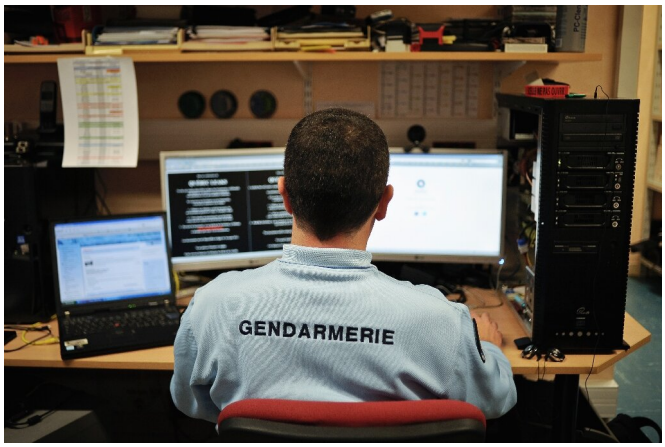
French cyberpolice break up massive 'botnet' ring

28 August 2019



French police said more than 850,000 computers, mainly in Latin America, were being controlled from a server in the Paris region

French police have neutralised a hacking operation that had taken control of more than 850,000 computers, mainly in Latin America, while also managing to remove the malware from the infected devices.

The agents went into action last spring after the Czech antivirus firm Avast alerted them to the software worm, called Retadup, that was being controlled by a server in the Paris region.

The C3N cybercrime unit at the French gendarmerie, which carried out the counterattack with help from the US Federal Bureau of Investigation, called it a "world first" in a statement late Tuesday.

"It's a huge operation" given the number of computers infected, said Gerome Billois, a cybersecurity expert at the French IT services firm Wavestone.

Police first made a copy of the server orchestrating the attack, which allowed them to then hack into it and surreptitiously take control.

They then ordered all the infected computers to uninstall the Retadup malware, which police said was allowing the pirates to create the Monero cryptocurrency.

Retadup is also suspected of being used in several ransomware attacks and data thefts, the gendarmerie said.

"Don't click on links if you're not sure who sent you the email," Colonel Jean-Dominique Nollet, head of the C3N unit, told France Inter radio on Tuesday.

"Don't click on attachments either, and use up-to-date antivirus programmes, even free ones," Nollet said. "And try not to do anything stupid on the internet."

According to Avast, nearly 85 percent of the infected computers did not have antivirus programmes, while others had them but they had been deactivated.