Biometric Authentication Could Be an Achilles Heel for Metaverse Security

Trend Micro research highlights risks posed by more seamless log-in technology

DALLAS, Oct. 18, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released a new report warning that exposed biometric data creates a serious authentication risk across a wide range of digital scenarios, including the metaverse.

To read a full copy of the report, *Leaked Today, Exploited for Life: How Social Media Biometric Patterns Affect*, please visit: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/leaked-today-exploited-for-life-how-social-media-biometric-patterns-affect-your-future

"Research from Trend Micro reveals the risks posed by exposed biometric data and what users need to know to protect themselves."

William Malik, vice president of infrastructure strategies at Trend Micro said, "The use of biometrics is championed by some as a more secure, easier to use alternative for passwords. However, unlike passwords, our features can't be easily changed. So a compromise could have a long-lasting impact on users. Hijacking a user's metaverse profile in the future could be similar to gaining complete access to their PC today."

Trend Micro defines the metaverse as: "a cloud distributed, multi-vendor, an immersive-interactive operating environment that users can access through different categories of connected devices."

As such, those able to impersonate individuals inside this new iteration of the web could gain access to everything from online banking accounts and cryptocurrency stores to highly sensitive corporate data.

As outlined in the report, threat actors in the future may be able to use stolen or leaked biometric data to trick connected devices, such as VR/AR headsets, into logging them in as someone else. That could open the door to data theft, fraud, extortion, and much more.

Metaverse user profiles may also be an attractive target as a valuable source of additional biometric data, such as detailed 3D user models that mimics a person's real-life bio features.

In this new computing environment, two of thethree factors typically used to authenticate will be registered with the software maintaining the metaverse, for example.

Trend Micro's report is intended to generate more dialog in the IT and security community about how to head off such potential risks. It warns that huge volumes of biometrics details, including face, voice, iris, palm, and fingerprint patterns, are already being exposed online in high enough quality to trick authentication systems.

It can be found in images and audio content posted on social media and messaging platforms, news media sites, and government portals that people use every day.

As well as helping threat actors bypass authentication checks, judicious use of leaked or stolen biometric data could also help to create deepfake models *en masse*, the report warns.

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: MEDIA CONTACT: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

Additional assets available online: Photos (1)

Additional assets available online: Photos (1)

https://newsroom.trendmicro.com/2022-10-18-Biometric-Authentication-Could-Be-an-Achilles-Heel-for-Metaverse-Security