Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Catherine Stupp

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA.

Euler Hermes declined to name the victim companies.

Law enforcement authorities and AI experts have predicted that criminals would use AI to automate cyberattacks. Whoever was behind this incident appears to have used AI-based software to successfully mimic the German executive's voice by phone. The U.K. CEO recognized his boss' slight German accent and the melody of his voice on the phone, said Rüdiger Kirsch, a fraud expert at Euler Hermes, a subsidiary of Munich-based financial services company Allianz SE.

Several officials said the voice-spoofing attack in Europe is the first cybercrime they have heard of in which criminals clearly drew on AI. Euler Hermes, which covered the entire amount of the victim company's claim, hasn't dealt with other claims seeking to recover losses from crimes involving AI, according to Mr. Kirsch.

Scams using AI are a new challenge for companies, Mr. Kirsch said. Traditional cybersecurity tools designed to keep hackers off corporate networks can't spot spoofed voices. Cybersecurity companies have recently developed products to detect so-called deepfake recordings.

It is unclear whether this is the first attack using AI or whether there are other incidents that have gone unreported or in which authorities didn't detect the technology in use, said Philipp Amann, head of strategy at Europol's European Cybercrime Center. Europol is the European police agency. While it is hard to predict whether there might soon be an uptick in cyberattacks using AI, Mr. Amann said hackers are more likely to use the technology if it makes attacks more successful or profitable.

The attackers responsible for defrauding the British energy company called three times, Mr. Kirsch said. After the transfer of the $243,000 went through, the hackers called to say the parent company had transferred money to reimburse the U.K. firm. They then made a third call later that day, again impersonating the CEO, and asked for a second payment. Because the transfer reimbursing the funds hadn't yet arrived and the third call was from an Austrian phone number, the executive became suspicious. He didn't make the second payment.

The money that was transferred to the Hungarian bank account was subsequently moved to Mexico and distributed to other locations. Investigators haven't identified any suspects, Mr.

Kirsch said.

It is unclear whether the attackers used bots to react to the victim's questions. If they did, it might have been even more difficult for law enforcement authorities to investigate, Mr. Amann said. A police investigation into the case has ended, Mr. Kirsch said. Europol wasn't involved.

Mr. Kirsch believes hackers used commercial voice-generating software to carry out the attack. He recorded his own voice using one such product and said the reproduced version sounded real.

A few software companies offer services that can quickly impersonate voices, said Bobby Filar, director of data science at Endgame, a cybersecurity company. "You don't need to be a Ph.D. in mathematics to use it." he said.

Another tactic hackers could use would be to stitch together audio samples to mimic a person's voice, which would likely require many hours of recordings. Security researchers demonstrated this technique at the Black Hat conference last year.

Attackers could use publicly available voice recordings to impersonate celebrities or executives.

"You can't go around and be silent the entire time. You're going to run into situations like this where you expose information that you never thought could be used against you," Mr. Filar said.

Applying machine-learning technology to spoof voices makes cybercrime easier, said Irakli Beridze, head of the Centre on AI and Robotics at the United Nations Interregional Crime and Justice Research Institute.

The U.N. center is researching technologies to detect fake videos, which Mr. Beridze said could be an even more useful tool for hackers. In the case at the U.K. energy firm, an unfamiliar phone number finally aroused suspicions. "Imagine a video call with [a CEO's] voice, the facial expressions you're familiar with. Then you wouldn't have any doubts at all," he said.

Write to Catherine Stupp at Catherine.Stupp@wsj.com