European police, FBI bust international cybercrime gang

March 6 2023, by Frank Jordans

German police said Monday they have disrupted a ransomware cybercrime gang tied to Russia that has been blackmailing large companies and institutions for years, raking in millions of euros.

Working with law enforcement partners including Europol, the FBI and authorities in Ukraine, police in Duesseldorf said they were able to identify 11 individuals linked to a group that has operated in various guises since at least 2010.

The gang allegedly behind the ransomware, known as DoppelPaymer, appears tied to Evil Corp, a Russia-based syndicate engaged in online bank theft well before ransomware became a global scourge.

Among its most prominent victims were Britain's National Health Service and Duesseldorf University Hospital, whose computers were infected with DoppelPaymer in 2020. A woman who needed urgent treatment died after she had to be taken to another city for treatment.

Ransomware is the world's most disruptive cybercrime. Gangs mostly based in Russia break into networks and steal sensitive information before activating malware that scrambles data. The criminals demand payment in exchange for decryption keys and a promise not to dump the stolen data online.

In a 2020 alert, the FBI said DoppelPaymer had been used since late 2019 to target critical industries worldwide including healthcare,

emergency services and education, with six- and seven-figure ransoms routinely demanded.

An analyst with the cybersecurity firm Emsisoft, Brett Callow, said DoppelPaymer has published data stolen from about 200 companies, including in the U.S. defense sector, which resisted payment. And given DoppelPaymer's suspected connection through Evil Corp to the FSB—the successor to Russia's KGB spy agency—"the bust could provide law enforcement with some exceptionally valuable intel," he said.

Dirk Kunze, who heads the cybercrime department with North Rhine-Westphalia state police, said at least 601 victims have been identified worldwide, including 37 in Germany. Europol said victims in the United States paid out at least 40 million euros ($42.5 million) to the gang between May 2019 and March 2021 to release important data that was electronically locked using the malware.

The group specialized in "big game hunting," said Kunze, and ran a professional recruitment operation, luring new members with the promise of paid vacation and asking applicants to submit references for past cybercrimes.

He said police conducted simultaneous raids in Germany and Ukraine on Feb. 28, seizing evidence and detaining several suspects.

Three further suspects couldn't be apprehended as they were beyond the reach of European law enforcement, Kunze said.

German police identified the fugitives as Russian citizens Igor Turashev, 41, and Irina Zemlyanikina, 36, and 31-year-old Igor Garshin, who was born in Russia but whose nationality wasn't immediately known.

Turashev is wanted by U.S. authorities since late 2019 in connection with cyberattacks carried out using a predecessor to DoppelPaymer, known as BitPaymer, that is linked to Evil Corp. The U.S. government offered a $5 million reward in 2019 for information leading to the capture of its alleged leader, Maxim Yakubets.