Europol and Microsoft disrupt world’s largest infostealer Lumma

By Europol

Published: 2025-05-21 · Archived: 2026-04-05 21:47:47 UTC

Europol’s European Cybercrime Centre has worked with Microsoft to disrupt Lumma Stealer (“Lumma”), the world’s most significant infostealer threat.

This joint operation targeted the sophisticated ecosystem that allowed criminals to exploit stolen information on a massive scale. Europol coordinated with law enforcement in Europe to ensure action was taken, leveraging intelligence provided by Microsoft.

Between 16 March and 16 May 2025, Microsoft identified over 394 000 Windows computers globally infected by the Lumma malware. In a coordinated follow-up operation this week, Microsoft’s Digital Crimes Unit (DCU), Europol, and international partners have disrupted Lumma’s technical infrastructure, cutting off communications between the malicious tool and victims. In addition, over 1 300 domains seized by or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to Microsoft sinkholes.

The Head of Europol’s European Cybercrime Centre, Edvardas Šileris, said: “This operation is a clear example of how public-private partnerships are transforming the fight against cybercrime. By combining Europol’s coordination capabilities with Microsoft’s technical insights, a vast criminal infrastructure has been disrupted. Cybercriminals thrive on fragmentation – but together, we are stronger.”

What is Lumma?

Lumma, the world’s largest infostealer, was a sophisticated tool that enabled cybercriminals to collect sensitive data from compromised devices on a massive scale. Stolen credentials, financial data, and personal information were harvested and sold through a dedicated marketplace, making Lumma a central tool for identity theft and fraud worldwide.

The Lumma marketplace operated as a hub for buying and selling the malware, providing criminals with user-friendly access to advanced data-stealing capabilities. Its widespread use and accessibility made it a preferred choice for cybercriminals looking to exploit personal and financial data.

A coordinated response across the world

Europol acted as the central point in Europe for intelligence sharing and coordination. After receiving critical intelligence from Microsoft, Europol’s European Cybercrime Centre enriched this information and provided Member States with a view of the threat landscape to ensure a clear understanding of the network’s operations.

Acting as a facilitator for Member States, Europol played a crucial role in deconfliction, ensuring that overlapping investigations were identified and managed effectively. By gathering all relevant intelligence and making sure that

impacted Member States received the necessary information promptly, Europol enabled a quick response.

In a coordinated move, the United States Department of Justice (DOJ) seized the Lumma control panel, which was critical to the Lumma marketplace.

Microsoft's collaboration with Japan's Cybercrime Control Center (JC3) also led to the suspension of Lumma infrastructure based in Japan, further dismantling the criminal network.

Delivering security through partnerships

This operation demonstrates Europol's strategy of delivering security through public-private partnerships, a cornerstone of its approach to combating crime in the digital age. In an increasingly interconnected world, the fight against cyber threats cannot be won by law enforcement alone.

Public-private partnerships allow Europol to bridge the gap between the private sector's technical expertise and law enforcement's operational capabilities. By leveraging the strengths of each, Europol can deliver more impactful results, disrupting cybercriminal operations at their core.

The cooperation with Microsoft in this operation was carried out under Article 26 of Europol's Regulation, which allows Europol to receive information from and collaborate with private parties for the prevention and combat of serious crime.

Microsoft is a member of Europol's Advisory Group on Internet Security.

Read Microsoft's announcement here.
