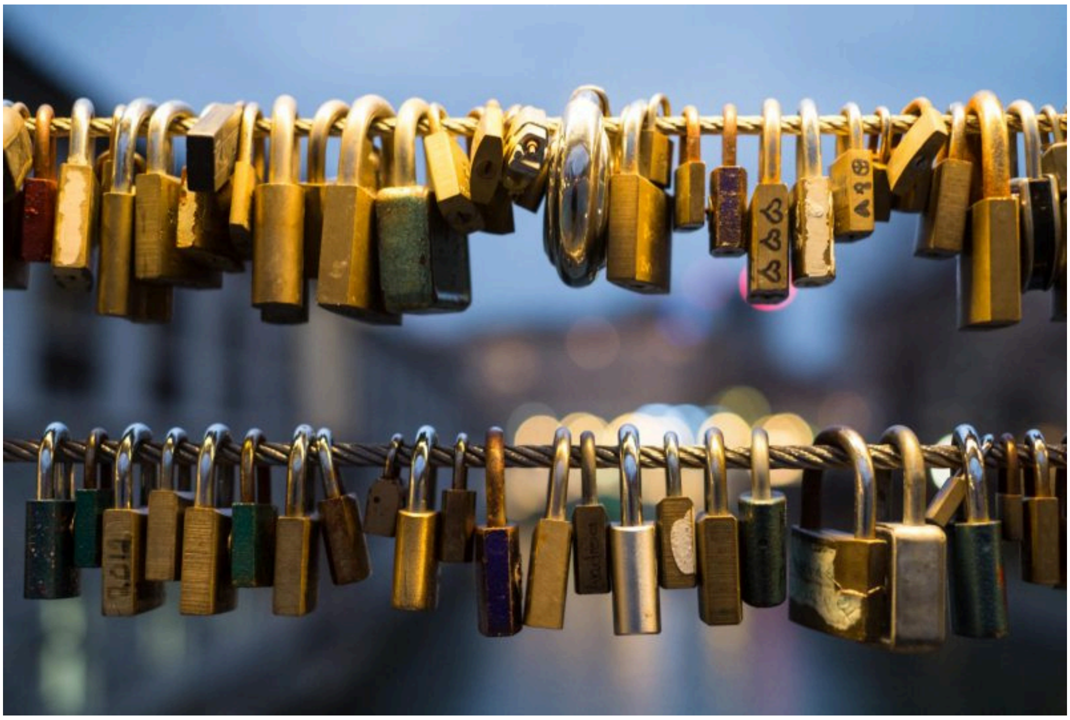

Europe’s Ransomware Spiral: A Preview of What Awaits the U.S.

Infosources™

August 23, 2025

Europe is facing a ransomware crisis, with infection rates now up to four times higher than in the United States. What looks like a regional problem is in fact a warning: attackers are refining tactics in Europe that will inevitably be deployed against U.S. organizations. The surge is fueled by the spillover of the war in Ukraine, the rise of ransomware-as-a-service groups, and a shift from pure encryption to data theft and reputational extortion. Europe’s struggle is less an isolated incident than a glimpse of America’s near future.

The surge of ransomware infections in Europe, now three to four times higher than in the United States, should not be read as a regional anomaly. Europe has traditionally been seen as a benchmark in cybersecurity, with stronger regulations, centralized oversight, and tighter cooperation between private and public actors. If attackers are breaching that framework at scale, it raises a pressing question: what happens when the same tactics are applied with full force against the United States?

The European case highlights several converging problematics. First is **geopolitical spillover**: the war in Ukraine has opened a new front in cyberspace, with pro-Russian hacktivists, criminal syndicates, and ransomware-as-a-service affiliates attacking European infrastructures once considered off-limits. Airports, media outlets, and government networks are now targets, showing the erosion of prior taboos. The result has been a 28% increase in malware incidents, enabled by persistent neglect of basic cyber hygiene—unpatched vulnerabilities, exposed ports, outdated firewalls, and weak credentials.

Second is the **evolution of extortion models**. Ransomware actors no longer rely solely on encryption to drive payments. They have shifted toward data exfiltration, reputational blackmail, and direct outreach to customers and partners. In Europe, more than half of victim organizations still pay, even with intact backups—demonstrating that the real leverage lies not in disruption of operations but in the threat of exposure. This dependency on concealment has become one of the greatest structural weaknesses for defenders.

Third is the **illusion of immunity among U.S. organizations**. Many still assume that layered defenses and backups will protect them, underestimating attackers' ability to adapt and exploit reputational vulnerabilities. Moreover, small and midsize businesses, often overlooked, now represent a disproportionate share of victims, with supply chains serving as vectors that can compromise even well-defended enterprises. Law enforcement actions, such as **Operation Cronos**, have shown that coordinated crackdowns can disrupt ransomware networks and dismantle infrastructure. Yet these victories remain fleeting. As long as ransom payments flow and reputational pressure drives compliance, groups quickly reorganize, adapt their tactics, and re-emerge under new brands.

Info

Operation Cronos, the global law enforcement operation that took down Lockbit, one of the world's most harmful ransomware groups, is a major breakthrough in the fight against cybercrime. The operation, announced on February 20, was led by the UK's National Crime Agency (NCA) and the FBI. The results of the operation were unprecedented: on top of seizing LockBit's data leak site and affiliate panel, law enforcement agencies seized 34 servers operated by LockBit, closed 14,000 "rogue accounts" involved with data exfiltration or the group's infrastructure" and froze 200 cryptocurrency accounts linked to LockBit and its affiliates. LockBit's bespoke data exfiltration tool, known as Stealbit, was also seized. Security researchers Vx-underground also claimed that at least 22 Tor sites associated with LockBit had been seized and/or taken down by law enforcement. In addition, two LockBit actors have been arrested in Poland and Ukraine at the request of the French judicial authorities. Three international arrest warrants and five indictments have also been issued by the French and US judicial authorities. Some of the key elements of the operation were displayed on the LockBit data leak site homepage, in a display mimicking how the ransomware group would announce new victims.

EUROPOL
OPERATION CRONOS
10
< COUNTRIES IN TASKFORCE CRONOS />
2
< ARRESTS />
MORE THAN
200
< CRYPTOCURRENCY ACCOUNTS FROZEN />
34
< SERVERS TAKEN DOWN />
14 000
< ROGUE ACCOUNTS CLOSED />
< LAW ENFORCEMENT HAS TAKEN CONTROL OF THE TECHNICAL INFRASTRUCTURE AND LEAK SITE />

The European wave underscores a deeper problem: **the resilience gap**. Organizations have invested in recovery strategies but not in transparency and trust. Attackers exploit this asymmetry, knowing that silence and fear of reputational fallout compel payments. Unless U.S. defenders internalize Europe's experience—treating patching as life-critical, preparing communication playbooks for exposure, and abandoning the belief that size provides safety—the same scenario will unfold domestically.

Europe's ransomware surge is less a local crisis than a warning shot. Whether the United States learns from it, or repeats it, remains an open question.

ⓘ **Info**

A playbook or **predefined, practical communication plan** is essentially a step-by-step guide or template that answers:

Who communicates: Which team members or leaders are responsible for speaking to customers, partners, regulators, or the press.

What to communicate: Key messages that explain the situation honestly but carefully (e.g., what happened, what data may be at risk, what actions are being taken).

When to communicate: How quickly updates should be sent after detecting an incident, and how often to follow up.

How to communicate: Which channels to use (emails to customers, public statements, press releases, website banners, social media, etc.). The idea is that during a crisis, you don't have time to invent your messaging from scratch.

A **communication playbook** ensures the response is **coordinated, transparent, and fast**, which helps protect trust and reduces the leverage criminals gain by threatening exposure.