Kaspersky Lab welcomes recent law enforcement operation against Carbanak group

“The recent success in the fight against the Carbanak cybercriminal group is very good news for the whole industry and highlights how the exchange of information between countries is especially important in countering cybercrime,” says Sergey Golovanov, Principal Security Researcher in the Global Research & Analysis Team, Kaspersky Lab.

Carbanak is an advanced persistent threat (APT)-like campaign, using targeted attack tools to hit financial institutions around the world for the main purpose of theft.

It was uncovered in 2015 by Kaspersky Lab together with INTERPOL, Europol and a number of other law enforcement authorities based on incident back to 2013. At the time, the group was using a range of tools, including a program called Carbanak. After the publication of Kaspersky Lab’s findings in 2015, the group adapted its tools and started to use Cobalt-strike malware as well as its servers’ names and infrastructure.

The group uses social engineering techniques, such as phishing emails with malicious attachments (for example Word documents with embedded exploits), to target employees in financial institutions of interest. Once a victim is infected, the attackers install a backdoor designed for espionage, data theft and remote management of the infected system, looking for financial transaction systems.

At the time of discovery, Kaspersky Lab researchers estimated that the Carbanak group had stolen up to a $1 billion. Since 2013, the group has hit more than 100 banks, e-payment systems and other financial organizations, in at least 30 countries in Europe, Asia, North and South America, and other regions, stealing more than billions of dollars from victims.

Based on the successful research into Carbanak, in 2016, Kaspersky Lab discovered two groups acting in a very similar way to Carbanak – Metel and GCMAN. They were attacking financial organizations using covert APT-style reconnaissance and customized malware, along with legitimate software and new, innovative schemes to cash out. Other actors have also implemented Carbanak-like techniques, tactics and procedures, for instance Lazarus and Silence.

Given the international scale of these actors’ activities, we believe that there are dozens of people involved in this cybercrime activity. Discovered artefacts in the malicious files and victims’ computers suggest that the creators of the Carbanak malware are Russian-speaking. Although, to perform cybercriminal activities in each country the group generally also looked for a native speaker.