5 NEW EXOTIC CYBER-THREAT TRENDS FOR 2020

The third decade of the 21st century is upon us and technology is making large leaps that are almost impossible to keep up with. Staying cyber-aware is the key to safeguarding against ever-evolving cyber-threats and vulnerabilities. The following are cyber-threat trends you can expect to see in 2020 and beyond:

1 Deep Fake Videos

With the drastic advancement of deep fake video technology, it is now possible to produce near-perfect indistinguishable-to-the-eye deep fake videos impersonating real people. This could include people in positions of power and who have had plenty of video exposure on the internet, which makes every inch of their face available for threat actors to map with artificial neural networks. After, for example, making a deep fake of your CEO, threat actors can use it for social engineering, fraud, data or monetary theft, reputation damage and security breaches that can wreak havoc on any organization's or even state's continuity.

2 Voice Changers

Just like deep fake videos, a voice changer tool may utilize advanced machine learning algorithms to "learn" the individual characteristics of someone's voice from a multitude of sources. A threat actor can then use the tool to "sound like someone else" while making a call, in real time. This method can be used for identity theft, impersonating a person in a place of power when talking to people who are familiar with that voice. Although a useful technology for threat actors, frauds like this have been occurring for decades by talented voice impersonators.

3 Widened Cyberattack Surface

The increasing interconnectivity of smart devices in the last decade has improved our lives by making it easier for us to combine functionalities across devices. This, however, has made it potentially easier for threat actors to gain access to sensitive data by compromising an easy-to-hack Internet of Things (IoT) device. Remember the 2017 casino hack using a fish tank's Bluetooth thermostat that resulted in high-roller personal data theft? Now imagine smartwatches, smartphones, headphones, cars, all interconnected, all potential gateways for a malicious breach.

4 5G Threats

Related to the widening cyberattack surface, 5G vastly increases the range, and therefore susceptibility to attack, of wireless devices together with their reach of cyberattackers. By expanding the possibilities of interconnected devices, 5G technology also provides a new opportunity for threat actors to exploit. Within the scope of connected smart cars, smart cities, and smart business and state infrastructure, 5G can potentially be used to breach networks for malicious purposes from a distance greater than Wi-Fi or 4G channels could ever achieve. This also emboldens threat actors since it reduces the risk of them getting caught by allowing them to attempt wireless data breaches and cyberattacks from greater distances.

5 Identity Theft

The rapid adoption of new technologies, the cyber-threat landscape is changing faster than you can blink, resulting in a widened cyberattack surface and new sophisticated cyberattack methods that traditional antivirus and firewall protection is simply impossible to catch up with. With the wide use of Internet of Things (IoT) devices and the increasing reliance on automation, we are now potentially more susceptible to identity theft than ever before. In 2019, we saw a drastic rise in new account fraud and account takeovers that coincide with an even greater number of data theft occurrences involving data theft methods such as formjacking. From 2020 and beyond, we expect to see identity theft fraud resulting from more novel and elaborate cyberattack methods that empower criminals to steal and assimilate sensitive personal data.

HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades Str.
2012 Strovolos, Nicosia
T +357 22 463600 **F** +357 22 463563 **E** info@odysseycs.com

www.odysseycs.com

ODYSSEY™ cybersecurity

OFFICES CYPRUS | GREECE | USA | UK | KSA