INTERNATIONAL CRACKDOWN ON ANTI-SPYWARE MALWARE

05 Feb 2018

Press Release

A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. This case was investigated by the South West Regional Organised Crime Unit and coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America.

Once installed upon a victim's computer, a user of the Luminosity Link RAT was free to access and view documents, photographs and other files, record all the keystrokes entered and even activate the webcam on the victim's computer – all of which could be done without the victim's knowledge.

These joint actions were carried out back in September 2017, the details of which can now only be released due to operational reasons.

Europol's European Cybercrime Centre (EC3) supported the countries in their efforts to identify EU citizens by providing analytical support and by facilitating information exchange in the framework of the Joint Cybercrime Action Taskforce, hosted at Europol's headquarters in The Hague.

Victims across the world

The investigation uncovered a network of individuals who supported the distribution and use of the RAT across 78 countries and sold it to more than 8 600 buyers via a website dedicated to hacking and the use of criminal malware. Luminosity Link cost as little as EUR 40.00 and required little technical knowledge to be deployed.

Victims are believed to be in the thousands, with investigators having already identified evidence of stolen personal details, passwords, private photographs, video footage and data. Forensic analysis on the large number of computers and internet accounts seized continues.

Steven Wilson, Head of Europol's European Cybercrime Centre, said: "Through such strong, coordinated actions across national boundaries, criminals across the world are finding out that committing crimes remotely offers no protection from arrests. Nobody wants their personal details or photographs of loved ones to be stolen by criminals. We continue to urge everybody to ensure their operating systems and security software are up to date".

Prevention advice

The public and businesses can follow simple steps to help protect themselves from malware, including:

- Update your software, including anti-virus software;
- Install a good firewall;
- Don't open suspicious email attachments or URLs – even if they come from people on your contact list;
- Create strong passwords.

For more prevention advice on how to protect yourself against Remote Access Trojans, check our crime prevention advice.

EN Remote Access Trojans [1.04 MB]

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES	European Cybercrime Center (EC3)
SUPPORT &	Operational coordination • Information exchange • Analysis • Strategic • Operational

---

Source URL: https://www.europol.europa.eu/newsroom/news/international-crackdown-anti-spyware-malware