Global IT services provider Inetum hit by ransomware attack

By Ionut Ilascu

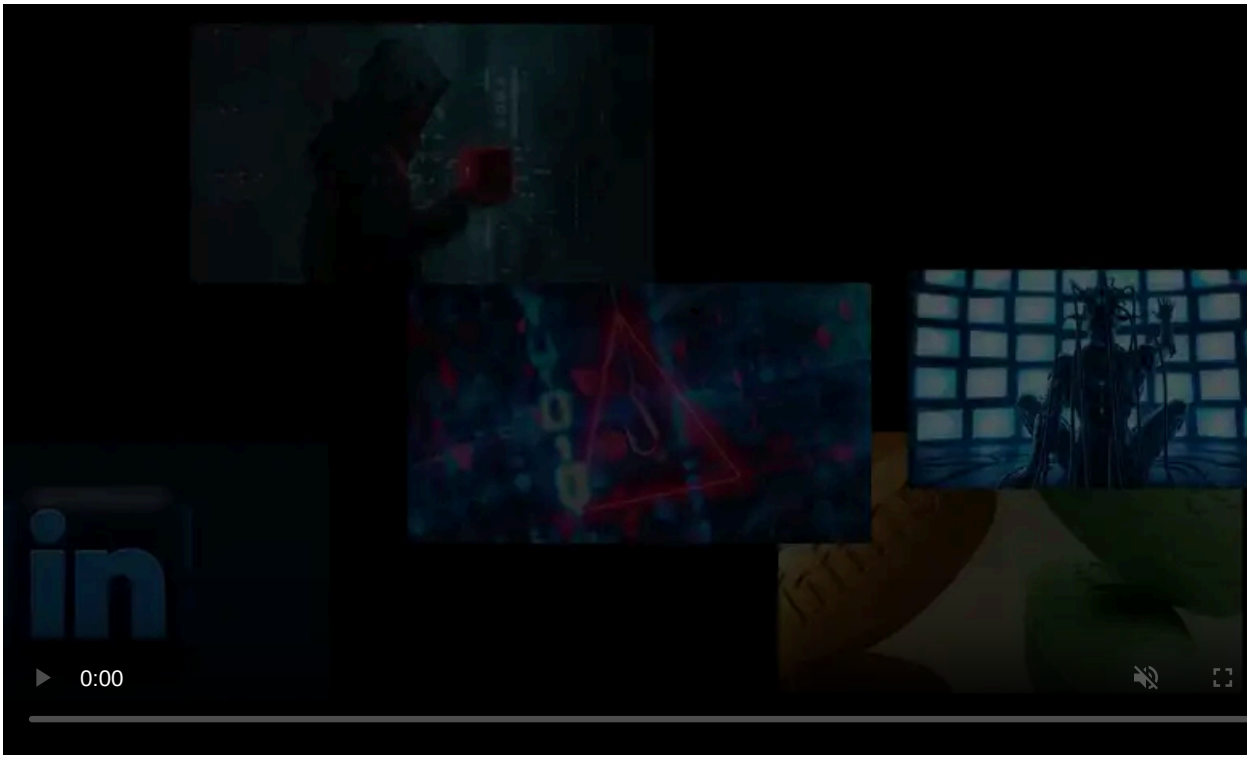
Published: 2021-12-24 · Archived: 2026-04-05 16:08:27 UTC

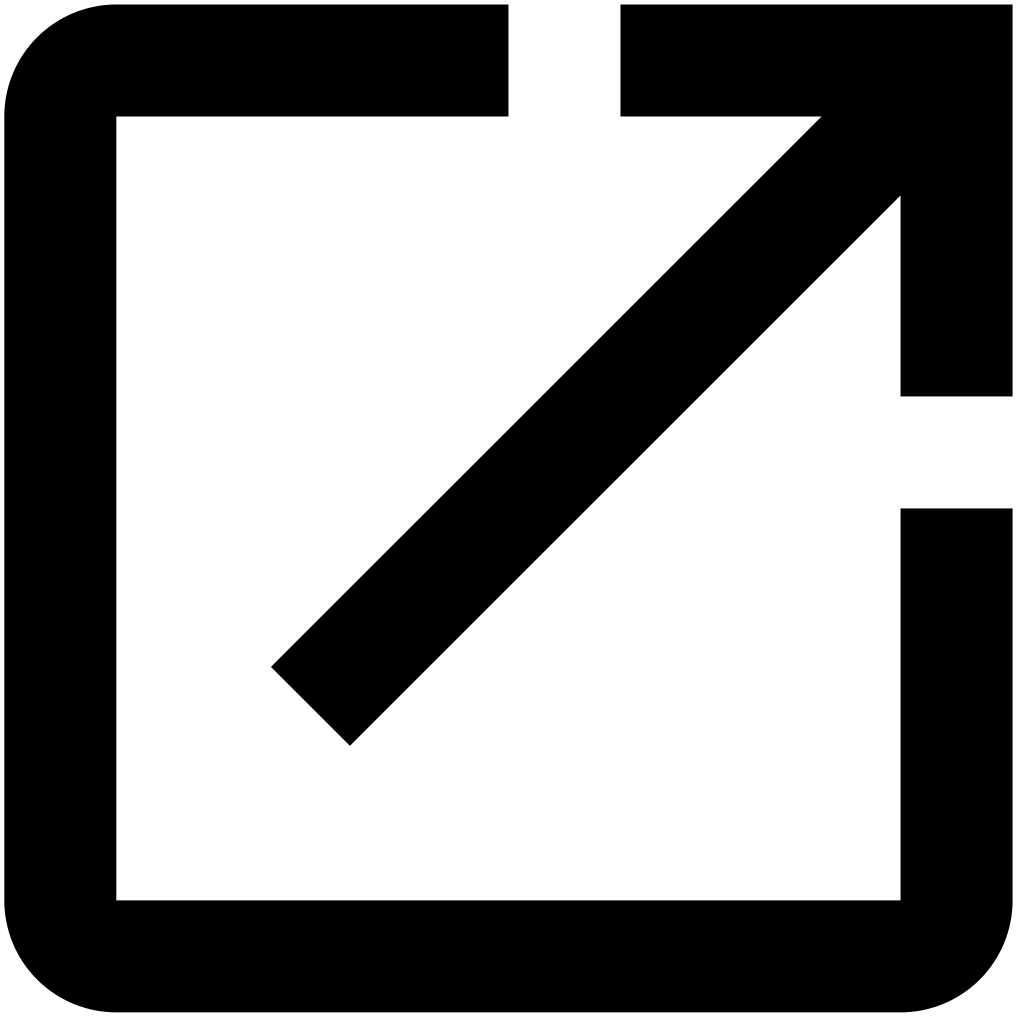
Less than a week before the Christmas holiday, French IT services company Inetum Group was hit by a ransomware attack that had a limited impact on the business and its customers.

Inetum is active in more than 26 countries, providing digital services to companies in various sectors: aerospace and defense, banking, automotive, energy and utilities, healthcare, insurance, retail, public sector, transportation, telecom and media.

Limited impact

As a services provider for a large number of companies and with a revenue of almost $2 billion, the group is an attractive target for ransomware gangs.


0:00



On Sunday, December 19, Inetum became the target of a ransomware attack that affected some of its operations in France and did not spread to larger infrastructures used by the customers.

“None of the main infrastructures, communication, collaboration tools or delivery operations for Inetum clients has been affected,” the company assures in a press release on Thursday.

The Group’s crisis unit acted quickly to protect sensitive connections that could put clients at risk if compromised. To this end, the operational teams isolated all servers on the affected network and terminated client VPN connections.

An initial investigation determined the ransomware strain used in the attack and that the recent critical Log4j vulnerability was not exploited during the incident.

Inetum Group did not disclose the name of the malware used but according to Valéry Marchive, editor-in-chief at French publication LeMagIt, the attackers used BlackCat ransomware, also known as ALPHV and Noberus.

The file-encrypting malware is written in Rust, which is atypical for ransomware operations and has been used in attacks since at least November 18, as discovered by researchers at Symantec, a Broadcom company.

BlackCat has plenty of advanced features and comes with a very flexible configuration that allows it to spread to other computers, terminate virtual machines and ESXi hypervisors, as well as wipe them.

Inetum Group has notified authorities about the attack and is collaborating with specialized cybercrime units. A third party has also been called in for incident response services.

At the moment, delivery operations to customers are safe, and messaging and collaboration systems remain unaffected, the company notes.

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