USERS OF REMOTE ACCESS TROJANS ARRESTED IN EU CYBERCRIME OPERATION

20 Nov 2014

Press Release

This week, Europol and several law enforcement and judicial authorities carried out an action against EU citizens, mainly teenagers and young adults, who are suspected of using remote access trojans (RATs) to commit cybercrimes.[1] The action and house searches resulted in the arrest of 15 individuals in several European countries.[2]

The individuals arrested are suspected of misusing remote access trojans to commit various types of cybercrime, which can include theft of personal information, DDoS attacks and extortion. The operation, led by France, took place in the framework of EMPACT - the EU's multi-annual policy cycle - working with Europol's European Cybercrime Centre (EC3) and the involved European authorities. EC3 supported seven countries in their efforts to identify individuals misusing these types of RATs, by hosting two operational coordination meetings, collating intelligence and providing analytical support.

An important aim of this European action is to inform the general public about the threat posed by this type of malware. Examples of some well-known RATs are Blackshades, Poisonivy, and DarkComet. Similar investigations and operations are to be expected next year.

Troels Oerting, Head of the European Cybercrime Centre (EC3), commented on the operation: "Today an alliance of EU law enforcement agencies joined forces to send a strong signal to the criminals using this toxic RAT malware and, at the same time, engage with the predominantly younger individuals involved, to discourage them from pursuing this criminal path. Crimes committed online are sometimes perceived to be 'less serious' by these young offenders as they cannot physically see the victim or the effects of their crimes. Of course this is simply not the case and their criminal activities will not be tolerated in cyberspace."

---

[1] Remote access Trojans are malware that are used to spy on victims' computers (to access personal information, record on-screen activity, record webcam and microphone activity, collect passwords or credit card information). Remote access trojans are different from legitimate 'remote administration tools' that are often used in corporate networks to assist computer users or install software remotely, with the consent and knowledge of the users.

They are often used in serious and organised online crime to collect protected information from

corporate or government networks, but they are also targeted at individuals to defraud the victims using the information collected. However, sometimes the motivation of the criminals is also described as the simple leisure of looking into other people's privacy. In all instances, the use of remote access trojans is an offence in most countries and in all countries of the European Union (illegal computer access, illegal collection of personal data, breach of privacy legislation).

[2] Estonia, France, Romania, Latvia, Italy, United Kingdom.

For further information about Europol, please contact:

Lisanne Kosters, Europol Corporate Communications, +31 70 302 5001

EN How to protect yourself against Remote Access Trojans* and other malware. [934.51 KB]

CRIME AREAS Cybercrime
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
COUNTRIES Estonia • France • Italy • Latvia • Romania • United Kingdom
ENTITIES European Cybercrime Center (EC3)