McAfee, FireEye's top 8 cyberthreat predictions for 2022

McAfee Enterprise and FireEye's 2022 Threat Predictions were released earlier this week, and examine the top cybersecurity threats they predict enterprises will face in 2022.

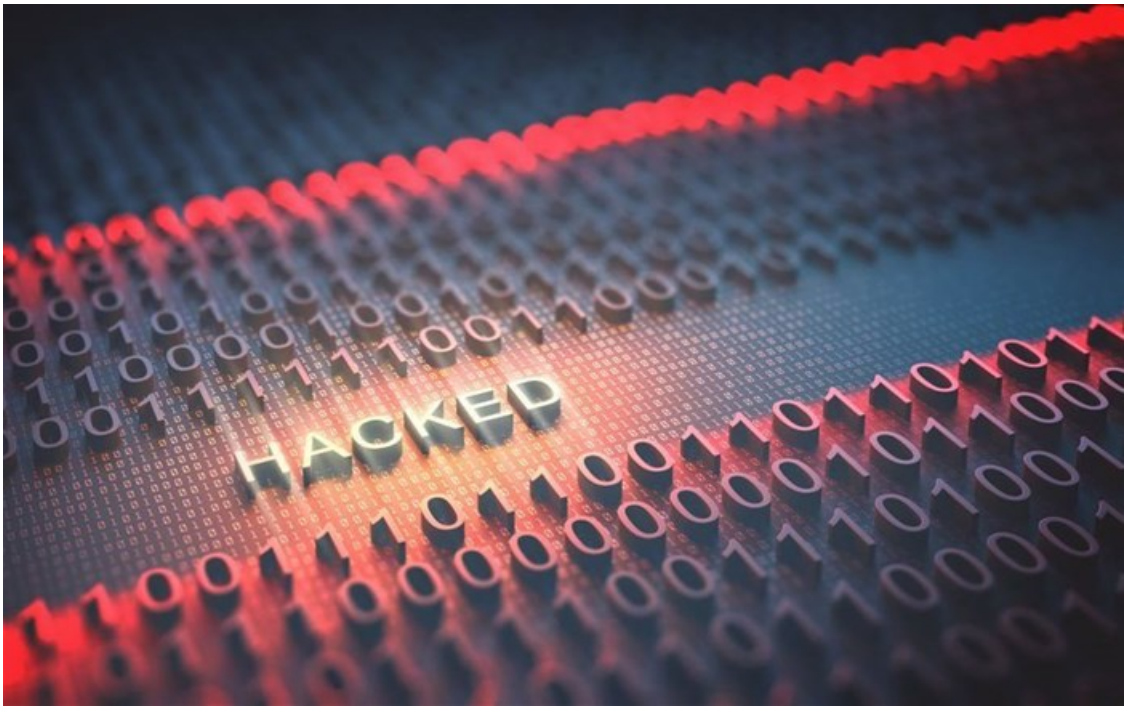

Image source: © ktsdesign – 123RF.com

Bad actors have taken note of successful tactics from 2021, including those making headlines tied to ransomware, nation states, social media and the shifting reliance on a remote workforce. We expect them to pivot those into next years' campaigns and grow in sophistication, wielding the potential to wreak more havoc across the globe. Skilled engineers and security architects from the recently combined entity offer a preview of how the threat landscape might look in 2022 and how these new or evolving threats could potentially impact enterprises, countries, and civilians.

"Over this past year, we have seen cybercriminals get smarter and quicker at retooling their tactics to follow new bad actor schemes – from ransomware to nation states – and we don't anticipate that changing in 2022," said Raj Samani, fellow and chief scientist of the combined company. "With the evolving threat landscape and continued impact of the global pandemic, it is crucial that enterprises stay aware of the cybersecurity trends so that they can be proactive and actionable in protecting their information."

2022 cybersecurity forecast: Deepfakes, cryptocurrency and mobile wallets

27 Oct 2021

McAfee Enterprise & FireEye 2022 predictions:

1. **Lazarus wants to add you as a friend.** Nation States will weaponize social media to target more enterprise professionals, looking to infiltrate organisations for their own criminal gain.

2. **Help wanted: Bad guys with benefits.** Nation States will increase their offensive operations by leveraging cybercriminals, prompting companies to audit their visibility and learn from operations conducted by actors targeting their sectors.

3. **Game of ransomware thrones.** Self-reliant cybercrime groups will shift the balance of power within the RaaS eco-kingdom from those who control the ransomware to those who control the victim's networks.

4. **Ransomware for dummies.** Less-skilled operators won't have to bend the knee in RaaS model power shift as they leverage the expertise encoded by more skilled ransomware developers.

5. **Keep a close eye on API.** 5G and IoT traffic between API services and apps will make them increasingly lucrative targets, causing unwanted exposure of information.

6. **Hijackers will target your application containers.** Expanded exploitation of containers and vulnerable applications will lead to endpoint resource takeovers.

7. **Zero cares about zero-days.** The time to repurpose vulnerabilities into working exploits will be measured in hours and there's nothing you can do about it... except patch.