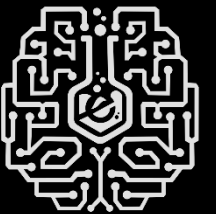




So you think IoT DDoS botnets are dangerous Bypassing ISP and Enterprise Anti-DDoS with 90's technology

Dennis Rand

<https://www.ecrimelabs.com>



eCrimeLabs

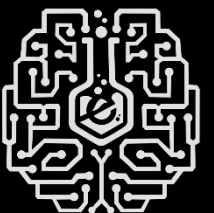
About me

I'm a security researcher and founder of eCrimeLabs, based out of Denmark.

With more than 20 years of experience in offensive and defensive security.

Started in **offense** worked with vulnerability research and exploitation and have moved to **defense** in form of incident response and threat hunting, but still like to mix it up.

In "spare-time" I like to see the world through a camera lens, yes I'm a canon person.



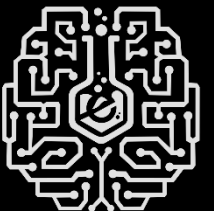
eCrimeLabs

Disclaimer

This talk is **not** a guide how to perform a DDoS attack, or recommendation to do so.

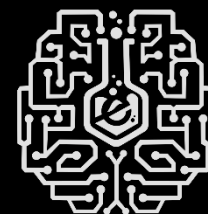
The goal is to give you **insight** into current threats.

This presentation will contain **no** cats.



Overview

- Background on project, why I started this
- Protocol history
- Anti-DDoS solutions implementations
- Legacy protocols VS "super" modern IoT botnets.
- Protocols – New and old
- Taking down the world – Max Pain



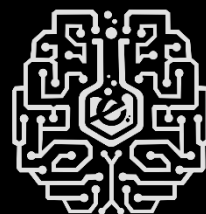
Motivation and thesis



While working at large telco SOC in Denmark, doing DDoS mitigation I was wondering why a majority of the attacks were trivial and easily mitigated.

And I wanted to see if I could figure out why 90% of the attacks occurred primarily out of China and Russia.

This was where I came to think of the “Max Pain Attack” thesis



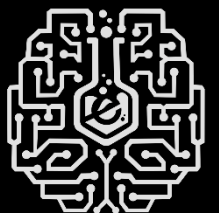
Initial idea and data gathering



During my research my dataset have been focused on UDP services

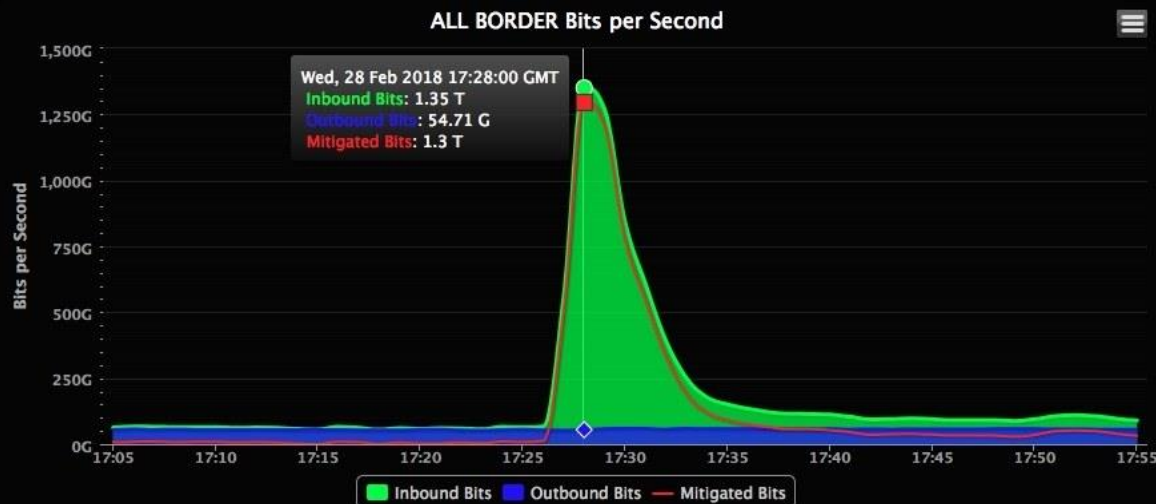
I started my research in the beginning of 2016 and are currently covering 20 services and 21 attack patterns.

I've proven it with UDP but the content of the problem (Max Pain) can easily adopt additional services and botnets.



Protocol history

First publicly found example of misuse is DNS dated back to **1999** and the latest addition to the abused UDP protocols are "Memcached" breaking the record on UDP amplification up to **51.200** times.



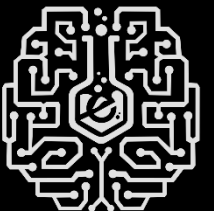
```
List: bugtraq
Subject: Possible Denial Of Service using DNS
From: smaster \(\) sail ! it
Date: 1999-07-30 22:00:10
[Download message_RAW]
```

SPJ-002-000:

```
.....+[ s0ftpr0ject 99 ]+.....
:::[ Digital Security for Y2K ]+:::
:::.....
:::'.g#$$"$$#. .g#$$"$$#. $#. `::
:: $$$$ $$$$ $$$$ $$$$ $$$$ ::
:: $$$$ $$$$ $$$$ $$$$ $$$$ ::
:: `$$$$$$$$$n $$$$ $$$$ $$$$ ::
:: $$$$ $$$$ $$$$ $$$$ $$$$ ::
:: `$$$$$$$$$' `$$$ $$$$ ::
:: $$$$ $$$$ $$$$ $$$$ $$$$ ::
:: `$$$$$$$$$' `$$$ $$$$ ::
:::.....
:::+[ Security Advisory, 002-000 ]+:::
`.....+[ July 19, 1999 ]+.....'
```

Possible Denial Of Service using DNS

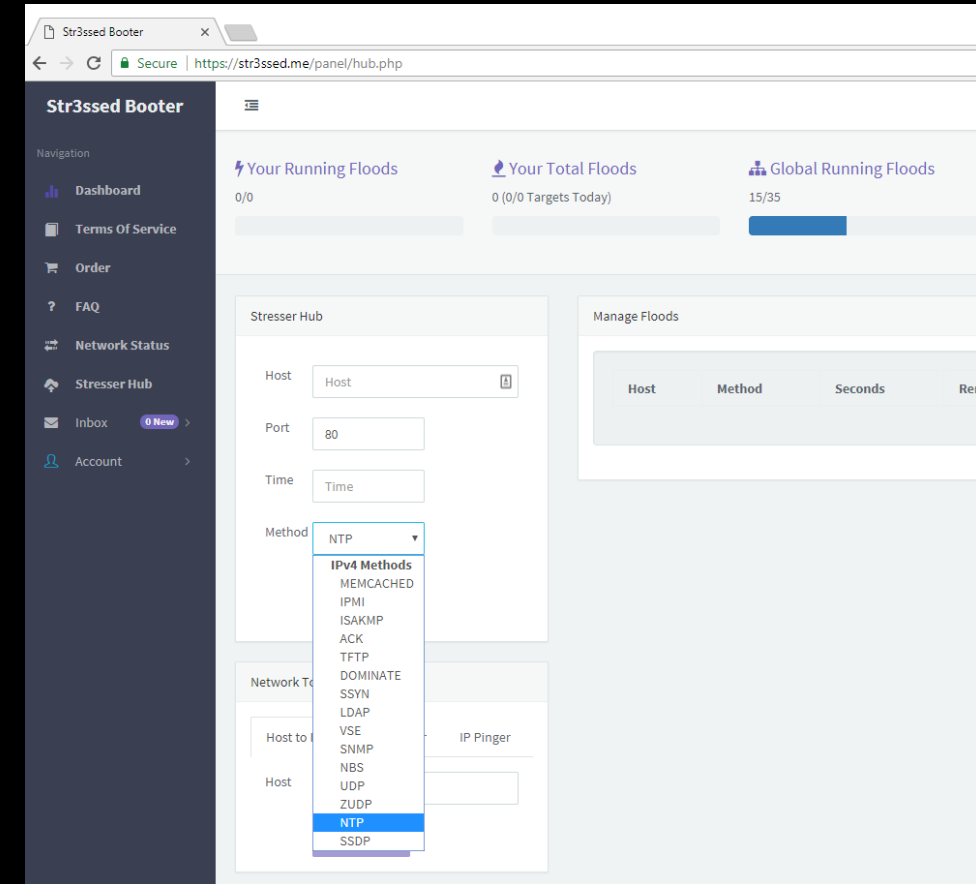
by |scacco| <scacco@s0ftpj.org>



Booters and Stressers

Booters or Stressers are all over the place and do perform "effective" attacks, but they do their business on a "DDoS Harder and not Smarter"

Also even stressers uses Cloudflare



Checking your browser before accessing boot4free.com.

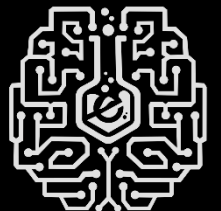
This process is automatic. Your browser will redirect to your requested content shortly.
Please allow up to 5 seconds...

[DDoS protection by Cloudflare](#)
Ray ID: 41eeef7937083d5b

Boot4free.com

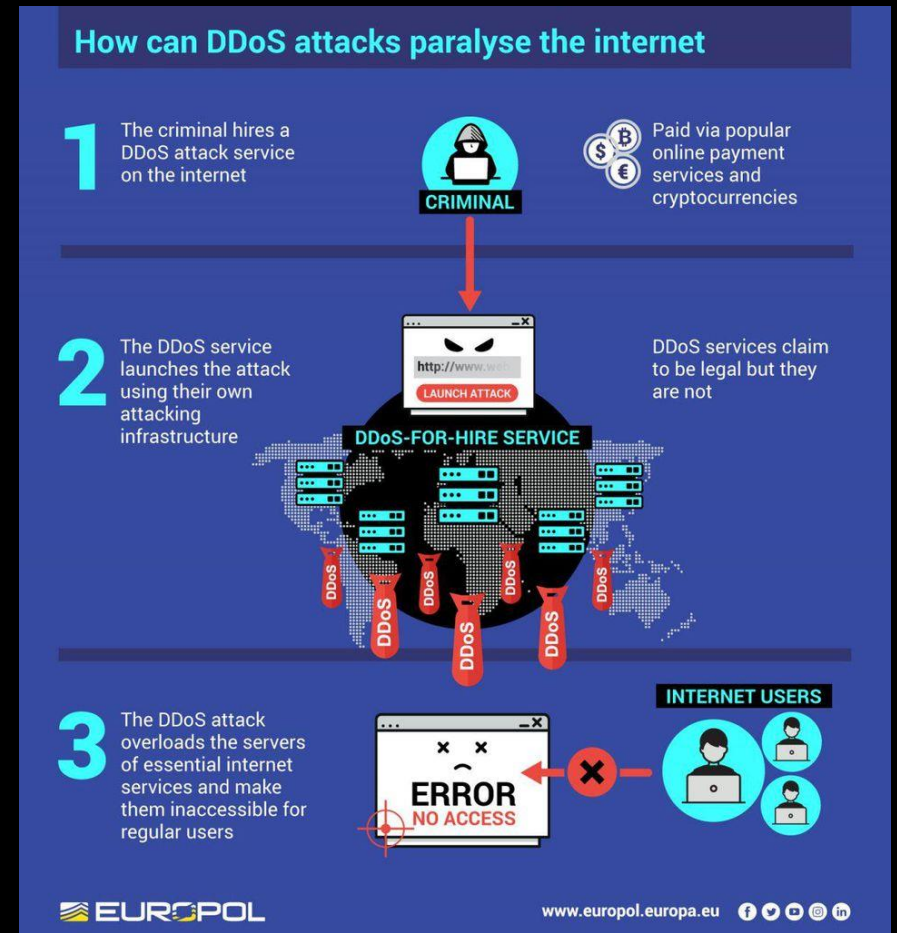
Simple 30 seconds attack, just spread out over the world with a "Chargen" attack

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
46.16.187.186	33,117	24 M	33,117	24 M	0	0	Netherlands	Amsterdam	36351	SoftLayer Technologies Inc.
42.117.7.46	24,164	16 M	24,164	16 M	0	0	Vietnam	Hanoi	18403	The Corporation for Financing & Promoting Technology
110.153.9.243	14,093	11 M	14,093	11 M	0	0	China	Ürümqi	4134	No.31,Jin-rong Street
195.38.32.100	11,583	6340 k	11,583	6340 k	0	0	Russia	Yekaterinburg	12389	Rostelecom
167.157.46.7	7,990	6103 k	7,990	6103 k	0	0	Bolivia	Cochabamba	6568	Entel S.A. - EntelNet
88.198.215.250	6,398	4608 k	6,398	4608 k	0	0	Germany	—	24940	Hetzner Online GmbH
50.245.83.125	6,736	4091 k	6,736	4091 k	0	0	United States	Gadsden	7922	Comcast Cable Communications, LLC
119.160.128.92	7,441	3762 k	7,441	3762 k	0	0	Brunei	Bandar Seri Begawan	10094	Telekom Brunei Berhad
46.50.171.23	8,864	3677 k	8,864	3677 k	0	0	Russia	Novosibirsk	21127	JSC Zap-Sib TransTeleCom, Novosibirsk
120.35.5.43	5,907	3235 k	5,907	3235 k	0	0	China	Fuzhou	4134	No.31,Jin-rong Street
121.188.89.226	3,061	2292 k	3,061	2292 k	0	0	Republic of Korea	—	4766	Korea Telecom
119.204.66.20	2,769	2175 k	2,769	2175 k	0	0	Republic of Korea	Daejeon	4766	Korea Telecom
216.228.85.32	5,562	2024 k	5,562	2024 k	0	0	United States	Huntsville	14793	API Digital Communications Group, LLC
42.121.119.176	3,231	1689 k	3,231	1689 k	0	0	China	Hangzhou	37963	Hangzhou Alibaba Advertising Co.,Ltd.
197.232.2.83	2,323	1223 k	2,323	1223 k	0	0	Kenya	Nairobi	36866	JTL
121.199.61.204	1,404	972 k	1,404	972 k	0	0	China	Hangzhou	37963	Hangzhou Alibaba Advertising Co.,Ltd.
121.40.122.86	509	336 k	509	336 k	0	0	China	Hangzhou	37963	Hangzhou Alibaba Advertising Co.,Ltd.
198.46.125.101	793	276 k	793	276 k	0	0	United States	—	6128	Cablevision Systems Corp.
109.81.193.74	202	215 k	202	215 k	0	0	Czechia	Prague	5610	O2 Czech Republic, a.s.
82.127.254.113	284	87 k	284	87 k	0	0	France	—	3215	Orange
50.126.225.70	92	70 k	92	70 k	0	0	United States	Willard	5650	Frontier Communications of America, Inc.
68.195.201.30	75	52 k	75	52 k	0	0	United States	Elmwood Park	6128	Cablevision Systems Corp.



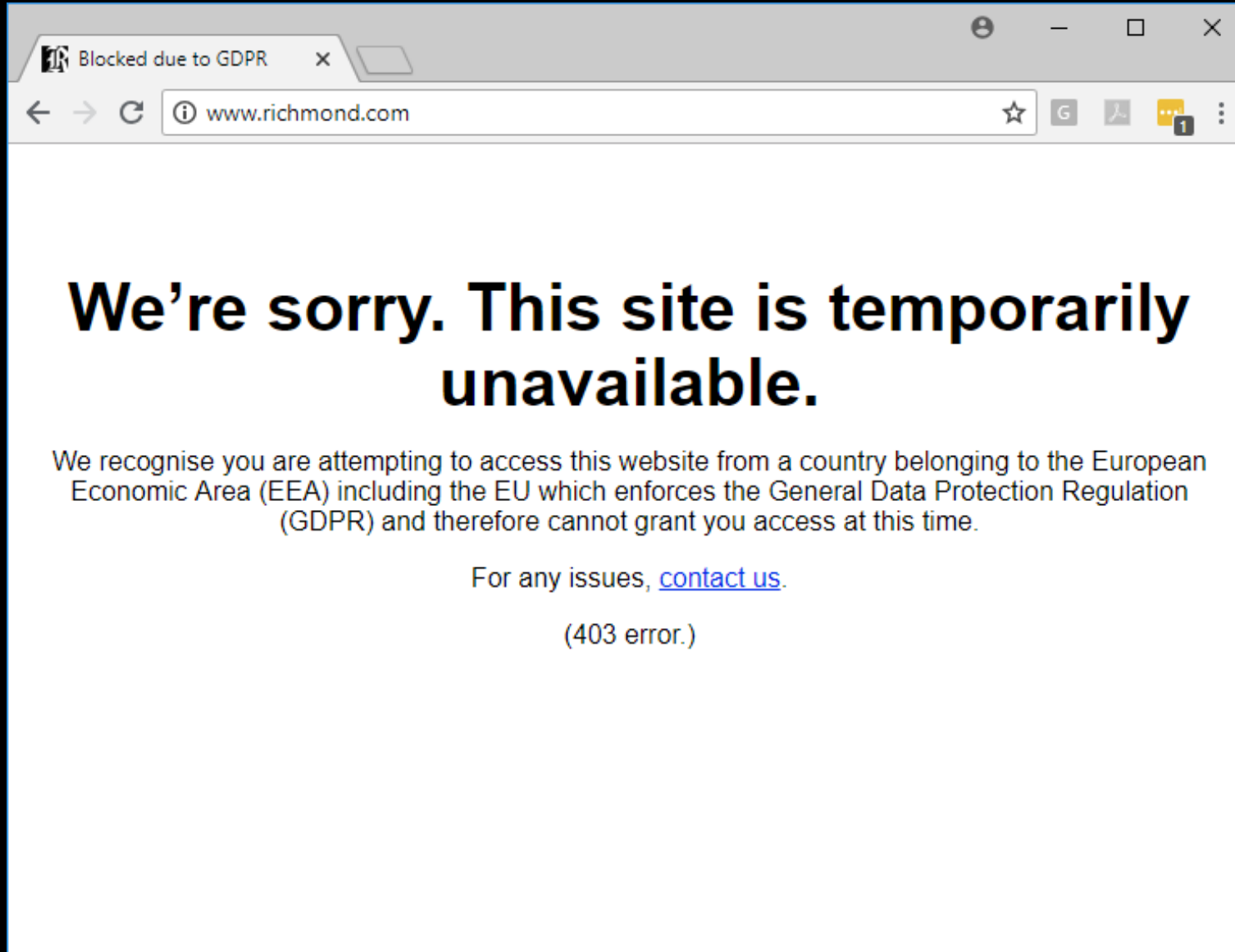
BUT Takedowns do happen

The screenshot shows the top navigation bar of the Europol website with links for 'ABOUT EUROPOL', 'ACTIVITIES & SERVICES', 'CRIME AREAS & TRENDS', 'PARTNERS & AGREEMENTS', and 'CAR PRO'. Below the navigation is a breadcrumb trail: 'HOME > NEWSROOM > WORLD'S BIGGEST MARKETPLACE SELLING INTERNET PARALYSING DDOS ATTACKS TAKEN DOWN'. The main headline reads 'WORLD'S BIGGEST MARKETPLACE SELLING INTERNET PARALYSING DDOS ATTACKS TAKEN DOWN'. The article is dated '25 April 2018' and is a 'Press Release'. It features social media sharing icons for print, Facebook, Messenger, Twitter, LinkedIn, and WhatsApp. The first paragraph states: 'Webstresser.org sold Distributed Denial of Service attacks that could knock the internet offline for as little as EUR 15.00 a month'. The rest of the article text is partially visible, mentioning the arrest of administrators on 24 April 2018.



Source: <https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down>

And sometimes DDoS is not required



The image shows a web browser window with a single tab titled "Blocked due to GDPR". The address bar displays "www.richmond.com". The main content area features a large, bold heading: "We're sorry. This site is temporarily unavailable." Below this, a paragraph explains: "We recognise you are attempting to access this website from a country belonging to the European Economic Area (EEA) including the EU which enforces the General Data Protection Regulation (GDPR) and therefore cannot grant you access at this time." A link labeled "contact us" is provided for further assistance. At the bottom, it notes "(403 error.)".

We're sorry. This site is temporarily unavailable.

We recognise you are attempting to access this website from a country belonging to the European Economic Area (EEA) including the EU which enforces the General Data Protection Regulation (GDPR) and therefore cannot grant you access at this time.

For any issues, [contact us](#).

(403 error.)

UDP Protocols

There has been an average of **19.000.000+** potential vulnerable services exposed every month measured over the last 5 months.

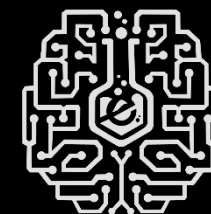
Attack protocol	Request byte size	Average / Maximum Amplification factor		Attacker controlled (amp factor)	Numbers (May 2018)
CHARGEN(UDP/19)	1 byte	261	6958	NO	12.942
DNS(UDP/53)	37 bytes	14	110	YES	656.138
SSDP/UPNP(UDP/1900)	94 bytes	34	999	NO*	5.786.313
Portmap(UDP/111)	40 bytes	4	249	NO	1.802.163
SIP(UDP/5060)	128 bytes	3	19	NO	1.549.374
TFTP(UDP/69)	10 bytes	3	99	YES	1.268.058
NetBIOS(UDP/137)	50 bytes	3	299	NO	601.869
MSSQL(UDP/1434)	1 byte	156	2449	NO	120.919
Steam(UDP/27015)	25 bytes	7	199	NO	32.807
NTP(UDP/123) - MONLIST	8 bytes	68	2449	YES	556.912
NTP(UDP/123) - READVAR	12 bytes	22	198	NO	3.927.654
SNMP(UDP/161)	40 bytes	34	553	NO	2.509.475

Attack protocol	Request byte size	Average / Maximum Amplification factor		Attacker controlled	Numbers (May 2018)
mDNS(UDP/5353)	46 bytes	5	44	NO	9580
QOTD(UDP/19)	2 bytes	69	591	NO	4071
ICABrowser(UDP/1604)	42 bytes	47	516	NO	2325
Sentinel(UDP/5093)	6 bytes	168	666	NO	1569
RIPv1(UDP/520)	24 bytes	11	309	NO	1364
Quake3(UDP/27960)	14 bytes	57	99	NO	569
CoAP(UDP/5683)	21 bytes	16	97	NO	279.588
LDAP(UDP/389)	52 bytes	53	99	NO	48.931
Memcached(UDP/11211)	15 bytes	73	100	YES	25.510

Data record in and out-bound are without UDP packet header, meaning **pure data**.

UPnP Port Forwarding

<https://www.imperva.com/blog/2018/05/new-ddos-attack-method-demands-a-fresh-approach-to-amplification-assault-mitigation/>



eCrimeLabs

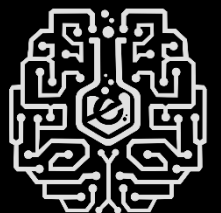
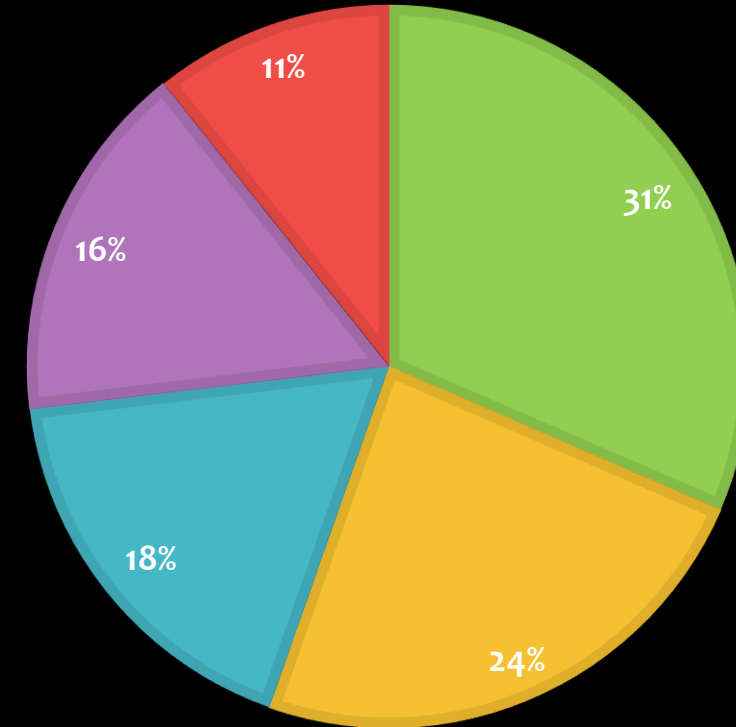
Protocol and country preferences

These are top countries and ASN's based on numbers.

Protocol attack	Country	AS Name	AS Number
NTP - Monlist (All)	Brazil	CLARO S.A.	AS28573
NTP - Monlist (Amp factor > 1000)	Korea	CJ Hello Co., Ltd.	AS17839
NTP - Readvar	US	Windstream Communications LLC	AS7029
Portmap - V2 DUMP Call	US	EGIHosting	AS18779
SNMP - v2c public - getBulkRequest	Brazil	CLARO S.A.	AS28573
TFTP - RRQ	US	Cox Communications Inc.	AS22773
DNS - Standard query ANY	US	Unified Layer	AS46606
SIP OPTIONS Request	Portugal	Servicos De Comunicacoes E Multimedia S.A.	AS3243
SSDP/UPNP - M-SEARCH * HTTP/1.1	China	No.31,Jin-rong Street	AS4134
Netbios - Name query NBSTAT *	US	Choopa, LLC	AS20473
MSSQL CLNT_BCASST_EX message	US	GoDaddy.com, LLC	AS26496
LDAP objectClass=* with 0 attributes	US	Comcast Cable Communications, LLC (Microsoft Corporation)	AS7922 (AS8075)
MEMCACHED STATS request	US	Micfo, LLC.	AS53889
STEAM A2S_INFO request	US	Choopa, LLC	AS20473
CoAP Resource Discovery - /.well-known/core	China	Guangdong Mobile Communication Co.Ltd.	AS9808
mdns - List all currently registered services	US	Level 3 Parent, LLC	AS3549
chargen - Single byte	Italy	Telecom Italia	AS3269
Citrix Requesting Published Applications list	US	AT&T Services, Inc.	AS7018
qotd - Single carriage return/newline	Korea	Korea Telecom	AS4766
sentinel license	US	SoftLayer Technologies Inc.	AS36351
rip - RIPv1 request	US	Comcast Cable Communications, LLC	AS7922
QUAKE3 getstatus	US	Choopa, LLC	AS20473

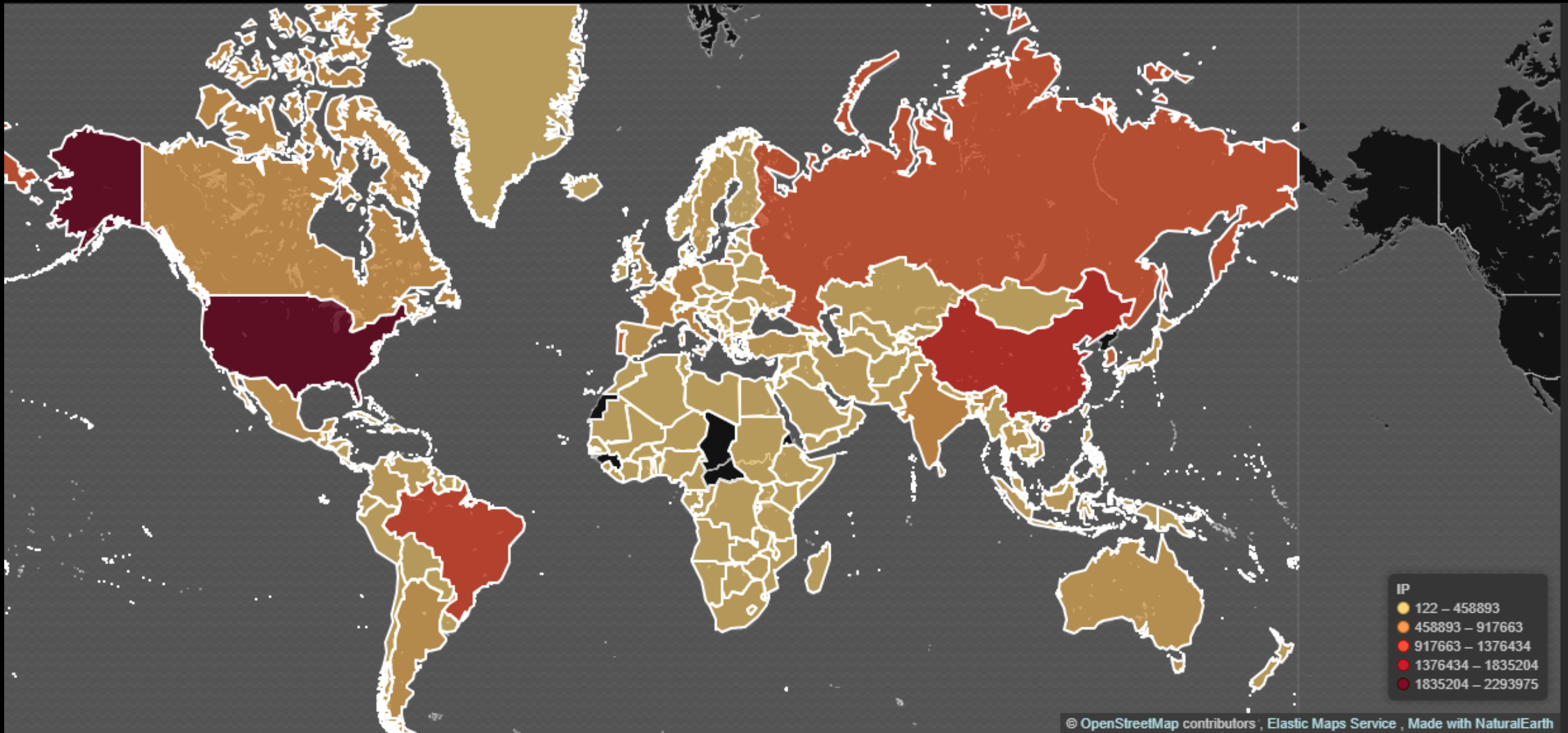
TOP 5 COUNTRIES

■ US ■ China ■ Russia ■ Brazil ■ Korea

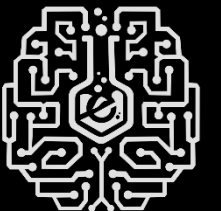


Global view

A global view of potential vulnerable UDP services



© OpenStreetMap contributors, Elastic Maps Service, Made with NaturalEarth



IoT attacks up ↗ UDP Volumetric down ↘

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

● Major cyber attack disrupts internet service across Europe and US



▲ Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

enisa European Union Agency for Network and Information Security

Home > Publications > Cyber security info notes > Major DDoS Attacks Involving IoT Devices

Navigation menu

TechRepublic SEARCH Digital Transformation Cloud Big Data AI IoT More

Major DDoS Attacks Involving IoT Devices

Published November 03, 2016
Type Suggested Reading

Introduction

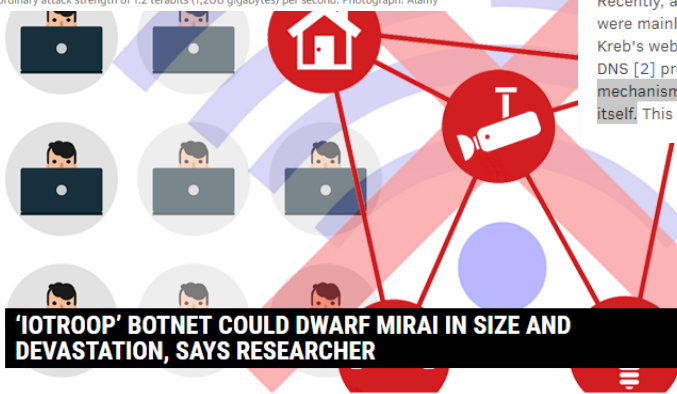
Recently, a series of massive (Distributed Denial-of-Service) DDoS [1] attacks have occurred. They were mainly propagated through compromised Internet of Things (IoT) devices and targeted Brian Krebs's website, "Krebs on Security", OVH, a known Web hosting provider, and "Dyn", a well-established DNS [2] provider. These massive attacks have highlighted the risks resulting from inadequate security mechanisms in Internet of Things (IoT) devices, together with their devastating effects on the Internet itself. This note provides an overview of these attacks through a series of suggested articles.

SECURITY

DDoS attacks increased 91% in 2017 thanks to IoT

In Q3 2017, organizations faced an average of 237 DDoS attack attempts per month. And with DDoS-for-hire services, criminals can now attack and attempt to take down a company for less than \$100.

By Alison DeNisco Rayome | November 20, 2017, 5:45 AM PST



'IOTROOP' BOTNET COULD DWARF MIRAI IN SIZE AND DEVASTATION, SAYS RESEARCHER

by Tom Spring

October 20, 2017, 2:17

ForbesBrandVoice® What is this?

FEB 4, 2018 @ 01:14 PM 888

DDoS Attacks Evolve To Conscript Devices Onto The IoT

CenturyLinkVoice
Your Link To What's Next FULL BIO

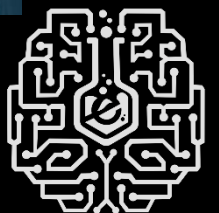
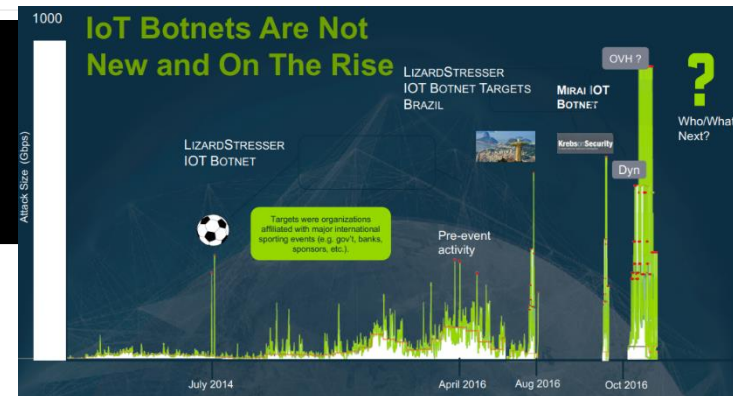
Russ Banham, CenturyLink

The number of cybersecurity attacks skyrocketed in frequency and increased in complexity as the internet of things (IoT) spread its wings in 2017.

Vendor Access Control

Affordable cyber security for enterprise environment. Control access to secrets.

Pleasant Solutions



eCrimeLabs

IoT attack history – And they are potent

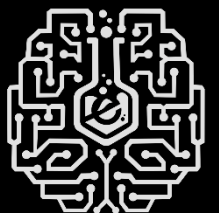
Around October 2016 the first alert on Mirai reached the surface attacking Brian Krebs' security blog (krebsonsecurity.com)

Breaking the public record of 620 Gbps with a 1Tbps attack,

Later in September 1.1 - 1.5Tbps against OVH



The screenshot shows the US-CERT website interface. At the top left is the Department of Homeland Security logo and the US-CERT logo (United States Computer Emergency Readiness Team). A search bar is on the top right. Below the header is a navigation menu with links for HOME, ABOUT US, CAREERS, PUBLICATIONS, ALERTS AND TIPS, RELATED RESOURCES, and C' VP. The main content area features an alert titled "Alert (TA16-288A) Heightened DDoS Threat Posed by Mirai and Other Botnets" with a "More Alerts" link. Below the title, it states "Original release date: October 14, 2016 | Last revised: October 17, 2017" and includes social sharing buttons for Print, Tweet, Send, and Share. The "Systems Affected" section lists "Internet of Things (IoT)—an emerging network of devices (e.g., printers, routers, video cameras, smart TVs) that connect to one another via the Internet, often automatically sending and receiving data". The "Overview" section begins with "Recently, IoT devices have been used to create large-scale botnets—networks of devices infected with self-propagating malware—that can execute crippling distributed denial-of-service (DDoS) attacks. IoT devices are particularly susceptible to malware, so protecting these devices and connected hardware is critical to protect systems and networks."



Botnets vs Legit services pros and cons

Seen from an **attackers** perspective

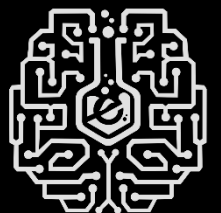


Legit UDP services abused

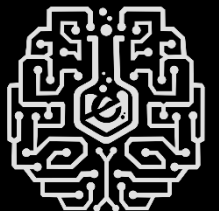
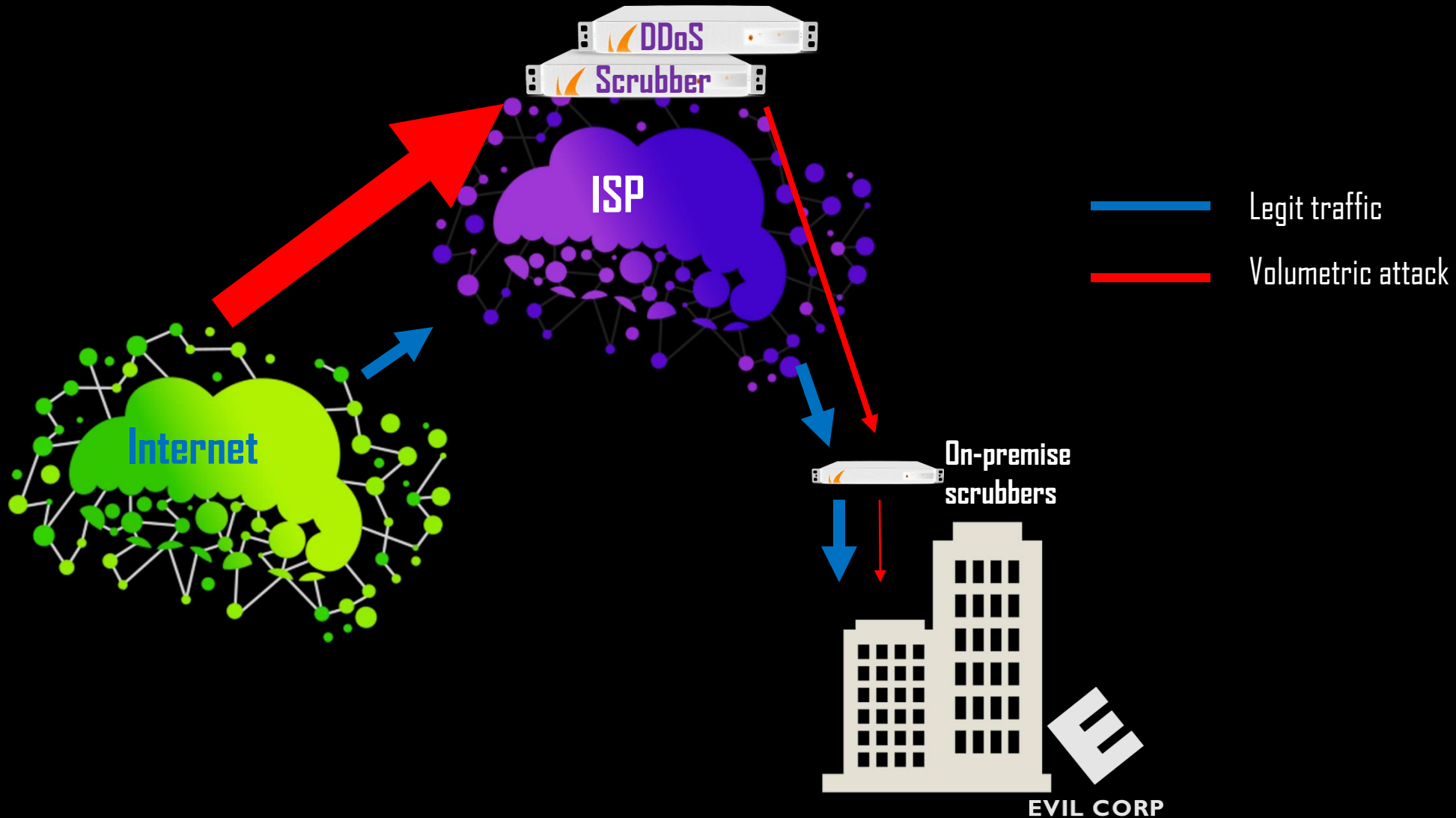
Legit	Pros	Cons
Bigger chance for these services NOT to be shut down	😊	
Many have uptime SLA's	😊	
You don't get real-time insight if services are up		😡
Media attention usually only result in minor effect	😊	
LE and bluetteams can in some cases contact service owner (server based services)		😡
Locating the origin of attack can be more or less impossible.	😊	

Infected devices (Endpoint/IoT)

Legit	Pros	Cons
Bigger chance for these services to be shut down		😡
Media attention results in massive attention and workforces.		😡
You usually have real-time insight if services are up	😊	
LE and Bluetteams usually have harder time contacting owner of device.	😊	
By analyzing botnet infected devices you can get knowledge of infrastructure		😡

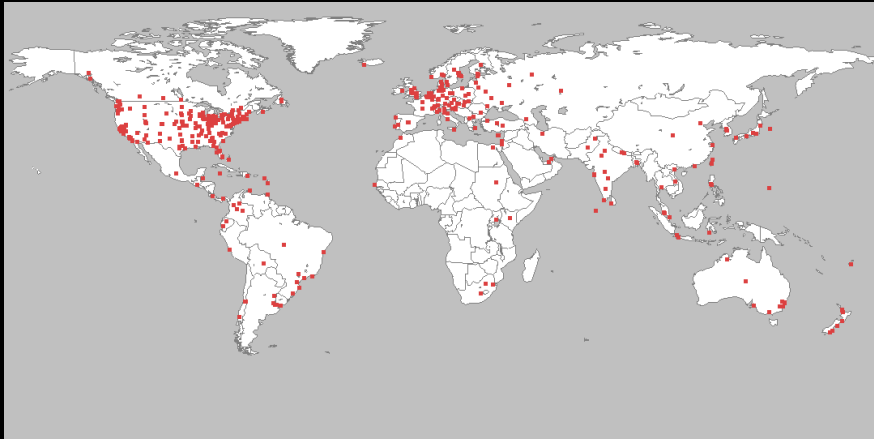


Anti-DDoS infrastructure implementation

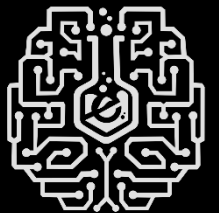
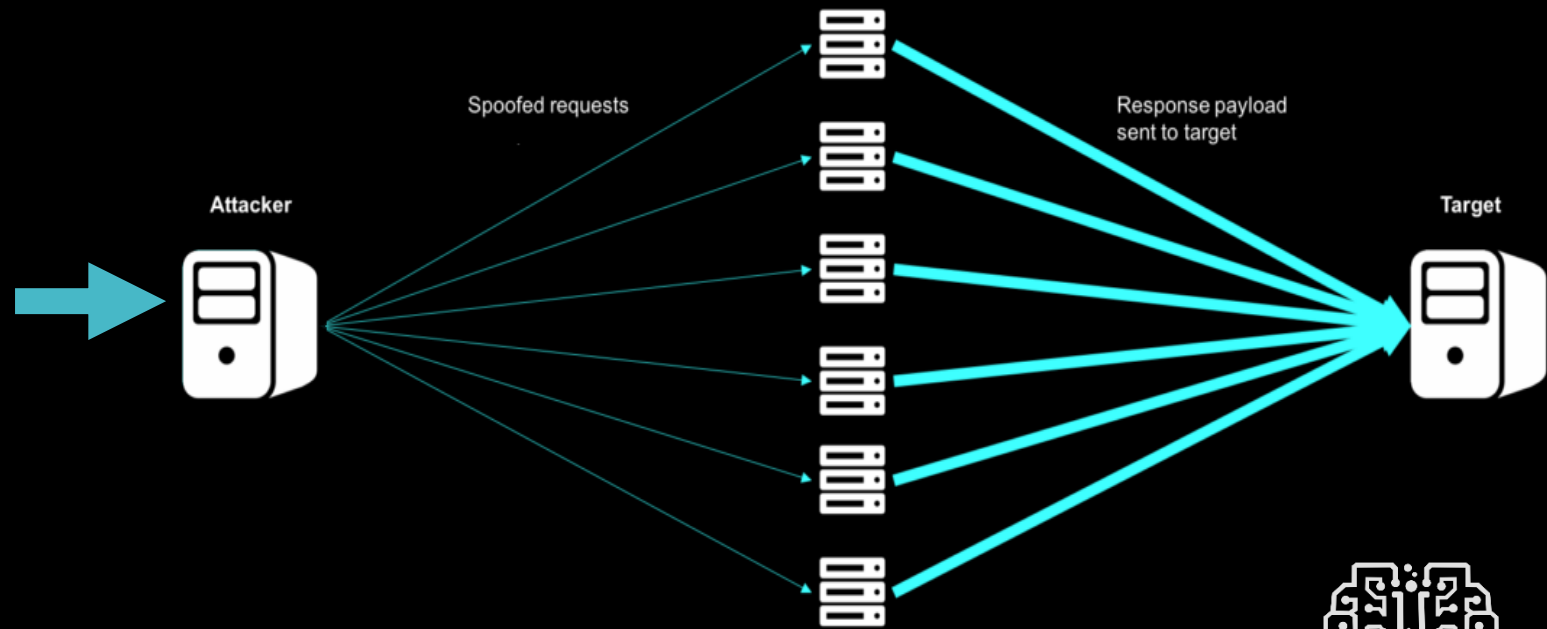


Why is UDP amplification attacks even possible

Lack of BCP38 implementation, allows IP source spoofing



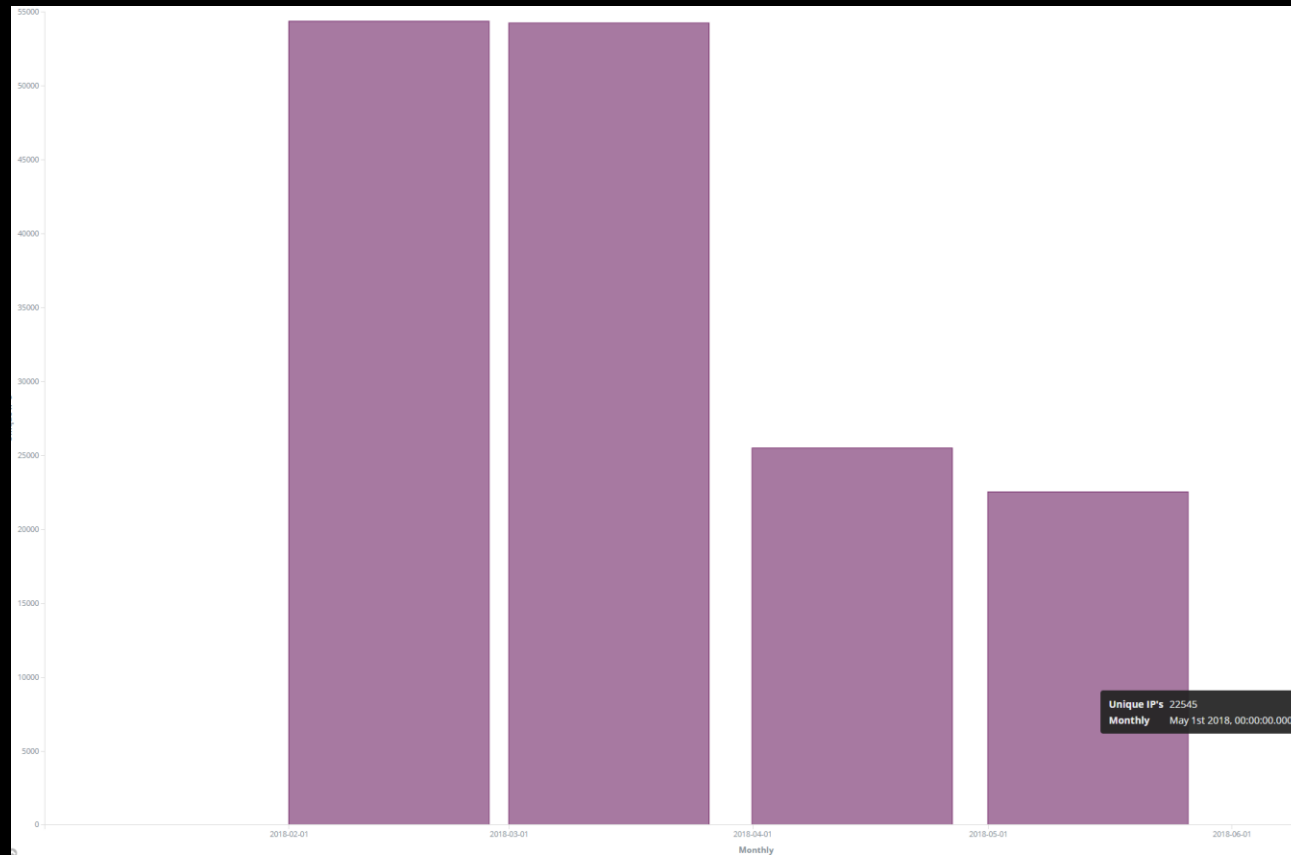
Source CAIDA (Center for Applied Internet Data Analysis)
<https://www.caida.org/projects/spoofers/>



Memcached

An example of - If it poses a high enough risk we do learn At least for a while. **22545** potential Memcached services still exposed.

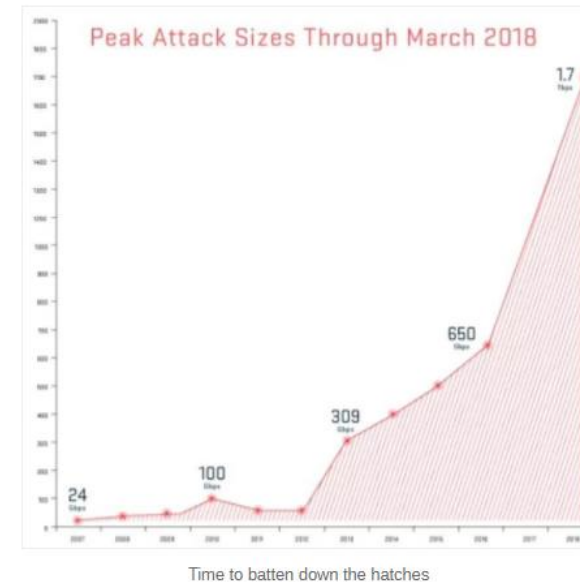
Attack protocol	Request byte size	Average / Maximum Amplification factor		Attacker controlled
Memcached(UDP/11211)	15 bytes	73	100 51.200	YES



Memcached DDoS: The biggest, baddest denial of service attacker yet
Distributed denial of service attacks just got turned up to 11 with Memcrashed, an internet assault that can slam a website with over a terabyte of bad traffic.

working | March 1, 2018 -- 23:38 GMT (23:38 GMT) | Topic: Security

Harbor Networks is now reporting that a US service provider suffered a 1.7Tbps attack earlier this month. In this case, there were no outages as the provider had taken adequate safeguards, but it's clear that the memcached attack is going to be a feature network managers are going to have to take seriously in the future.

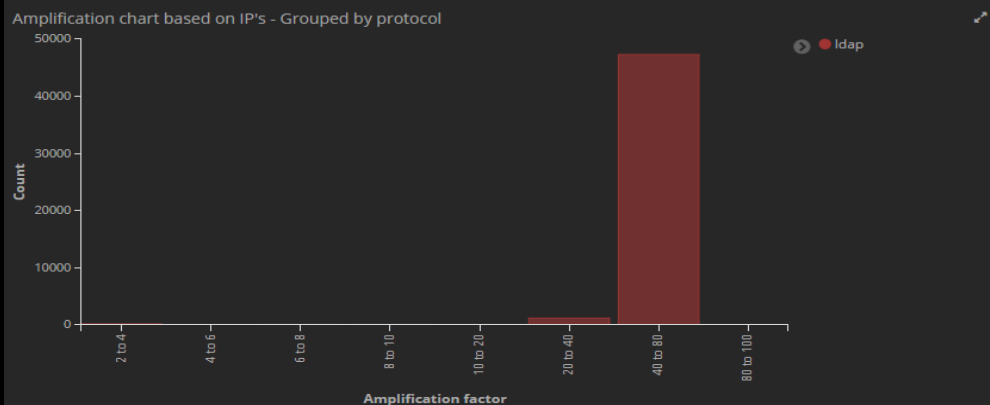
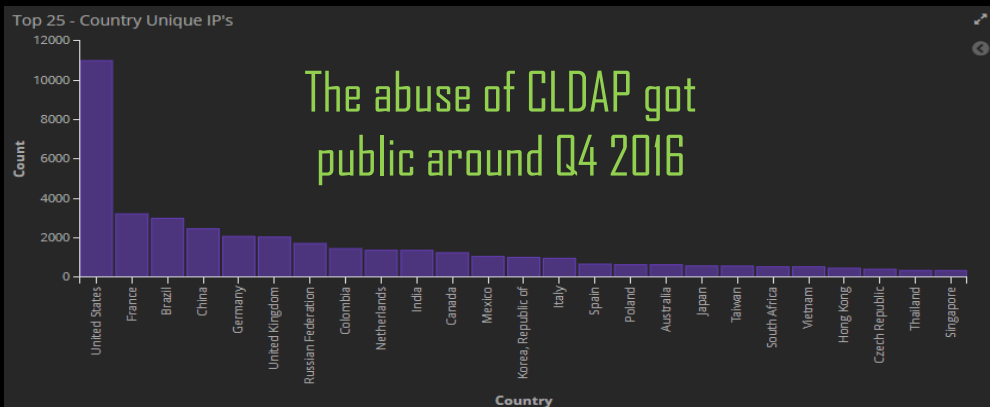




Example of the lacking pre-analysis

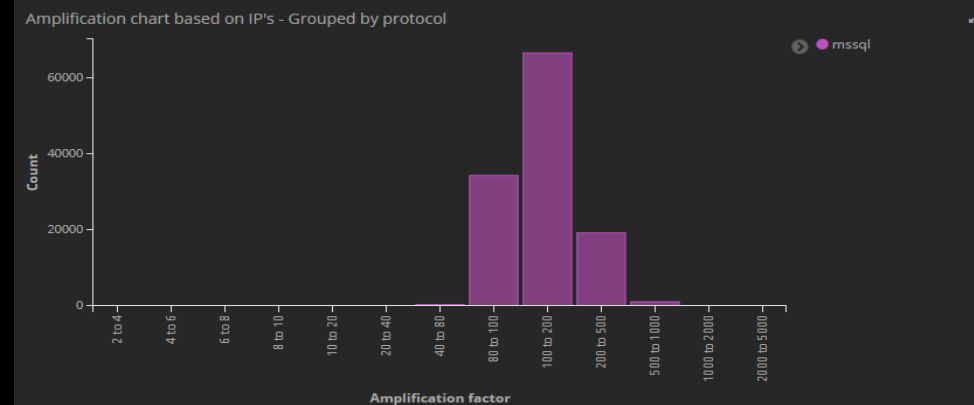
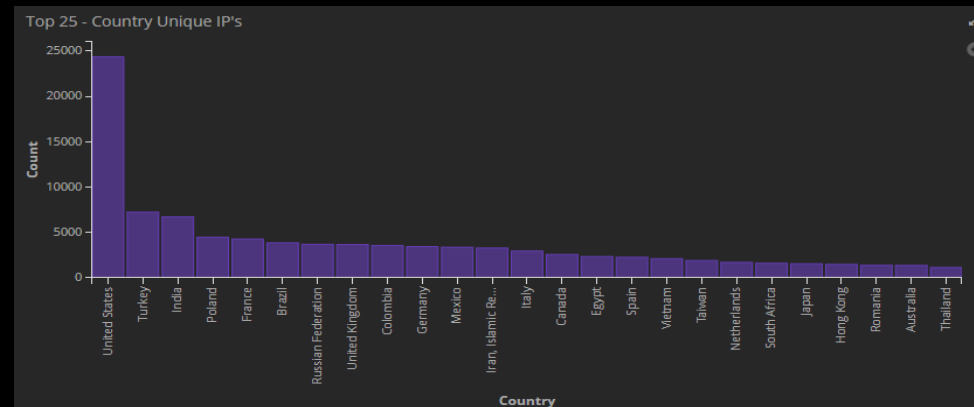
LDAP (52 bytes)

MSSQL (1 bytes)



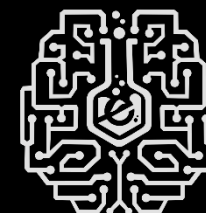
Unique vulnerable IP's and Services

Unique Vulnerable services
48931



Unique vulnerable IP's and Services

Unique Vulnerable services
120919



CoAP - <http://coap.technology/>



"The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things."

"The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation."

Why would you do this to me?



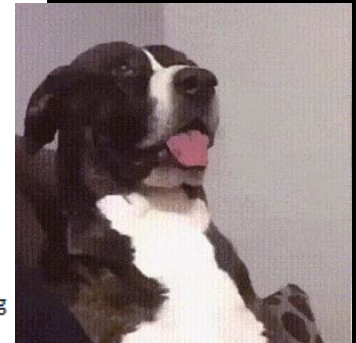
RFC 7252 - The Constrained Application Protocol (CoAP)

Secure | <https://tools.ietf.org/html/rfc7252>

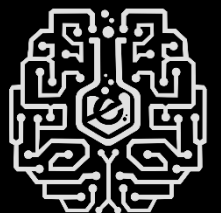
Finally, a proxy that fans out Separate Responses (as opposed to piggybacked Responses) to multiple original requesters may provide additional amplification (see [Section 11.3](#)).

11.3. Risk of Amplification

CoAP servers generally reply to a request packet with a response packet. This response packet may be significantly larger than the request packet. An attacker might use CoAP nodes to turn a small attack packet into a larger attack packet, an approach known as amplification. There is therefore a danger that CoAP nodes could become implicated in denial-of-service (DoS) attacks by using the amplifying properties of the protocol: an attacker that is attempting to overload a victim but is limited in the amount of traffic it can generate can use amplification to generate a larger amount of traffic.



Why are we **designing** UDP protocols in **2014** that we know will give us issues in the future ?



CoAP – IoT protocol

Attack protocol	Request byte size	Average / Maximum Amplification factor		Attacker controlled
CoAP(UDP/5683)	21 bytes	16	97	NO

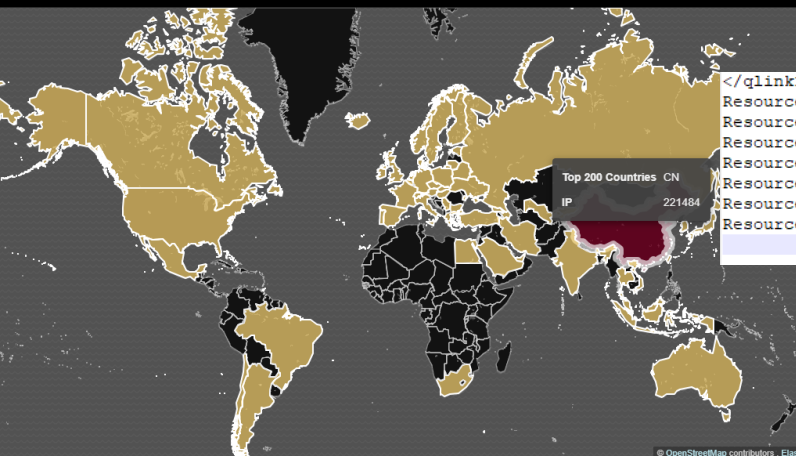
This is a protocol that are slowly gaining some momentum

Between November and December 2017 the number jumped from **6.500** IP's to **26.000**

May 2018 global numbers stated **220.000+**

The major jump is based out of three Mobile networks in China where CoAP implementation has become popular

AS Name ↕	AS Number ↕	Unique IP Per service ↕
Guangdong Mobile Communication Co.Ltd.	AS9808	99794
Shandong Mobile Communication Company Limited	AS24444	76358
China Mobile communications corporation	AS56046	19811
China Mobile communications corporation	AS56041	4886



```
</qlink>,</qlink/request>;title="Qlink-Request
Resource",</qlink/wlanest>;title="Qlink-WLAN
Resource",</qlink/success>;title="Qlink-Success
Resource",</qlink/ack>;title="Qlink-ACK
Resource",</basic>,</basic/show>;title="Qlink-SHOW
Resource",</basic/regist>;title="Qlink-Regist
Resource",</basic/searchgw>;title="SearchGW
Resource",</well-known/core>
```

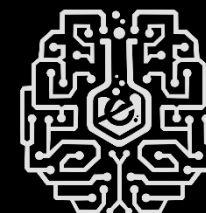
Could be related to "<http://qlink.mobi>" – The world's first decentralized mobile network.



PINKY AND THE BRAIN
TAKE OVER ~~THE~~ DOWN
THE
WORLD

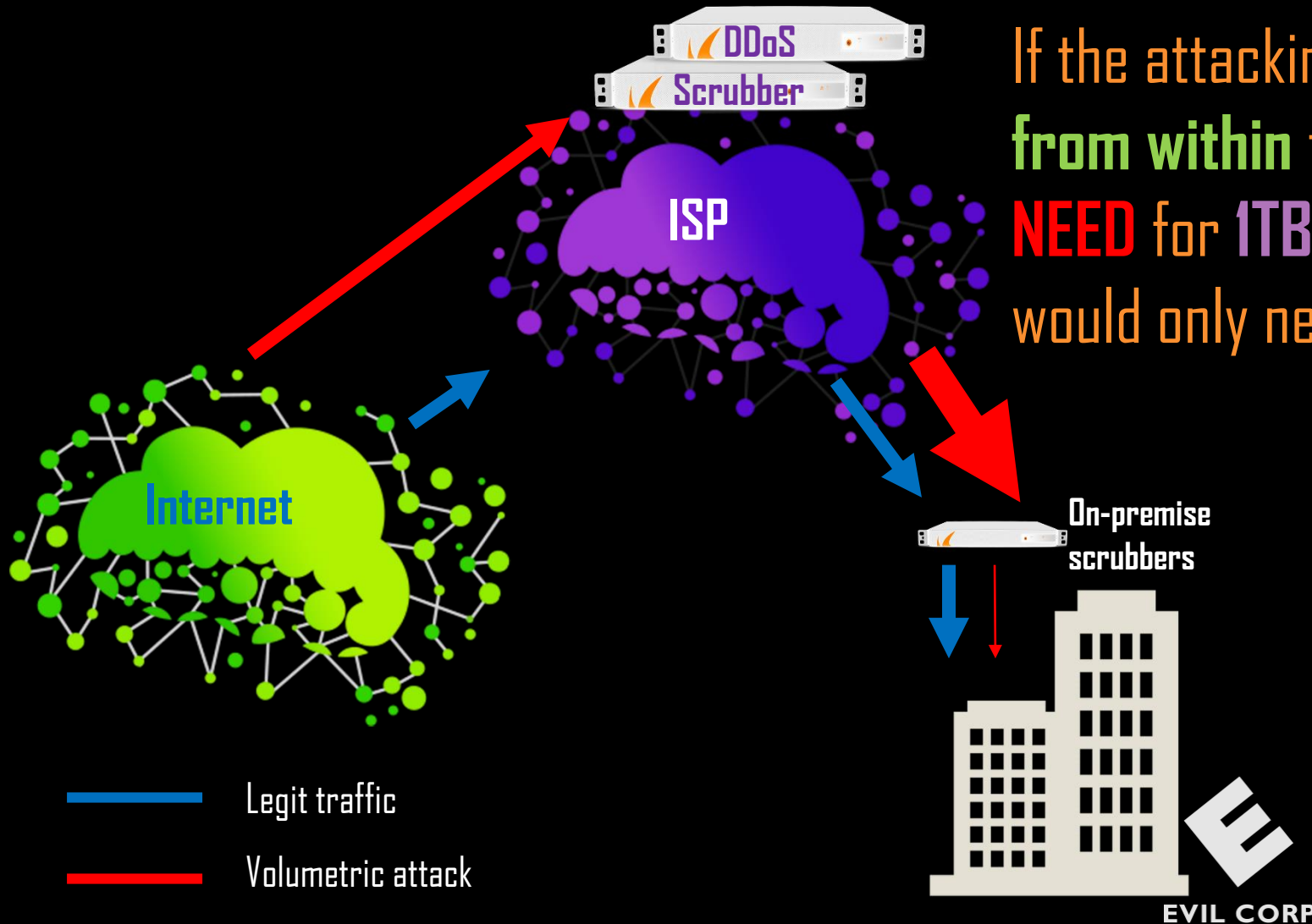


Flake



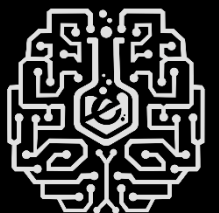
eCrimeLabs

MaxPain attack modeling



- Legit traffic
- Volumetric attack

If the attacking host list can be found from within the ISP network, **NO MORE NEED** for 1TBps+ traffic, the attacker would only need to reach line speed.



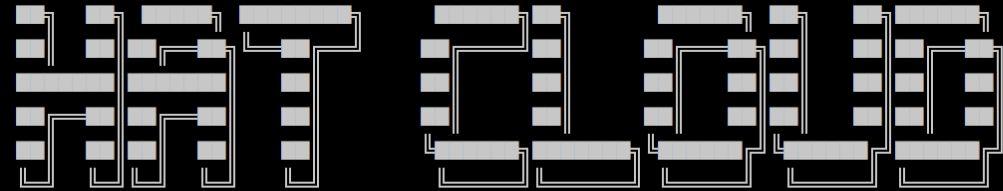
Pre-target analysis



Prior to attacking or choosing the sources of attack a minimal analysis could be made, to identify if there are any UDP service open.

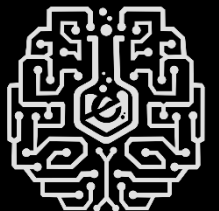
NIST SP 800-115 part 4.2 "Network Port and Service Identification"

- OSINT gathering
 - IP's
 - CIDR's
 - ASN
 - Traceroute
 - Geo-location
 - Peering partners
- Port scan (UDP services)
- Service scan (DNS, NTP, etc.)

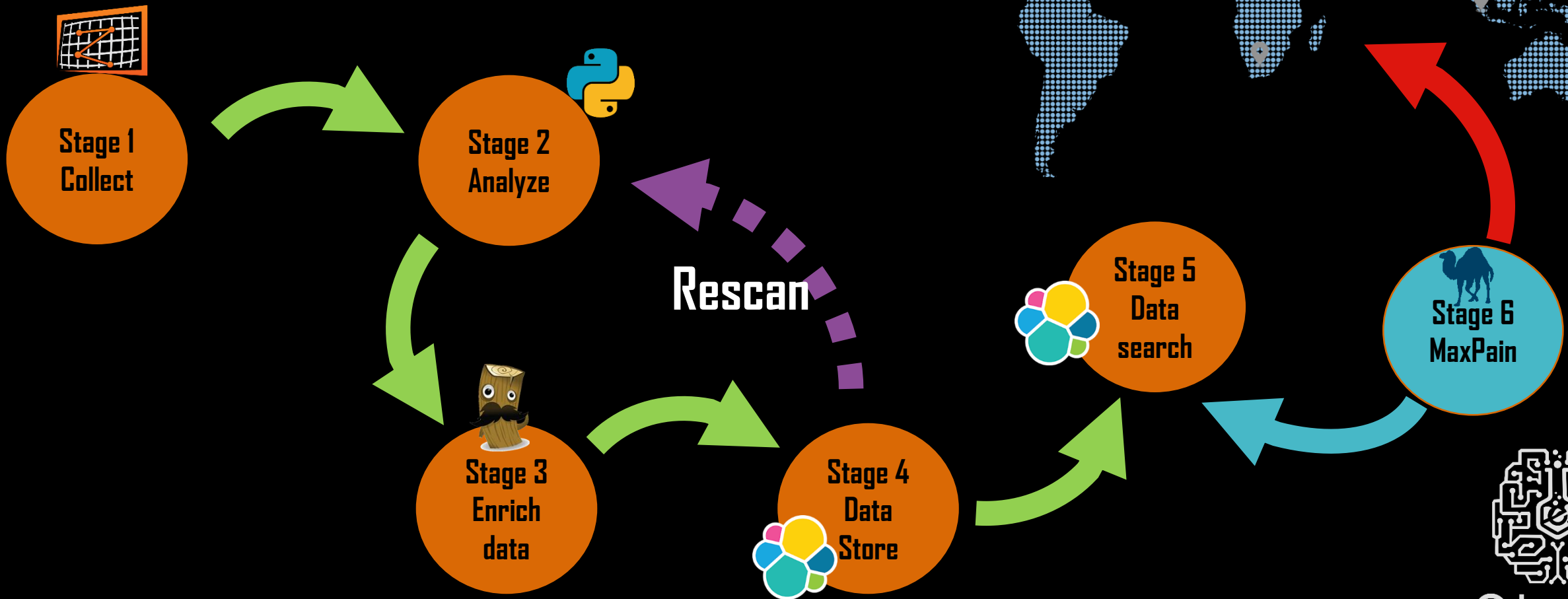


Tool for identifying real IP of CloudFlare protected website.
fb.com/hatbashbr/
github.com/hatbashbr/

```
[+] Site analysis: discordapp.com
[+] CloudFlare IP is 104.16.58.5
[+] Real IP is 52.5.181.79
[+] Hostname: ec2-52-5-181-79.compute-1.amazonaws.com
[+] City: Ashburn
[+] Region: US
[+] Location: 39.0481,-77.4728
[+] Organization: AS14618 Amazon.com, Inc.
```



The different stages



Stage 1 – Data gathering



Scanning the internet today on the IPv4 space is a rather trivial task and many performs this so using the OSINT available. Only success criteria is to find open ports

- Rapid7 Open data
- Censys.io
- Shodan



SHODAN

RAPID7

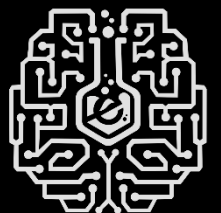


censys

-
- Other none-disclosed sources
 - Zmap runs for specific services



zmap



eCrimeLabs



Stage 2 – Data analysis

Sending a single request to each service and measuring

Time and response

```

PAYLOAD = {
  'dns': ('{}\x01\x00\x00\x01\x00\x00\x00\x00\x01' +
        '{}\x00\x00\xff\x00\xff\x00\x00\x29\x10\x00' +
        '\x00\x00\x00\x00\x00\x00'),
  'snmp': ('\x30\x26\x02\x01\x01\x04\x06\x70\x75\x62\x6c' +
        '\x69\x63\xa5\x19\x02\x04\x71\xb4\xb5\x68\x02\x01' +
        '\x00\x02\x01\x7f\x30\x0b\x30\x09\x06\x05\x2b\x06' +
        '\x01\x02\x01\x05\x00'),
  'ntpmon': ('\x17\x00\x02\x2a' + '\x00'*4), # Monlist
  'ntpread': ('\x16\x02\x00\x01' + '\x00'*8), # Readvar
  'ssdp': ('M-SEARCH * HTTP/1.1\r\nHOST: 239.255.255.250:1900\r\n' +
        'MAN: "ssdp:discover"\r\nMX: 2\r\nST: ssdp:all\r\n\r\n'),
  'chargen': ('\x00'),
  'qotd': ('\r\n'),
  'mdns': ('\x00'*5 + '\x01' + '\x00'*6 + '\x09\xff' + 'services' +
        '\x07\xff' + 'dns-sd' + '\x04' + '_udp' + '\x05' + 'local' +
        '\x00\x00\x0c\x00\x01'),
  'portmap': ('\x65\x72\x0a\x37\x00\x00\x00\x00\x00\x00\x02\x00\x01\x86\xa0' +
        '\x00\x00\x00\x02\x00\x00\x00\x04' + '\x00'*16),
  'netbios': ('\x05\x08\x00\x00\x00\x01\x00\x00\x00\x00\x00' +
        '\x20\x43\x4b\x41\x41\x41\x41\x41\x41\x41\x41' +
        '\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41' +
        '\x41\x41\x41\x41\x41\x41\x41\x41\x00\x00\x21\x00\x01'),
  #
  'tftp': ('\x00\x00\x00\x01\x45\x55\x50\x4c\x2d\x45\x4e\x2e\x70\x64\x66\x00\x6f\x63\x00\x10\x74\x65\x74\x00'),
  'tftp': ('\x00\x01\x58\x00\x6f\x63\x74\x65\x74\x00'),
  'sentinel': ('\x7a\x00\x00\x00\x00'),
  'mssql': ('\x02'),
  'quake3': ('\xff\xff\xff\xff' + 'getstatus' + '\x10'),
  'icabrowser': ('\x2a\x00\x01\x32\x02\xfd\xa8\xe3' + '\x00'*20 + '\x21\x00\x02' + '\x00'*11),
  'coap': ('\x40\x01\x7d\x70\xbb\xe2\x77\x65\x6c\x6c\x2d\x6b\x6e\x6f\x77\x6e\x04\x63\x6f\x72\x65'),
  'rip': ('\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10'),
  'ldap': ('\x30\x84\x00\x00\x00\x2d\x02\x01\x01\x63\x84\x00\x00\x00\x24\x04\x00\x0a\x01\x00' +
        '\x0a\x01\x00\x02\x01\x00\x02\x01\x00\x01\x01\x00\x87\x0b\x6f\x62\x6a\x65\x63\x74' +
        '\x63\x6c\x61\x73\x73\x30\x84\x00\x00\x00\x00'),
  'steam': ('\xff\xff\xff\xff\x54\x53\x6f\x75\x72\x63\x65\x20\x45\x6E\x67\x69\x6E\x65\x20\x51\x75\x65\x72\x79\x00'),
  'memcached': ('\x00\x00\x00\x00\x01\x00\x00stats\r\n'),
  'sip': ('OPTIONS sip:n SIP/2.0\r\nVia:SIP/2.0/UDP m;branch=f;rport;alias\r\nFrom:<sip:n@n>;tag=r\r\nTo:<sip:2@2>\r\nCall-ID:5\r\nCSeq:4 OPTIONS\r\n\r\n')
}

```

```

JSON
├── base
│   ├── attack_type : "ssdp - M-SEARCH * HTTP/1.1"
│   ├── victim : "2.105.13.xxx"
│   ├── port : 1900
│   ├── protocol : "ssdp"
│   ├── domain : ""
│   ├── runtime_start : 1525111993162
│   ├── runtime_stop : 1525113281496
│   └── data_entries : 101465
├── data
│   └── 0
│       ├── start_time : 1525111999738
│       ├── stop_time : 1525112005843
│       ├── soldier : "176.212.90.74"
│       ├── sent : 94
│       ├── recieved : 2274
│       ├── amp_factor : 24
│       ├── sent_data : "TS1TRUFSQ0ggKiBIVFRQLzEuMQ0KSE9TVDogMjM5LjE1NS4yNTUuMjUwOjE5MDANck1BTjogInNzZHA6ZGZyY292ZXliDQpNWDogMg0KU1Q6IHZHA6YWxsDQoNCg=="
│       └── recvd_data : "SFRUUC8xLjEgMjAwIE9LDQpDQUNIRS1DT05UuK9MOIBfYXgtYWdlPTEyMA0KU1Q6IHVwbm9A6cm9vdGRldmJzQ0KVVNOOIB1dWlkojA5OWEyNjJxLWM2OWMlNDdjOC05M2QzLTIzjgXN"

```

Rate limiting would for attackers be included in the tests



Stage 3 – Data analysis and enrichment



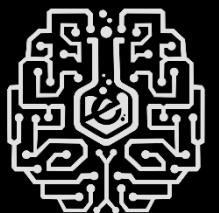
- Create fingerprint
- Create doc_id

```
if [src_ip] and [dst_ip] {
  fingerprint {
    concatenate_sources => true
    method => "MD5"
    key => "dadosmon"
    source => [ "dst_ip", "dst_port", "proto", "attack_desc" ]
  }
}

document_type => "event"
document_id => "%{start_ts}%{stop_ts}%{fingerprint}"
```

Enrichment

- Country Code (e.g. US)
- AS name
- AS Number
- Remove anything with an amplification below 2

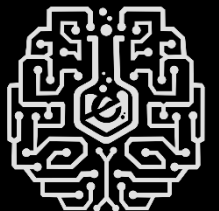


Stage 4 – Data storage

- Amplification factor
- Sent Bytes
- Received bytes
- Time in milliseconds
- Protocol
- Attack description
- Country code2
- Country name
- Destination IP
- Destination Port
- Destination ASN
- Destination ASN number



Field	Type	Value
@timestamp	Q Q □ *	May 21st 2018, 21:51:39.766
t _id	Q Q □ *	152693229963615269322997664eb016a98a77a953f65b60
t _index	Q Q □ *	dadosmon_2018
# _score	Q Q □ *	-
t _type	Q Q □ *	event
# amp_factor	Q Q □ *	17
t attack_desc	Q Q □ *	dns - Standard query ANY
t domain	Q Q □ *	cpsc.gov
# dst_geoiip.area_code	Q Q □ *	757
# dst_geoiip.coordinates	Q Q □ *	-76, 37
t dst_geoiip.country_code2	Q Q □ *	US
t dst_geoiip.country_name	Q Q □ *	United States
# dst_geoiip.dma_code	Q Q □ *	544
# dst_geoiip.latitude	Q Q □ *	37
📍 dst_geoiip.location	Q Q □ *	-76.4936, 37.0736
# dst_geoiip.longitude	Q Q □ *	-76
📄 dst_ip	Q Q □ *	209.10.80.104
t dst_port	Q Q □ *	53
t dst_whois.asn	Q Q □ *	QUALITY INVESTMENT PROPERTIES RICHMOND, LLC
t dst_whois.number	Q Q □ *	A553907
t fingerprint	Q Q □ *	4eb016a98a77a953f65b607e7845ebec
t proto	Q Q □ *	dns
# recv_bytes	Q Q □ *	660
# resp_time_ms	Q Q □ *	130
# sent_bytes	Q Q □ *	37
# src_geoiip.coordinates	Q Q □ *	9, 56
t src_geoiip.country_code2	Q Q □ *	DK
t src_geoiip.country_name	Q Q □ *	Denmark
# src_geoiip.latitude	Q Q □ *	56
📍 src_geoiip.location	Q Q □ *	8.973800000000011, 56.139299999999999
# src_geoiip.longitude	Q Q □ *	9
📄 src_ip	Q Q □ *	2.105.13.142
t src_whois.asn	Q Q □ *	Tele Danmark
t src_whois.number	Q Q □ *	A53292
# start_ts	Q Q □ *	1526932299636
# stop_ts	Q Q □ *	1526932299766
t type	Q Q □ *	dadosmon





Stage 5 - Formulas

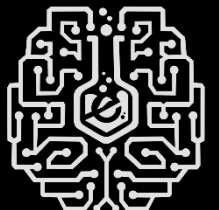
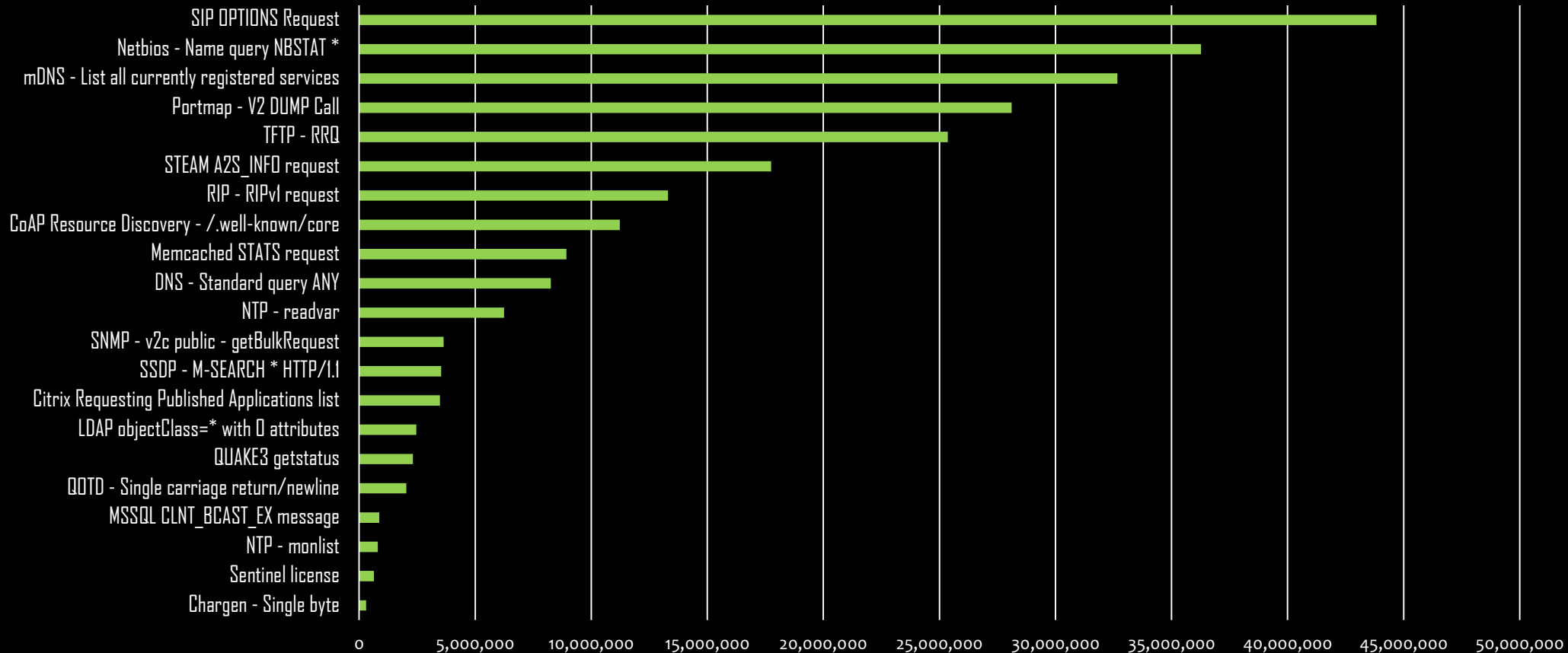
Bandwidth Amplification Factor

$$BAF = \frac{\text{size(UDP packet sent to victim)}}{\text{size(UDP packet sent from attacker)}}$$

uh = UDP header ≈ 47 bytes

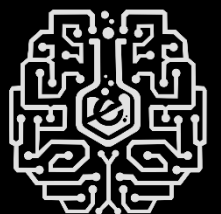
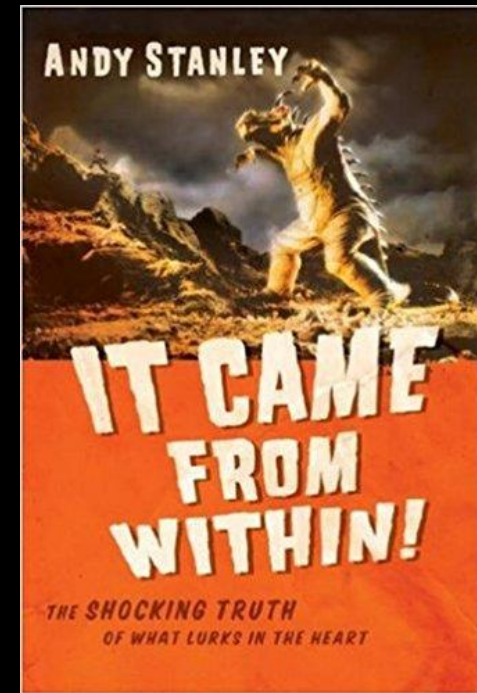
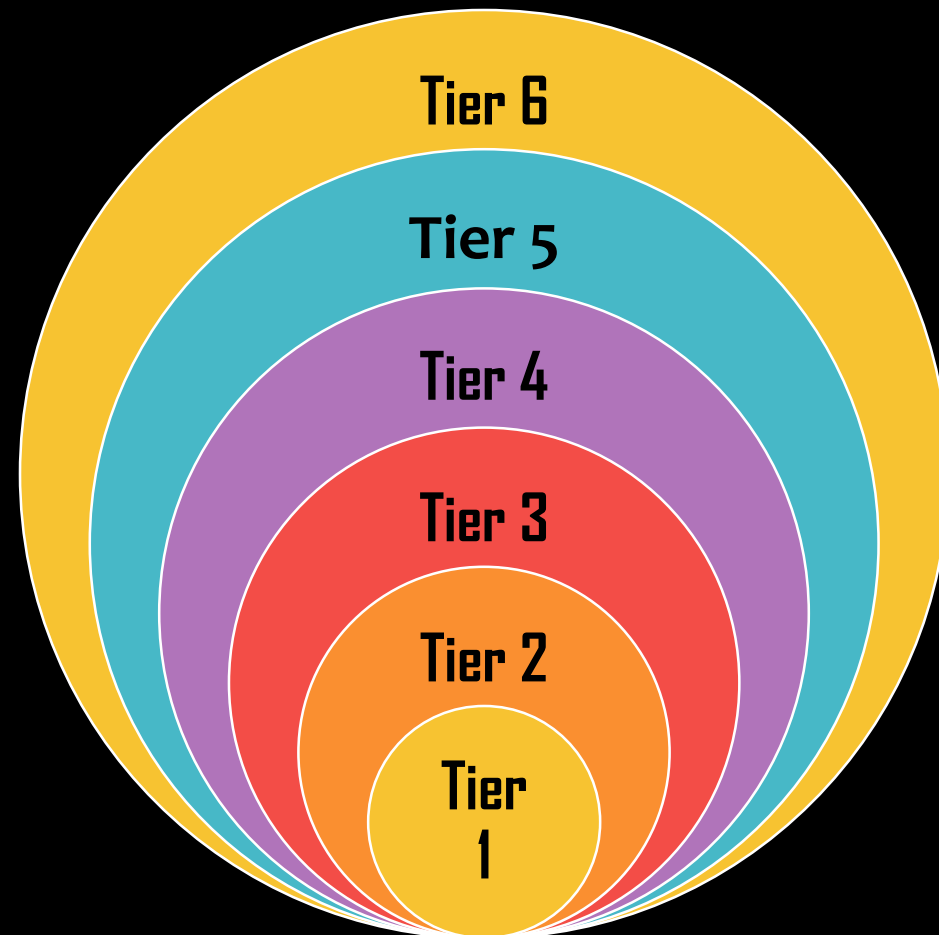
$$PEF = (\text{Sent bytes} + uh) * \frac{(x \text{ Gbit}) * 134217728 \text{ bytes}}{(\text{Average Recieved bytes} + uh)}$$

Protocol effectiveness (PEF) – Spoofed traffic required



Stage 5 – Data Search

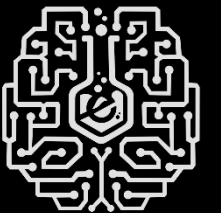
Stage 5 has been split up into tier searches in order to find systems who can be used as close to the target as possible.



DISCLAIMER



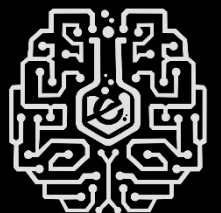
NO animals, people, websites or networks were harmed in the making of this demonstration all the information gathered is based on OSINT information and 3 years of "scanning" the internet.



Stage 5 – The rippling effect



For demonstration I use
<http://www.richmondgov.com/>



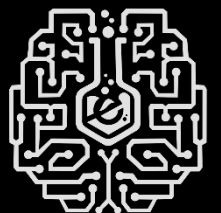


Stage 5 – Data Search - Tier 1

<http://www.richmondgov.com/> resolves to 65.202.206.55

In the Tier 1 search we look for anything within 65.202.206/24

Attack type	Amount
NTP – Readvar	2
Portmap – V2 DUMP Call	2
DNS – Standard query ANY	2



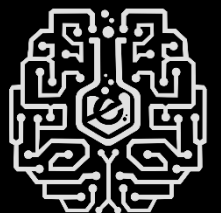


Stage 5 – Data Search - Tier 2



The original IP is actually within **65.192.0.0/11** so we search for this

Attack type	Amount
NTP – Readvar	1.653
Portmap – V2 DUMP Call	1.550
snmp - v2c public - getBulkRequest	270
dns - Standard query ANY	102
netbios - Name query NBSTAT *	75
SIP OPTIONS Request	69
ssdp - M-SEARCH * HTTP/1.1	41
ntp – monlist	40
tftp – RRQ	35
MSSQL CLNT_BCAST_EX message	15



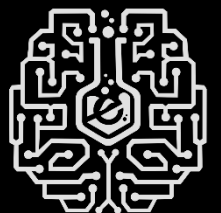


Stage 5 – Data Search - Tier 3



We now reached the ASN stage "AS54883" and "AS701"

Attack type	Amount
NTP – Readvar	8.372
ssdp - M-SEARCH * HTTP/1.1	2.978
portmap - V2 DUMP Call	2.440
snmp - v2c public – getBulkRequest	2.002
netbios - Name query NBSTAT *	1.651
ntp – monlist	1.524
SIP OPTIONS Request	1.251
tftp – RRQ	714
dns - Standard query ANY	702
MSSQL CLNT_BCAST_EX message	307



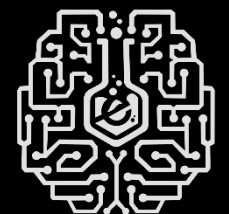


Stage 5 – Data Search - Tier 4



- Upstream Peering partners for AS54883 and AS701 is about 7 → AS21508, AS1339, AS1299, AS209, AS3356, AS703, AS2497

Attack type	Amount
NTP – Readvar	25.528
snmp - v2c public - getBulkRequest	8.110
portmap - V2 DUMP Call	5.632
SIP OPTIONS Request	4.352
tftp - RRQ	3.655
ssdp - M-SEARCH * HTTP/1.1	3.548
netbios - Name query NBSTAT *	3.072
dns - Standard query ANY	2.576
ntp – monlist	2.124
MSSQL CLNT_BCAST_EX message	520



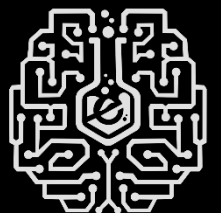


Stage 5 – Data Search - Tier 5



If for some reason there should still be missing hosts to reached the wanted attack size Country is choosed: US

Attack type	Amount
NTP – Readvar	798.465
portmap - V2 DUMP Call	466.895
snmp - v2c public – getBulkRequest	194.008
dns - Standard query ANY	191.273
tftp – RRQ	153.798
SIP OPTIONS Request	111.373
ssdp - M-SEARCH * HTTP/1.1	105.685
netbios - Name query NBSTAT *	73.012
ntp – monlist	37.476
MSSQL CLNT_BCAST_EX message	21.789





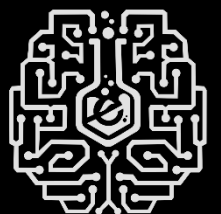
Stage 5 – Data Search - Tier 6



If for some reason there should **still** be missing hosts to reached the wanted attack size Country is choosed: **Not US**

Attack type	Amount
NTP – Readvar	2.890.438
snmp - v2c public – getBulkRequest	1.639.650
ssdp - M-SEARCH * HTTP/1.1	1.222.938
SIP OPTIONS Request	1.168.383
portmap - V2 DUMP Call	1.091.785
tftp – RRQ	716.650
ntp – monlist	390.691
dns - Standard query ANY	384.083
netbios - Name query NBSTAT *	331.874
CoAP Resource Discovery - /.well-known/core	181.746

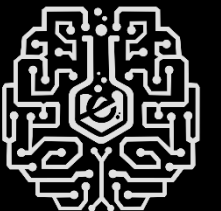
Never found Tier 6 to be needed



Max Pain threat analysis

Proof-of-Concept developed to identify and tie it all together.

Max Pain performs an extraction of potential vulnerable hosts that can be abused within each tier.



DEMONS

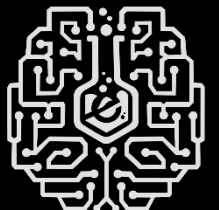
```
Max Pain v.1.0
:+ydNNNNNds
:yNNNNNNNNNNNd/
-dNNNNNNNNNNhssNMh
:NNNNNNNNMs:      :Mm
/MMNNNNNd-      +N+
:NNNNNN/::./sdd-yd:
-NNNNNNMN./ss.  h-
+NNNNNNMo  --  +
/+      +NNMmMMNd/
sMMs      --+NNNNNNh+-  o/:..
mMMs      /NNNNNm/  -yMNdhmNy:
-mMMy      -odMMmyhNMdNNNNNNNo:--
+MMMd:      hMMMMhMNNNNNNNNNNmmho-
o/NNMMN/      -MMNNNMNNNNNNNNNNNNNNNy.
.mNNNNNN+      .ohosmNNNNNNNNNNNNNNNN/
+hNNNNNNM/      :m-  o/NNNNNNNNNNNNNNNNNNNN
--/mNNNNNM/      .oNm  -dNNNNNNNNNNNNNNNNNNNN
dhyhMMNNNo      -dMMh  ./dNNNNNNNNNNNNNNNNNNNN
+MMNNNNMy      omMMMy:shNNNNNNNNNNNNNNNNNNNN
+NNNNNNMd      .hNNMMdMMNNNNNNNNNNNNNNNNNNNN
/MMNNNNNNMM--dMmMMNN  yMMNNNNNNNNNNNNNNNNNNNN
oMMNNNNNNMM+mNNNNNNMd  dMMNNNNNNNNNNNNNNNNNNNN
.NNNNNNNNdNNNNNNMh  .NNNNNNNNNNNNNNNNNNNNNN
oMMNNNNNNmNNNNNNMy  +MMNNNNNNNNNNNNNNNNNNNN
hMMNNNNNNMMNNNNNNM-  MNNNNNNNNNNNNNNNNNNNNNN
dMMNNNNNMNNNNNNM:  NNNNNNNNNNNNNNNNNNNNNNN
dMMNNMdMMNNNNMMN  NNNNNNNNNNNNNNNNNNNNNNN
dMMNNdMMNNNNMMo  MNNNNNNNNNNNNNNNNNNNNNN
hMMNNMMNNMMMo  .MMNNNNNNNNNNNNNNNNNNNNNN
yMMNNNNNNMMY  .MMNNNNNNNNNNNNNNNNNNNNNN
/mMMNNNNNNMMN  MNNNNNNNNNNNNNNNNNNNNNNNN
:MMNNNNNNMM/  m (c)2018 Dennis Rand MM
:MMNNNNMM.  MNNNNNNNNNNNNNNNNNNNNNNNN
```

TRATATION

```
===== USAGE =====
--target 127.0.0.1 (Target IP to analyze)
--cidr 24 (Below CIDR Range for Tier 1 search)
--days 30 (Amount of days to seach back in ELK)
--amp 2 (Minimal amplification factor required)
--sec 25 (Expected average requests per second to send out)
--tier_min 1
--tier_max 4
--sort recv_bytes (amp_factor or recv_bytes)

--debug (Show Debug mode)
--simulate (Don't query Elastic)
--anon (Anonymize threat report)
```

```
=====
TIER Description:
Tier 1 - Is systems within a 24 CIDR of target
Tier 2 - checks systems within announced CIDR of target
Tier 3 - Systems within AS number detected for IP
Tier 4 - Upstream Peering partners of tier 3 AS
Tier 5 - Systems within the same Country as the IP
Tier 6 - Systems outside of country related to IP
=====
```



The problem

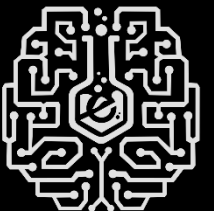
The problem described in the research is not only applicable to UDP service but can directly be adopt/merged with Botnet's, and other vulnerable services as well .

GREETINGS PROFESSOR FALKEN

HELLO

A STRANGE GAME.
THE ONLY WINNING MOVE IS
NOT TO PLAY.

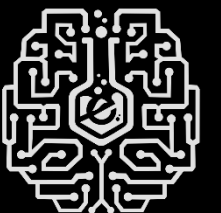
HOW ABOUT A NICE GAME OF CHESS?



What can be done or are we at a **GAME OVER** state

THANK YOU FOR PLAYING

- **Digital hygiene** for your own networks and ISP's (Liability)
(<http://bgpranking.circl.lu/>)
- Should we start distributing lists of vulnerable services and block them – Spamhaus style (<https://www.spamhaus.org/drop/>)
- BCP38 – Antispoofing, however does not affect infected devices



Thanks to

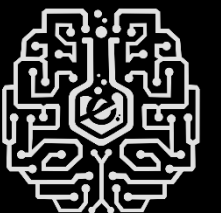
**SPECIAL
THANKS**

A big thanks to **Rapid7** and specially **Jon Hart** for helping me, by adding new protocols to their internet-wide scanners and going a long way to help me as much as possible.

SSDVPS.DK for supporting the research and providing a free of charge server, for my research.

Mikael Vingaard (<https://honeypot.dk>) for doing sanity checks.

And all who have listened to me ranting over the years



The core research data set

```
/*
 * -----
 * "THE BEER-WARE LICENSE" (Revision 2):
 * I'm releasing these files. As long as you retain this notice you
 * can do whatever you want with this stuff. If we meet some day, and you think
 * this stuff is worth it, you can buy me a beer in return Dennis Rand
 * -----
 */
```

DATA MINING



2016 - <https://bit.ly/2FBoUi4>

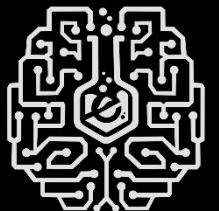
https://www.dropbox.com/sh/uwvlo3mcajt8zc8/AADN_Bvt0tmX0Fc8BKYRkVUta?dl=0

33 GB bz2 compressed JSON

2017 - <https://bit.ly/2HNisGN>

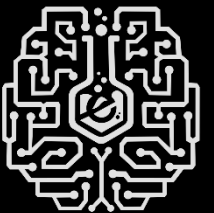
<https://www.dropbox.com/sh/syv5hiae30jk0b3/AADy09ktrM3Q3liE8L79BLNza?dl=0>

118 GB bz2 compressed JSON



Thank you for your time

Hope you enjoyed the show and did
not fall asleep



eCrimeLabs