PROLIFIC CYBERCRIMINAL SUSPECTED OF SPREADING RANSOMWARE ARRESTED BY POLISH POLICE

17 Mar 2018

Press Release

This week, the Polish Police, in close cooperation with the Belgian Federal Police and Europol, has arrested a Polish national, known online as "Armaged0n", who is suspected of having encrypted several thousands of computers and having committed a series of online attacks on various Polish companies between 2013 and 2018. The detainee will have to answer to 181 charges in court, including money laundering and computer fraud.

The investigation, conducted by the District Prosecutor's Office in Warsaw and the Polish Police National Headquarters, unveiled that the suspect had gone into hiding in Belgium. He was arrested on 14 March 2018 upon trying to enter Poland.

The suspect infected computer systems by spreading ransomware via email pretending to impersonate official correspondence from well-known companies, such as telecommunication providers, retailers, banks, etc. Once installed upon a victim's computer, the ransomware encrypted the files on the infected system, offering a decryption key in return for a ransom payment of USD 200 – 400. The suspect carried out such online campaigns on average every 3 to 4 weeks, and invested the criminal profits into cryptocurrencies.

Alongside spreading ransomware, the suspect also infected computer systems with a virus which

stole bank account login credentials previously copied to the clipboard without the victim's knowledge. The suspect then wired money online to accounts he controlled, subsequently using pre-paid payment cards to cash out the profits.

Europol supported the investigation providing analytical support and by facilitating information exchange between all involved parties. The Polish Police has developed a decryption tool for the ransomware spread by "Armaged0n" and are appealing to people who think they have fallen victim to this online fraudster to seek help at their nearest police station.

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
COUNTRIES	Belgium • Poland
SUPPORT & SERVICES	Operational coordination • Information exchange • Analysis • Strategic

---

Source URL: https://www.europol.europa.eu/newsroom/news/prolific-cybercriminal-suspected-of-spreading-ransomware-arrested-polish-police