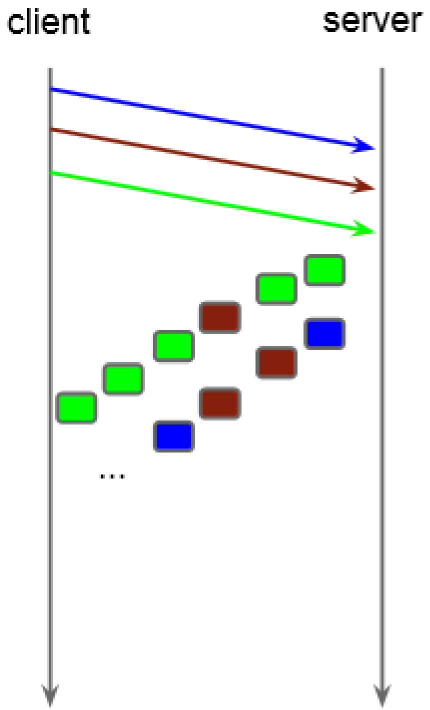
- Pipelining



In a view from L3, no much connections seen.

L7 HTTP DDoS Detection Problems

- SPDY & HTTP/2



Multiplexed stream

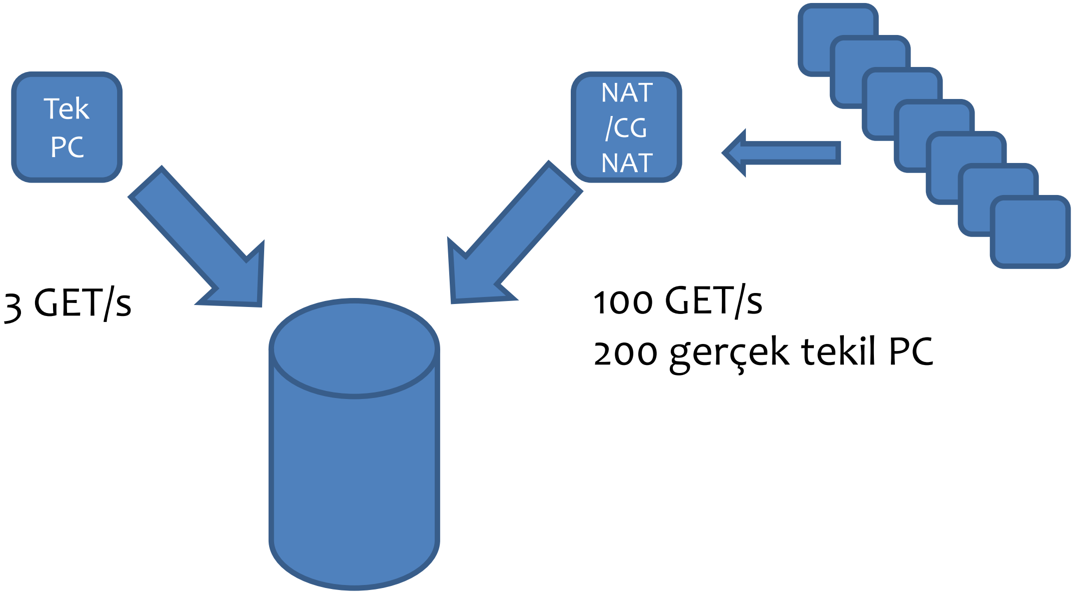
Stream priorization

Stateful HTTP header compression

Also for SPDY, shadow in L3 is different.

L7 HTTP DDoS Detection Problems

- Rate and threshold based L3 methods and even threshold based L7 methods are erroneous when in NAT'ed and one-to-one traffic.



L7 HTTP DDoS Detection Problems

- Sometimes, detailed inspection can be faulty:

```
/index.php?id=4348583
/index.php?id=1249584
/index.php?id=6747637
/index.php?id=2874656
/index.php?id=5657576
/index.php?id=0954767
```

Non-smart deep inspection may sense this sample as legitimate.

L7 HTTP DDoS Detection Problems

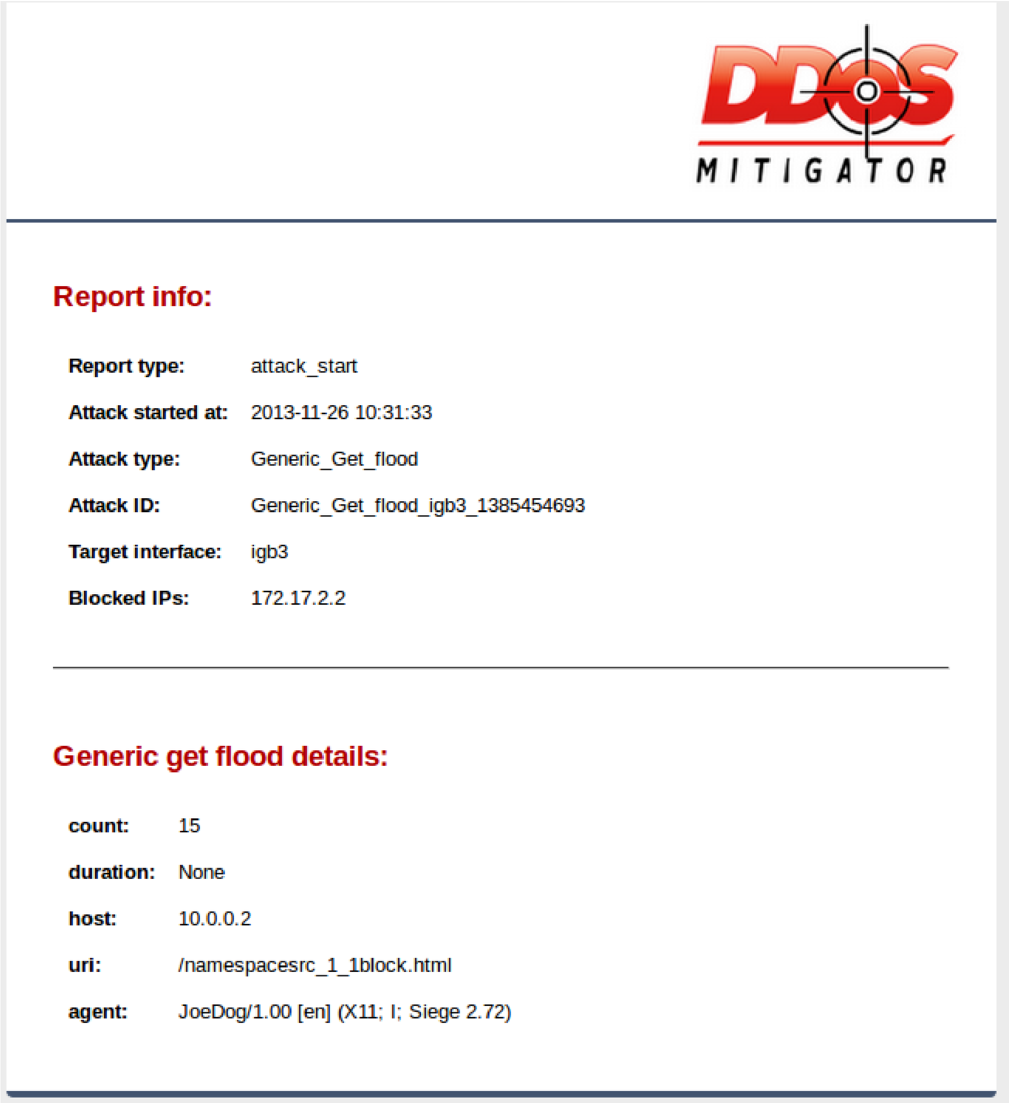
Trying to prevent L7 attacks with L3 methods lead unacceptable false positives.

Even inspection in Layer 7 requires being smart.

HTTP için Deep DDOS Inspection (DDI™)

- DDI™ inspects L7
  - NAT, Single PC recognition
  - Protocol conformance
  - URL change check
  - Robot detection in URL and HTTP headers
  - Detection of known attacks tools
  - POST content check

Protocol Specific Reporting



Report info:

Report type:	attack_start
Attack started at:	2013-11-26 10:31:33
Attack type:	Generic_Get_flood
Attack ID:	Generic_Get_flood_igb3_1385454693
Target interface:	igb3
Blocked IPs:	172.17.2.2

Generic get flood details:

count:	15
duration:	None
host:	10.0.0.2
uri:	/namespacesrc_1_1block.html
agent:	JoeDog/1.00 [en] (X11; I; Siege 2.72)

Case Study

Customer Type: Datacenter

L7 NTP Floods

NTP Flood

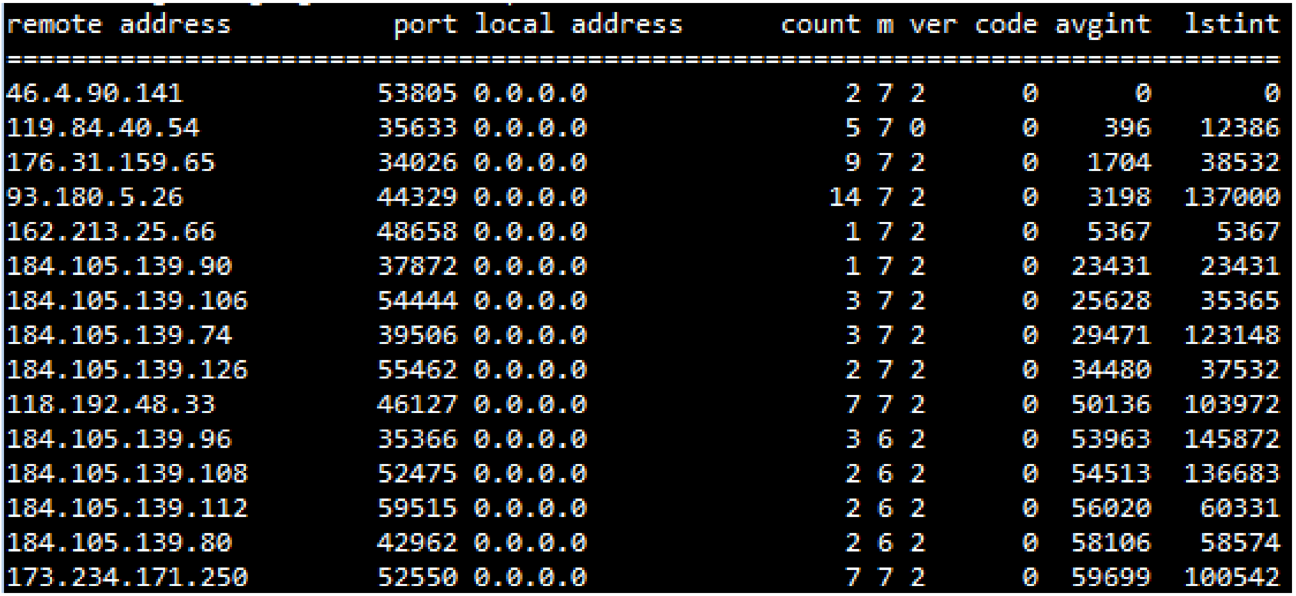
- NTP is old protocol working on UDP.
  - UDP: No source IP check

- NTP Protocol is problematic
  - monlist: NTP server will list latest 600 clients IP address
  - iostats: NTP server will list server statistics
  - Running protocol commands without authentication

- 400 Gbps of attack has been recorded (Cloudflare)
- **HARPP CERT** has resisted to **14 Gbps of SYN Flood.**

NTP Flood

# ntpdc –c monlist NTPIP

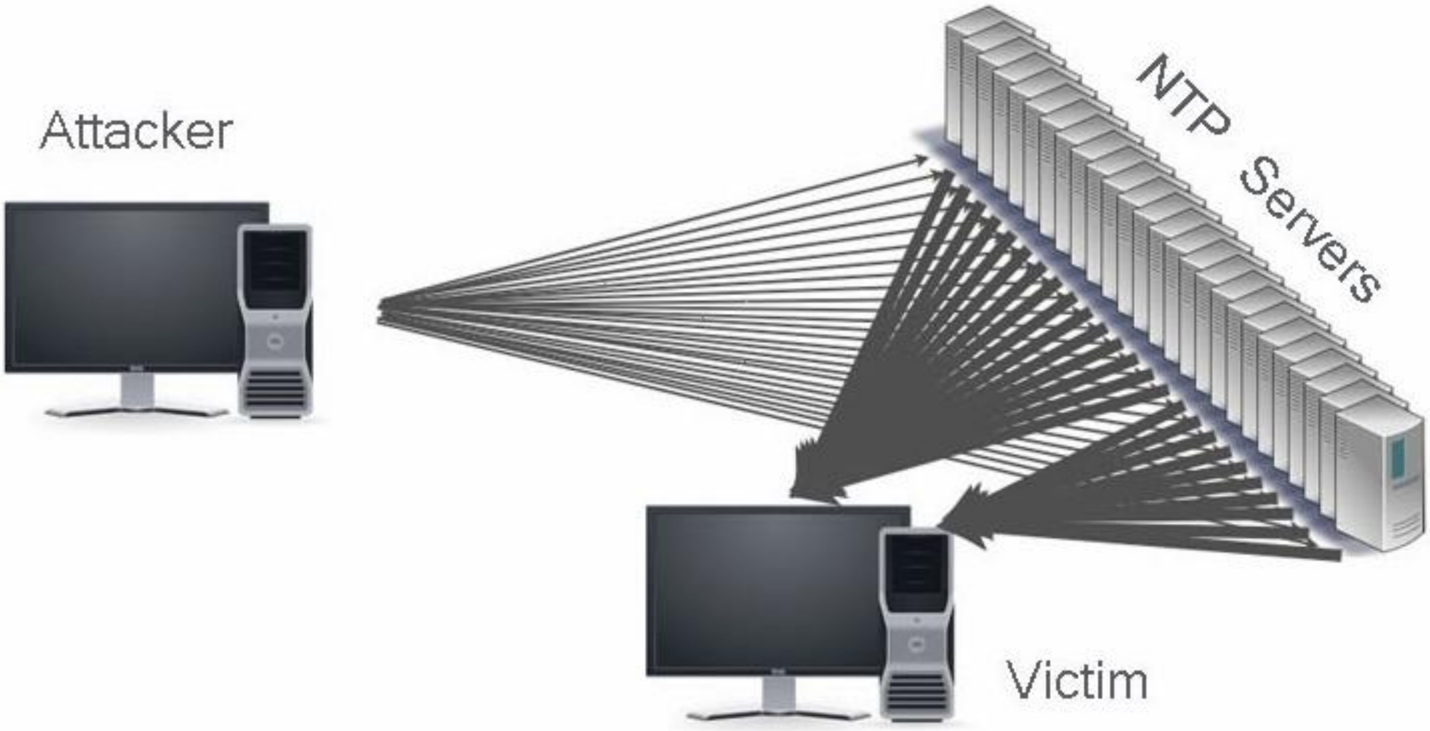


```
remote address          port local address      count m ver code avgint  lstint
===============================================================================
46.4.90.141            53805 0.0.0.0                2 7 2      0      0       0
119.84.40.54           35633 0.0.0.0                5 7 0      0    396   12386
176.31.159.65          34026 0.0.0.0                9 7 2      0   1704   38532
93.180.5.26            44329 0.0.0.0               14 7 2      0   3198  137000
162.213.25.66          48658 0.0.0.0                1 7 2      0   5367    5367
184.105.139.90         37872 0.0.0.0                1 7 2      0  23431   23431
184.105.139.106        54444 0.0.0.0                3 7 2      0  25628   35365
184.105.139.74         39506 0.0.0.0                3 7 2      0  29471  123148
184.105.139.126        55462 0.0.0.0                2 7 2      0  34480   37532
118.192.48.33          46127 0.0.0.0                7 7 2      0  50136  103972
184.105.139.96         35366 0.0.0.0                3 6 2      0  53963  145872
184.105.139.108        52475 0.0.0.0                2 6 2      0  54513  136683
184.105.139.112        59515 0.0.0.0                2 6 2      0  56020   60331
184.105.139.80         42962 0.0.0.0                2 6 2      0  58106   58574
173.234.171.250        52550 0.0.0.0                7 7 2      0  59699  100542
```

Request: 60 Byte

Response: 50x-300x

NTP Flood



NTP Flood

- L7 inspection finds monlist/iolist request & responses and block easily.
- ISP cooperation is must.

More information on attack and defense:

http://www.harppddos.com/ntp-reflection-attack/

HARPP

ddos mitigator

Case Study

Customer Type: Gaming

Application specific plugins

Gaming

- Knightonline, Teamspeak, Counterstrike, Metin2

- %25 of World e-gaming market is MMO (Massively Multiplayer Online Games)
- Remark: %2 of Canadian GDP is gaming

- Gaming development practices are not good at security. Secure development & Secure design
- Connection rate thresholds for games are very low

- Gaming is competitive. Hitting below the belt is common.

Gaming

Sample Game: Knight Online

KO uses 3 different port. For example, 12001, 12023, 12100. These ports is connected in order.

12100 -> 12023 -> 1201

Each port has different simultaneous connection and packet frequency

12001: 1-3

12023: 1

12100: 1-2

80 pps is minimum at 12001.

Connections from internet cafes are common.

Connection count and server software resistance are low. It is compulsory to inspect according to game characteristics.

Gaming

- HARPP Application Protection Ecosystem
  - HARPP KO plugin check port connection order and packet frequency for botnet and application specific slowloris attacks.
- Other plugins
  - Teamspeak
  - SIP
  - UDP Spoof Detection
  - HTTP
  - …

HARPP
ddos mitigator

Future DDoS Predictions

Future DDoS Predictions

- **Today:**
  - More than 30 common DoS/DDoS types (except application specific exploits)

- **Future:**
  - APT characteristics in DDoS
  - Migration to L7
  - Out of sight nw NTPs
  - Real user mimic

Mobile Rises

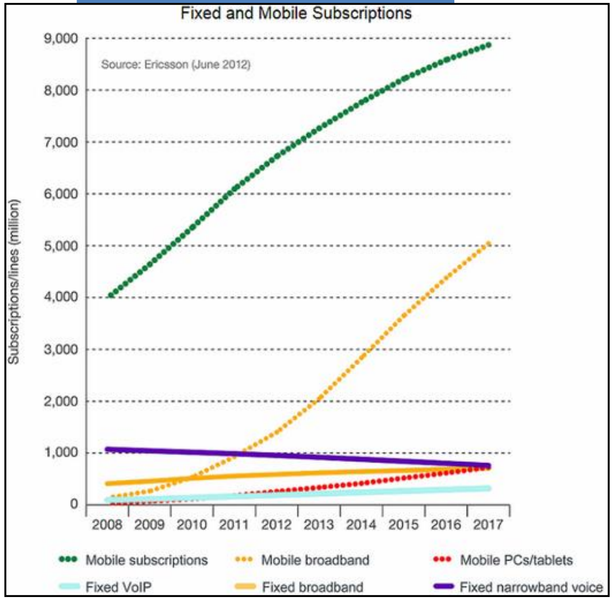
Mobile surpasses fixed

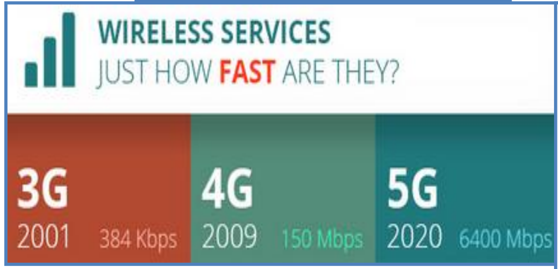
Mobile is faster

Internet is diversified.

~

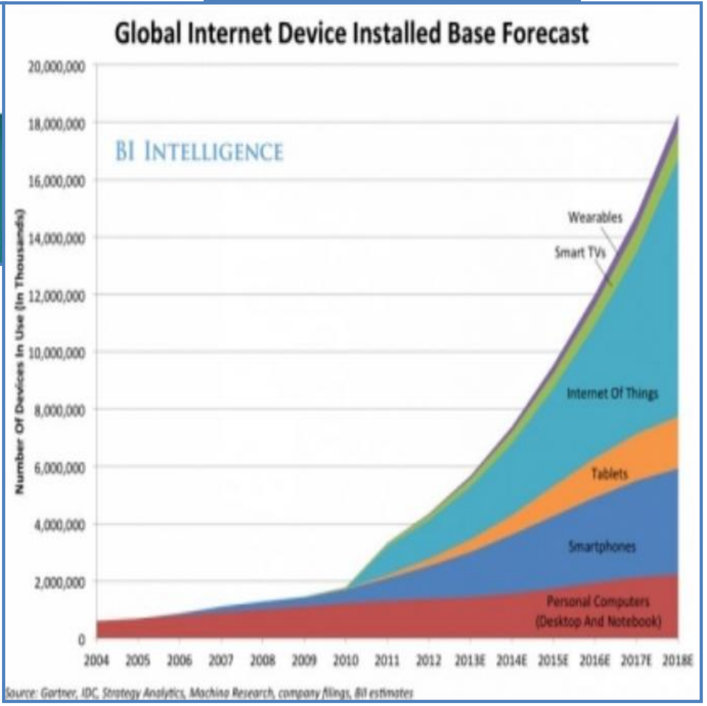
Security threats are diversified





WIRELESS SERVICES
JUST HOW FAST ARE THEY?

3G	4G	5G
2001 384 Kbps	2009 150 Mbps	2020 6400 Mbps

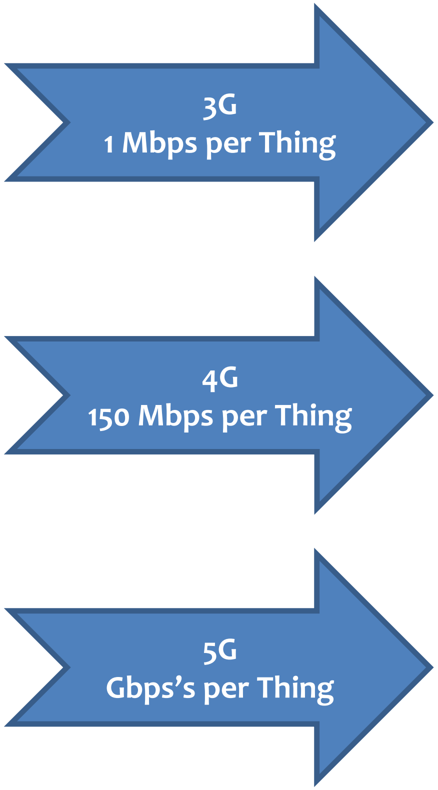


Source: Gartner, IDC, Strategy Analytics, Machina Research, company filings, BI estimates

Mobile based DDoS

+

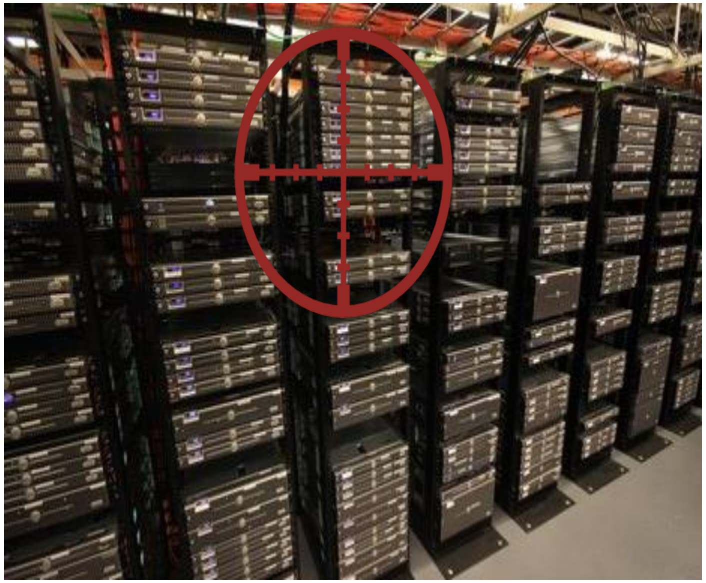
Things (Trillions of)



3G
1 Mbps per Thing

4G
150 Mbps per Thing

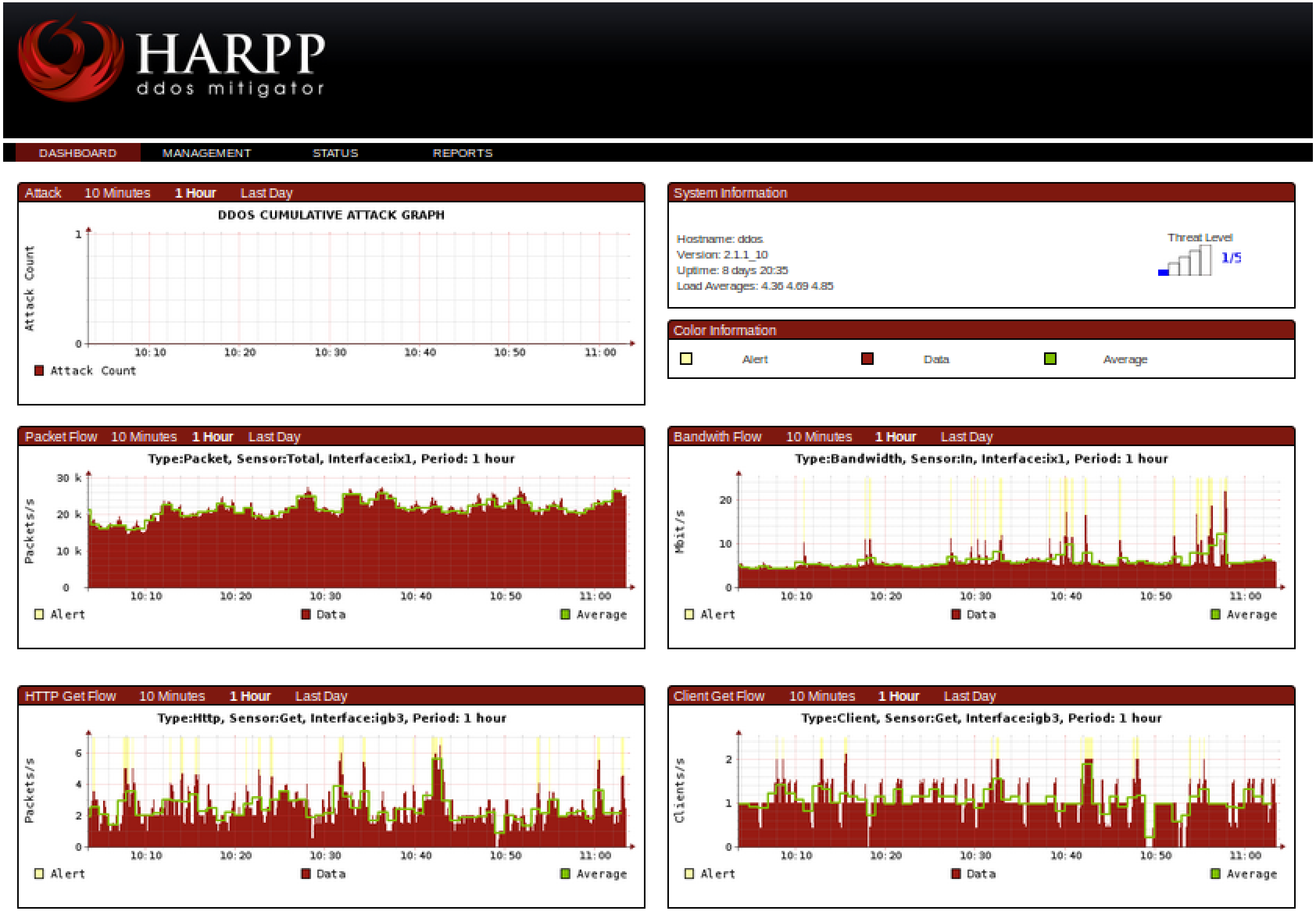
5G
Gbps's per Thing



HARPP
ddos mitigator

HARPP

HARPP’s Dashboard



System Information

Hostname: ddos
Version: 2.1.1_10
Uptime: 8 days 20:35
Load Averages: 4.36 4.69 4.85

Threat Level 1/5

Color Information

☐ Alert 🟥 Data 🟩 Average

DDOS CERT

Our Computer Emergency Response Team is ready when you need help!

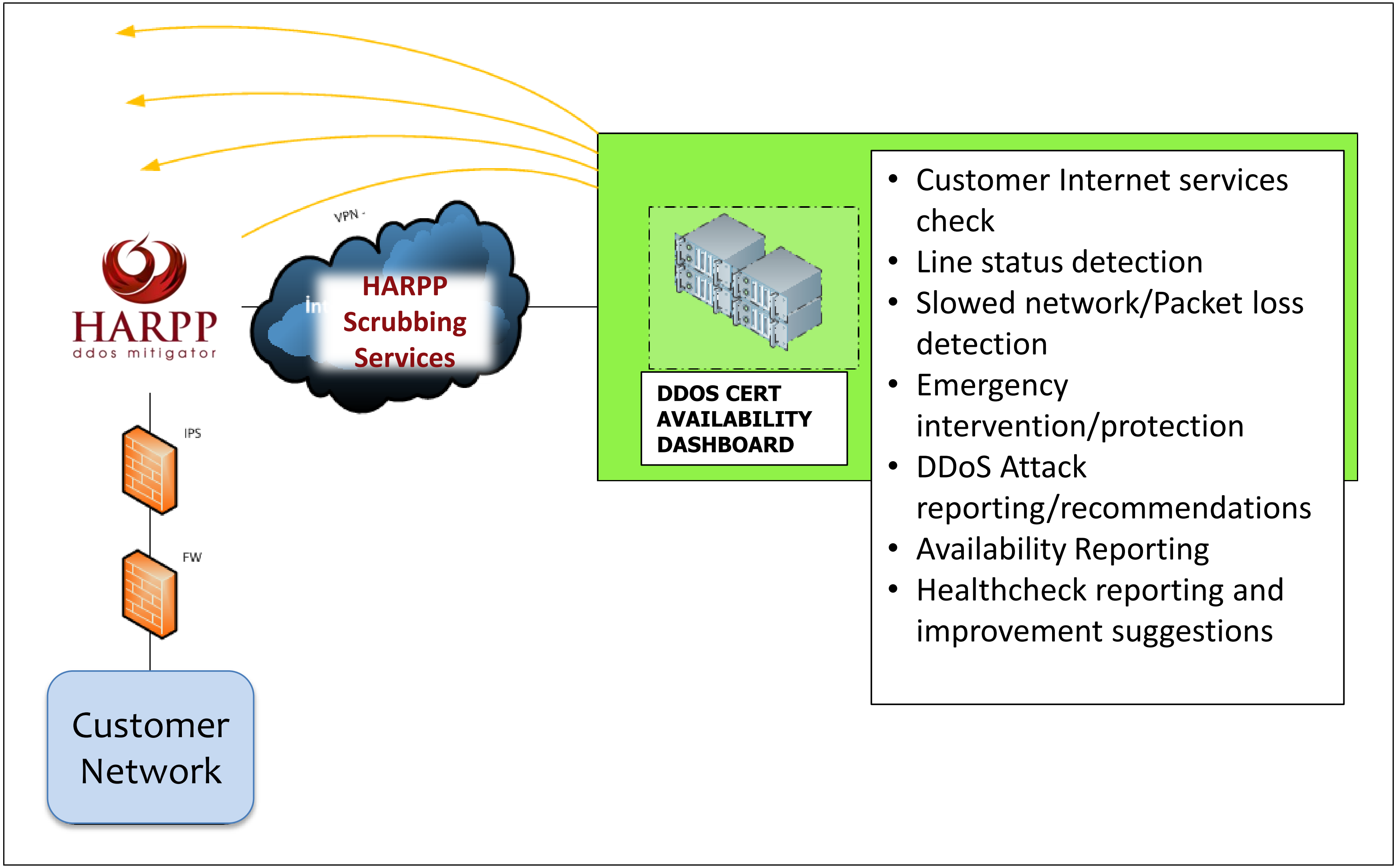
DDOS CERT

Computer Emergency Response Team

7-24-365

GLOBAL SUPPORT

HARPP DDOS CERT

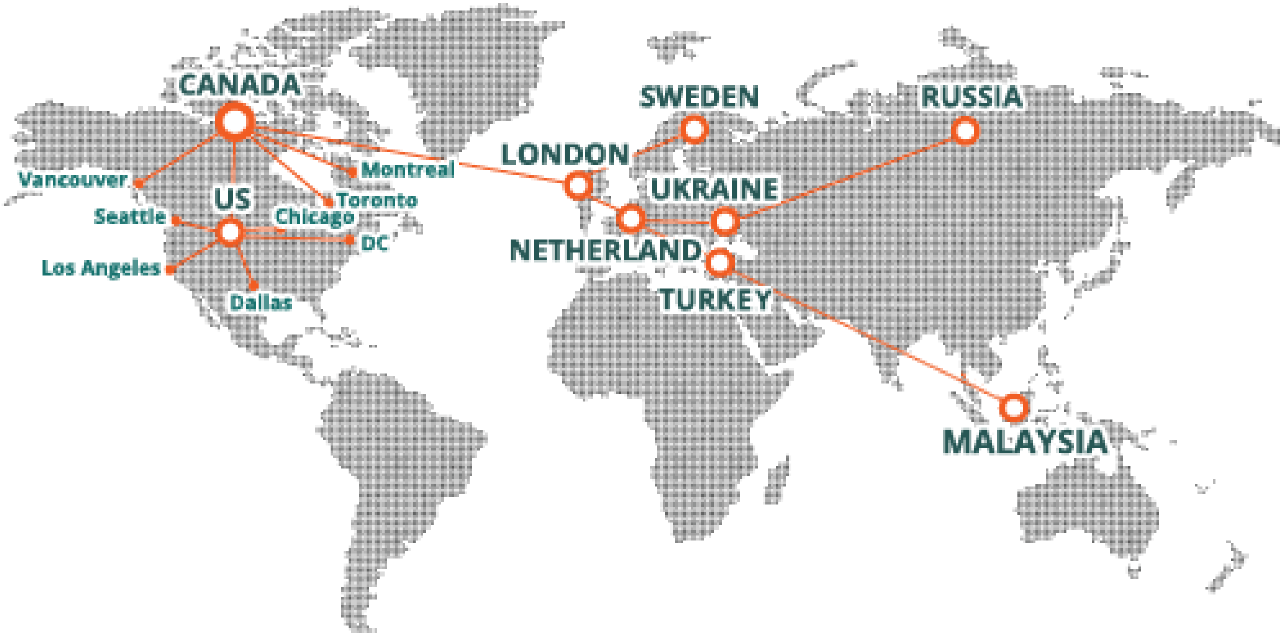


- Customer Internet services check
- Line status detection
- Slowed network/Packet loss detection
- Emergency intervention/protection
- DDoS Attack reporting/recommendations
- Availability Reporting
- Healthcheck reporting and improvement suggestions

HARPP Scrubbing Services

HARPP Scrubbing Services

- Standard*
- Premium**



* Standard Scrubbing services provide up to 1-5-10 Gbit of volumetric attack protection

** Premium Scrubbing Services provide Up to 500 Gbit of volumetric attack protection

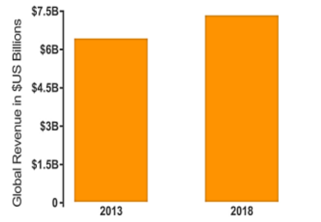
Security (Growth & Threats)

WORLDWIDE SECURITY MARKET GROWTH

- The worldwide security technology and services market is forecast to reach **$67.2** billion in 2013, **up 8.7** percent **from $61.8** billion in 2012.
- **The market is expected to grow to more than $86 billion in 2016.** (Gartner, Inc.)

NETWORK SECURITY MARKET GROWTH

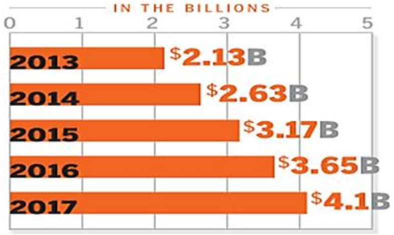
The network security appliance and software market is expected to reach $7.3 billion by 2018



© Infonetics Research, *Network Security Appliances and Software Quarterly Market Share, Size, and Forecasts*, March 2014

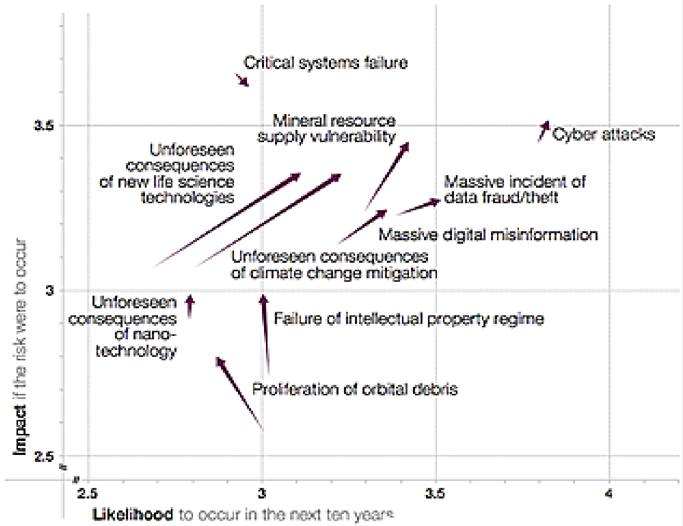
CLOUD-BASED SECURITY MARKET GROWTH

The cloud-based security services market is rising

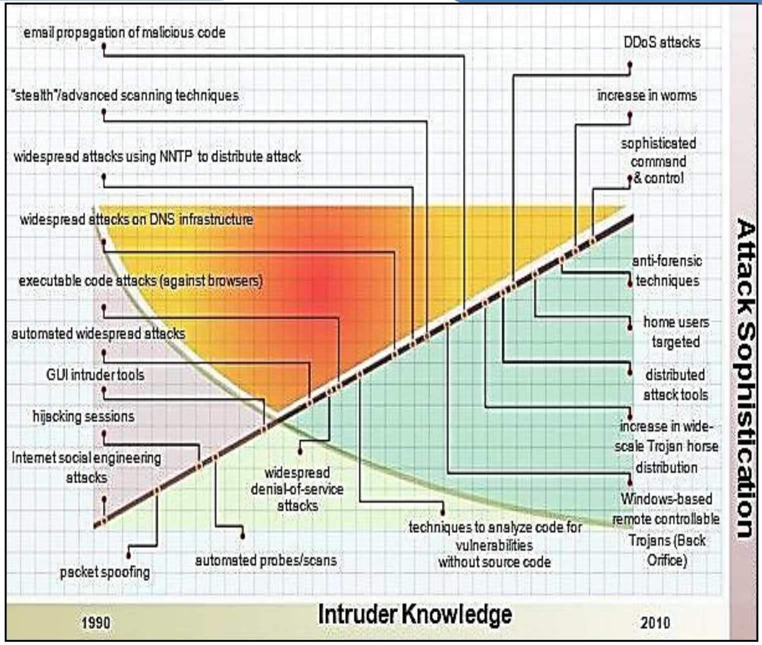


SOURCE: GARTNER

Technological



Source: World Economic Forum



email propagation of malicious code
"stealth"/advanced scanning techniques
widespread attacks using NNTP to distribute attack
widespread attacks on DNS infrastructure
executable code attacks (against browsers)
automated widespread attacks
GUI intruder tools
hijacking sessions
Internet social engineering attacks
packet spoofing
automated probes/scans
widespread denial-of-service attacks
techniques to analyze code for vulnerabilities without source code
DDoS attacks
increase in worms
sophisticated command & control
anti-forensic techniques
home users targeted
distributed attack tools
increase in wide-scale Trojan horse distribution
Windows-based remote controllable Trojans (Back Orifice)
Attack Sophistication
Intruder Knowledge
1990
2010

Thank you

For your further questions:
oguz at labrisnetworks.com

Labris NETWORKS

HARPP ddos mitigator

Get in touch..

Labris Networks Headquarters
T: +90 312 210 1491
info@labrisnetworks.com

Labris Networks International Markets office
Levent İstanbul

Labris Networks CWL İstanbul
Yıldız Teknik Üniversitesi

Eastern Europe Sales Offices – Prague&Warsaw
T: +420 220 994 422, ee-sales@labrisnetworks.com

UK Sales Office
T: +44 7703 503242, eu-sales@labrisnetworks.com

HARPP
ddos mitigator

This document is provided as a convenient comparis
The datasheet for any product or service can be foun
consulted for the most updated specifications.