CrowdStrike 2025 European Threat Landscape Report: Ransomware Hits Region at Record Pace

Europe ranks as second largest eCrime target globally amid intensifying "Big Four" nation-state activity

AUSTIN, Texas--(BUSINESS WIRE)--Nov. 3, 2025-- Fal.Con Europe 2025, Barcelona-- CrowdStrike (NASDAQ: CRWD) today released the 2025 European Threat Landscape Report, revealing that European organizations accounted for nearly 22% of global ransomware and extortion victims — second only to North America. Ransomware operations are moving faster than ever, with CrowdStrike observing adversary groups like SCATTERED SPIDER increasing ransomware deployment speed by 48%, with the average attack now taking just 24 hours.

Adversaries operating in and targeting Europe benefited from underground marketplaces commoditizing services like Malware-as-a-Service, initial access brokerage, and phishing toolkits. In parallel, state-sponsored adversaries from Russia, China, North Korea, and Iran expanded regional targeting across industries, reflecting the growing convergence of eCrime and geopolitical threats.

European Threat Landscape Report Highlights:

Based on frontline intelligence from CrowdStrike Counter Adversary Operations, which tracks more than 265 named adversaries, the report reveals:

- **Ransomware Attacks Reach Historic Highs**: Since January 1, 2024, more than 2,100 victims across Europe were named on extortion leak sites. The U.K., Germany, France, Italy, and Spain were the most targeted nations, with 92% of cases involving file encryption and data theft. Fueling Big Game Hunting operations, 260 initial access brokers advertised to over 1,400 European organizations.
- **Russia and North Korea Escalate Threats**: Russia-nexus actors continued to target Ukraine conducting credential phishing, intelligence collection, and destructive operations targeting government, military, energy, telecom, and utilities. DPRK-nexus actors expanded targeting of European defense, diplomatic, and financial institutions, combining espionage with cryptocurrency theft to advance strategic interests.
- **Underground Ecosystems Evolve**: English- and Russian-language forums — including BreachForums, a successor to RaidForums whose administrators were linked to actors in France and the U.K., remain central to Europe's eCrime ecosystem, enabling the exchange of stolen data, malware, and criminal services. Platforms like Telegram, Tox, and Jabber facilitated collaboration, recruitment, and monetization among threat actors.
- **Physical Crime Goes Digital**: Violence-as-a-Service emerged as a growing threat across Europe, with threat actors using Telegram-based networks to coordinate physical attacks, kidnappings, and extortion tied to cryptocurrency theft. Groups connected to "The Com" ecosystem and hybrid adversaries like RENAISSANCE SPIDER are bridging cyber and physical operations, offering payments for sabotage, arson, and targeted violence.
- **China Concentrates its Modus Operandi:** Chinese state-sponsored adversaries targeted industries in 11 countries, exploiting cloud infrastructure and software supply chains to steal intellectual property. Persistent campaigns focused on healthcare and biotechnology, with VIXEN PANDA emerging as the most prolific threat to European government and defense entities.
- **Iranian Operations Expand to Europe:** IRGC-linked actors ramped up phishing, hack-and-leak, and DDoS campaigns against the U.K., Germany, and the Netherlands. HAYWIRE KITTEN claimed responsibility for a DDoS attack against a Dutch news outlet, while multiple Iran-nexus actors masqueraded as hacktivists to obscure state-sponsored espionage efforts.

"The cyber battlefield in Europe is more crowded and complex than ever," said Adam Meyers, head of Counter Adversary Operations at CrowdStrike. "We're seeing a dangerous convergence of criminal innovation and geopolitical ambition, with ransomware crews using enterprise-grade tools and state-backed actors exploiting global crises to disrupt, persist, and conduct espionage. In this high-stakes environment, intelligence-led defense powered by AI and guided by human expertise is the only combination designed to stop cyber threats."

Download the full 2025 European Threat Landscape Report to gain valuable insights and mitigation strategies to stay ahead of cyber adversaries in Europe's increasingly complex threat landscape.

About CrowdStrike

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Instagram

Start a free trial today: https://www.crowdstrike.com/trial

View source version on businesswire.com: https://www.businesswire.com/news/home/20251103919255/en/

Media Contact
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike