INTERNATIONAL ACTION AGAINST DD4BC CYBERCRIMINAL GROUP

12 Jan 2016

Press Release

On 15 and 16 December, law enforcement agencies from Austria, Bosnia and Herzegovina [1], Germany[2] and the United Kingdom[3]joined forces with Europol in the framework of an operation against the cybercriminal group DD4BC (Distributed Denial of Service – DDoS - for Bitcoin).

The action was initiated as part of a global law enforcement response against the criminal organisation. Key members of the organised network were identified in Bosnia and Herzegovina by the UK Metropolitan Police Cyber Crime Unit (MPCCU) which provided vital information to the investigation. Police authorities from Australia, France, Japan, Romania, the USA[4], Switzerland and INTERPOL supported the coordinated activities.

Operation Pleiades resulted in the arrest of a main target and one more suspect detained. Multiple property searches were carried out and an extensive amount of evidence was seized.

The operational activity, initiated by Austria, was supported by Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT). Operational meetings were organised in The Hague to discuss and plan coordinated law enforcement actions against DD4BC. On the action days, Europol deployed a mobile office, allowing direct access to Europol's forensic tools and its databases for cross-checking, analysing and exchanging intelligence in real time.

Distributed Denial of Service (DDoS) attacks remain a considerable threat in the European Union and beyond. This type of extortion attack has become a well-established criminal enterprise and has affected thousands of victims globally, with the number of unreported incidents believed to be much higher. The absence of reporting by private companies and individuals poses particular difficulties in law enforcement's efforts to prosecute these cyber threats.

The DD4BC group is exploiting the increasing popularity of pseudonymous payment mechanisms and has been responsible for several Bitcoin extortion campaigns since mid-2014. DD4BC primarily targeted the online gambling industry, but has recently broadened their activity to the financial services and entertainment sector as well as other high-profile companies. Businesses that pay the ransom to the blackmailers risk appearing vulnerable and being targeted again for a higher amount.

Wil van Gemert, Europol's Deputy Director Operations said, "Law enforcement and its partners have to act now to ensure that the cyberspace affecting nearly every part of our daily life is secure against

new threats posed by malicious groups. These groups employ aggressive measures to silence the victims with the threat of public exposure and reputation damage. Without enhanced reporting mechanisms law enforcement is missing vital means to protect companies and users from recurring cyber-attacks. Police actions such as Operation Pleiades highlight the importance of incident reporting and information sharing between law enforcement agencies and the targets of DDoS and extortion attacks."

Find out how to report cybercrime online in the EU.

[1] Ministry of Interior, Republic of Srpska
[2] Bundeskriminalamt
[3] Metropolitan Police Cyber Crime Unit (MPCCU)
[4] Federal Bureau of Investigation (FBI), US Secret Service (USSS)

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES ORGANISATIONS	European Cybercrime Center (EC3) • Joint Cybercrime Action Taskforce (J-CAT) • Interpol

---