BSIDES LUXEMBOURG

(Amplification) Attack of the Clones

/usr/bin/whoami

Beverley MacKenzie	Scott MacKenzie
20 years in: Network Operations, Infrastructure, System Administration, I T Audit, Compliance & Risk Assessment. **Education** MSc Information Security, Royal Holloway, London University Presently undertaking a: Ph.D. Cyber Security, Abertay University Research area: Blockchain & IoT **Qualifications** AAT Certified Accountant ISO27001 Lead Auditor	Over 20 years experience across IT & Security covering many flavours of *NIX, Architecture and Engineering. General Technophile. **Education** BSc Chemistry MBA Open University MSc Information Security, Royal Holloway, London University **Qualifications** ISC2 CISSP Crest Registered Technical Security Architect **Contact** @Cyber_Scott

Agenda

- Background concepts
- In the beginning there were Smurfs and Fraggles
- Mitigation techniques for Slowloris Case Study and how they are applicable to other DDOS
- Spamhaus vs Cyberbunker
- CDN
- IoT attacks
- Mirai
- Persirai
- Questions & Answers

Protocol distinction

- Layer 3 & 4, Network attacks include:
  - SYN Flood, UDP Flood, TCP Flood attacks
  - ICMP
  - Malformed packets
- Layer 7, Application attacks include:
  - HTTP Flood, DNS query Flood, DNS amplification

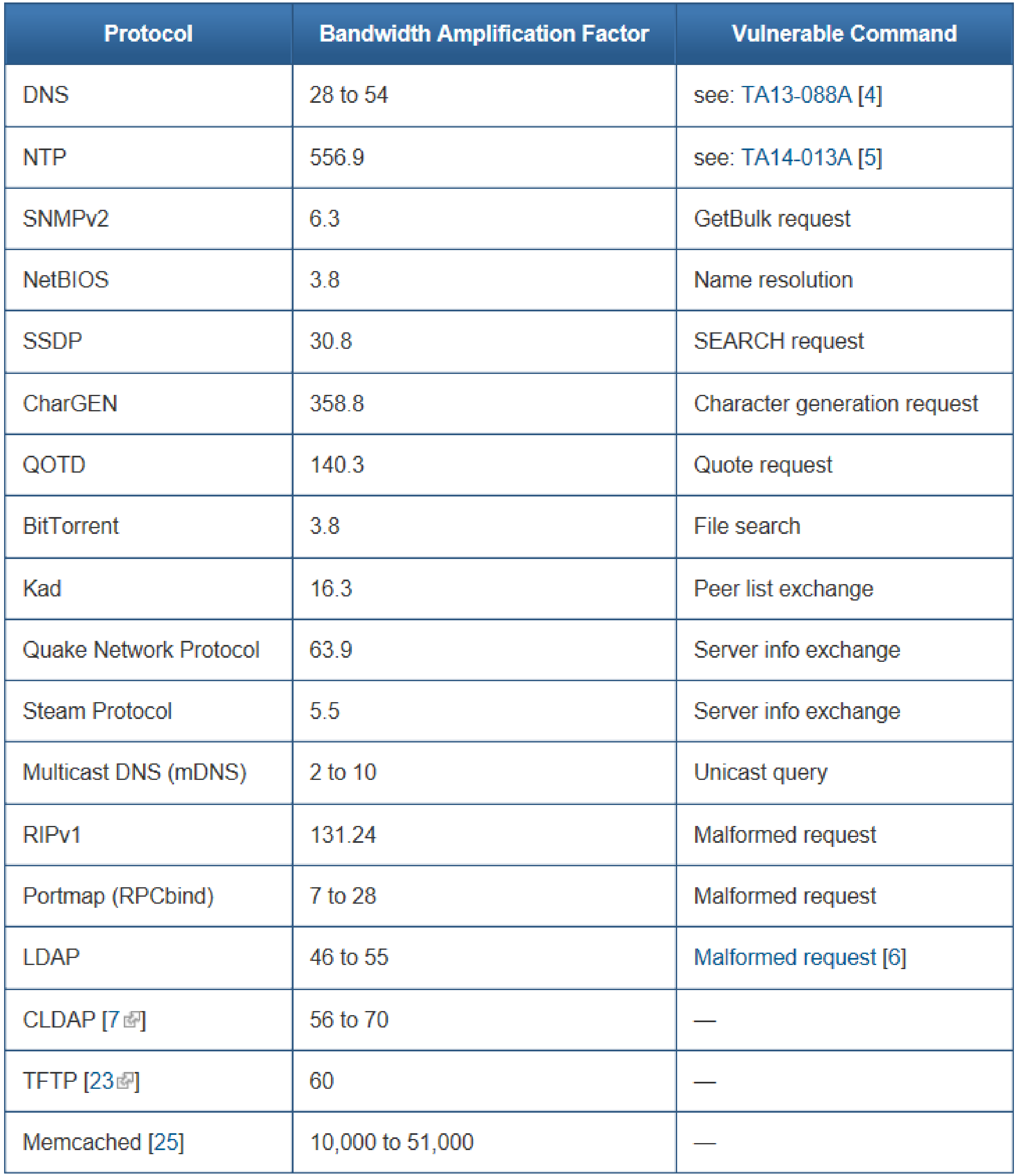
Reflection

- The attacker sends packets with the **forged** IP address of the target as the source address of the packets to different destinations. The destination servers respond to target with the response to the sent packets from the attacker.

Amplification

- A small number of packets from attackers will elicit a large number of packets directed to the target system. Amplification technique is often combined together with the reflection technique to create a large attack on to a target.

Bandwidth Amplification Factor

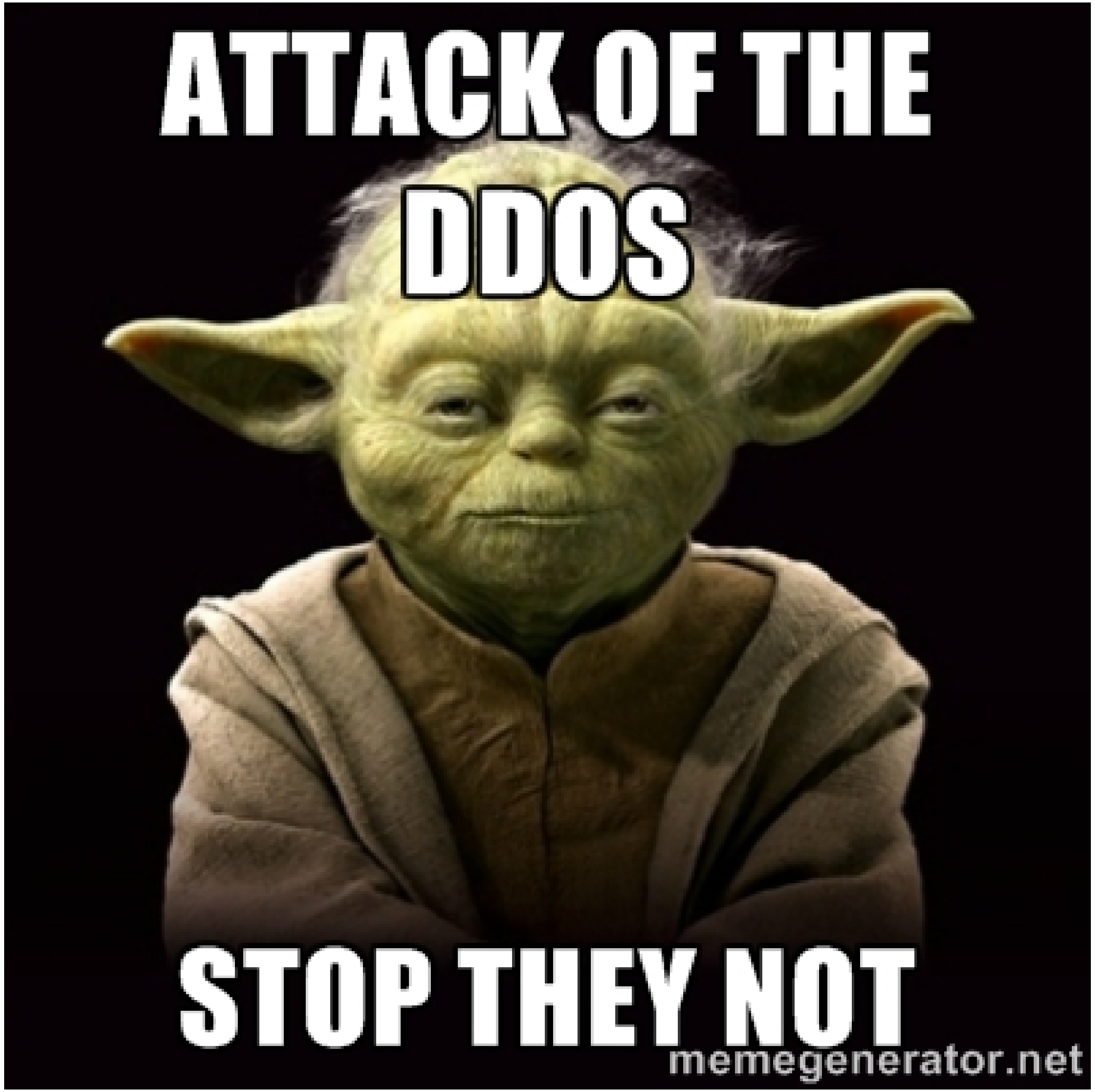


Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—

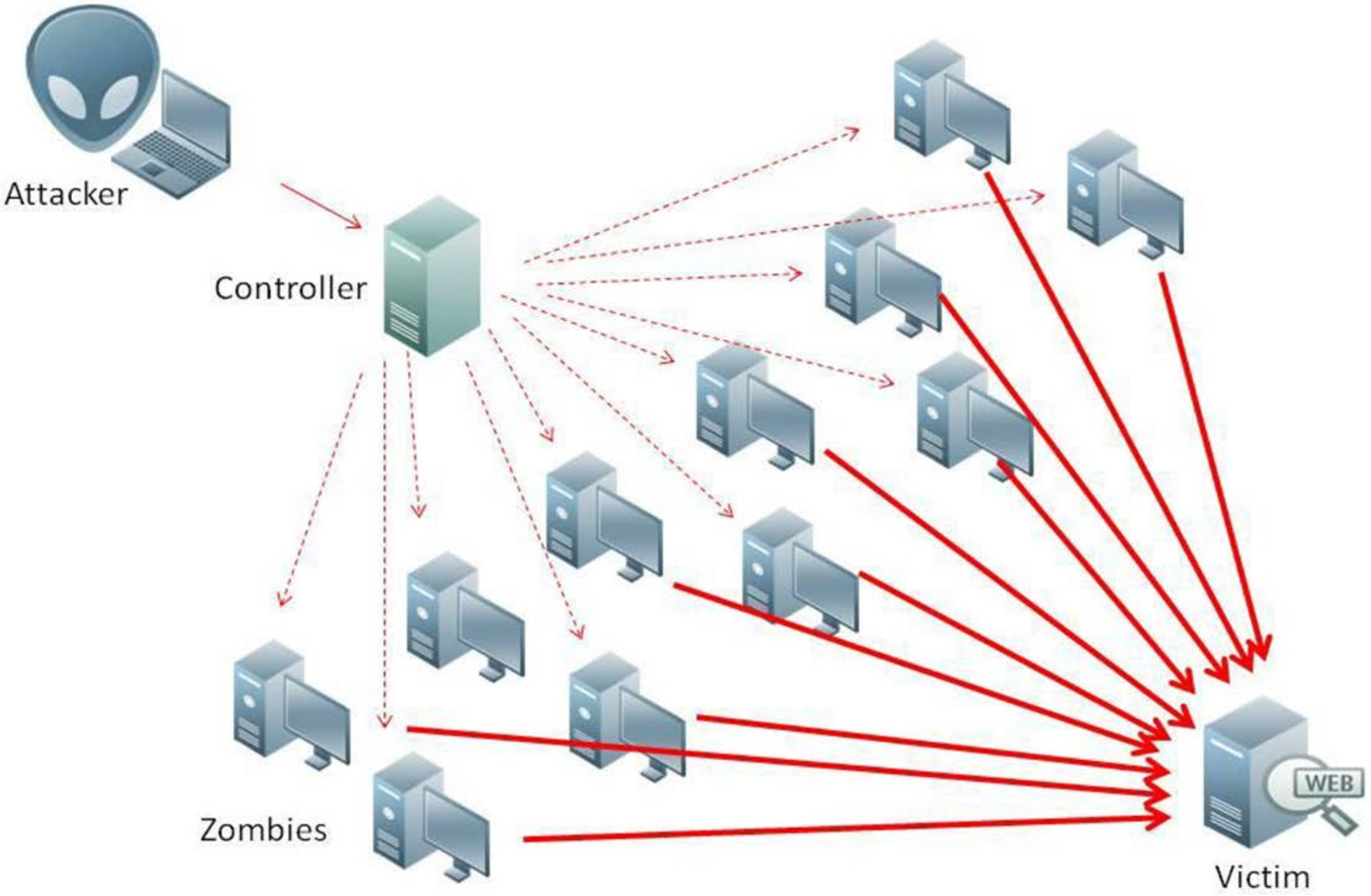
Source: https://www.us-cert.gov/ncas/alerts/TA14-017A

Flood attacks

- In Flood attacks, the attacker (normally a botnet) directly sends a large volume of IP traffic to the victim machine to congest its network resources preventing legitimate user access.
- Common attacks are SYN flood and UDP flood


ATTACK OF THE DDOS
STOP THEY NOT
memegenerator.net

What is DDOS



Smurfs & Fraggles

In the beginning there was Tfreak (1997)…

…and Tfreak created Dos, and Dos was…

Smurfs & Fraggles

- SMURF ATTACK:
  A large number of ICMP echo packets with the intended victims spoofed source IP address are broadcast to a computer network using an IP broadcast address.

- FRAGGLE ATTACK:
  Basically smurf with a UDP twist. An attacker sends a large amount of UDP traffic to ports 7 (echo) and 19 (chargen) to an IP Broadcast Address, with the intended victim's spoofed source IP address

Mitigating Smurfs & Fraggles

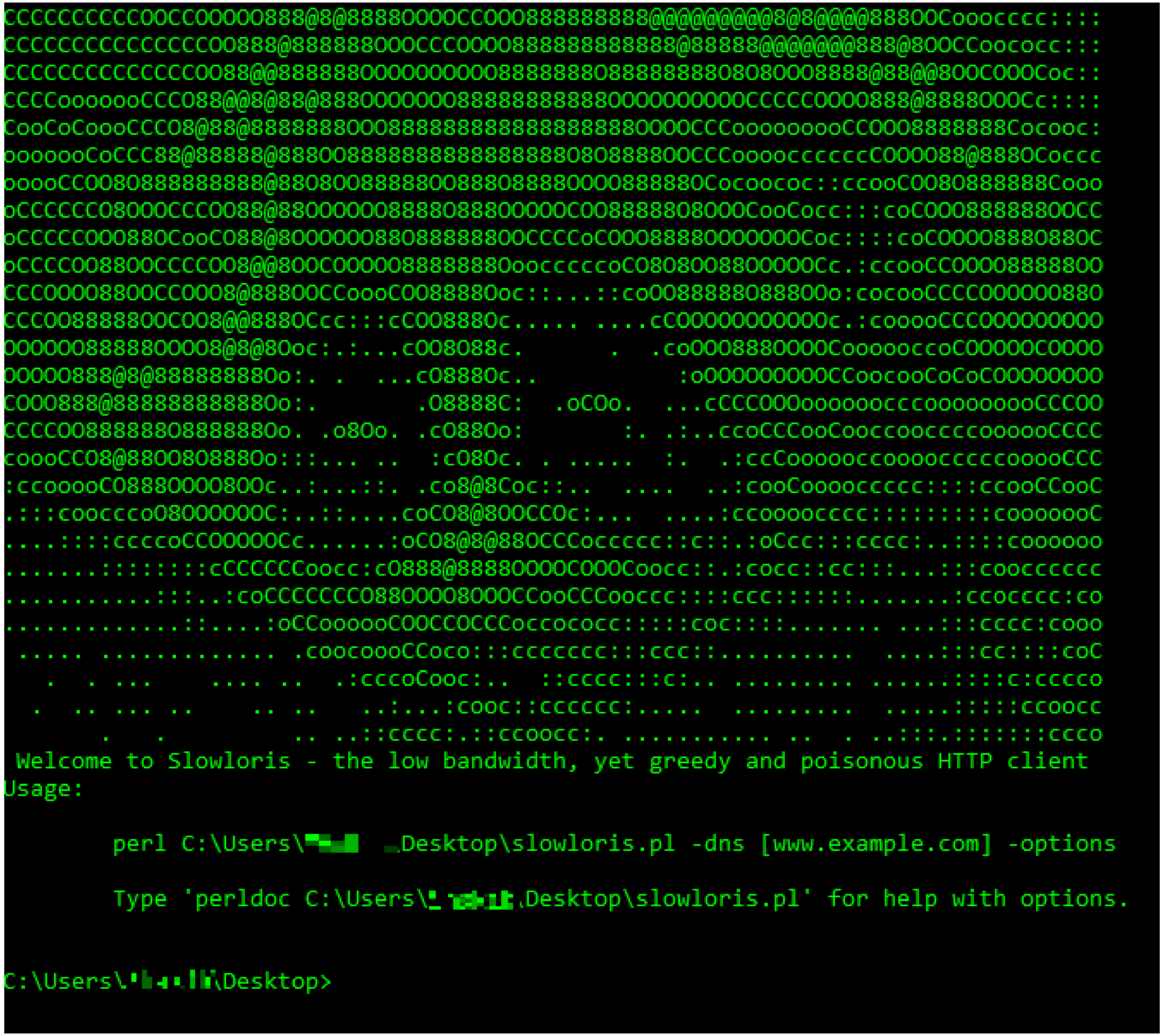
- Turn off unneeded services
- Block UDP ports 7 and 19
- Disable IP broadcasting capabilities
- Block inbound and outbound ICMP echo and echo reply (consider only at your edge routers/firewalls, since this is needed for network diagnostics)
- CAR – Cisco's Committed Rate Access Traffic Filtering Tool
- Configure similar filtering as CAR in your firewalls / routers

Mitigating Smurfs & Fraggles

- BCP 38 / rfc 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
  - Can only be truly affective if all ISPs implement
  - This filtering requires ISP to check packets network address before forwarding packets.
  - If the packet is using a network address that is not applicable to the ISP’s range then the packets should be dropped.
  - Also another aspect of rfc 2827 is filtering based on only forwarding traffic with legitimate network addresses.
- Powertec
- Netscan

Slowloris

This tool is named for a primate that characteristically moves slowly. The advantage of this tool is that is allows the attacker to initiate attacks that consume limited resources but can still cause impressive amounts of damage.



```
CCCCCCCCCCOOCCOOOOO888@8@8888OOOOCCOOO888888888@@@@@@@@@8@8@@@@888OOCooocccc::::
CCCCCCCCCCCCCCCCOO888@8888880OOCCCOOOO88888888888@88888@@@@@@@888@8OOCCoococc:::
CCCCCCCCCCCCCCOO88@@88888OOOOOOOOOOO8888888O8888888808080008888@88@@800COOOCoc::
CCCCoooooooCCCO88@@8@88@888OOOOOOOO88888888888888OOOOOOOOOOCCCCCOOOO888@8888OOOCc::::
CooCoCoooCCCO8@88@8888888OOO8888888888888888888888OOOOCCCoooooooooCCOOO8888888Cocooc:
ooooooCoCCC88@88888@888OO88888888888888888888O8O88888OOCCCooooccccccCOOOO88@888OCoccc
ooooCCOO8O888888888@88O8OO888888OO888O8888OOOO88888OCocoococ::ccooCOO8O888888Cooo
oCCCCCCO8OOOCCCOO88@88OOOOOO8888O888OOOOOCOO888888O8OOOCooCocc:::coCOOO88888800CC
oCCCCCOOO88OCooCO88@8OOOOOO88O8888888OOCCCCoCOOO88888OOOOOOOCoc::::coCOOOO8888O880C
oCCCCOO88OOCCCCOO8@@8OOCOOOOO8888888OoocccccoCO8O8OO88OOOOOCc.:ccooCCOOOO888888OO
CCCOOOO88OOCCOOO8@888OOCCoooCOO8888Ooc::...::coOO88888O8888OOo:cocooCCCCOOOOOO880
CCCOO8888880OCOO8@@888OCcc:::cCOO888Oc.....  ....cCOOOOOOOOOOOc.:cooooCCCOOOOOOOOO
OOOOOO88888OOOO8@8@8Ooc:.:...cOO8O88c.        .   .coOOO888OOOOCoooooccoCOOOOOCOOOO
OOOOO888@8@8888888880o:.  .   ...cO888Oc..            :oOOOOOOOOOCCoocooCoCoCOOOOOOOO
COOO888@888888888888Oo:.         .O8888C:   .oCOo.   ...cCCCOOOooooooccoooooooooCCCOO
CCCCOO888888O888888Oo.  .o8Oo.  .cO88Oo:          :.  .:..ccoCCCooCooccoocccoooooCCCC
coooCCO8@88OO8O888Oo:::...  ..   :cO8Oc.  .  .....   :.   .:ccCoooooccoooocccccooooCCC
:ccooooCO888OOOO8OOc..:...::.  .co8@8Coc::..   ....   ..:cooCoooocccc:::ccooCCooC
.:::cooccco08OOOOOOC:..::....coCO8@8OOCCOc:...   ....:ccooooccc::::::::coooooooC
....::::ccccoCCOOOOOCc......:oCO8@8@88OCCCoccccc::c::.:oCcc::cccc:..::::coooooo
.......::::::::cCCCCCCoocc:cO888@8888OOOOCOOOCoocc::.:cocc::cc:::...:::coocccccc
...........:::..:coCCCCCCCO88OOOO8OOOCCooCCCooccc:::ccc:::::.......:ccocccc:co
..............::....:oCCoooooCOOCCOCCCoccococc::::coc:::....... ...:::cccc:cooo
 ..... ............. .coocoooCCoco::ccccccc:::ccc::..........  ....:::cc:::coC
   .   .  ...     .... ..  .:cccoCooc:..   ::cccc:::c:..  .........  .....::::c:cccco
  .   ..  ...  ..     ..  ..   ..:...:cooc::cccccc:.....   .........  .....:::::ccoocc
       .     .            ..  ..::cccc:.::ccoocc:.  ...........  ..   .  ..:::.:::::::ccco
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:

        perl C:\Users\[redacted]Desktop\slowloris.pl -dns [www.example.com] -options

        Type 'perldoc C:\Users\[redacted]Desktop\slowloris.pl' for help with options.


C:\Users\[redacted]Desktop>
```

Slowloris

- HTTP GET requests to occupy all available HTTP connections permitted on a web server
- Vulnerability in **thread-based web servers** (like Apache) which wait for entire HTTP headers to be received before releasing the connection
- Apache waits 300 seconds (default) for incomplete HTTP requests, re-set as soon as the client sends additional data
- The malicious user opens numerous requests to the webserver, but does not finish the HTTP GET request by sending the [CRLF]
- Evades, IDS and IPS systems since the attack does not contain malformed requests

Mitigation for Slowloris

- Three most popular mitigations using Apache:
  - Use mod_reqtimeout
    - Allows the setting of a bytes per second rate to deliver HTTP header data and a max time for header delivery to complete, otherwise an HTTP 408 REQUEST TIME OUT is sent back
    - Allows a similar, separate setting for body data rate and completion
  - Use mod_qos
    - Allows prioritisation of HTTP requests, sets limits on connection numbers for source IP, disables HTTP KeepAlive above a certain connection threshold, configures a minimum bytes per second throughput rate
  - Use mod_security
    - This is a Web Application Firewall (WAF) for Apache HTTP server, with many options
    - Key for Slowloris, it can track how many times an HTTP 408 error is triggered, if this happens more than a certain number of times, within a defined period, then future connections from this IP are dropped by issuing a TCP FIN packet

Mitigation for Slowloris

- An HTTP loadbalancer (such as an F5 Big-IP) by default would wait for the complete request before forwarding to the threaded webserver. Since Slowloris only affects threaded webservers.
- A non threaded webserver, like NGINX will resist a typical Slowloris attack, however, in default config NGINX (below v 1.5.9) is still vulnerable to a Goloris (Slowloris for NGINX) attack. (Later versions were patched to stop slow POST body connections).
- IPTABLES Linux firewall allows you to limit the number of connections from an IP as well limit the connections per second (can exclude proxies)

Other well known tools

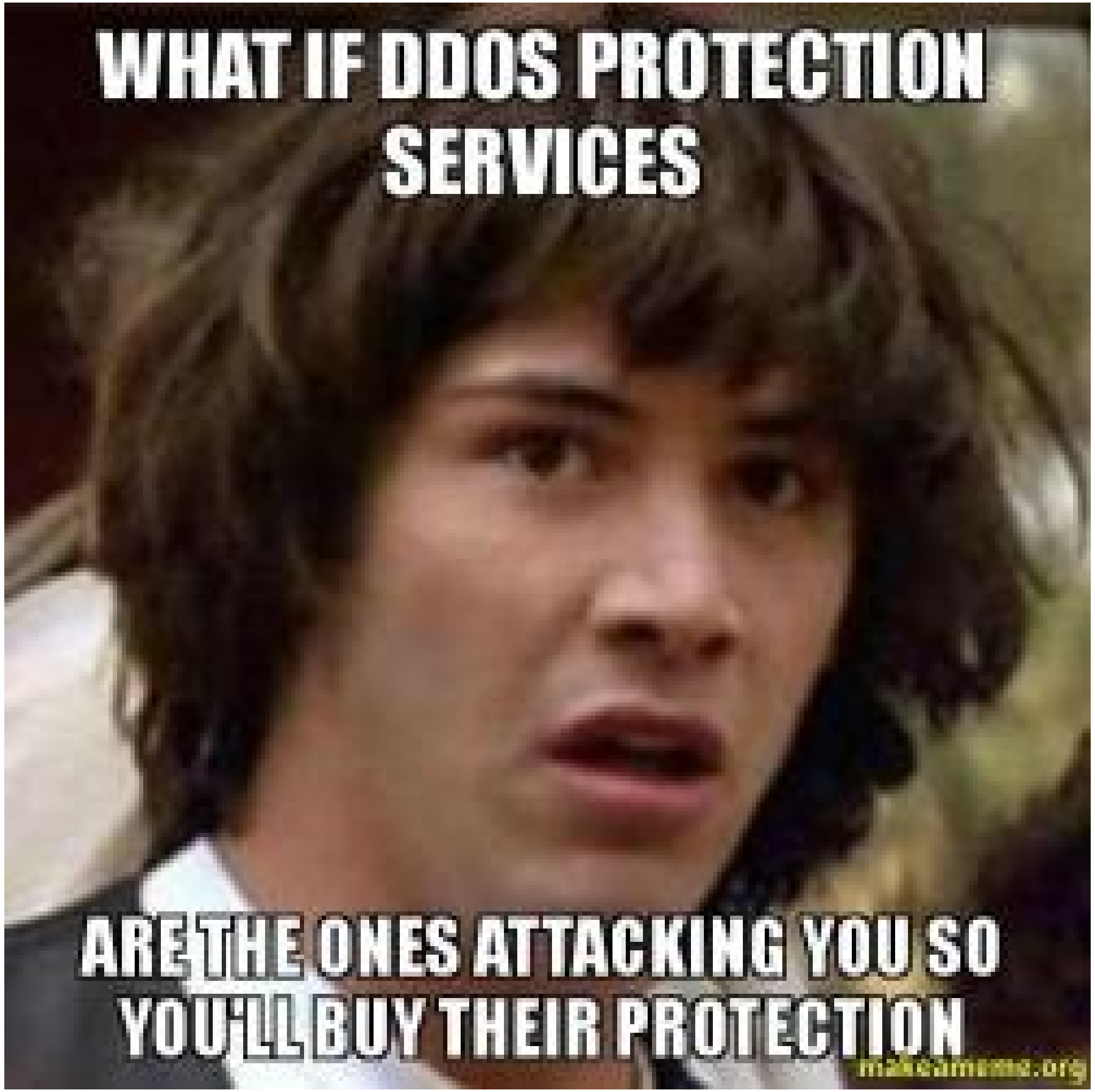
- Tribe Flood Network (TFN)—TFN can launch ICMP, Smurf, UDP, and SYN flood attacks at will against an unsuspecting victim. TFN has the distinction of being the first publicly available DDoS tool.
- RUDY (R-U-Dead-Yet)—Like LOIC, this tool offers attackers a choice of DoS or DDoS attacks. RUDY provides the ability to launch high-impact HTTP DDoS attacks.
- DDOSIM-Layer 7 DDOS Simulator—This tool is yet another popular attack tool that can simulate multiple attack sources (bots).
- DAVOSET—This software utilizes functionality abuse and XML External Entities (XXE) vulnerabilities to attack a designated victim.

Spamhaus vs CyberBunker

- CyberBunker, a Dutch hosting company based in a Cold War nuclear bunker, whose website states it hosts "services to any Web site 'except child pornography and anything related to terrorism'".
- October 2011, Spamhaus identified CyberBunker as providing hosting for spammers
- March 2013, Spamhaus added CyberBunker to its blacklist.
- A DDoS attack, peaking at 300 Gbit/s, was launched against Spamhaus. This utilised DNS amplification attacks via open resolvers.
- Mitigated by Cloudflares Anycast routing technique that distributed the IP address across 23 datacentres around the world.

Response Rate Limiting

- RRL, or Response Rate Limiting, is an enhancement to implementations of the DNS protocol that can help mitigate DNS amplification attacks
- RRL helps mitigate DNS denial-of-service attacks by reducing the rate at which authoritative servers respond to high volumes of malicious queries. The RRL mechanism is part of BIND 9.10, and was available as a software build option in BIND 9.9.4.
- There is a high probability, if hundreds of packets per second arrive with very similar source addresses asking for similar or identical information, they are part of an attack. The RRL software detects patterns in arriving queries, and when it finds a pattern that suggests abuse, it can reduce the rate at which the replies are sent.


WHAT IF DDOS PROTECTION SERVICES
ARE THE ONES ATTACKING YOU SO YOU'LL BUY THEIR PROTECTION
makeameme.org

Content Delivery Network or Content Distribution Network (CDN)

- Geographically distributed network of proxy servers and data centres
- Suitable for caching static content, particularly images, movies, large PDFs, which are often sought after in Layer 7 type exhaustive HTTP GET requests
- Free CDNs and Commercial CDNs exist that include: Cloudflare, BootstrapCDN, Akamai, Azure CDN, Amazon CloudFront and many others.
- Private CDNs where companies/organisations stand up their own CDN rather than choosing a commercial offering.

Phlashing / permanent Denial of Dervice

- Phlashing is a permanent denial of service (DoS) attack that exploits a vulnerability in network-based firmware updates. Such an attack is currently theoretical but if carried out could render the target device inoperable.
- PhlashDance is a tool created by Rich Smith used to detect and demonstrate PDoS vulnerabilities demonstrated at the 2008 EUSecWest Applied Security Conference in London.
- This is not a commonly seen DoS attack, since criminals are more interested in exploiting compromised devices rather than destruction. However, depending on the motive of the attacker, this would be very significant if deployed against critical infrastructure, smart electric meters, electric car charging networks etc.

Blackholing

- A countermeasure to mitigate a DDoS attack in which network traffic is routed into a “black hole,” and is lost.
- Both legitimate and malicious network traffic is routed to a null route or black hole and dropped from the network.
- BGP is generally used to facilitate blackholing. This technique is generally more suitable for service providers and very large organisations.

IoT DDOS

- Two categories:
  - IoT under attack, eg:
    - RFID blocking,
    - Wireless jamming
  - IoT as the attacker
    - Command injection
    - Remote code installation
    - Command and control established
    - Bot master is incontrol

IoT – what are they?

- Small form computers, that are embed in many devices:
  - Cameras
  - Medical equipment's
  - Routers
- By 2020 there will 21 billion devices and 250 million will be in cars
- Heterogeneous network
- Interoperable issues
- Security issues with:
  - Integrity
  - Confidentiality
  - Authorisation

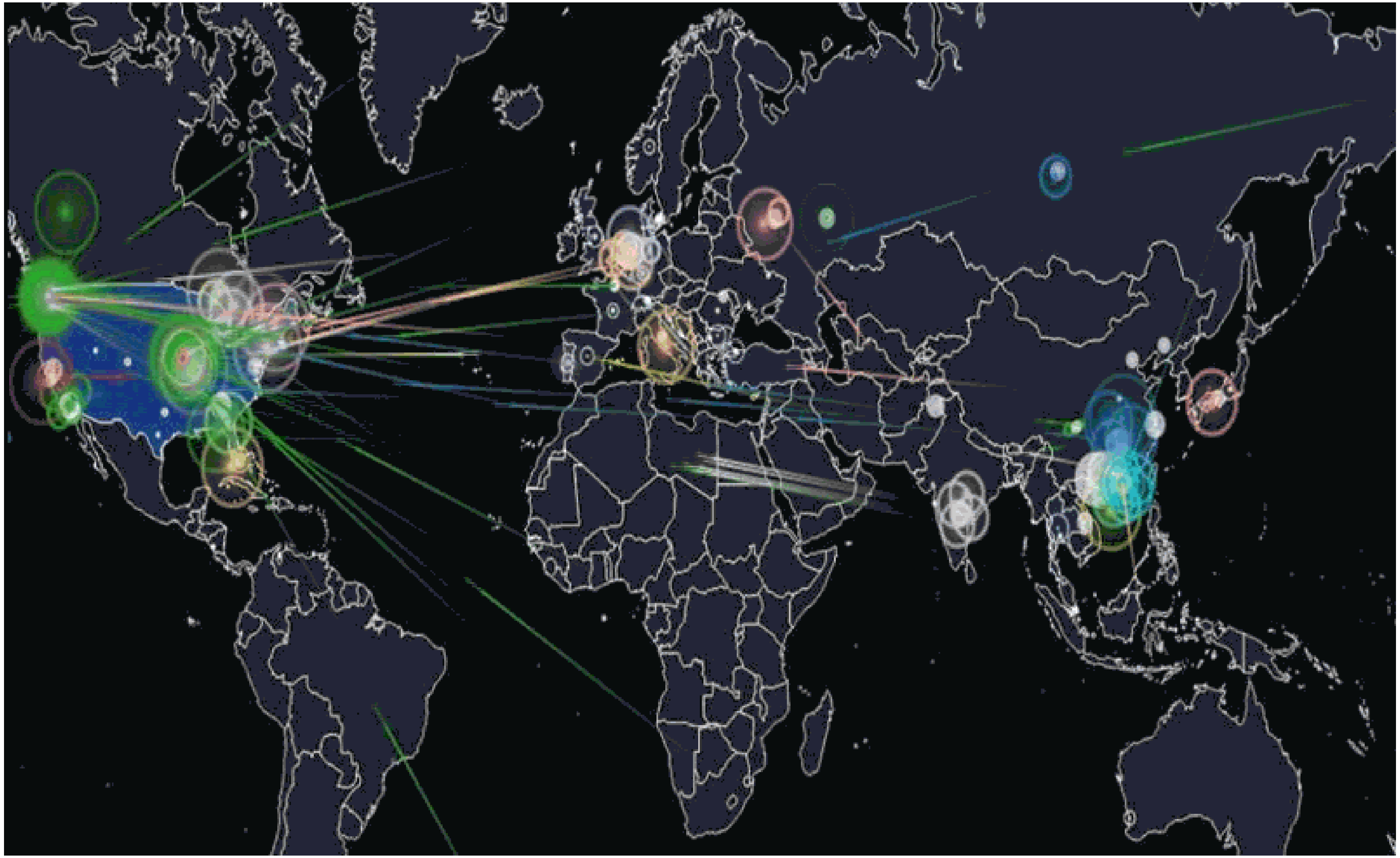
IoT Attacks

- Smart Teddy Bear
  - 800000 users accounts leaked (not so smart)

- CIA and MI5
  - Weeping Angel, Hello Barbie and cloud pets

- Mirai
- Persirai
- Linux MOOSE

Mirai

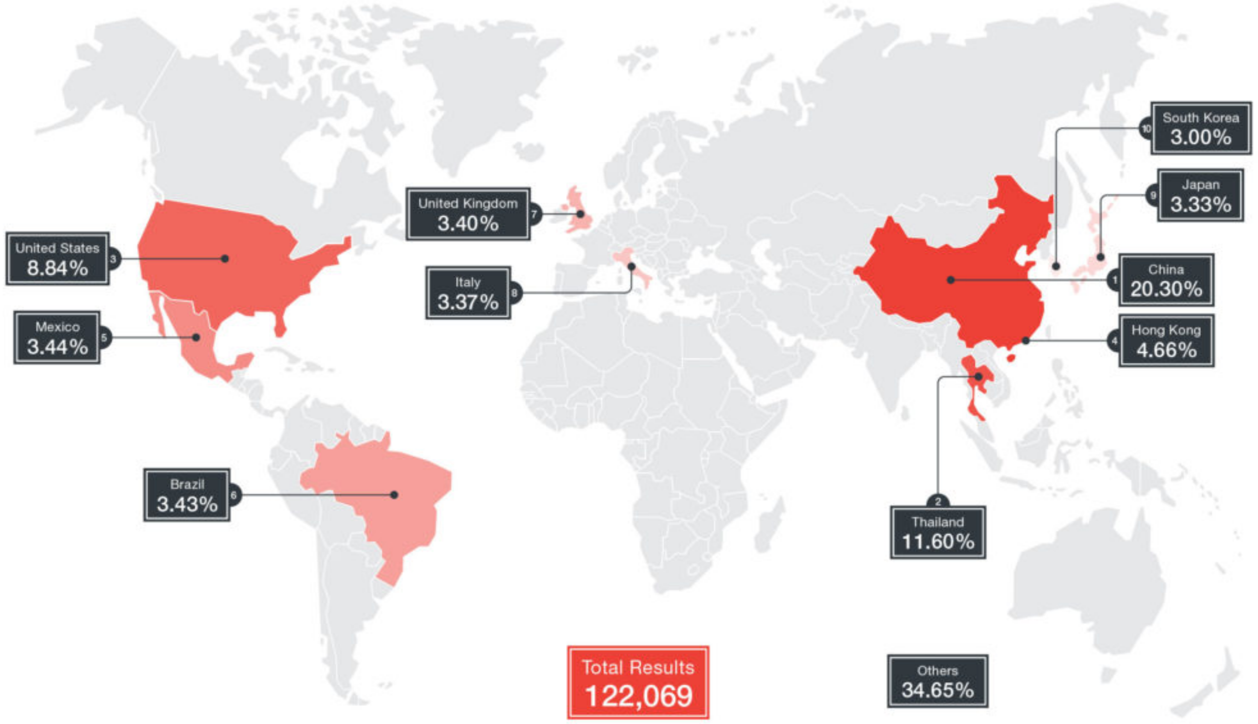


Mirai attack on Dyn

- Friday October 21, 2016 Thousands of DNS look up requests were made by IoT devices
- Over loaded the system and blocked Dyn and their customers
- This knocked out Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter and many others.
- Dyn suffered in the aftermath, where it los over 14,000 domains.

Persirai: IoT Botnet Targets IP Cameras

- May 2017,
- Malware that targeted over 1,000 different models of IP camera
- Trend Micro used shodan to enumerate the number of devices vulnerable to Persirai.
- Persirai can perform User Datagram Protocol (UDP) DDoS attack with SSDP packets without spoofing IP address
- Affected IP cameras plug and play mechanisms
- High visibility
- Easy to access
- 120,000 IP web cameras are vulnerable



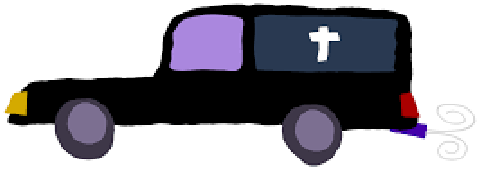
The Future of IoT DDoS Attacks

- Linux MOOSE
  - A family of malware that have monetised IoT Botnets
  - Affects Linux based routers
  - Uses command and Control Centre architecture
  - Steals unencrypted network traffic and passes it to the bot operator
  - Generally used to steal HTTP cookies on social network sites
  - Used in the ego market to create fraudulent actions such as followers, viewers and likes
  - Botnets for hire

IoT DDOS Mitigations

- Patching
- In the case of Mirai, remove the infected device from the network, reboot (because Mirai exists only in dynamic memory) and change the default password.

In 2015 Chrysler Fiat recalled 1.4 million vehicles, following the vehicle hacking exploits



IoT DDOS Mitigations

- Anti Malware for IoT
- Disable plug ang play
- Unique Password for each IoT device
- Change Default Password on first use
- IDS /IPS for IoT M2M network
- Monitor port 2323 and 23 for attempt to gain access
- Standardisation
  - 6lowpan
  - 802.14.5

IoT DDOS Mitigations

- Kirchoff law … Security by Obscurity is no Security at all…

Europol takedown Webstresser.org

- 25 April, 2018: Dutch Police and the UK's National Crime Agency arrested the admins of Webstresser.org and seized the website.
- Europol’s European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) supported the investigation from the onset by facilitating the exchange of information between all partners.
- Webstresser allowed you to rent its services, and those services happen to be an array of Distributed Denial of Service attacks. Six of its admins spread out across, Canada, Croatia, Scotland, and Serbia have all been taken into custody.
- The hardware used has also been seized. The infrastructure was located in the United States, Germany, and the Netherlands.
- Webstresser.org sold Distributed Denial of Service attacks that could knock the internet offline for as little as EUR 15.00 a month

Booters & Stressors

- DDoS as a Service has sprung up

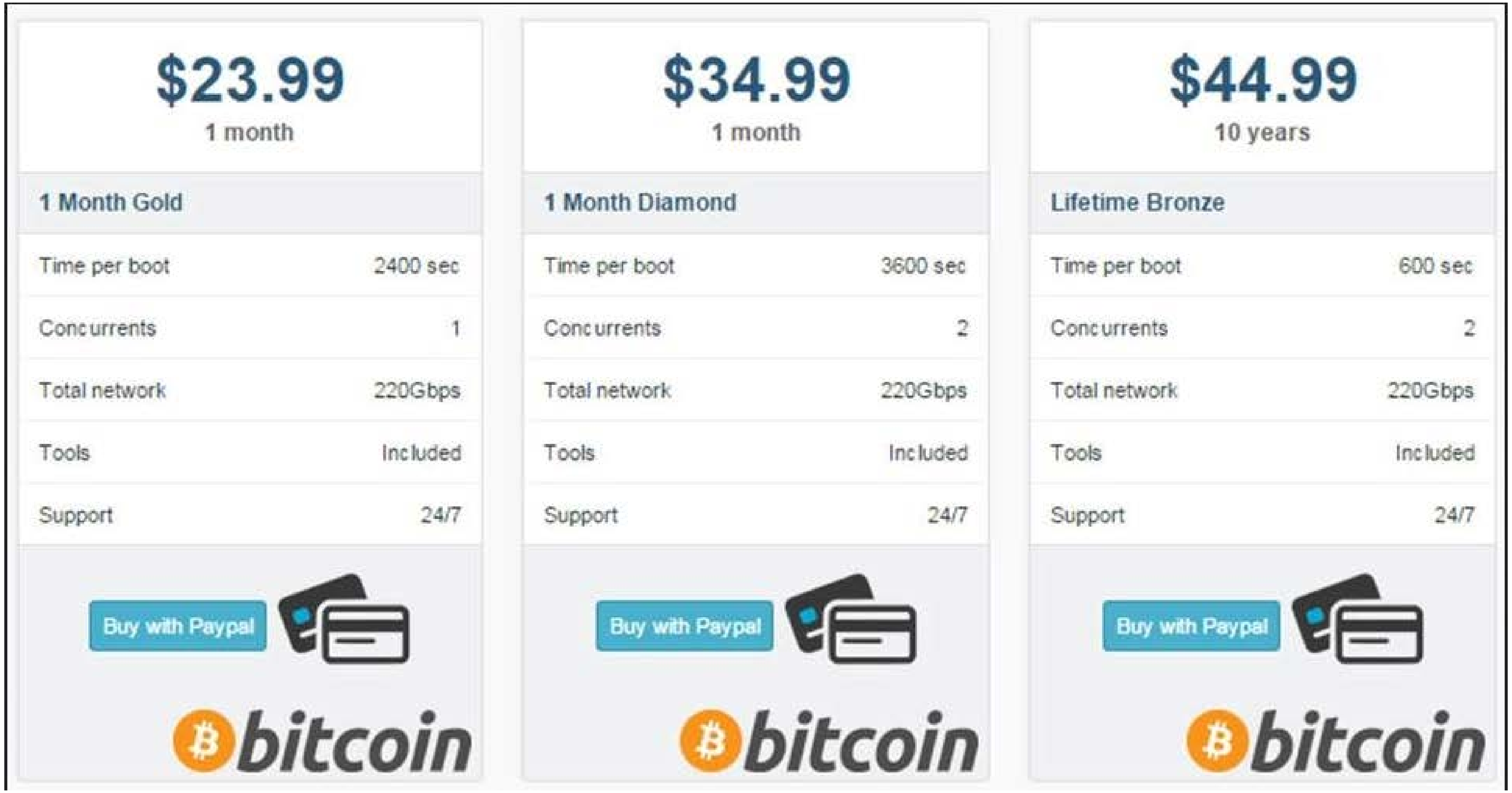
over the last few years.

- These DDoS services are usually selling access to DDoS botnets, which are in turn being “subleased” to subscribers.
- Some DDoS service providers imply their services test the resilience of servers and call themselves “stressers”.
- Others are happy to call themselves Booters or DDoSer’s

DDOS Attacker Motivation

1. Financial / Economic Gain
2. Revenge
3. Idealogical belief
4. Intellectual Challenge
5. Cyberwarfare

Adverts for DDOS Services



$23.99
1 month

1 Month Gold

Time per boot	2400 sec
Concurrents	1
Total network	220Gbps
Tools	Included
Support	24/7

$34.99
1 month

1 Month Diamond

Time per boot	3600 sec
Concurrents	2
Total network	220Gbps
Tools	Included
Support	24/7

$44.99
10 years

Lifetime Bronze

Time per boot	600 sec
Concurrents	2
Total network	220Gbps
Tools	Included
Support	24/7

Takeaway

- Patch everything, regularly.
- Disable UPnP on their routers to prevent devices within the network from opening ports to the external Internet without any warning.
- Website owners optimise your servers, use F5’s or equivalent, use WAFs, cache images, pdf’s etc.
- Disable DNS and NTP to accept queries from anyone on the Internet
- Use the RFC 5635, 3882, 3704 and BCP38 as a guide.
- Block connections from TOR endpoints, if your users have no good reason to connect from them e.g. you are a commerce site

/usr/bin/whoami

Beverley MacKenzie	Scott MacKenzie
20 years in Infrastructure, System Administration, Audit, Compliance & Risk Assessment **Education** MSc: Information Security, Royal Holloway, London University. Presently undertaking a: Ph.D. Cyber Security, Abertay University Research area: Blockchain & IoT **Qualifications** AAT Certified Accountant ISO27001 Lead Auditor	Over 20 years experience across IT & Security covering many flavours of *NIX, Architecture and Engineering. General Technophile. **Education** BSc Chemistry MBA Open University MSc Information Security, Royal Holloway, London University. **Qualifications** ISC2 CISSP Crest Registered Technical Security Architect **Contact** @Cyber_Scott

Internet Standards and RFCs

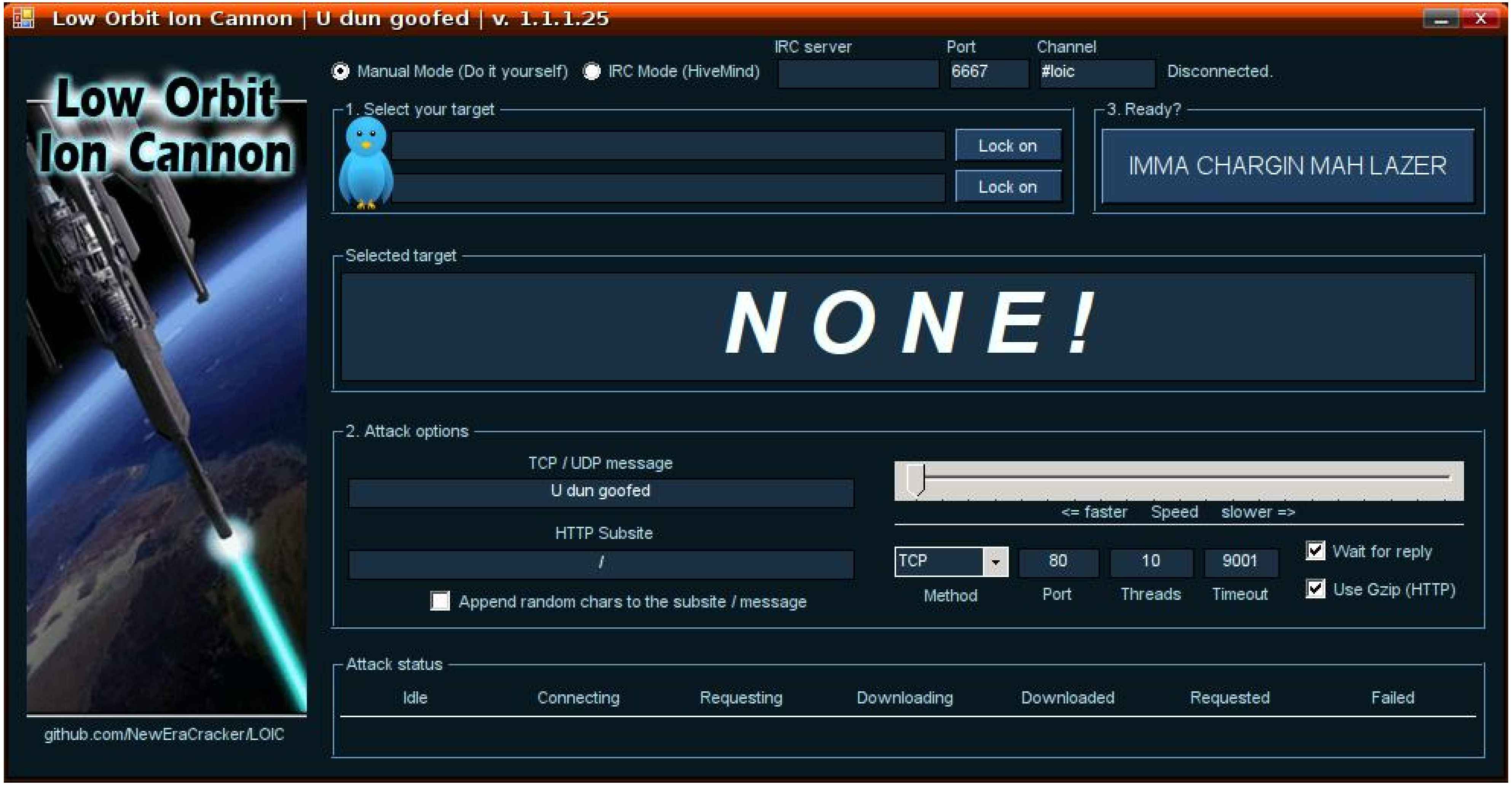
- rfc 5635 - Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)
- rfc 3882 - Configuring BGP to Block Denial-of-Service Attacks
- rfc 3704 - Ingress Filtering for Multihomed Networks
- BCP 38 / rfc 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

A long time ago, in a galaxy far, far away...
I DON'T ALWAYS DDOS
LOLZ
BUT WHEN I DO IT'S SUPER COOL
...DOUCHE
www.Rivalhost.com

SO YOU USED THE LOIC TO TAKE DOWN YOUR HIGH SCHOOL'S WEBSITE?
PLEASE TELL ME ALL OF YOUR PROTIPS
quickmeme.com

DDOS
will you?
DDOS
DDOS

LOIC (Low Orbit Ion Cannon)



Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.25

● Manual Mode (Do it yourself) ○ IRC Mode (HiveMind)

IRC server: Port: 6667 Channel: #loic Disconnected.

1. Select your target

3. Ready?

Selected target: NONE!

2. Attack options

TCP / UDP message: U dun goofed

HTTP Subsite: /

☐ Append random chars to the subsite / message

<= faster Speed slower =>

Method: TCP Port: 80 Threads: 10 Timeout: 9001

☑ Wait for reply

☑ Use Gzip (HTTP)

Attack status

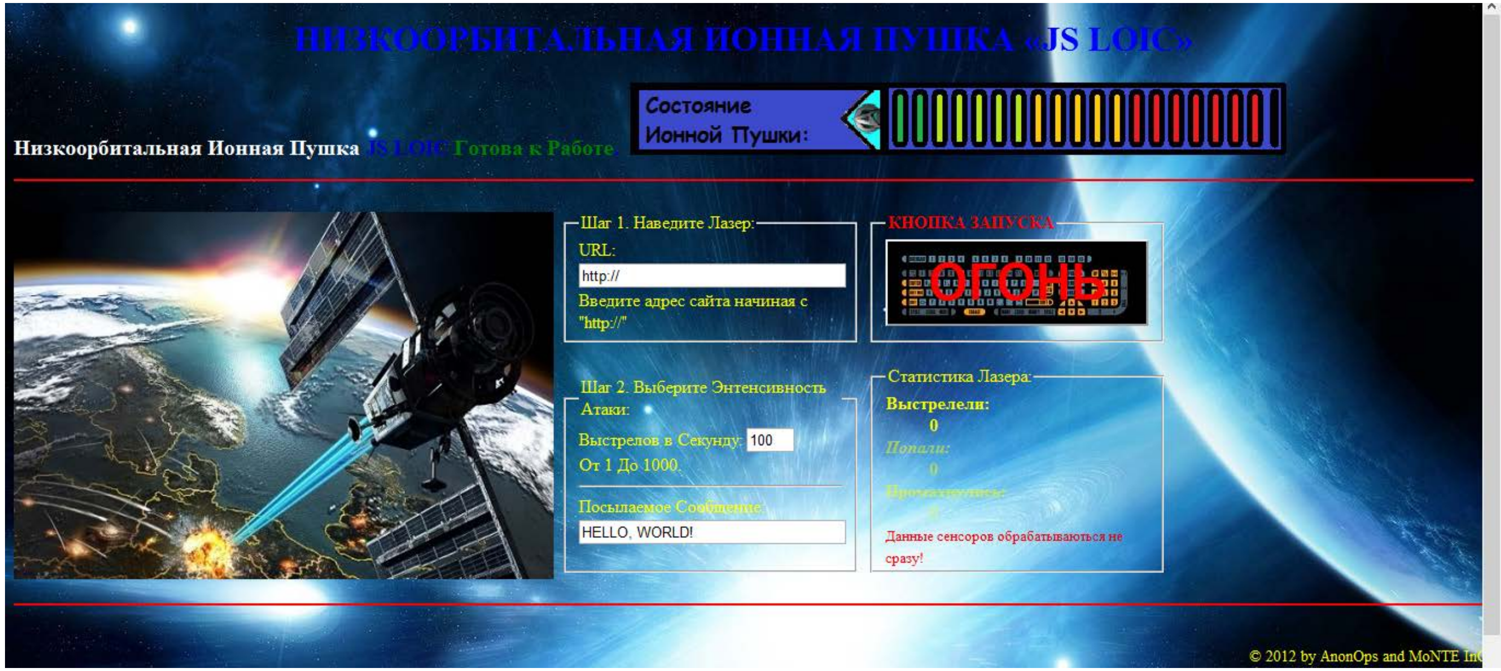
Idle Connecting Requesting Downloading Downloaded Requested Failed

github.com/NewEraCracker/LOIC

LOIC (Low Orbit Ion Cannon)

- In addition to launching DoS attacks, LOIC works well in coordinating large numbers of bots in launching DDoS attacks.

- Also available in other languages
- Became well known due to its use by the Hactivist group Anonymous



НИЗКООРБИТАЛЬНАЯ ИОННАЯ ПУШКА «JS LOIC»

Низкоорбитальная Ионная Пушка JS LOIC Готова к Работе

Состояние Ионной Пушки:

Шаг 1. Наведите Лазер:

URL: http://

Введите адрес сайта начиная с "http://"

КНОПКА ЗАПУСКА

Шаг 2. Выберите Энтенсивность Атаки:

Выстрелов в Секунду: 100

От 1 До 1000.

Посылаемое Сообщение:

HELLO, WORLD!

Статистика Лазера:

Выстрелели:
0

Попали:
0

Промахнулись:
0

Данные сенсоров обрабатываются не сразу!

© 2012 by AnonOps and MoNTE In

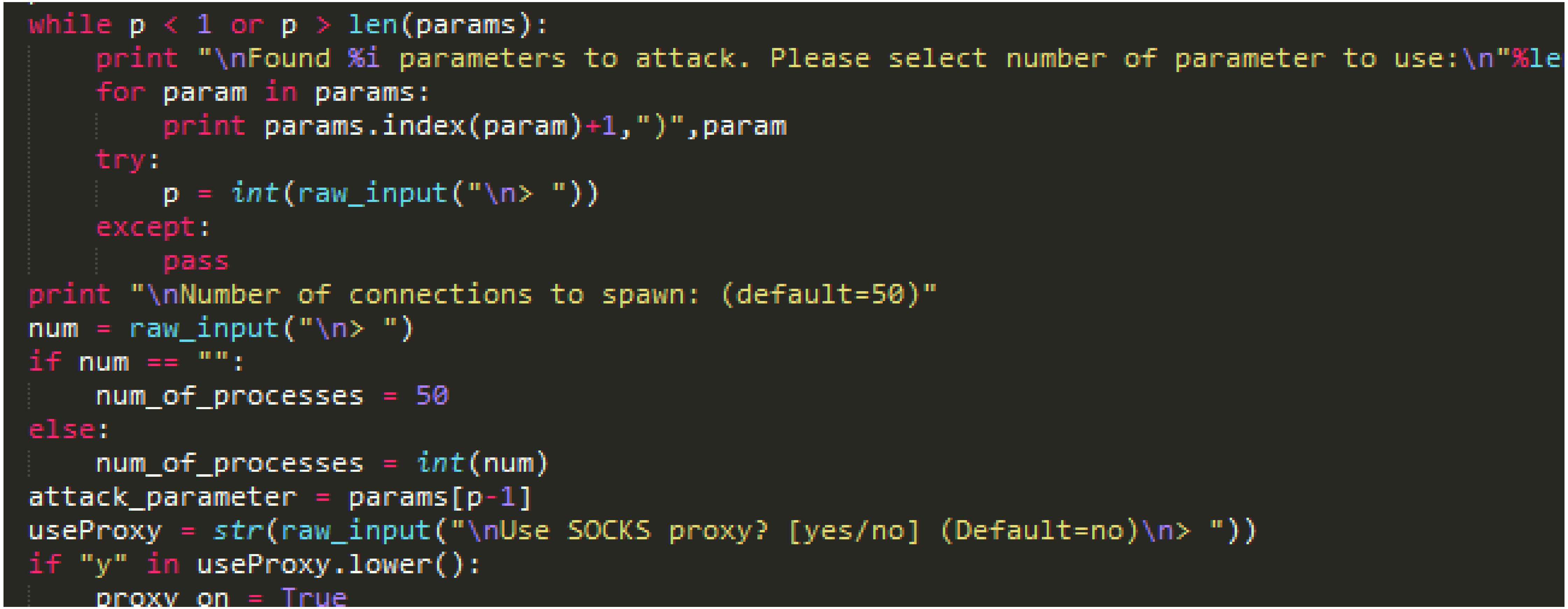
HOIC (High Orbit Ion Cannon)

- This tool was developed to replace LOIC. It offers many of the same advantages of LOIC but adds new features and capabilities. HOIC focuses on DDoS attacks and requires a minimum of 50 bots to launch a scalable attack.

Typical Bottlenecks in DDoS attacks

- The most common failure during a DDoS attack is one of three things:
- The firewall at the front of the network
- The server under attack
- The Internet capacity of the network

RUDY



```
while p < 1 or p > len(params):
    print "\nFound %i parameters to attack. Please select number of parameter to use:\n"%le
    for param in params:
        print params.index(param)+1,")",param
    try:
        p = int(raw_input("\n> "))
    except:
        pass
print "\nNumber of connections to spawn: (default=50)"
num = raw_input("\n> ")
if num == "":
    num_of_processes = 50
else:
    num_of_processes = int(num)
attack_parameter = params[p-1]
useProxy = str(raw_input("\nUse SOCKS proxy? [yes/no] (Default=no)\n> "))
if "y" in useProxy.lower():
    proxy_on = True
```