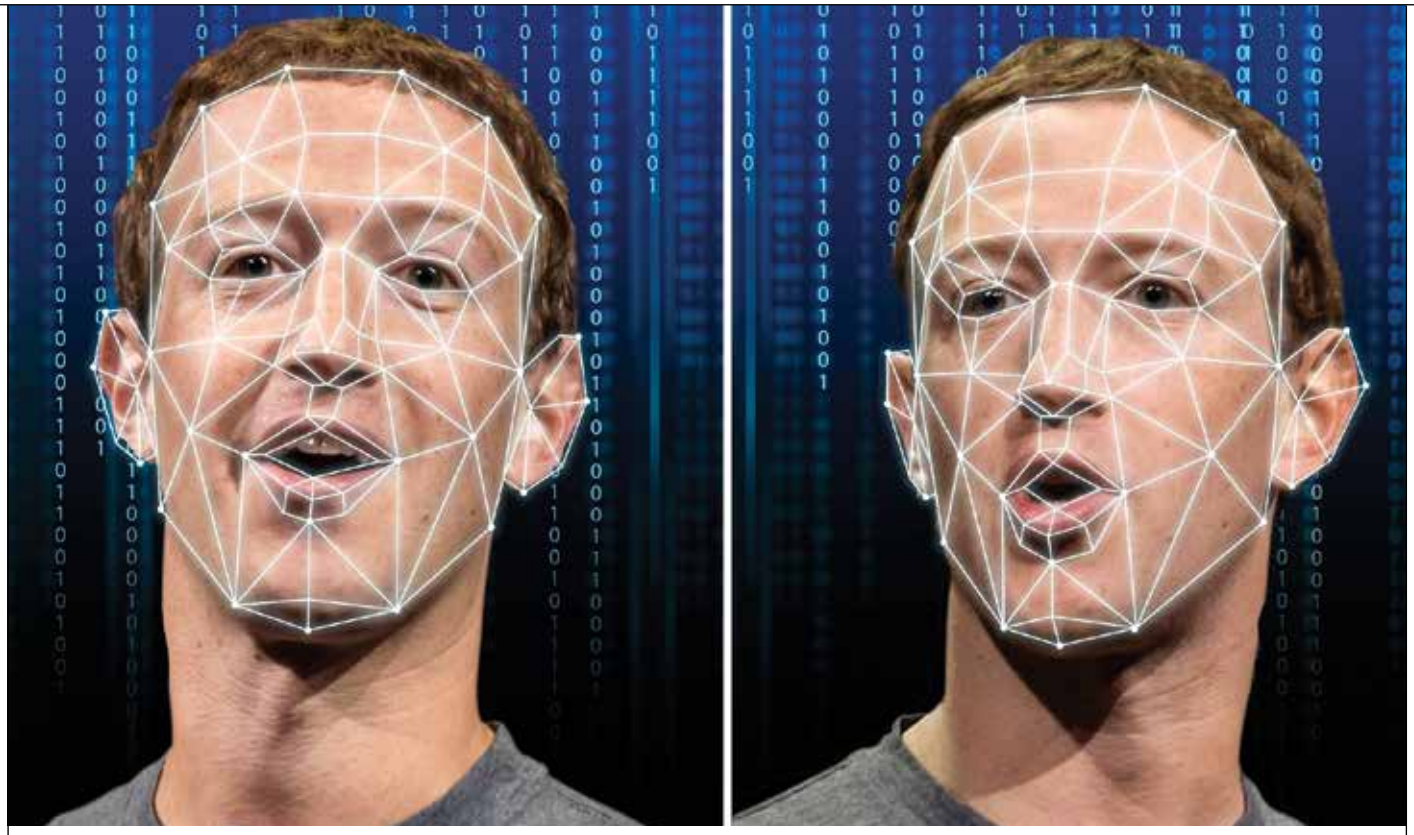

DEEPFAKES: THE NEW PANDEMIC ON THE HORIZON

Last year there were plenty of headlines on organisations suffering from ransomware, phishing and cyber attacks, with the Colonial Pipeline attack in May and Kaseya cyberattack in July making national headlines. This year, however, there may be a new threat – deepfakes.

Deepfakes are synthetic media in which a person is impersonated using artificial intelligence to trick people into thinking that it's actually them. They are a new technique that can be used by threat actors to carry out frauds, scams and social engineering tricks on organisations.

Alon Arvatz, Senior Director of Product Management at IntSights – a Rapid7 Company – explains: "Deepfakes are not yet a trend, and so far, we haven't seen a lot of attacks leveraging deepfakes as a method. However, the technique is something that is emerging and we're starting to see signs that suggest it will be a trend to be wary of in the future. Using artificial intelligence, cybercriminals or fraudsters use deepfake technology to either impersonate the face or voice – or both – of a person in order to carry out scams, fraud and social engineering attacks.

"Based on the hacker chatter that we track on the Dark Web, we've seen traffic around deepfake attacks increase by 43 percent since 2019. Based on this, we can definitely expect hacker interest in deepfake technology to rise and will inevitably see deepfake attacks becoming a more utilised method for hackers in 2022. Furthermore, like many other cyberattack methods, we predict that threat actors will look to monetise the use of deepfakes by starting to offer deep-fake-as-a-service, providing less skilled or knowledgeable hackers with the tools to leverage these attacks through just the click of a button and a small payment."

Dr. Nikolay Gaubitch, Director of Research at Pindrop, continues: "Throughout the pandemic the use of video as a means for communication both for personal use and in the workplace increased exponentially. This opened up new opportunities for fraudsters who already have the voice channels as one of their preferred means as part of their attacks. One side effect of this increased remote communications is a drive in innovation in audio and visual tools, some good, some not so good. The one that has received a lot of attention, is deepfakes.

"In 2021, we saw deepfakes on the rise. They've been harmlessly used in the media such as documentaries and we've even seen technology companies building deepfake tools with the potential for customer use. As with all technology, it can be used for both good and malicious purposes, and we know that fraudsters already have the capabilities to create deepfakes to con businesses.

"Deepfakes are not just image and video related, voice synthesis (making a machine sound like somebody) and voice conversion (making a human talker sound like someone else) are growing trends and fraudsters are increasingly taking advantage of innovative tools. These techniques are not so well-known to the public because of the limited real-word applications available today, however it is a very real threat and a tactic we have already seen fraudsters adopt, for example, the recent $35-million bank heist.

"With fraudsters looking to hone their skills and capabilities to create both deepfakes and voice synthesis, I predict they will only increase in popularity as we move through 2022. It is therefore vital that businesses be aware of these new techniques and adopt the appropriate technology to combat them."

By mapping a subject's face with specialist software, facial features can be manipulated for nefarious purposes

Alon Arvatz – Senior Director of Product Management at IntSights, a Rapid7 Company – is a veteran of an elite cybersecurity intelligence unit where he led and coordinated global cyber intelligence campaigns."

Nikolay Gaubitch – Director of Research at Pindrop – is the co-author of more than 50 scientific publications and patents, the co-editor of the book Speech Dereverberation and he served as an Associate Editor of the journal IET Signal Processing.