Threat Landscape

As March unfolds, there is an extensive discourse surrounding AI, examining its evolving role and impact on digital security. One of the most recent reports stems from a partnership between Microsoft Threat Intelligence and OpenAI. Based on the collaboration and information-sharing, OpenAI disrupted the operations of five state-affiliated malicious actors. The actors were attempting to leverage OpenAI services for tasks such as querying open-source information, translating, identifying coding errors, and executing basic coding tasks. (1)

Both OpenAI (1) and Microsoft (2) emphasize the need to address significant and evolving threats in the field of cybersecurity and AI. OpenAI is focused on tackling limitations in their current models for such tasks, while Microsoft is announcing principles to shape policies and actions. The goal for Microsoft is to mitigate risks associated with the use of their AI tools and APIs by nation-state advanced persistent threats (APTs), advanced persistent manipulators (APMs), and cybercriminal syndicates. Despite these distinct approaches, the shared commitment is evident in proactively addressing and combatting threats within the realm of AI and cybersecurity.

Each year, during the first quarter, Norway releases three public threat and risk assessments. This year, they were issued on February 12th, featuring the following titles:

Risiko 2024, published by The Norwegian National Security Authority (NSM). (3)
Fokus 2024, published by The Norwegian Intelligence Service (NIS). (4)
Nasjonal Trusselvurdering 2024, published by The Norwegian Police Security Service (PST). (5)

In the upcoming months, we will spotlight key insights provided in the cyber threat assessments, commencing with NSMs views on the AI discussion. They state that artificial intelligence and machine learning will become essential for distinguishing malicious activity from legitimate operations. These technologies play a crucial role in analyzing and uncovering cyber operations against Norwegian businesses. However, artificial intelligence models have inherent vulnerabilities exploitable by threat actors. The role of artificial intelligence can influence operations and use AI-generated content to manipulate public opinion and social stability. And AI itself can become a new target for cyber operations exploiting entirely new types of vulnerabilities. For instance, a third-party service provider could implant a cryptographic backdoor in the model. (3)

NSM highlights the importance of understanding limitations, safeguarding against vulnerabilities, and exercising caution in third-party interactions to ensure model integrity and data security. They also underscore the importance of Norwegian authorities and industries staying abreast of AI developments to ensure safe and reliable utilization of the technology in the future. “Secure application and regulation of artificial intelligence require human intelligence”. (3)

Most recent online cybersecurity risks (6)

- Bumblebee Malware Reappears After Four-Month Hibernation
- Critical Microsoft Exchange Vulnerability
- Linux Command Not Found Feature Used to Distribute Malware
- MrAgent Ransomware Tool Automates VMware ESXi Infection
- New TicTacToe Dropper Delivers Several Types of Malware to Infected Devices
- North Korean APT Breached South Korean Presidential Staff

(1) https://openai.com/blog/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors
(2) https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
(3) https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2024
(4) https://www.etterretningstjenesten.no/publikasjoner/focus
(5) https://www.pst.no/alle-artikler/artikler/ntv-2024/
(6) https://innovatecybersecurity.com/security-threat-advisory/