TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

CYBER THREATS TO LOOK FOR IN 2020

follow us: @tataadvanced

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

With the advent of new technologies, the doors of complex cybersecurity challenges have opened. This advancement has provided cyber criminals with thousands of opportunities to exploit and damage an organisation's cybersecurity infrastructure.

Let us have a look at some of the prominent cybersecurity threat areas that organisations must watch out for in 2020.

01. Over the last decade, Internet-connected smart devices used in offices and homes have proliferated. Most of these devices do not have enough security features installed, which allows attackers to coerce the device and enter an organisation's network.

02. All through 2019, ransomware kept standing out as truly newsworthy and will continue to be a prevalent threat in 2020. It is still the most reliable way for hackers to make money.

03. Deepfake attacks have shown a remarkable growth in past few years. With the help of advanced analytic technology, Generative Adversarial Networks (GANs), the threat actors can now produce fake but incredibly realistic videos and images that are difficult for humans to identify. In 2020, Deepfake attacks are likely to be an insidious threat to the cyber security landscape.

follow us: @tataadvanced

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

04. Since Microsoft has announced that the support and updates for Windows 7 will not be available after 14 January 2020, the probability of cyber attacks targeting PCs running that operating system is predicted to go high. The company has suggested users to install newer Windows 10 to mitigate such possible negative scenarios.

05. The advent and global adoption of 5G infrastructure technology will bring a new wave of 5G compatible devices, which would demand more security. Accordingly, the companies will be required to reassess their security paradigms for providing a secure and reliable mobile platform.

06. Since 2016, web-skimming (or e-skimming) attacks have compromised thousands of e-commerce websites to collect customers payment card information. Over the time, the threat actors performing e-skimming attacks have also evolved and are ready to target small- and medium-sized businesses as well as government agencies.

07. With the recently developed malicious rootkits, the hacktivists will now attempt to compromise the supply chain of legitimate software packages by deploying hard-to-detect malware. The level of associated risk is high as the implanted malware would be difficult to remove even after formatting the system.

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

08. Threat actors are now exploring the innovations in technology to create a new wave of cyber attacks involving machine learning and artificial intelligence. They have developed a new AI-powered malware that has the potential to automate human skills and processes, and can significantly increase the scale of damage caused by malware attacks.

09. Recently, a major security flaw was observed in the Huawei MateBook systems running the company's PCManager software. The software comprised an insecure driver that allowed underprivileged users to create processes with high-level privileges. Such loopholes let attackers to exploit the vulnerability and circumvent the device's security by using asynchronous procedure calls to further interrupt system processes and run malicious code.

10. As an alternative to email, the hackers are now using interactive social media platforms like WhatsApp, Facebook, Instagram and LinkedIn to entice victims into immediate actions such as calling a deceitful contact number, visiting a malicious website or downloading files containing mobile malware. Such attacks are now becoming an emerging threat to the cyber space.