International crackdown on RAT spyware, which takes total control of victims' PCs

Joint Eurojust-Europol press release

29 November 2019

A hacking tool that was able to give full remote control of a victim's computer to cybercriminals has been taken down as a result of an international law enforcement operation targeting the sellers and users of the Imminent Monitor Remote Access Trojan (IM-RAT).

The investigation, led by the Australian Federal Police (AFP), with international activity coordinated by Eurojust and Europol, resulted in an operation involving numerous judicial and law enforcement agencies in Europe, Colombia and Australia. The seamless cross-border interaction between the various authorities was supported on law enforcement level through the Joint Cybercrime Action Taskforce (J-CAT) and on judicial level through the European Judicial Cybercrime Network (EJCN).

Coordinated law enforcement activity has now ended the availability of this tool, which was used across 124 countries and sold to more than 14 500 buyers. IM-RAT can no longer be used by those who bought it.

Search warrants were executed in Australia and Belgium in June 2019 against the developer and one employee of IM-RAT. Subsquently, an international week of actions was carried out this November, resulting in the takedown of the Imminent Monitor infrastructure and the arrest at this stage of 13 of the most prolific users of this Remote Access Trojan (RAT). Over 430 devices were seized and forensic analysis of the large number of computers and IT equipment seized continues.

Actions were undertaken this week in the framework of this operation in the following countries: Australia, Colombia, Czechia, the Netherlands, Poland, Spain, Sweden and the United Kingdom.

A powerful computer highjacking tool

This insidious RAT, once installed undetected, gave cybercriminals free rein to the victim's machine. The hackers were able to disable anti-virus and anti-malware software, carry out commands such as recording keystrokes, steal data and passwords and watch the victims via their webcams. All that could be done without a victim's knowledge.

This RAT was considered a dangerous threat due to its features, ease of use and low cost. Anyone with the nefarious inclination to spy on victims or

steal personal data could do so for as little as US$25.

Victims are believed to be in the tens of thousands, with investigators having already identified evidence of stolen personal details, passwords, private photographs, video footage and data.

Daniela Buruiana, National Member for Romania at Eurojust and Chair of its Cybercrime Team, said: *'The cybercriminals selling and using the IM-RAT affected the computers of tens of thousands of victims worldwide. We would like to thank all the judicial and law enforcement authorities involved for the excellent results achieved in this operation. These authorities have shown an extremely high level of commitment and legal and technical expertise. Effective cooperation and coordination among all the relevant actors are vital in overcoming the obstacles to investigations due to the global scale and technical sophistication of this type of crime.'*

Steven Wilson, Head of Europol's European Cybercrime Centre (EC3), said: *'We now live in a world where, for just US$25, a cybercriminal halfway across the world can, with just a click of the mouse, access your personal details or photographs of loved ones or even spy on you. The global law enforcement cooperation we have seen in this case is integral to tackling criminal groups who develop such tools. It is also important to remember that some basic steps can prevent you falling victim to such spyware: we continue to urge the public to ensure their operating systems and security software are up to date.'*

Avoiding RAT-ing

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

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

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