

Police arrest Conti and LockBit ransomware crypter specialist

By Bill Toulas

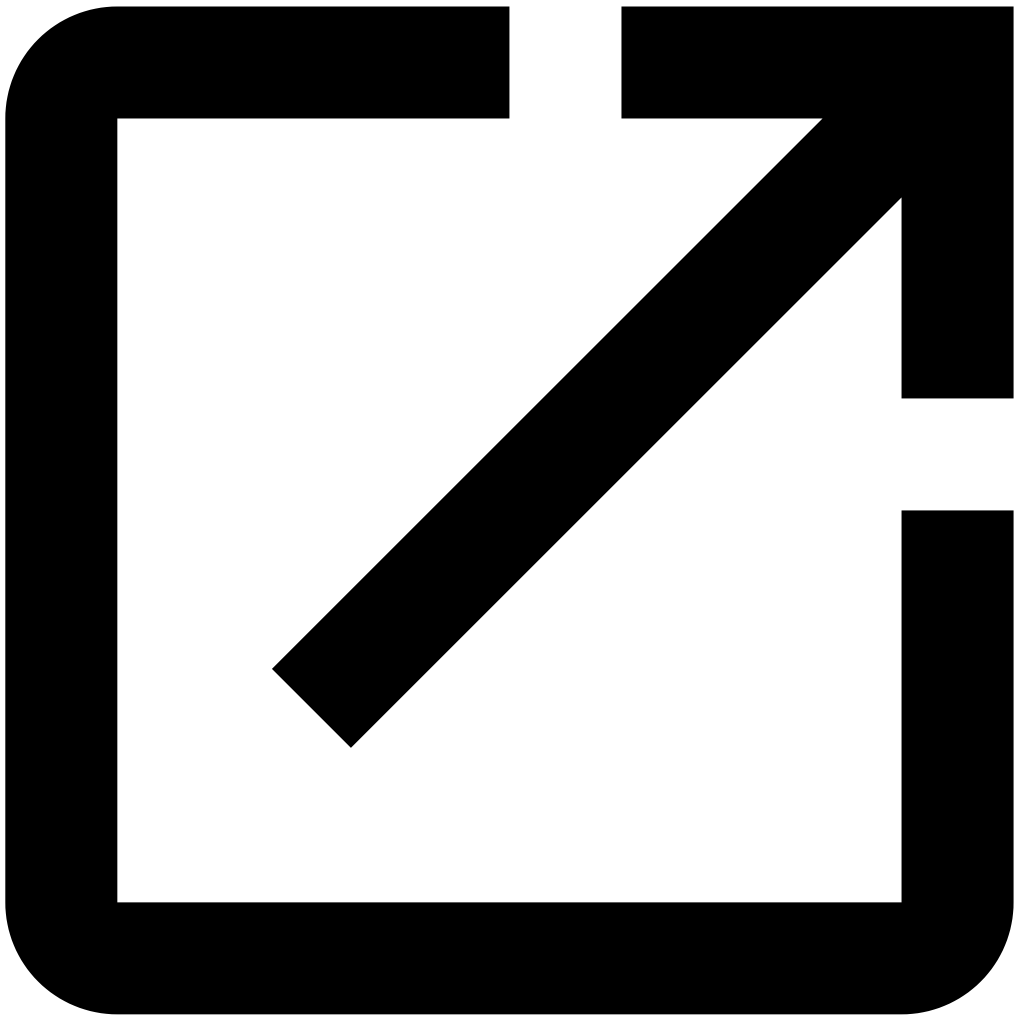
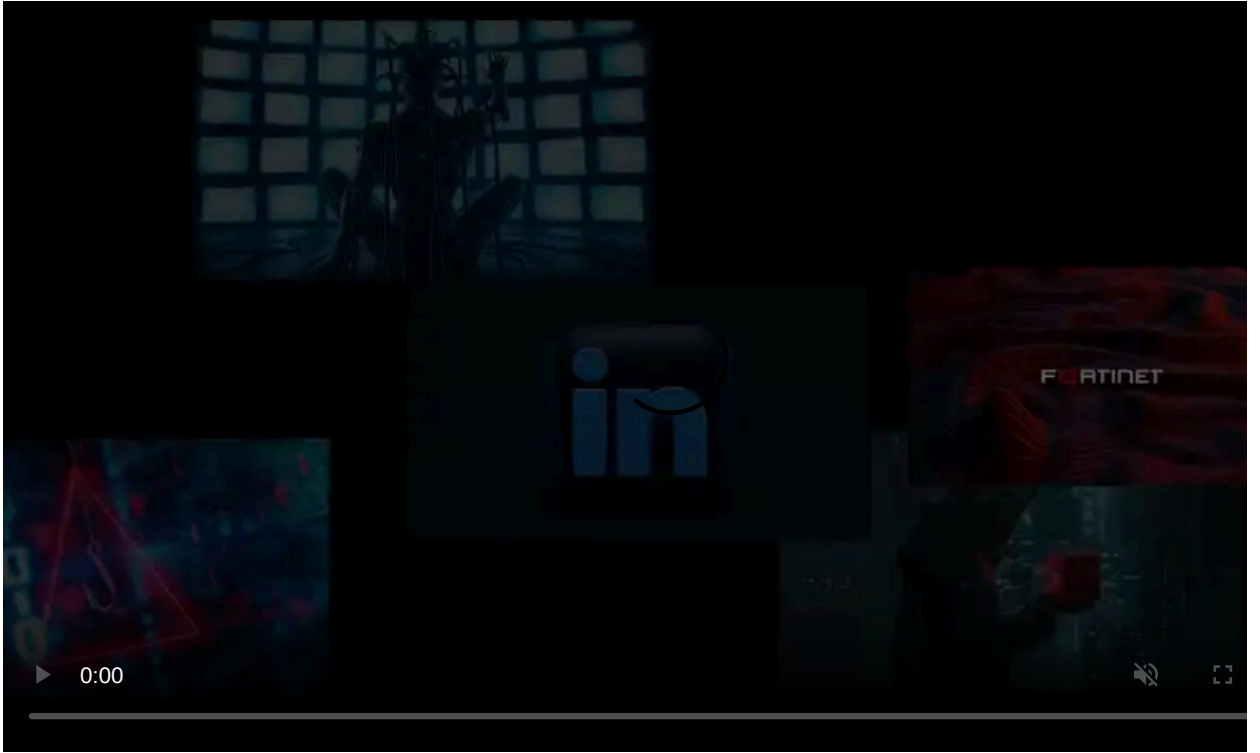
Published: 2024-06-12 · Archived: 2026-04-05 19:17:45 UTC



The Ukraine cyber police have arrested a 28-year-old Russian man in Kyiv for working with Conti and LockBit ransomware operations to make their malware undetectable by antivirus software and conducting at least one attack himself.

The investigation was backed by information shared by the Dutch police who responded to a ransomware attack on a Dutch multinational, followed by data-theft extortion.

The man was arrested on April 18, 2024, as part of the '[Operation Endgame](#)' law enforcement operation that took down various botnets and their main operators.



Visit Advertiser website [GO TO PAGE](#)

As the Conti ransomware group used some of those botnets for initial access on breached endpoints, evidence led investigators to the Russian hacker.

The Ukrainian police reported that the arrested individual was a specialist in developing custom crypters for packing the ransomware payloads into what appeared as safe files, making them FUD (fully undetectable) to evade detection by the popular antivirus products.

The police found that the man was selling his crypting services to both the Conti and LockBit cybercrime syndicates, helping them significantly increase their chances of success on breached networks.

The [Dutch police confirmed](#) at least one case of the arrested individual orchestrating a ransomware attack in 2021, using a Conti payload, so he also operated as an affiliate for maximum profit.

"As part of the pre-trial investigation, police, together with patrol officers of the special unit "TacTeam" of the TOR DPP battalion, conducted a search in Kyiv," reads the Ukraine [police announcement](#).

"Additionally, at the international request of law enforcement agencies in the Netherlands, a search was conducted in the Kharkiv region."



As a result of these searches, computer equipment, mobile phones, and handwritten notes were seized for further examination.

The investigation into the programmer's activities and precise involvement in the Conti and LockBit attacks is currently underway.

The suspect has already been charged with Part 5 of Article 361 of the Criminal Code of Ukraine (Unauthorized interference in the work of information, electronic communication, information and communication systems, electronic communication networks) and faces up to 15 years imprisonment.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/police-arrest-conti-and-lockbit-ransomware-crypter-specialist/>