INNOVATION SNAPSHOTS

Volume 3 Issue 5 September 2023

FRAUDGPT: A NEW THREAT USING GENERATIVE AI

Nowadays, more and more cybercriminals are using tools and programs based on large language models (LLMs) such as ChatGPT for malicious purposes including scams and frauds. While Artificial Intelligence (AI) helps make some mechanical jobs faster, it has also been bringing with it new and dangerous threats.

After WormGPT, a chatbot used in hacking campaigns for large-scale attacks, FraudGPT has been available on several dark web forums and Telegram since July 2023. FraudGPT is also a chatbot that has been trained on fraudulent datasets and mainly used for malware code creation and phishing. Through the creation of emails, messages, and websites, FraudGPT can trick victims to share sensitive data such as passwords and financial details. The chatbot can make the user install apps that are intended to extort payments, download seemingly harmless attachments that actually carry viruses that can leak data or even forge documents.

Being based on LLMs, the new chatbot makes the messages highly credible and increasingly difficult to recognize. In fact, the software can customize the messages or emails sent to each victim to appear more authentic. The subscription cost for using FraudGPT ranges from $200 monthly to $1,000 every six months to $1,700 annually. The service is promoted by a user who goes by the name 'Canadian Kingpin' who claims that there have been more than 3,000 confirmed sales. FraudGPT has no guidelines on content moderation and uses generative AI to help users commit cybercrimes.

Sources: https://www.cloudbooklet.com/fraudgpt-the-new-ai-tool-for-cybercriminals/; https://indianexpress.com/article/technology/artificial-intelligence/what-is-fraudgpt-dark-webs-dangerous-ai-for-cybercrime-8866138/

NEW YORK STATE PARK POLICE DEPLOY DRONES TO MONITOR SHARK ATTACKS

Recently, five shark attacks occurred in two days in Long Island's (USA) seaside area. The New York State Park Police officers at Jones Beach, working in coordination with the lifeguards, are planning to make significant use of drone technology to keep the beaches and swimmers safe.

Drone activity is monitored by patrols inside a van, equipped with screens and computers, parked near the seaside. The drones are able to identify suspicious marine activity or spot the presence of sharks. They are equipped with latest generation cameras that can detect and view the movement of fishes underwater even from a height of about 7 meters. By checking the images captured by drones, officers can take immediate action, warn swimmers to keep away from the water, and also consider closing the beach. The idea of adopting drone technology for these purposes goes back to 2017, but it has seen a major acceleration due to recent attacks.

At Jones Beach, there are designated lanes near the shore where drones are flown. New York State Park Police have stated that normally, they do not operate them over crowds and therefore their use is dedicated to surveillance of the possible presence of sharks in the proximity. Police also clarified that the use of drones can also be deployed for other purposes, for example, in rescue or searches for missing people at sea.

With special additions to unmanned aerial vehicles such as infrared cameras, spotlights, and speakers, the operations mentioned above can also be carried out at night. According to New York State Park Police, in the future, drones may already be able to provide life jackets during rescue or guide the person in distress to the shore.

Source: https://amp.cnn.com/cnn/2023/08/14/tech/shark-drones-jones-beach-new-york/index.html

STEALING DATA THROUGH ACOUSTIC KEYBOARD ATTACKS

With the increase of technology-enabled crimes and threats, law enforcement work becomes increasingly challenging. Researchers at different British universities have published a study about the possibility to steal sensitive data simply by analysing the noise emitted by the keyboard whenever typing on a computer.

While the potential dangers of acoustic keyboard attacks in terms of data security had been exposed and demonstrated before, the new study has developed a deep learning model that can perform these attacks much more effectively. The idea revolves around the interaction of sound, machine learning and data mining — the system uses sound waves to hack sensitive data and works through an algorithm trained with deep learning machine method.

The devices used to carry out the study are a smartphone and a laptop. Specifically for training the system, the scholars pressed each key on the keyboard of a MacBook Pro (for a total of 36 keys A-Z and 0-9) 25 times, recording the sound with an iPhone resting a short distance away from the laptop. The captured data recorded from the smartphone physically placed near the laptop keyboard showed an accuracy rate of 95%. The experiment was also conducted for video conferencing applications such as Zoom and Skype, with keystrokes recorded using the built-in function generating an accuracy rate of 93% for the former and 91.7% for the latter.

Source: https://arxiv.org/pdf/2308.01074.pdf

DID YOU KNOW?

The Singapore Police Force has implemented the "Automated Armoury System" designed to streamline the management of firearms and enhance the security protocols of the police force. The Automated Armoury System is a smart locker system integrated with Radio-Frequency Identification (RFID) technology and Two-Factor Authentication (2FA). This system allows police officers to perform self-withdrawal and return of side arms and tasers, promoting efficiency and reducing administrative burdens.

DELHI POLICE TO USE BLOCKCHAIN TECHNOLOGY FOR FORENSIC EVIDENCE

The Delhi Police, in collaboration with the Delhi Forensic Science Laboratory (DFSL), has started using blockchain technology to record the chain of custody for evidence. Having trained at least 1,500 personnel for its use and analysing over 3,000 forensic samples, this tool will promote a transparent and unalterable chain of processing evidence. Additionally, as it features a decentralized and encrypted method of storing and sharing information within a distinct chain of blocks, the data is secure from fraud and hacking.

Utilizing DFSL's e-forensic application, this tool has been integrated into the Inter-Operable Criminal Justice System that promotes a secure transfer of information between the police, forensics, courts and prisons. In line with the multi-layered criminal justice system, each step, from the registration of a case to the preparation of forensic report forms a 'block' with a unique identification code. Similarly, in addition to a distinct QR code for each forensic sample, every time evidence is transferred to a different officer, a new block is formed to document the time and individual concerned.

Besides enhancing efficiency, accountability, and inter-departmental coordination within the criminal justice system, it will also build trust in the investigation process. By automating the process of evidence collection and evaluation, this secure tool restricts access of forensic experts to details of victims and suspects and of the investigation officer to forensic evidence prior to report formation. This ensures a transparent and tamper-free investigation, as opposed to previously close interactions between the investigation officers and forensic experts prior to final reports.

Source: https://www.hindustantimes.com/cities/delhi-news/delhi-forensic-science-laboratory-implements-blockchain-technology-for-transparent-evidence-record-101692294375620.html

INTERPOL
Innovation Centre
INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510
T: +65 65503569
Email: IC-Snapshots@interpol.int