Trend Micro Empowers Organizations to Tackle Malicious AI

Advanced XDR is the key to managing emerging cyber threats

DALLAS, Aug. 10, 2023 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today shared more details of its ongoing commitment to protect global customers around the world from emerging AI threats.

Jon Clay, VP of threat intelligence at Trend:"AI tools like ChatGPT are taking the world by storm, but the technology is already being used by opportunistic threat actors to take advantage of gaps in enterprise security. Trend is leading the way globally in mitigating these threats through a prolific output of groundbreaking research and its own use of AI to supercharge both ASRM and XDR."

Trend successfully blocked 73 billion threats for its global customer base in the first half of 2023, marking a 16% year-on-year increase. Those figures illustrate both the growing power of its threat detection capabilities and the sheer scale of today's threat landscape.

Emerging malicious AI tools including WormGPT and FraudGPT are already being built on top of open-source generative AI platforms to democratize cybercrime, making hackers more productive and attacks more likely to succeed.

Trend™ Research recently revealed how threat actors are strengthening impersonation tactics by combining deepfake and AI voice cloning technology with generative AI for more effective virtual "virtual kidnapping" scams. Adversaries leverage ChatGPT to filter and fuse large datasets to victim selection, and deepfakes are deployed to deceive victims into believing a close relation has been kidnapped to extort a ransom.

Separate research from Trend uncovered the use of generative AI in training and supporting new threat actors, including activities such as:

- Developing malicious polymorphic code
- Creating detection-resistant malware
- Creating highly convincing phishing emails for business email compromise (BEC) and webpages in multiple languages
- Creating hacking tools
- Identifying and analyze vulnerabilities
- Identifying card data for fraud
- Accelerating tactic and technique learning

These tools are continually improved by cybercriminals and made accessible through subscription-based pricing to further reduce barriers to entry for aspiring hackers. The development and deployment of malicious AI has put escalating pressure on security teams to detect and respond to threats earlier and faster to ensure quicker containment and minimal damage.

Empowering security teams to detect and respond to malicious AI use, Trend Vision One™ leverages its own generative AI through the Companion virtual assistant, in addition to AI app detection models, to help SOC analysts match the speed and polymorphic nature of AI-driven attacks. It features:

- **XDR Incident Feature:** Accelerating threat event understanding, saving time spent researching and contextualizing alerts. On average it saves three minutes per alert, amounting to several hours per user per week.
- **Command-Line Feature:** Streamlining and simplifying decoding complex scripts. Analysts save additional time with productivity gains of up to 40 minutes of manual investigation time.
- **Search Query Generator:** Transforming plain-language search queries into formal search syntax, saving up to one hour of time spent hunting by assisting users with query development and field name, operator and value identification.

Trend has been at the forefront of AI-powered solutions with current and planned AI/ML and generative AI investments and historical leadership in the domain since 2005, including tooling designed to detect BEC attacks. Its Writing Style DNA technology learns "normal" email writing style from previous messages and flags when emails deviate from this baseline. It blocked over 130,000 BEC attacks for customers in this manner throughout 2022.

To find out more about the number one-ranked XDR platform Trend Vision One™, please visit: https://www.trendmicro.com/en_us/business/products/one-platform.html

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for

environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2023-08-10-Trend-Micro-Empowers-Organizations-to-Tackle-Malicious-AI