Ransomware Gang Arrested for Spreading Locky to Hospitals

By Tara Seals

Published: 2020-05-18 · Archived: 2026-04-05 13:43:47 UTC

A group of four people calling themselves “Pentaguard” were arrested in house raids.

A cybercriminal gang have been arrested for spreading the Locky ransomware among hospitals, among other crimes.

In an operation spearheaded by Romania’s law enforcement department, four people have been taken into custody after their houses were raided – three in Romania and one in neighboring Moldova.

Prosecutors at the Directorate for Investigating Organized Crime and Terrorism (DIICOT) are charging the group with illegal operations with computer devices and programs, illegal access to a computer system, alteration of computer data integrity and computer forgery.

According to a media statement from DIICOT [translated with Google Translate], the crime group formed at the beginning of the year, calling themselves “Pentaguard.”

There were two prongs of their operation. First, they used SQL injection to compromise and deface websites, targeting websites operated by “several public institutions (institutions of central and local public administration, government) and private (financial-banking, cultural, education, etc.), in Romania and the Republic of Moldova.”

Secondly, they distributed ransomware like Locky to carry out extortion campaigns; and they spread remote access trojans (RATs) to help them steal data. These attacks were directed against several public institutions both in Bucharest and elsewhere, and more were planned.

“The information we have obtained so far showed that they intended to launch attacks, including ransomware attacks, in the near future, on some public health institutions in Romania (generally hospitals),” according to the release. They used “social engineering by sending a malicious executable application, from the ‘Locky’ or ‘BadRabbit’ (computer virus) families, hidden in an e-mail and in the form of a file that apparently would come from other government institutions, regarding the threat of COVID-19.”

The infamous Maze ransomware group and others said that they would back off amidst the coronavirus pandemic – before coming back in that sector with a vengeance. Overall, healthcare organizations of all stripes continue to be attacked.

For instance, in April, the Clop ransomware group attacked biopharmaceutical company ExecuPharm and leaked “select corporate and personnel information” on underground forums in what’s known as a double-extortion attack. ExecuPharm, a Pennsylvania-based subsidiary of the U.S. biopharmaceutical giant Parexel, provides

clinical trial management tools for biopharmaceutical companies. The attack was initiated through phishing emails that were sent to ExecuPharm employees.

“Through this type of attack, there is the possibility of blocking and severely disrupting the functioning of the IT infrastructure of those hospitals, part of the health system, which plays a decisive and decisive role at this time, to combat the pandemic with the new coronavirus,” said Romanian officials.
