Is Antivirus Software Enough in 2020?

Back in the heady days of dial-up connections and the early internet, a solid antivirus program was considered enough to protect your home or work PC from the handful of threats making the rounds.

Fast forward 20 years and the “threat landscape”, to borrow from cybersecurity parlance, has shifted considerably. Yesteryear’s trojans and worms still exist, but they have been joined by an increasingly sophisticated group of malicious codes that are engineered specifically to bypass the basic cybersecurity most internet users rely on.

Further complicating the risk to today’s net users is just how connected we are. The single home computer has given way to smart devices in our pockets, on our wrists, and even running our thermostats. Greater connectivity is a boon for convenience, but it’s also a boon for cybercriminals seeking to infiltrate networks and garner data.

Antiviruses, while they still have their place and use, are simply not enough to protect individuals and businesses from the level of threats running rife on the interwebs.

Below are some of the developments cybersecurity experts are concerned about in 2020 and a few tools you need in your cybersecurity arsenal.

Artificial Intelligence (AI) enhanced cyber attacks

Machine learning and AI have triggered significant changes across all industries and to consumers. AI is in use in manufacturing, security, marketing, and countless other fields. Once the preserve of dystopian fiction, artificial intelligence is now mainstream. Have an Alexa in your house? You have an AI-enabled device.

While it might be incredibly helpful to us, AI is also giving cybercriminals a helping hand. The very same capabilities used to find and prevent cyberattacks are put to clever use by hackers in the form of adaptive malicious threats.

AI Fuzzing

Fuzzing is a practice of exploring a system to expose threats and vulnerabilities and is traditionally carried out by professional cybersecurity experts. AI fuzzing is the same process but bolstered by the capabilities of smart AI tools.

Hackers have now begun using AIF to commit crimes, despite the difficulties involved in creating these incredibly complex fuzzing systems. According to research by leading cybersecurity vendor Secure Computing, hackers are actively sharing their fuzzing findings with other cybercriminals in forums and chat rooms, further increasing the threat level.

Machine Learning positioning

Like AIF above, Machine Learning (ML) positioning is another key cybersecurity tool that has been exploited by threat actors.

An ML database can swiftly pull up information from any malware script that has been detected in that past, so when tweaked or brand new malware is detected, the ML system can automatically examine and block the code because similar events have been malicious. ML techniques like this enabled security group Cylance to uncover a campaign by OceanLotus, a hacking group linked to Vietnam, as reported by ZDNet.

However, if hackers infiltrate an ML system and inject instructions, the whole process of threat detection and elimination can be significantly hindered.

2020's threats are a far cry from what many of us think cybersecurity efforts are focused on. To counter the ever-evolving nature of cybercrime, individuals and companies alike need to first understand that a single antivirus program alone can't cut the security mustard, and take steps to up the ante when it comes to digital defenses.

VPN protection

Many users rely on a VPN app for privacy, but perhaps the best thing a Virtual Private Network offers is advanced encryption techniques that keep data transmissions safe and secure. For offices, consider installing a VPN router so that the whole network is protected rather than single devices.

Anti-malware programs

In many ways, anti-malware software is like an antivirus program for the modern net user. Like antiviruses, these digital tools also detect standard threats, but they go further than that and find and quarantine more advanced threats delivered through social engineering tactics.

Vulnerability scanners

Vulnerability scanners are fully automated tools that scour networks looking for any issues or areas of potential concern, and they're essential to organizations and individuals who handle client data. In fact,

vulnerability scanning is frequently mandated by government or industry cybersecurity standards.

While the threat level has certainly increased in 2020 savvy internet users and organizations can still prevent data breaches and attacks by attending to more than just the basics of security. Keep your antivirus, but make sure it’s backed up by tools that meet modern threats.