AUTHORITIES ACROSS THE WORLD GOING AFTER USERS OF BIGGEST DDOS-FOR-HIRE WEBSITE

28 Jan 2019

Press Release

The takedown by law enforcement in April 2018 of the illegal marketplace webstresser.org as part of Operation Power OFF has given authorities all over Europe and beyond a trove of information about the website's 151 000 registered users. Coordinated by Europol and the Joint Cybercrime Action Taskforce (J-CAT) with the support of the Dutch Politie and the British National Crime Agency, actions are currently underway worldwide to track down the users of these Distributed Denial of Service (DDoS) attacks. webstresser.org is believed to have been the world's biggest marketplace to hire DDoS services, having helped launched over 4 million attacks for as little as € 15.00 a month.

In the United Kingdom a number of webstresser.org users have recently been visited by the police, who have seized over 60 personal electronic devices from them for analysis as part of Operation Power OFF. UK police are also conducting a number of live operations against other DDoS criminals; over 250 users of webstresser.org and other DDoS services will soon face action for the damage they have caused.

The impact of successful DDoS attacks globally was highlighted recently by the sentencing of a 30-year-old hacker to almost three years imprisonment in the UK after being found guilty of carrying out DDoS attacks against Liberia's leading mobile phone and internet company, using rented botnets and stressers before developing his own botnet. At their peak in November 2016, these DDoS attacks crashed the West African country's entire internet access with one attack resulting millions of pounds worth of damage.

In the Netherlands, the police and the prosecutor's office have developed a dedicated project, known as Hack_Right, to deal with young first-time offenders in order to prevent them from going onto more serious crimes. A Dutch user of webstresser.org has already received this alternative sanction.

The countries to join the fight against DDoS attacks are Belgium, Croatia, Denmark, Estonia, France, Germany, Greece, Hungary, Ireland, Lithuania, Portugal, Romania, Slovenia, Sweden, Australia, Colombia, Serbia, Switzerland, Norway and the United States.

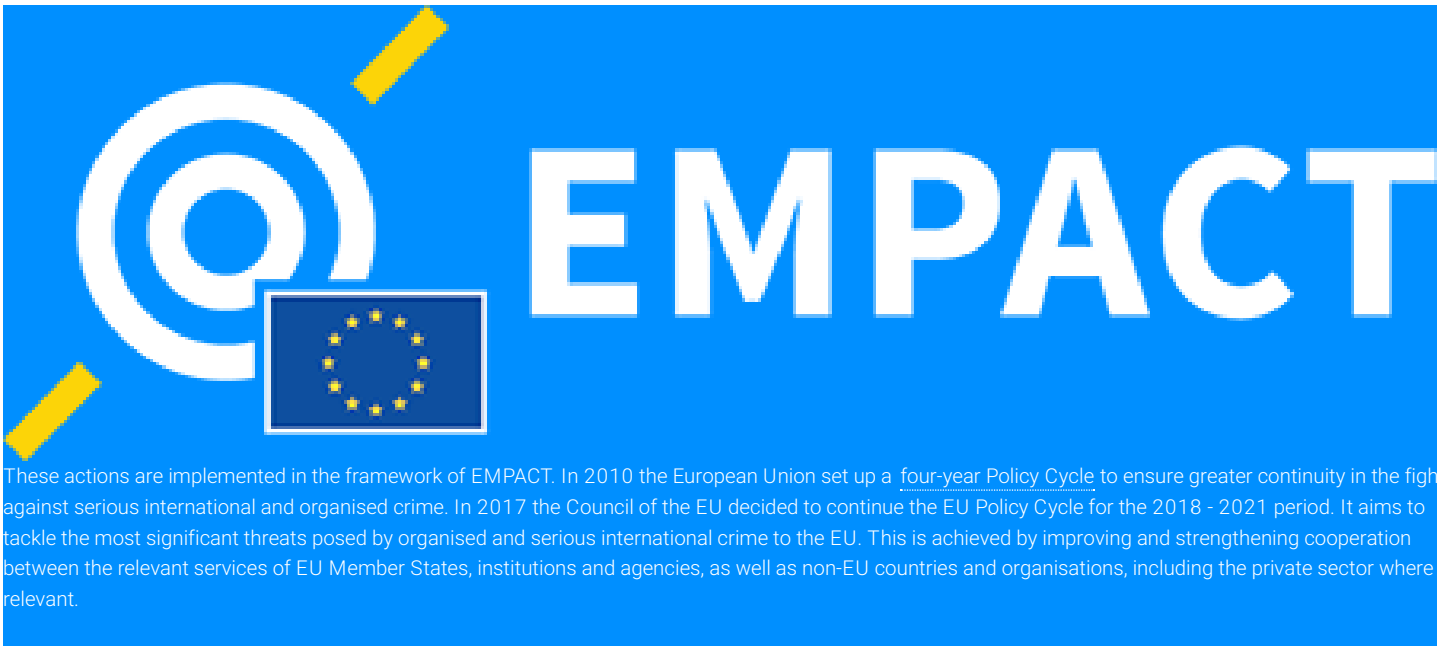
While some are focusing their actions against the users of webstresser.org specifically, law enforcement agencies around the world have intensified their activities against the users of DDoS booter and stresser services more generally. To this effect, the FBI seized last December 15 other DDoS-for-hire websites, including the relatively well known Downthem and Quantum Stresser. Similarly, the Romanian police has taken measures against the administrators of 2 smaller-scale DDoS platforms and has seized digital evidence, including information about the users. Size does not matter – all levels of users are under the radar of law enforcement, be it a gamer booting out the competition out of a game, or a high-level hacker carrying out DDoS attacks against commercial targets for financial gain.

The DDoS-for-hire trend is a pressing issue, mainly due to how easily accessible it has become. Stresser and booter services have effectively lowered the entry barrier into cybercrime: for a small nominal fee, any low-skilled individual can launch DDoS attacks with the click of a button, knocking offline whole websites and networks by barraging them with traffic. The damage they can do to victims can be considerable, crippling businesses financially and depriving people of essential services offered by banks, government institutions and police forces.

Emboldened by a perceived anonymity, many young IT enthusiasts get involved in this seemingly low-level crime, unaware of the consequences that such online activities can carry. Cybercrime isn't a victimless crime and it is taken extremely seriously by law enforcement. The side effects a criminal investigation could have on the lives of these teenagers can be serious, going as far as a prison sentence in some countries.

Skills in coding, gaming, computer programming, cyber security or anything IT-related are in high demand and there are many careers and opportunities available

to use these wisely.



CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES ORGANISATIONS	European Cybercrime Center (EC3)
	Federal Bureau of Investigation (FBI)
SUPPORT & SERVICES	Operational coordination • Operational support • Information exchange • Analysis

---

Source URL: https://www.europol.europa.eu/newsroom/news/authorities-across-world-going-after-users-of-biggest-ddos-for-hire-website