New Report Finds that Criminals Leverage AI for Malicious Use - And It's Not Just Deep Fakes

Europol, UNICRI and Trend Micro uncover current and future threats of AI and how to combat them

DALLAS, Nov. 19, 2020 /PRNewswire/ -- A jointly developed new report by Europol, the United Nations Interregional Crime and Justice Research Institute (UNICRI) and Trend Micro Incorporated (TYO: 4704; TSE: 4704) looking into current and predicted criminal uses of artificial intelligence (AI) was released today. The report provides law enforcers, policy makers and other organizations with information on existing and potential attacks leveraging AI and recommendations on how to mitigate these risks.

The complete results of this research are available here: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml.

"AI promises the world greater efficiency, automation and autonomy. At a time where the public is getting increasingly concerned about the possible misuse of AI, we have to be transparent about the threats, but also look into the potential benefits from AI technology." said Edvardas Šileris, Head of Europol's Cybercrime Centre. "This report will help us not only to anticipate possible malicious uses and abuses of AI, but also to prevent and mitigate those threats proactively. This is how we can unlock the potential AI holds and benefit from the positive use of AI systems."

The report concludes that cybercriminals will leverage AI both as an attack vector and an attack surface. Deepfakes are currently the best-known use of AI as an attack vector. However, the report warns that new screening technology will be needed in the future to mitigate the risk of disinformation campaigns and extortion, as well as threats that target AI data sets.

For example, AI could be used to support:

- Convincing social engineering attacks at scale
- Document-scraping malware to make attacks more efficient
- Evasion of image recognition and voice biometrics
- Ransomware attacks, through intelligent targeting and evasion
- Data pollution, by identifying blind spots in detection rules

"As AI applications start to make a major real-world impact, it's becoming clear that this will be a fundamental technology for our future," said Irakli Beridze, Head of the Centre for AI and Robotics at UNICRI. "However, just as the benefits to society of AI are very real, so is the threat of malicious use. We're honored to stand with Europol and Trend Micro to shine a light on the dark side of AI and stimulate further discussion on this important topic."

The paper also warns that AI systems are being developed to enhance the effectiveness of malware and to disrupt anti-malware and facial recognition systems.

"Cybercriminals have always been early adopters of the latest technology and AI is no different. As this report reveals, it is already being used for password guessing, CAPTCHA-breaking and voice cloning, and there are many more malicious innovations in the works," said Martin Roesler, head of forward-looking threat research at Trend Micro. "We're proud to be teaming up with Europol and UNICRI to raise awareness about these threats, and in so doing help to create a safer digital future for us all."

The three organizations make several recommendations to conclude the report:

- Harness the potential of AI technology as a crime-fighting tool to future-proof the cybersecurity industry and policing
- Continue research to stimulate the development of defensive technology
- Promote and develop secure AI design frameworks
- De-escalate politically loaded rhetoric on the use of AI for cybersecurity purposes
- Leverage public-private partnerships and establish multidisciplinary expert groups

About Europol's European Cybercrime Centre (EC3)

Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. Our focus is on cybercrime committed by organised crime groups, which generate large profits (online fraud), seriously harm victims (online child sexual exploitation) or impact critical infrastructure and information systems in the EU, including cyber-attacks. Since its establishment, Europol's EC3 has made a significant contribution to the fight against cybercrime: it has been involved in hundreds of high-profile operations and hundreds on-the-spot operational-support deployments resulting in hundreds of arrests. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

About UNICRI

The United Nations Interregional Crime and Justice Research Institute was established in 1968. Within the broad scope of its mandate, the Institute contributes, through research, training, field activities and the collection, exchange and dissemination of information, to the formulation and implementation of improved policies in the field of crime prevention, justice and emerging security threats, due regard being paid to the integration of such policies within broader policies for socio-economic change and development, and to the protection of human rights.

In 2017, UNICRI opened its Centre for Artificial Intelligence and Robotics in The Hague, the Netherlands, with a view towards advancing understanding of artificial intelligence, robotics and related technologies vis-à-vis crime prevention, criminal justice, the rule of law and security. The Centre seeks to share knowledge and information on the potential beneficial applications of these technologies and to contribute to addressing any harmful effects and the malicious use. www.unicri.it

About Trend Micro

Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks. Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection. With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to 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.ca/2020-11-19-New-Report-Finds-that-Criminals-Leverage-AI-for-Malicious-Use-And-Its-Not-Just-Deep-Fakes