Deepfakes, Cryptocurrency and Mobile Wallets: Cybercriminals Find New Opportunities in 2022

blog.checkpoint.com/2021/10/26/deepfakes-cryptocurrency-and-mobile-wallets-cybercriminals-find-new-opportunities-in-2022

October 26, 2021

Check Point Software 2022 Cyber-security Predictions also anticipates an increase in supply chain attacks in the new year

Check Point® Software Technologies released its cyber-security predictions for 2022 detailing the key security challenges that organizations will face over the next year. While cybercriminals continue to leverage the impact of the COVID-19 pandemic, they will also find new opportunities for attack with deepfakes, cryptocurrency, mobile wallets and more.

"In 2021, cyber criminals adapted their attack strategy to exploit vaccination mandates, elections and the shift to hybrid working, to target organizations' supply chains and networks to achieve maximum disruption," said Maya Horowitz, VP Research at Check Point Software. "The sophistication and scale of cyber-attacks will continue to break records and we can expect a huge increase in the number of ransomware and mobile attacks. Looking ahead, organizations should remain aware of the risks and ensure that they have the appropriate solutions in place to prevent, without disrupting the normal business flow, the majority of attacks including the most advanced ones. To stay ahead of threats, organizations must be proactive and leave no part of their attack surface unprotected or unmonitored, or they risk becoming the next victim of sophisticated, targeted attacks"

Check Point Software's cyber-security predictions for 2022 cover globally-related developments; malware, privacy and cyber-conflicts; and technology cyber-security predictions.

Global cyber-security predictions for 2022:

Fake news 2.0 and the return of misinformation campaigns: The claim of 'fake news' surrounding contentious issues has become a new attack vector over previous years without people really understanding its full impact. Throughout 2021, misinformation was spread about the COVID-19 pandemic and vaccination information. The black market for fake vaccine certificates expanded globally, now selling fakes from 29 countries. Fake 'vaccine passport' certificates were on sale for $100-120 and the volume of advertisement groups and group sizes publishing sellers multiplied within the year. In 2022, cyber groups will continue to leverage these types of fake news campaigns to execute various phishing attacks and scams.

In addition, prior to the 2020 US presidential election, Check Point researchers spotted surges in malicious election-related domains and the use of “meme camouflage” aimed at shifting public opinion. In the run-up to the US midterm elections in November 2022, we can expect to see these activities in full effect and the return of misinformation campaigns on social media.

Supply chain cyber-attacks continue to grow, and governments will address the challenge: Supply chain attackers take advantage of a lack of monitoring within an organization’s environment. They can be used to perform any type of cyber-attack, such as data breaches and malware infections. The well-known SolarWinds supply chain attack stands out in 2021 due to its scale and influence, but other sophisticated supply chain attacks have occurred such as Codecov in April, and most recently, Kaseya. Kaseya provides software for Managed Service Providers (MSPs) and the REvil ransomware gang exploited the company to infect over 1,000 customers with ransomware. The group demanded a ransom of $70 million to provide decryption keys for all affected customers.

Supply chain attacks will become more common and governments will begin to establish regulations to address these attacks and protect networks. They will also look into collaborating with the private sectors as well as other countries to identify and target more threat groups operating on a global and regional scale.

In 2022, we also expect to discover more about the global impact of the infamous Sunburst attack. As investigations are still ongoing, security researchers will unveil some of the biggest questions regarding the attack: What were the attackers doing these networks, and how did they benefit from the massive attack?

The cyber ‘cold war’ intensifies: The cyber cold war is intensifying, and taking place online as more nation state actors push western governments to continue to destabilize society. Improved infrastructure and technological capabilities will enable terrorists groups and political activists to further their agendas and carry out more sophisticated, widespread attacks. Cyber-attacks will increasingly be used as proxy conflicts to destabilize activities globally.

Data breaches are larger scale and more costly: Going into 2022 we will see an increase in data breaches that will be larger scale. These breaches will also have the potential to cost organizations and governments more to recover. In May 2021, US insurance giant paid $40 million in ransom to hackers. This was a record, and we can expect ransom demanded by attackers to increase in 2022.

Technology cyber-security predictions for 2022:

Mobile malware attacks increase as more people use mobile wallets and payment platforms: In 2021, 46% of organizations had at least one employee download a malicious mobile application. The move to remote work for almost entire populations across the world during the COVID-19 pandemic saw the mobile attack surface expand dramatically, resulting in 97% of organizations facing mobile threats from several attack vectors. As mobile wallets and mobile payment platforms are used more frequently, cybercriminals will evolve and adapt their techniques to exploit the growing reliance on mobile devices.

Cryptocurrency becomes a focal point for cyberattacks globally: When money becomes purely software, the cyber security needed to protect against hackers stealing and manipulating bitcoins and altcoins is sure to change in unexpected ways. As reports of stolen crypto wallets triggered by free airdropped NFTs become more frequent, Check Point Research (CPR) investigated OpenSea and proved it was possible to steal crypto wallets of users by leveraging critical security. In 2022, we can expect to see an increase in cryptocurrency related attacks.

Attackers leverage vulnerabilities in microservices to launch large scale attacks: The move to the cloud and DevOps will result in a new form of botnet. With microservices becoming the leading method for application development, and microservices architecture being embraced by Cloud Service Providers (CSPs), attackers are using vulnerabilities found in microservices, to launch their attacks. We can also expect to see large-scale attacks targeting CSPs.

Attackers weaponize deepfake technology: Techniques for fake video or audio are now advanced enough to be weaponized and used to create targeted content to manipulate opinions, stock prices or worse. As in the case of other mobile attacks that rely on social engineering, the results of a phishing attack can range from fraud to more advanced espionage. For instance in one of the most significant deepfake phishing attacks, a bank manager in the United Arab Emirates fell victim to the threat actor's scam. Hackers used AI voice cloning to trick the bank manager into transferring $35 million. Threat actors will use deepfake social engineering attacks to gain permissions and access sensitive data.

Penetration tools continue to grow: Globally in 2021, 1 out of every 61 organizations was being impacted by ransomware each week. Ransomware will continue to grow, despite the efforts of law enforcement to limit this growth globally. Threat actors will target companies that can afford paying ransom, and ransomware attacks will become more sophisticated in 2022. Hackers will increasingly use penetration tools to customize attacks in real time and to live and work within victim networks. Penetration tools are the engine behind the most sophisticated ransomware attacks that took place in 2021. As the popularity of this attack method grows, attackers will use it to carry out data exfiltration and extortion attacks.