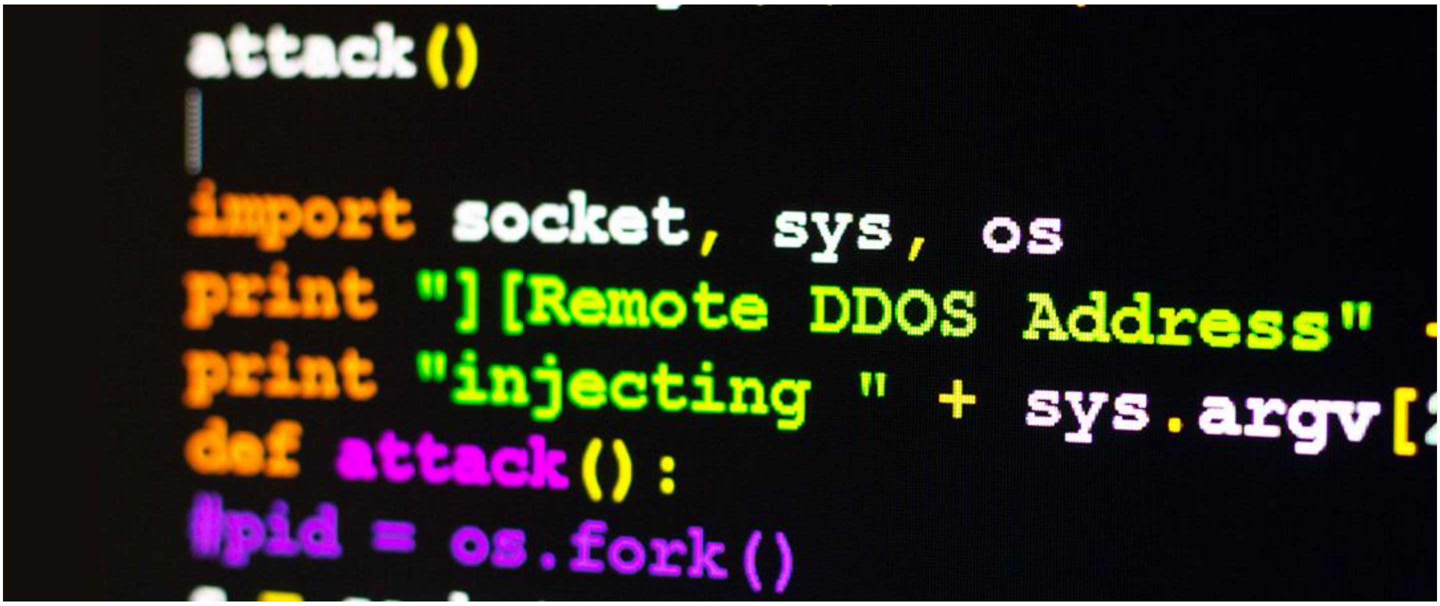
EUROPOL

WORLD'S BIGGEST MARKETPLACE SELLING INTERNET PARALYSING DDOS ATTACKS TAKEN DOWN

25 Apr 2018

Press Release

Webstresser.org sold Distributed Denial of Service attacks that could knock the internet offline for as little as EUR 15.00 a month



```
attack()

import socket, sys, os
print "][Remote DDOS Address"
print "injecting " + sys.argv[
def attack():
#pid = os.fork()
```

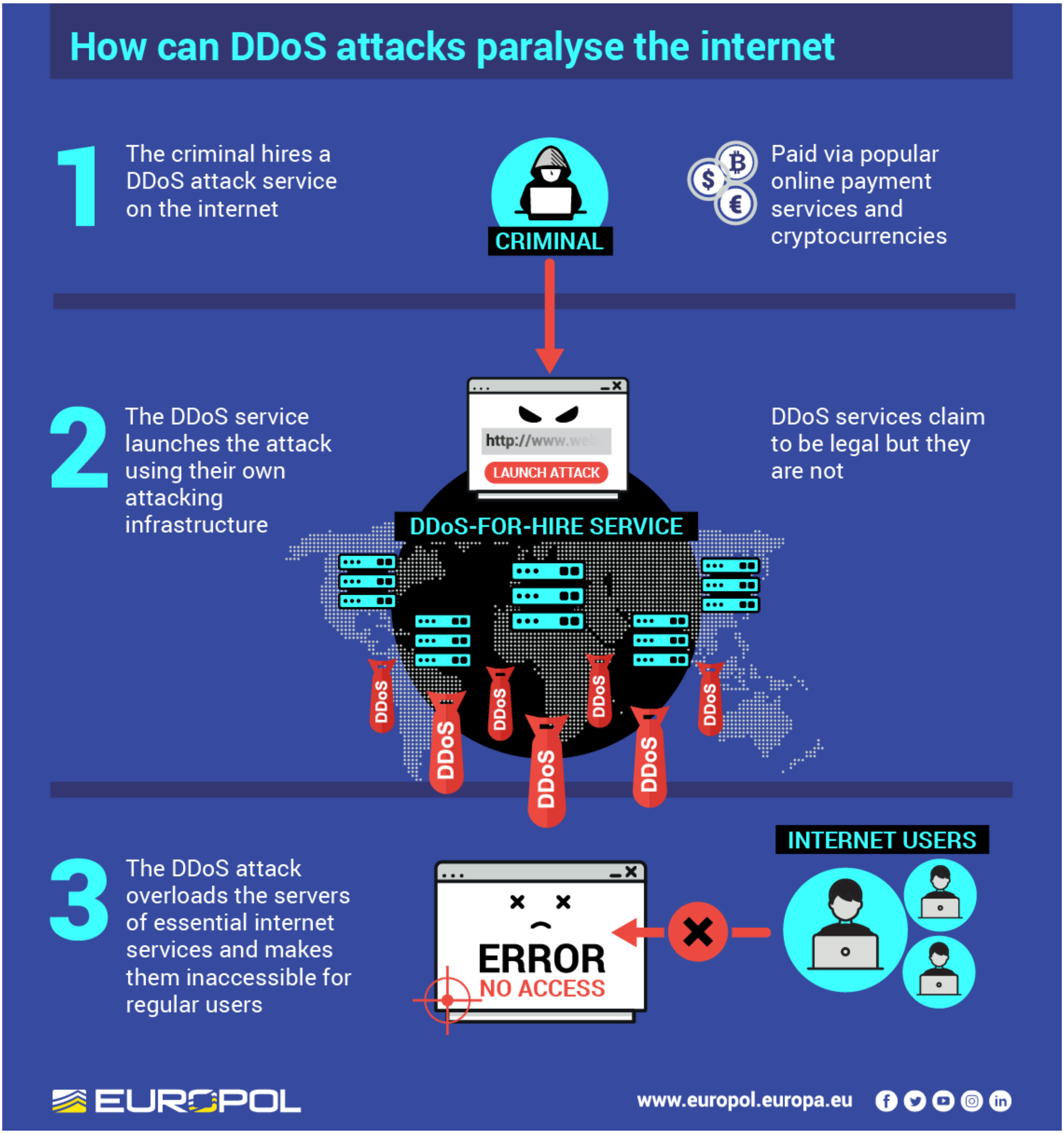
The administrators of the DDoS marketplace *webstresser.org* were arrested on 24 April 2018 as a result of Operation Power Off, a complex investigation led by the Dutch Police and the UK's National Crime Agency with the support of Europol and a dozen law enforcement agencies from around the world. The administrators were located in the United Kingdom, Croatia, Canada and Serbia. Further measures were taken against the top users of this marketplace in the Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada and Hong Kong. The illegal service was shut down and its infrastructure seized in the Netherlands, the US and Germany.

Webstresser.org was considered the world's biggest marketplace to hire Distributed Denial of Service (DDoS) services, with over 136 000 registered users and 4 million attacks measured by April 2018. The orchestrated attacks targeted critical online services offered by banks, government institutions and police forces, as well as victims in the gaming industry.

Devastation for hire

In a DDoS attack enabled by such a service, the attacker remotely controls connected devices to direct a large amount of traffic at a website or an online platform. Whether this traffic eats up the website's bandwidth, overwhelms the server, or consumes other essential resources, the end result of an unmitigated DDoS attack is the same: the victim website is either slowed down past the point of usability, or it's knocked completely offline, depriving users from essential online services.

It used to be that in order to launch a DDoS attack, one had to be pretty well versed in internet technology. That is no longer the case. With *webstresser.org*, any registered user could pay a nominal fee using online payment systems or cryptocurrencies to rent out the use of stressers and booters. Fees on offer were as low as EUR 15.00 a month, thus allowing individuals with little to no technical knowledge to launch crippling DDoS attacks.



How can DDoS attacks paralyse the internet

1 The criminal hires a DDoS attack service on the internet

Paid via popular online payment services and cryptocurrencies

2 The DDoS service launches the attack using their own attacking infrastructure

DDoS services claim to be legal but they are not

3 The DDoS attack overloads the servers of essential internet services and makes them inaccessible for regular users

International law enforcement cyber sweep

International police cooperation was central to the success of this investigation initiated by the Dutch National High Tech Crime Unit and the UK National Crime Agency, as the administrators, users, critical infrastructure and victims were scattered across the world.

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. A command and coordination post was set up at Europol’s headquarters in The Hague on the action day.

"We have a trend where the sophistication of certain professional hackers to provide resources is allowing individuals – and not just experienced ones – to conduct DDoS attacks and other kind of malicious activities online", said Steven Wilson, Head of Europol's European Cybercrime Centre (EC3). "It's a growing problem, and one we take very seriously. Criminals are very good at collaborating, victimising millions of users in a moment form anywhere in the world. We need to collaborate as good as them with our international partners to turn the table on these criminals and shut down their malicious cyberattacks."

"Stresser websites make powerful weapons in the hands of cybercriminals" said Jaap van Oss, Dutch Chairman of the Joint Cybercrime Action Taskforce (J-CAT). "International law enforcement will not tolerate these illegal services and will continue to pursue its admins and users. This joint operation is yet another successful example of the ongoing international effort against these destructive cyberattacks."

DDoS-ing is a crime

DDoS attacks are illegal. Many IT enthusiasts get involved in seemingly low-level fringe cybercrime activities, unaware of the consequences that such crimes carry. The penalties can be severe: if you conduct a DDoS attack, or make, supply or obtain stresser or booter services, you could receive a prison sentence, a fine or both.

The individuals that become involved in cybercrime often have a skill set that could be put to a positive use. 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 anyone with an interest in these areas.

EN How can DDoS attacks paralyse the internet [145.58 KB]

CRIME AREAS Cybercrime • High-Tech crime
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES European Cybercrime Center (EC3) • Joint Cybercrime Action Taskforce (J-CAT)
SUPPORT & SERVICES Operational coordination • Information exchange • Forensics • Analysis • Strategic • Operational

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