Unprotected Entry into the Metaverse Brings Accrued Cyber Risks

DUBAI, UNITED ARAB EMIRATES, July 20, 2022 /EINPresswire.com/ -- Enterprises that are considering joining the metaverse bandwagon have been put on high alert against imminent cyberattacks that could expose their valuable data to crippling cyberattacks, data exfiltration and breaches.

Candid Wuest VP Cyber Protection Research - Acronis

As brands get increasingly engulfed in the metaverse, largely driven by the exciting opportunities that this relatively new digital concept presents, IT and cybersecurity experts are seriously concerned that most of them are rushing to establish their presence without a proper cybersecurity strategy.

Metaverse, an attempt to create an immersive virtual world that combines augmented and virtual reality, includes economic and social spaces where users from anywhere in the world can enjoy a wide range of content and experiences.

This, according to cybersecurity experts, also significantly exposes individual internet users and brands that are playing in that space to a plethora of risks that could lead to a surge in cases of account hacking and tampering, phishing and assets theft.

“Metaverse is an exciting and futuristic concept that is creating enormous opportunities for enterprises as well as innovators. However, enterprises that are considering operating in that space should also be wary of the imminent cyber threats that come with new innovations. As soon as digital property in the 3D universe, for instance, becomes of value, cases of account hacking, theft, ransomware and phishing will also increase significantly. Partly to blame will be the lack of a solid cyber protection strategy to safeguard private and confidential information

from potential attackers," said Candid Wüest, VP of Cyber Protection Research, Acronis.

According to the Acronis Cyber Protection Week Global Report 2022, cybercriminals are exploiting the IT complexity to launch catastrophic cyberattacks. With most users still not fully aware of the magnitude of the cyber threats they are facing in the wake of increased metaverse adoption, daily data theft (credit card, identity, passwords, etc.), malware, phishing attacks are likely to increase by 200% by 2024 due to unpreparedness or lack of a cyber protection master plan.

Main risks

Device security remains high on the cyber protection priority list as platform and device hacking is widely expected to soar as the metaverse uptake also skyrockets. Threats and breaches to devices is likely to worsen and could subsequently also have actual terminal consequences in the physical world.

"For individual users of metaverse, hacking of metaverse-enabled devices like specific headsets, for instance, can cause seizures, if someone is epileptic. It can also hurt their vision or hearing at least temporarily as well as expose their physical location, and more," noted Candid Wüest.

Metaverse will not have entirely new security issues as it will have similar issues as the gaming industry. The explosive popularity of gaming, which is arguably the biggest segment of the entertainment industry, with over three billion regular participants, paints a picture of just how lucrative the metaverse can become for cybercriminals based on the number of users it can attract.

Data regulation

The lack of data collection and usage regulation has also emerged as a possible enabler of cyber threats within the virtual reality platform. This, IT security experts warn, could create a myriad of loopholes that cybercriminals could exploit to infiltrate private networks and gain unrestricted access to sensitive data from enterprises and individuals.

With regulation lacking, cybercrime could become the fastest-growing type of crime currently valued at US$1-2 trillion and growing at a faster rate. However, despite the commitment by social media giant Meta that it will invest US$50 million in external research that will primarily focus on privacy and security in the metaverse – including a partnership with the National University of Singapore, to investigate data use – more still needs to be done, especially by enterprises to secure their data.

These safeguard measures include a comprehensive artificial intelligence and machine learning-driven cyber protection strategy combined with vulnerability assessment and penetration testing. Other effective security measures include blockchain technology to identify users; tokens assigned by an organization and the use of biometrics in a headset to confirm user identity.

Metaverse warfare
While the concept of a virtual world was developed primarily for social platforms to help them boost engagement, the immersive multi-dimension will also create more opportunities for complex cyber-attacks.

“Metaverse for information warfare is now emerging as a real threat that could be used to spread malicious information. Issues such as deep fake news will be more convincing in the metaverse, news coverage will get more “gruesome”, and sports and entertainment will feel more real. Emotions will run high – which in theory a weakness used by threat actors, including politically motivated ones,” noted Candid Wüest.

Media Team
Matrix PR
+971 43430888
email us here
