# Cyber Attacks Are More Sophisticated Than Ever, With AI-Powered Attacks Posing the Greatest Risk

*Keeper Security Insight Report reveals IT leaders are unprepared for the new wave of threat vectors*

LONDON, UNITED KINGDOM, March 26, 2024 /EINPresswire.com/ -- Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and remote connections, today releases its 2024 Keeper Security Insight Report, The Future of Defense: IT Leaders Brace for Unprecedented Cyber Threats.

The survey of more than 800 IT and security leaders around the globe reveals the role emerging technology plays in the evolving threat landscape and how IT leaders are struggling to keep up. Survey respondents cite AI-powered attacks as the most serious emerging attack vector and the most challenging to handle. Cybercriminals are becoming increasingly sophisticated, breaking historically secure solutions and inflicting damage on vulnerable organisations across every sector. Cybersecurity is more critical now than ever before.

> Fighting evolving threats requires constant adaptation, underscoring the need for a proactive approach to cybersecurity."
>
> *Darren Guccione, CEO and Co-founder, Keeper Security*

Emerging technology fuels increasingly sophisticated attacks

Ninety-two percent of respondents reveal they've seen an increase in cyber attacks year-over-year. As cybersecurity incidents become more frequent, 95% of IT leaders say that cyber attacks are also more sophisticated than ever – and they are unprepared for this new wave of threat vectors.

IT leaders share the emerging attack vectors they're witnessing first-hand at their organisations:
AI-powered attacks (51%)
Deepfake technology and supply chain attacks – both 36%

Cloud jacking – 35%
Internet of Things (IoT) Attacks and 5G network exploits – both 34%
Fileless attacks – 24%

IT leaders report they are ill-equipped to defeat those emerging techniques, lacking defence for:
AI-powered attacks – 35%
Deepfake technology – 30%
5G network exploits – 29%
Cloud jacking – 25%
Fileless attacks – 23%

Even as they prepare to overcome emerging attack techniques, IT security leaders must face the problems of today: in fact, 73% of respondents report experiencing a cyber attack that resulted in monetary loss. Direct financial impact is one of many consequences of a successful cyber attack, along with business disruption, enduring revenue loss, customer and partner attrition and tarnished reputation.

“Malicious actors are wreaking havoc on vulnerable organisations in novel ways, leveraging emerging technology to execute devastating cyber attacks,” said Darren Guccione, CEO and Co-founder, Keeper Security. “Fighting evolving threats requires constant adaptation, underscoring the need for a proactive approach to cybersecurity – one that combines advanced defence mechanisms and basic best practices to identify evolving threats and defeat a cyberattack.”

Contending with today’s attacks
While novel threats cast a looming shadow, IT leaders are stretched thin as they combat today’s most common threat vectors, with the following types of attacks directly impacting their organisations:
Phishing – 61%
Malware – 59%
Ransomware – 49%
Password attacks – 38%

The explosion in AI tools has intensified problems like phishing attacks by increasing the believability of scams and enabling cybercriminals to deploy them at scale. Eighty-four percent of respondents said that phishing and smishing have become more difficult to detect with the rise in popularity of AI-powered tools, and revealed that AI-powered phishing is their top concern (42%) when it comes to AI security. In addition to phishing, malicious actors weaponise AI to speed up and scale other common attack techniques, such as password cracking.

Among the multitude of cyber attacks increasing in frequency, survey respondents cite:
Phishing – 51%
Malware – 49%

Ransomware – 44%
Password attacks – 31%

Stolen or weak passwords and credentials remain a leading cause of breaches. Fifty-two percent of survey respondents shared that their company's IT team struggles with frequently stolen passwords, underscoring the importance of creating and safely storing strong, unique passwords for every account.

The future of defence
As emerging technology intensifies existing attack vectors and creates new threats, the stakes are higher than ever for IT and security leaders. Despite the ever-evolving threat landscape, the fundamental rules of protecting an organisation in the digital age remain relevant. Integrating solutions that prevent the most prevalent cyber attacks, including password and privileged access management (PAM) solutions, creates a layered security approach that stands the test of time now and in the future.

Download the full report to learn more.
###

About Keeper Security
Keeper Security is transforming cybersecurity for people and organisations around the world. Keeper's affordable and easy-to-use solutions are built on a foundation of zero-trust and zero-knowledge security to protect every user on every device. Our next-generation privileged access management solution deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance. Trusted by millions of individuals and thousands of organisations, Keeper is the leader for best-in-class password and passkey management, secrets management, privileged access, secure remote access and encrypted messaging.

Charley Nash
Eskenzi PR
charley@eskenzipr.com

---