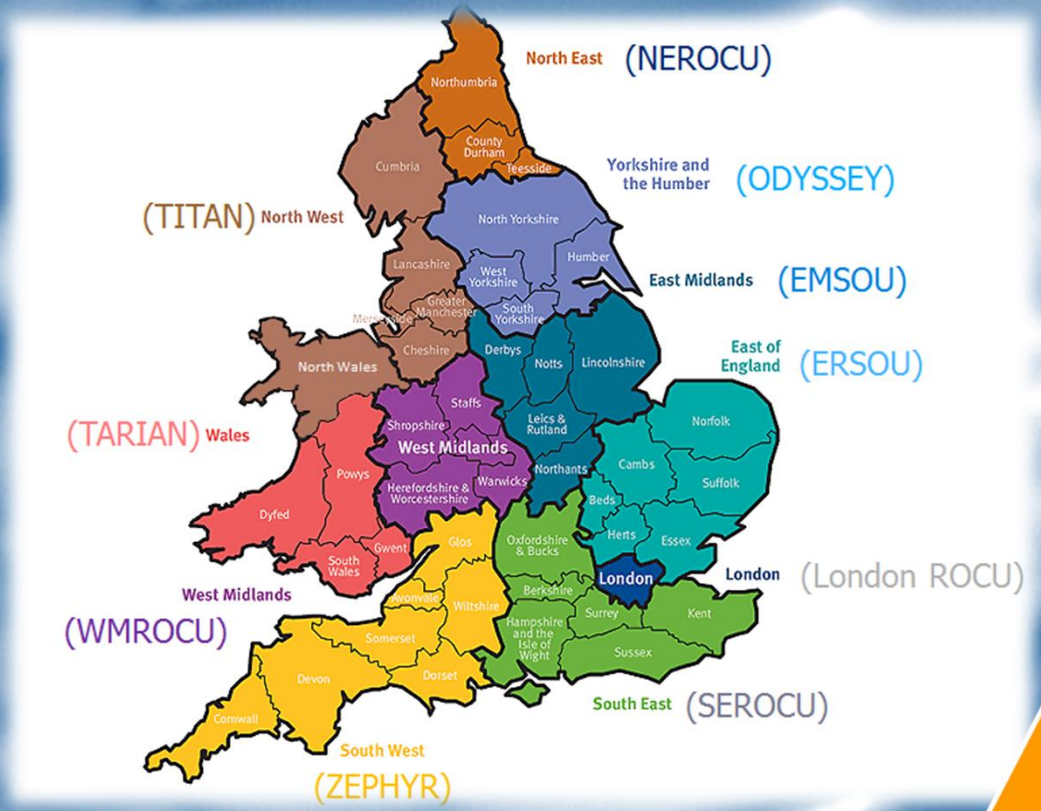
# Operation Polarity


Detective Sergeant

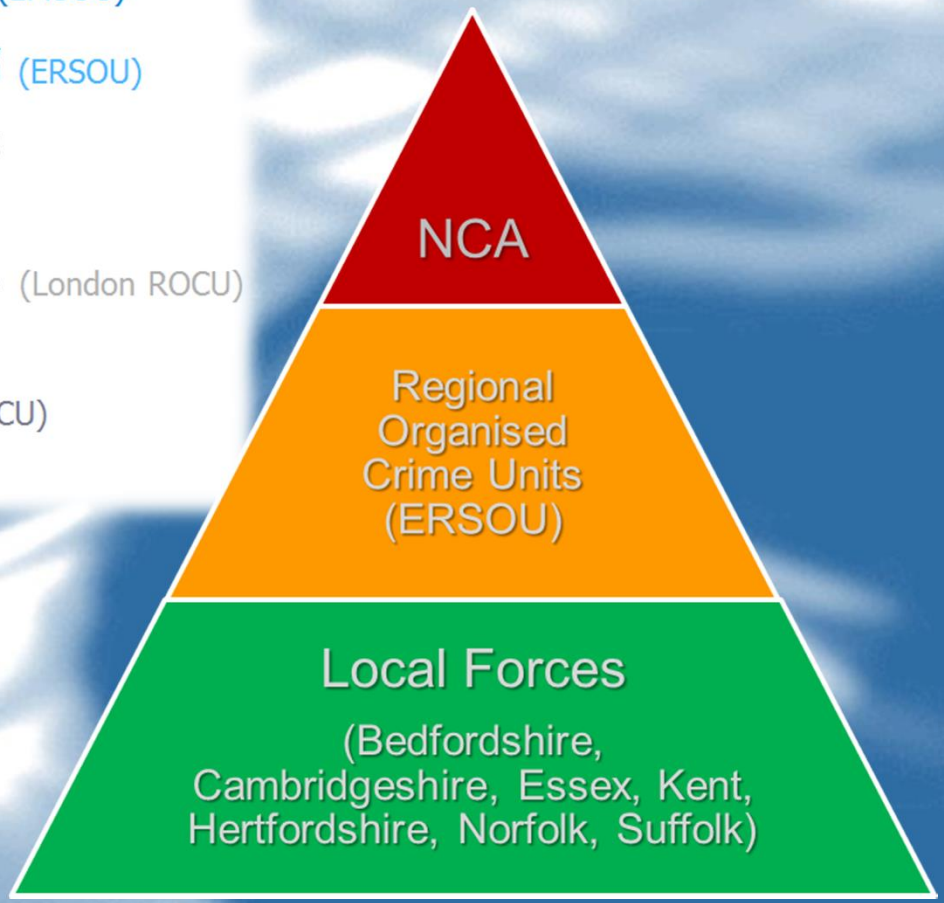
Bart Haley

Eastern Region Cybercrime Unit

# About ERSOU and ROCU's







# Background

Adam Mudd
Bn: 18/11/1996

Address: Kings Langley
Watford, Hertfordshire

Occupation: Computer Student West Herts College

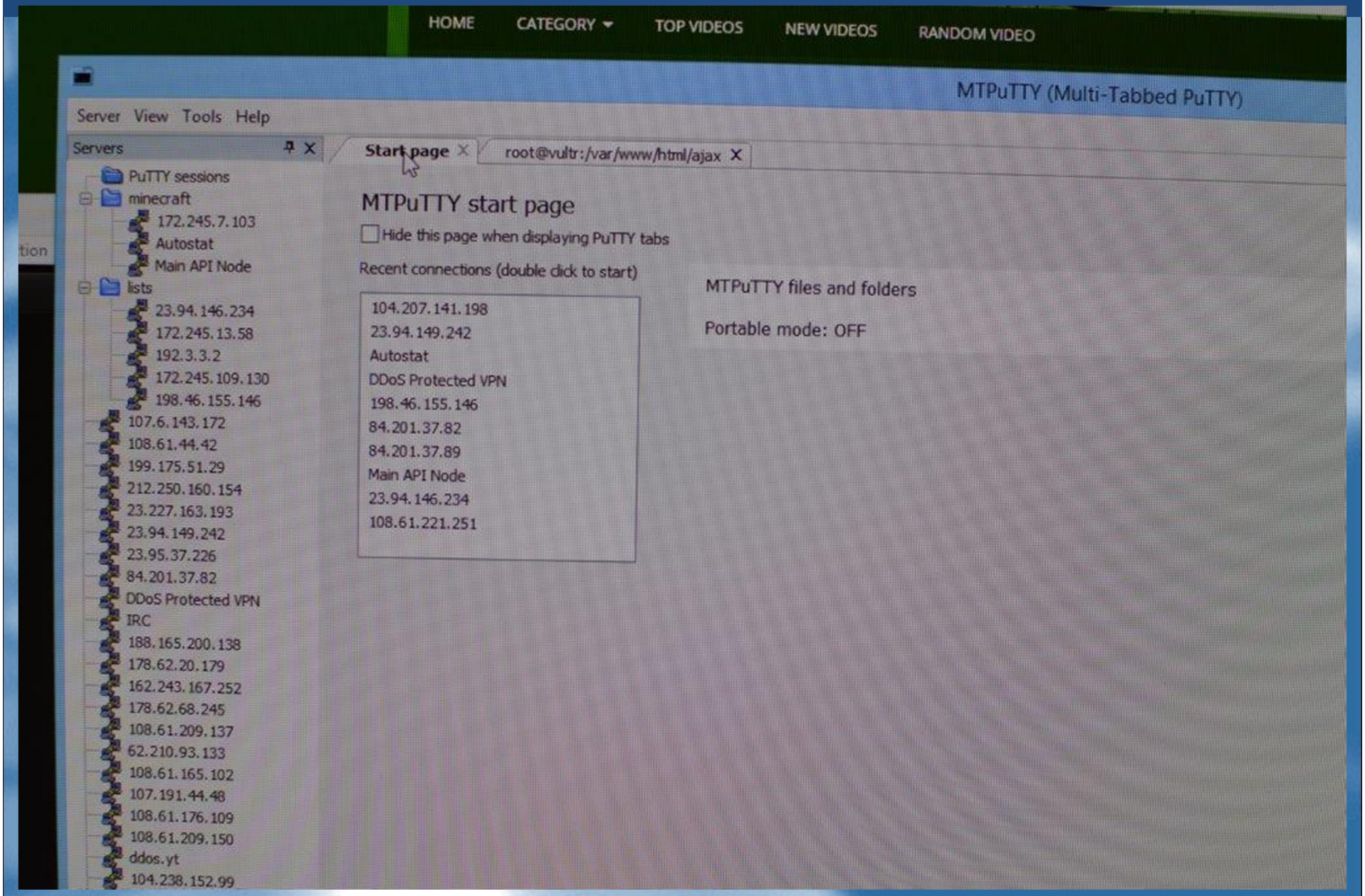
Diagnosed Autistic Spectrum Disorder

# Intelligence Case

- 2014 - Denial of Service Attacks on Lancashire and Cheshire Police.
- Titaniumstresser.net
- Domain Registered to : Joe James
- 20 Wrexham Road
- Fen Street
- Manchester IP22 9JJ
- The registered owner “themuddfamily”
- Search Warrant executed 3rd March 2015

# Scene Management

# Desktop – PuTTY list



# Items seized for examination….

- 26 x Exhibits in total

- Exhibit JAM/04032015 – Computer
- JAM/03032015 – Image of C Drive

- MO/1 – I phone

# Investigation priorities.

enquiries

- Suspect - Custody
- Property/Devices
- Financial

Eastern Region Special Operations Unit

Regional Organised Crime Unit

Eastern Region Special Operations Unit

Regional Organised Crime Unit

NCA
National Crime Agency

PayPal tm

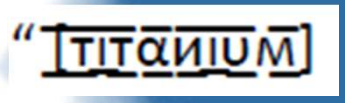
# iPhone 4 - MO/1

XRY – examination

Keyboard Cache – DDoSing, ddos, DDOS, titanhmstress, titaniumbooter

SMS – Bitcoin, Coinbase, LocalBitcoins – values in USD GBP

Emails – numerous back to 2013. Linked to Mudd but recipient name changed over time. Transactions relating to Paypal and from server companies.

Contacts – 7770 on Skype 


83 of these conversations used in evidence.

# Abbreviated examples of Skype conversations

Exhibit GJR/140316/8 (617) – conversation with " NAME " – MUDD is asked whether an IP is visible "when I ddos someone". MUDD replies "No they Can't. It gives hundreds of random IPS"

Exhibit GJR/160316/10 (638) – conversation with "NAME" a potential customer looking to purchase. During the conversation he asks "is this good DDoS?". MUDD replies "yes".

Exhibit GJR/180316/9 (662) – conversation with "NAME" – MUDD takes a complaint and is asked "Hey, someone is using your software to DDoS me.. Just to annoy me, is there any rules about that or is it allowed?" MUDD replies "its allowed".

# Computer – JAM/04042015/3

The computer contained  41 SQL backups of TitaniumStresser.net dating from late 2013 to March 2015.
36 of these contained user information – his clients.

1,738,828 distributed reflective denial of service attacks had been initiated against victims using the Titanium Stresser tool on a worldwide basis. These attacks were directed against 666,532 individual IP addresses or domain names. From the unified database 112,298 usernames are listed.

666,532 IP addresses attacked, 52,836 have been geographically located to the United Kingdom.

# Computer – JAM/04042015/3 - examination

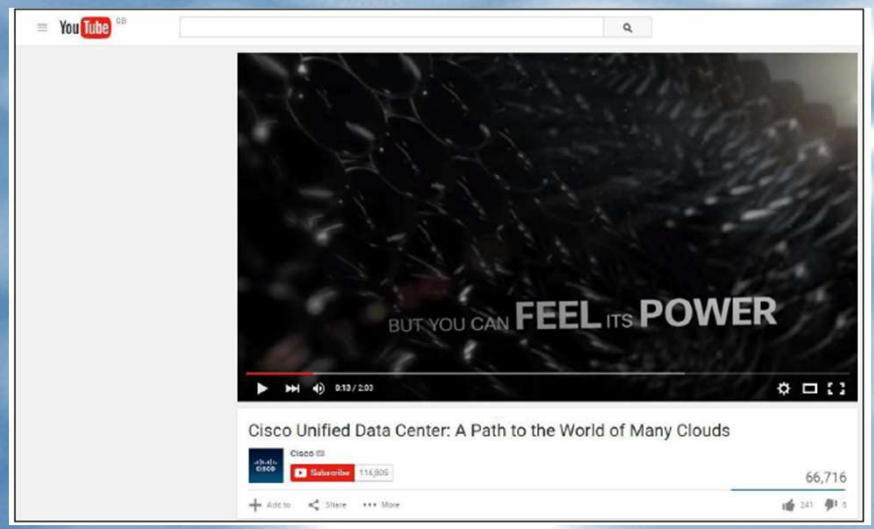
Examination by NCA = 116 page report.

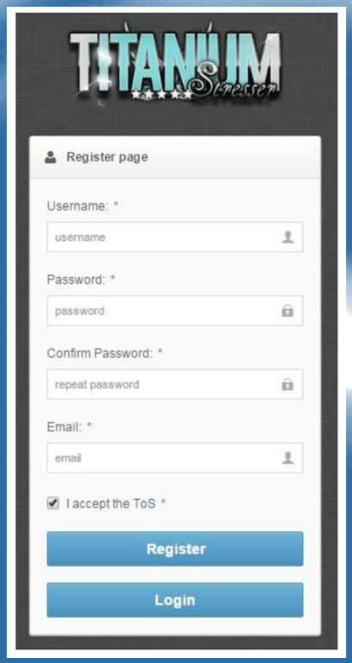
TitaniumStresser.net found to have been hosted on 16 IP addresses from 18th September 2013 until 18th January 2016.

Evidence found in a folder called “titanium” /Users/Adam/Documents/titanium

Website recreated from the code – this linked to a You Tube video of Cisco Systems when visiting the site.

Customers taken through log in or registration process.



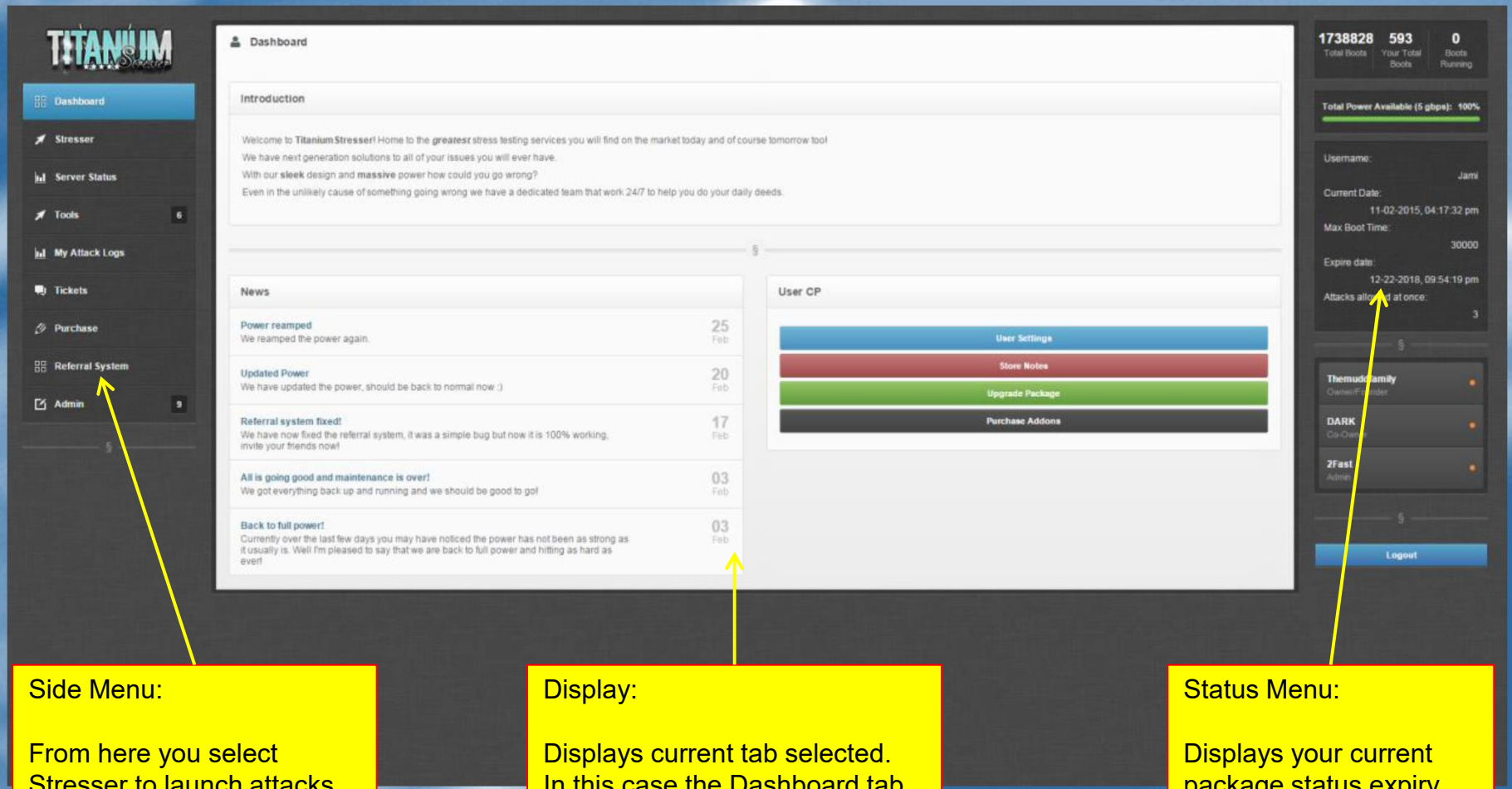



# Titanium subscriptions

Monthly Plans:

| | | |
|---|---|---|
| 100 Seconds \| MONTHLY | $2.99 | PayPal, PaySafecards, Credit Cards & Bitcoin |
| 180 Seconds \| MONTHLY | $4.99 | PayPal & Bitcoin |
| 500 Second \| MONTHLY | $9.99 | PayPal & Bitcoin |
| 1500 Seconds \| MONTHLY | $14.99 | PayPal & Bitcoin |
| 3500 Seconds \| MONTHLY | $19.99 | PayPal & Bitcoin |
| 7200 Second \| MONTHLY | $29.99 | PayPal & Bitcoin |
| 10800 Seconds \| MONTHLY | $49.99 | PayPal & Bitcoin |
| 30k Seconds \| MONTHLY | $69.99 | PayPal & Bitcoin |

# Titanium dashboard




Side Menu:

From here you select Stresser to launch attacks, Tools for variety of tools to assist in tracing an IP and to purchase a package.

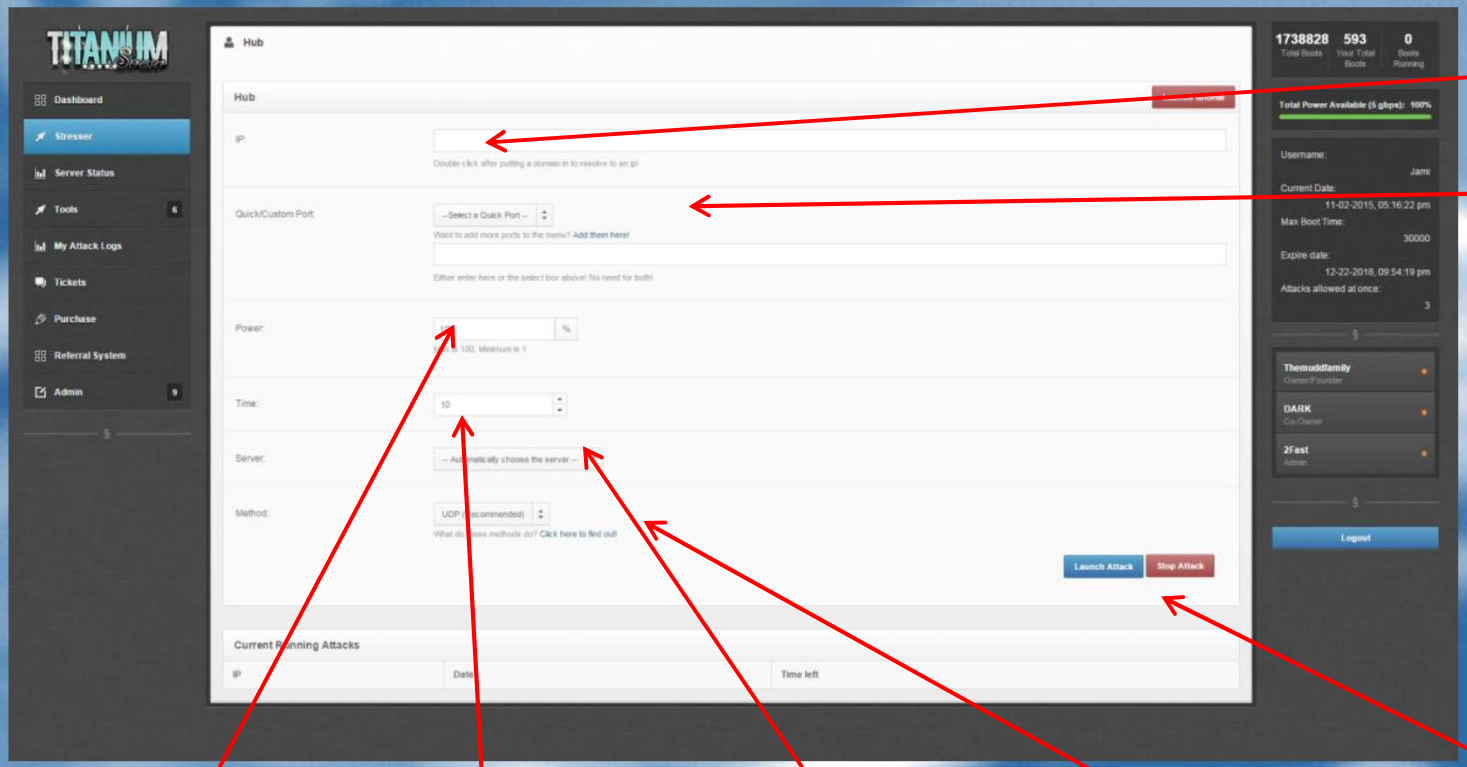
Display:

Displays current tab selected. In this case the Dashboard tab from the side menu is located.

Status Menu:

Displays your current package status expiry date, seconds allowance. Also shows your User details and total attacks carried out.

# Titanium dashboard




IP
You enter the target IP here.

Quick/Custom Port

You enter the "port" that your IP is located on here. Quick ports give popular choices such as Xbox Live, Playstation Network (PSN) and runescape.

Power

As a percentage, defaulted to 100% (true control of power is dictated by number of servers and usage of customers)

Time

Amount of seconds you wish to attack for.

Server

Choose the server you wish to use. (If left Titanium Stresser spread the load over all servers).

Method

There is a drop down tab for Method of attack. It recommends using UDP.

Attack Buttons

Once set up press Launch Attack (blue). Should you wish to halt the attack you press Stop Attack (red).

# Titanium Stresser how it worked.

In a DNS reflection attack the malicious actor (in our case TitaniumStresser.net) executes a large number of DNS queries while spoofing (pretending to be from) the primary IP address of the intended victim.

Used compromised DNS servers (know as open DNS resolvers) responding to the spoofed IP address. Sending a flood of unwanted traffic to the primary IP address of the target. This is amplified by another programme.

This flood of data packets can be a reduction in the quality of service of the internet (slower web traffic), loss of availability of websites, or loss of network resources or services.

# Significant attacks of Titanium Stresser - map

# Victim impact

Wiltshire College

Student purchased Titanium and attacked his college on 20 occasions in 2014. Taking down four college sites.

West Herts College

Mudd attacked the college he attended on four occasions in 2014. One occasion to avoid a an online test. Attack brought down the entire network across the region effecting 70 schools, colleges and Anglian universities including Cambridge.


Owned by JAGEX who spend a large amount of money mitigating such attacks.
The site was attacked over 25,000 times by Titanium.
The cost in January 2015 alone was £184,000.

# Money Laundering-

Transaction value from databases calculated.

Paypal – Unique transaction id's = $157,097 – 16,410 transactions in false names

Bitcoin – received 269.81 (value fluctuates) appx $74,306.00

Paysafe – card numbers = $6,221.15

Other criminality from marketing similar services.

# Further interviews with Police

Interview 1 : 4th March 2015
Prepared statement - designed Titanium to test firewalls T/C's not to be used for DDOS

4 further interviews : 9th September 2015 and 8th June 2016 – started as a legitimate tool to test Minecraft servers but used for DDOS.
Admitted used as DDOS service.
Methods of moving money through Paypal –
Admitted attacking his college.

# Conviction – Guilty plea – Central Criminal Court

BBC Sign in News Sport Weather iPlayer TV Radi

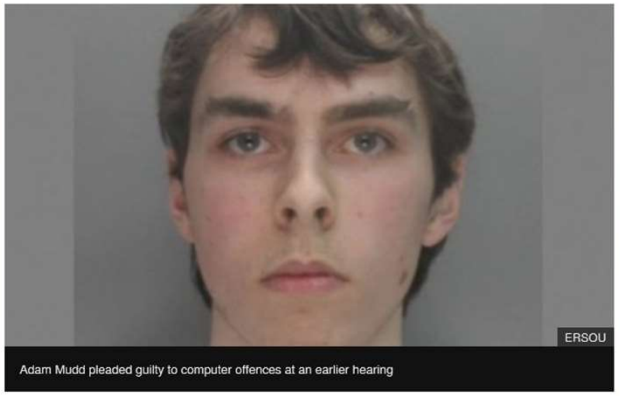
NEWS

Home UK World Business Politics Tech Science Health Education Entertain

England Regions Beds, Herts & Bucks

**Teenage cyber hacker Adam Mudd jailed for global attacks**

25 April 2017 | Beds, Herts & Bucks Share




Adam Mudd pleaded guilty to computer offences at an earlier hearing

A computer hacker has been jailed for two years for masterminding global online attacks as a teenager from his bedroom in Hertfordshire.

Mail Online News

<u>Sentenced Old Bailey 25th April 2017 :</u>

1. Carried out 594 DDOS attacks against 181 IP addresses – sec 3(1) (6) CMA 24 months

2. 1st Sep 13 – 4th Mar 15 supplied T stressor ,738,828 occasions. – sec 3A(5) CMA 9 mths conc

3. Conceal criminal Property 327 POCA 24 mths conc


CAMBRIDGE news

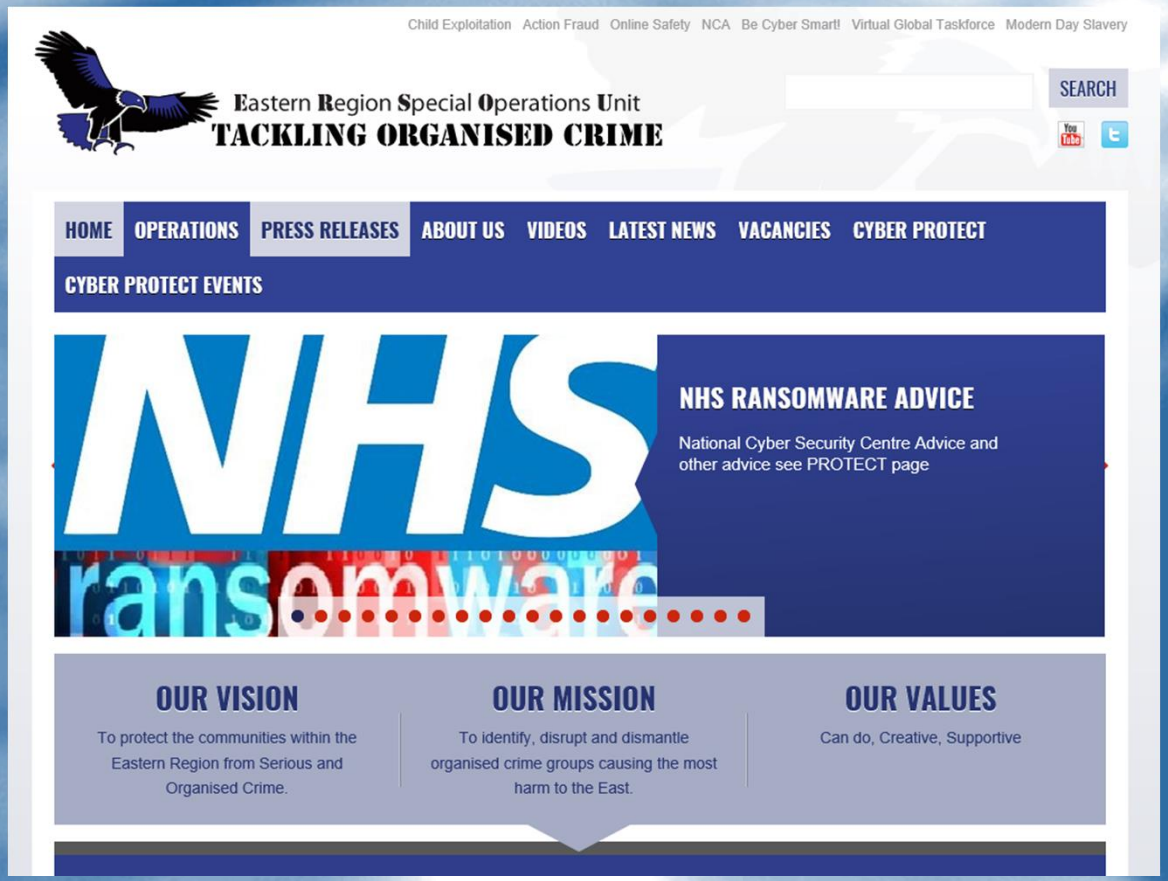
News › Cambridge News › Crime

**The teenage hacker who caused chaos at Cambridge University and cost a city company £6million**

Adam Mudd of King's Langley, Hertfordshire, was 16 when he created a program that earned him £386,000 through hacked

# End

## Any Questions




www.ersourocu.org.uk