News AI and machine learning Microsoft Copilot for Security

3 min read

Cyber Signals: Navigating cyberthreats and strengthening defenses in the era of AI

By Vasu Jakkal, Corporate Vice President, Security, Compliance, Identity, and Management

February 14, 2024

Threat trends

The world of cybersecurity is undergoing a massive transformation. AI is at the forefront of this change, and has the potential to empower organizations to defeat cyberattacks at machine speed, address the cyber talent shortage, and drive innovation and efficiency in cybersecurity. However, adversaries can use AI as part of their exploits, and it’s never been more critical for us to both secure our world using AI and secure AI for our world.

Today we released the sixth edition of Cyber Signals, spotlighting how we are protecting AI platforms from emerging threats related to nation-state cyberthreat actors.

In collaboration with OpenAI, we are sharing insights on state-affiliated threat actors tracked by Microsoft, such as Forest Blizzard, Emerald Sleet, Crimson Sandstorm, Charcoal Typhoon, and Salmon Typhoon, who have sought to use large language models (LLMs) to augment their ongoing cyberattack operations. This important research exposes incremental early moves we observe these well-known threat actors taking around AI, and notes how we blocked their activity to protect AI platforms and users.

We are also announcing Microsoft’s principles guiding our actions mitigating the risks of nation-state Advanced Persistent Threats, Advanced Persistent Manipulators, and cybercriminal syndicates using AI platforms and APIs. These principles include identification and action against malicious threat actors’ use notification to other AI service providers, collaboration with other stakeholders, and transparency.

In addition, Microsoft is helping the wider security community to understand and detect the emerging prospects of LLMs in attack activity. We continue to work with MITRE to integrate these LLM-themed tactics, techniques, and procedures (TTPs) into the MITRE ATT&CK® framework or MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems) knowledgebase. This strategic expansion reflects a commitment to not only track and neutralize threats, but also to pioneer the development of countermeasures in the evolving landscape of AI-powered cyber operations.

This edition of Cyber Signals shares insights into how threat actors are using AI to refine their attacks and also how we use AI to protect Microsoft.

Cybercriminals and state-sponsored actors are looking to AI, including LLMs, to enhance their productivity and take advantage of platforms that can further their objectives and attack techniques. Although threat actors’ motives and sophistication vary, they share common tasks when deploying attacks. These include reconnaissance, such as researching potential victims’ industries, locations, and relationships; coding, including improving software scripts and malware development; and assistance with learning and using both human and machine languages. Our research with OpenAI has not identified significant attacks employing the LLMs we monitor closely.

Microsoft uses several methods to protect itself from these types of cyberthreats, including AI-enabled threat detection to spot changes in how resources or traffic on the network are used; behavioral analytics to detect risky sign-ins and anomalous behavior; machine learning models to detect risky sign-ins and malware; Zero Trust, where every access request has to be fully authenticated, authorized, and encrypted; and device health to be verified before a device can connect to the corporate network.

In addition, generative AI has incredible potential to help all defenders protect their organizations at machine speed. AI's role in cybersecurity is multifaceted, driving innovation and efficiency across various domains. From enhancing threat detection to streamlining incident response, AI's capabilities are reshaping cybersecurity. The use of LLMs in cybersecurity is a testament to AI's potential. These models can analyze vast amounts of data to uncover patterns and trends in cyberthreats, adding valuable context to threat intelligence. They assist in technical tasks such as reverse engineering and malware analysis, providing a new layer of defense against cyberattacks. For example, users of Microsoft Copilot for Security have shown a 44% increase in accuracy across all tasks and a 26% faster completion rate. These figures highlight the tangible benefits of integrating AI into cybersecurity practices.[1]

As we secure the future of AI, we must acknowledge the dual nature of technology: it brings new capabilities as well as new risks. AI is not just a tool but a paradigm shift in cybersecurity. It empowers us to defend against sophisticated cyberthreats and adapt to the dynamic threat landscape. By embracing AI, we can help ensure a secure future for everyone.

Cyber Signals

See how Microsoft is protecting AI platforms from attempted abuse by nation-state cyberthreat actors.

Read the report >

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (@MSFTSecurity) for the latest news and updates on cybersecurity.

[1] What Can Copilot's Earliest Users Teach Us About Generative AI at Work? Microsoft. November 15, 2023.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads © Microsoft 2024