FINANCIAL EXPRESS
Read to Lead

Cyberspace and Digital Currency: Addressing unique challenges for improved data protection

Recent statistics show that the use of digital currencies has increased

According to Quick Heal's Annual Threat Report 2023, last year saw a number of crypto-jacking incidents

By Sanjay Katkar

The digital world today has expanded way beyond the scope of its usage as imagined three decades ago. With deeper penetration of internet services and subsequent rapid digitization in India and around the globe, the world has become an increasingly convenient place for both – internet users and cybercriminals. The global cybersecurity sector is keenly aware of the unique challenges that cyberspace and digital currency pose for data protection. The rise of digital currencies, such as Bitcoin, has introduced new risks and complexities to the world of cybersecurity

Recent statistics show that the use of digital currencies has increased significantly over the last few years, and this trend is expected to continue. Cryptocurrency mining, also known as coin mining, has lately become increasingly popular as a way to generate income by using computer resources to solve complex algorithms and earn digital currencies. However, cybercriminals have found ways to exploit this technology to steal computing resources from unsuspecting victims in a practice known as crypto-jacking, leading to unauthorized use of computer resources.

Beyond the allure of coin mining

According to Quick Heal's Annual Threat Report 2023, last year saw a significant number of crypto-jacking incidents were detected on Windows machines, with an average of 39,311 cases reported daily. One particular malware strain called SmokeLoader, which is known to distribute other malicious software like SystemBC and Raccoon Stealer 2.0, has been observed distributing a new type of clipper malware called Laplas Clipper. This malware is designed to target cryptocurrency users and steal their digital assets. More than 180 samples of the clipper malware have been identified, indicating that it is widely deployed.

The Laplas Clipper malware is typically distributed through malicious documents like Word or PDF files, sent through spam emails, or through targeted spear-phishing attacks. Once installed, the malware can monitor the victim's activities and steal sensitive information such as login credentials, digital wallets, and private keys. The criticality of this campaign is considered medium as it primarily targets cryptocurrency users, who are a specific subset of the population, but it has an international impact. The emergence of Laplas Clipper and other malware affecting digital currencies amply highlights how malicious entities can use these technologies to harm internet users.

Challenges with digital currencies and cyberspace

One of the main challenges of digital currencies is their decentralized nature. Unlike traditional currencies, which are backed by governments and financial institutions, digital currencies are not regulated by any central authority. This lack of regulation makes it difficult to monitor and prevent illegal activities, such as money laundering and terrorism financing. According to a report by the United Nations Office on Drugs and Crime, digital currencies are increasingly being used by criminal groups to facilitate illegal activities, such as drug trafficking and human smuggling.

Another challenge of digital currencies is the anonymity they offer. They allow users to conduct transactions without revealing their identity, making it difficult to trace the flow of money. This anonymity has made digital currencies attractive to criminals, as it allows them to move money across borders and avoid detection. Digital currencies are becoming the preferred method of payment for criminal activities, such as ransomware attacks and the sale of illegal goods and services. According to International Monetary Fund (IMF), without proper regulation, digital money could be a virtual safe haven for criminals' illicit financial transactions

In addition to these challenges, cyberspace presents its own set of risks and vulnerabilities. With the proliferation of connected devices, the volume of data generated and transmitted electronically has increased exponentially. This data includes sensitive personal and financial information, making it a prime target for cybercriminals. With 450 million records exposed, India suffered second-highest data breaches in 2022, accounting for 20 percent of all records exposed across the globe. Most of these breaches were a result of ransomware attacks and unsecured databases.

Addressing the unique challenges

The unique cybersecurity challenges posed by the widespread use of digital currencies and cyberspace requires organizations and governments to take a proactive approach to cybersecurity. This includes implementing robust cybersecurity measures to protect against data breaches and cyberattacks. Encryption, firewalls, and access control mechanisms are essential tools for protecting sensitive data in cyberspace. In the case of digital currencies, transaction monitoring and reporting mechanisms can help to detect and prevent illegal activities.

In addition to these technical measures, organizations and governments must also establish regulatory frameworks for digital currencies. AML and KYC requirements can help to ensure that digital currencies are not used for illegal activities. Governments can also work together to establish international standards and best practices for cybersecurity and digital currencies. On an individual and organizational level, users are advised to regularly update their operating systems and security software to protect against crypto-jacking and clipper malware attacks. It is also essential to avoid opening suspicious attachments, links, or emails from unknown sources.

As the popularity of cryptocurrencies continues to grow, so too will the threat of cyber criminals looking to exploit the technology for their own gain. Therefore, it is essential to remain vigilant and take appropriate measures to safeguard digital assets and computer resources.

The increasing reliance on cyberspace and digital currency has introduced new challenges in data protection. However, proactive cybersecurity measures and regulatory frameworks can help organizations and governments mitigate these risks and safeguard sensitive data. It is crucial to continuously improve cybersecurity to keep up with the evolving threats posed by cybercriminals. Policymakers and cybersecurity leaders must stay up-to-date on the latest trends and technologies to implement necessary measures to protect public interests.

In conclusion, addressing these unique challenges will require close collaboration between industry, government, and academia. Government can help by creating an environment that supports innovation as these new technologies need commitment for continuous innovation and improvements.

The author is joint managing director and chief technology officer, Quick Heal Technologies