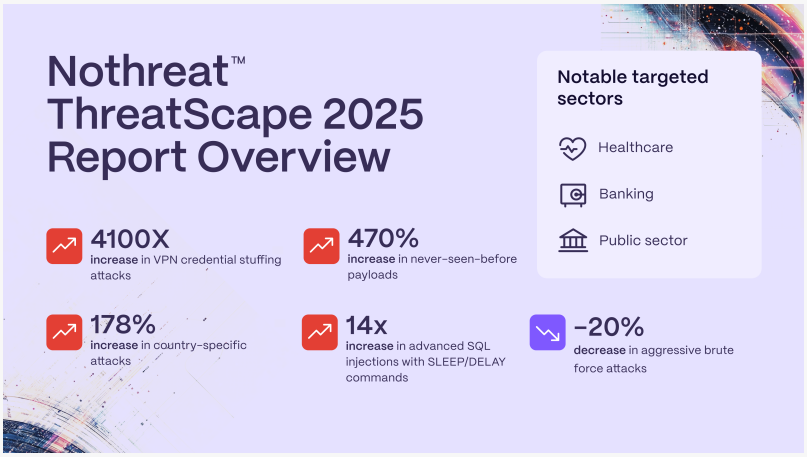
Nothreat: 470% Surge in Never-Seen-Before Payloads Signals a New Era in AI-Driven Cybersecurity

Nothreat™, a UK-based AI cybersecurity startup, has released its first ThreatScape 2025 report, providing an in-depth analysis of the cyber threats landscape.



Nothreat's ThreatScape 2025 Report

LONDON, UNITED KINGDOM, March 13, 2025 /EINPresswire.com/ -- Nothreat™, a UK-based AI cybersecurity startup valued at £40 million, has released its first ThreatScape 2025 report, providing an in-depth analysis of the cyber threats landscape. The report covers emerging cyber threats, evolving attack techniques, industry-specific threats including IIoT vulnerabilities, and the increasing sophistication of adversary tactics. It offers cybersecurity professionals a strategic understanding of the most pressing threats and the proactive measures required to mitigate them in the era of AI-driven attacks.

The research is based on the analysis of 16 million automated cyberattacks, a proportionally and randomly chosen sample from cyber traps deployed across 30 countries, including the United States, China, Azerbaijan, Germany, the Philippines, Japan, and others, throughout 2024.

Key Findings:

470% Surge in New Cyber Payloads
Adversaries are bypassing traditional defenses with never-before-seen threats, making AI-driven, real-time cybersecurity essential to combat evolving attack strategies.

4100X rise in VPN credential stuffing attacks
Automated credential-stuffing attacks have skyrocketed, enabling large-scale breaches of remote access systems and emphasizing the urgent need for stronger authentication defenses.

178% increase in country-specific attacks

Cybercriminals are exploiting regional vulnerabilities, increasingly targeting Tier 1 network infrastructure like enterprise firewalls and routers, highlighting the need for proactive security measures.

87% rise in human-driven IIoT attacks
Cyber and physical risks are converging, with adversaries combining automation and human intervention to infiltrate critical infrastructure at an unprecedented scale.

Shift from Brute Force to More Sophisticated Attacks
A 14x rise in SQL injection attacks reflects a shift to stealthier, time-based evasion techniques, while a 20% drop in brute force attacks suggests adversaries favor sophisticated automation over noisy intrusion attempts.

Industry-Specific Attacks Are Evolving with Sector-Focused Tactics
Healthcare faces the highest share of never-seen-before payloads (37%), while the public sector experiences the most country-specific attacks (66%), and banking follows closely with 51%, primarily targeting financial fraud and API exploits.

Nothreat's AI-driven cybersecurity solutions are specifically designed to counter the evolving landscape of cyber threats, leveraging continuous R&D and real-world intelligence. Nothreat AIoT Defender, an advanced lightweight software firewall, delivers real-time AI-powered threat detection, ensuring protection against zero-day attacks and previously unseen threats in IoT environments. Powered by the Nothreat Platform, CyberEcho, now protected under a U.S. patent, employs clone-based deception technology, creating adaptive threat traps to disrupt and neutralize targeted attacks before they escalate.

"The cyber threat landscape is shifting at an unprecedented pace," said Sergej Kostenko, CEO at Nothreat. "With adversaries deploying never-seen-before payloads at scale, traditional defenses are proving insufficient. Businesses must move beyond reactive security models and embrace AI-driven, proactive cybersecurity strategies that can anticipate and neutralize emerging threats in real time. The organizations that fail to adapt risk falling behind in a digital environment where threats evolve faster than ever before."

Nothreat will continue to release the ThreatScape report on a regular basis, delivering up-to-date intelligence on the latest cyber threats and attack trends shaping the security landscape.

To download the full ThreatScape 2025 report and learn more, visit https://nothreat.io.

About Nothreat

Nothreat is a leader in AI-powered cybersecurity solutions, offering real-time protection against evolving cyber threats. Our Continuous Learning AI detects zero-day threats with 99% accuracy,

identifying 55% more attacks than conventional systems. A key innovation is AIoT Defender, a lightweight, software-based firewall designed for IoT devices. Consuming only about 2 MB of RAM, it provides real-time, on-device protection without additional hardware.

Other products include CyberEcho with US and UK patent-pending Clone-Based Traps technology, the AI-driven Cybersecurity Event System (CES), and a 24/7 Security Operations Center (SOC). Nothreat's solutions integrate seamlessly with existing firewalls, requiring minimum infrastructure changes.

Contact
info@nothreat.io

Press Office
Nothreat
pd@perform.it.com
Visit us on social media:
Facebook
X
LinkedIn
