Digital Security
Progress. Protected.

THREATS WITHOUT BORDERS

Key Insights from ESET's Latest APT Report

Advanced Persistent Threats (APTs) operate in the shadows—stealthy, strategic, and often state-sponsored. Unlike ransomware and malware actors that rely on broad, opportunistic attacks, APT groups take a long-term approach, carefully crafting intrusions to infiltrate high-value targets and evade detection for months or even years. Defending against these threats requires more than reactive security—it demands global visibility and proactive intelligence. ESET's latest APT report leverages telemetry from millions of endpoints worldwide, providing critical insights into how these adversaries evolve, what industries they target, and the tactics they use to stay hidden.

Why Global Threat Intelligence Matters

For U.S. businesses, having access to global threat intelligence isn't just beneficial—it's essential. Cyber threats don't recognize borders, and many APT groups operate with geopolitical motivations that can have far-reaching consequences. By analyzing threat activity across different regions, industries, and attack surfaces, global telemetry helps businesses - no matter their location - anticipate risks before they become direct threats. ESET's extensive network of sensors and advanced analytics provide real-time visibility into emerging attack patterns, enabling organizations to strengthen their defenses, adapt security strategies, and mitigate risks proactively.

Key Findings From the Latest APT Report

ESET's latest APT report highlights major developments in the global threat landscape:

- China-aligned APTs expanded operations into Africa and the EU, with MirrorFace targeting a European diplomatic organization for the first time.
- North Korea-aligned groups, including Lazarus and Kimsuky, intensified attacks on cryptocurrency firms, defense contractors, and think tanks, leveraging cloud-based services and novel attack techniques.
- Iran-aligned actors ramped up espionage against financial firms in Africa, government entities in the Middle East, and transportation infrastructure in Israel.
- Russia-aligned cyberespionage groups continued widespread spearphishing campaigns, particularly against Ukraine, and leveraged new malware like WrongSens and LOADGRIP.
- Other notable APT activities included a FrostyNeighbor campaign in Poland, a likely APT attack on a Yemeni ISP using a Linux toolset, and the exploitation of a zero-day vulnerability in WPS Office for Windows by APT-C-60.

STAYING AHEAD OF EMERGING THREATS

ESET's global threat telemetry continuously monitors emerging and evolving threats, delivering a truly global perspective on cyber risk. ESET Threat Intelligence combines AI-driven analysis, machine learning, and expert human curation to provide organizations with real-time, actionable insights tailored to their specific security needs.

As APT groups refine their strategies, staying informed is more critical than ever. ESET's global presence and localized expertise helps businesses anticipate and counteract threats before they strike. Download the full report for an in-depth look at today's evolving APT landscape.

ESET Threat Intelligence Helps Organizations:

- Detect and mitigate threats before they escalate.
- Strengthen defenses against emerging malware trends.
- Gain deeper visibility into cybercriminal tactics and attack patterns, informed by global threat research.
- Translate alerts into actions with expert intelligence curation and AI assistance.

Explore ESET Business Solutions