METAVERSE OR METAWORSE?

Cybersecurity Threats Against the Internet of Experiences

Numaan Huq, Roel Reyes, Philippe Lin, and Morton Swimmer

TREND MICRO™ | research

Published by

Trend Micro Research

Written by

**Numaan Huq,
Roel Reyes,
Philippe Lin, and
Morton Swimmer**

Stock images used under license from
Shutterstock.com

Contents

The term “metaverse” was created by author Neal Stephenson for his 1992 cyberpunk novel Snow Crash. It describes the virtual reality (VR) world in which the book’s protagonist, Hiro, socializes, shops, and vanquishes real-world enemies through his avatar.[1] Hiro accesses the metaverse using a pair of VR goggles and a headset and appears inside the digital world as an avatar. Virtual spaces that allow people to explore and interact with massive virtual worlds using avatars (albeit minus the immersive VR experience that is the cornerstone of Snow Crash) already exist, mostly in the form of massively multiplayer online role-playing games (MMORPGs) such as *Roblox*, *Minecraft*, *Fortnite*, and *Second Life*.

Stephenson’s science fiction metaverse is an immersive virtual world in which players can escape and lead parallel lives. The real world metaverse that we can interact with today is a collection of disjointed VR worlds catering mostly to gamers rather than everyday users. All of that is expected to change in the next couple of years.

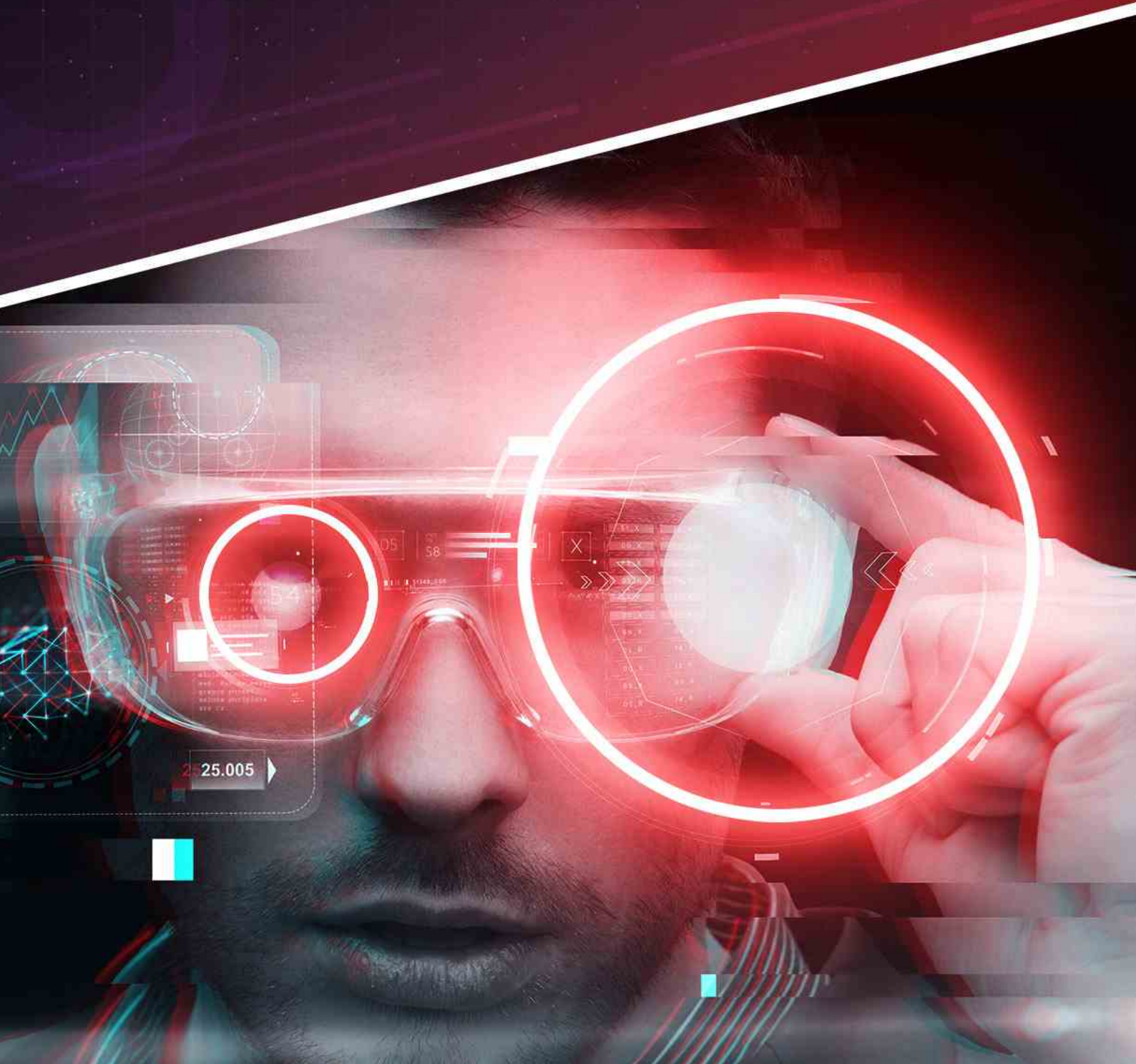
In October 2021, Facebook announced that they were going to rebrand themselves[2] as Meta and focus research and development efforts on building the metaverse. According to Facebook, “*the metaverse will feel like a hybrid of today’s online social experiences, sometimes expanded into three dimensions or projected into the physical world. It will let you share immersive experiences with other people even when you can’t be together – and do things together you couldn’t do in the physical world*.”[3] An immersive user experience not tied to a specific game or virtual reality application is long overdue, and Meta is the first tech giant to publicly pledge their support to building it.

With the advent of new and emerging technologies such as augmented/virtual/mixed/extended reality (AR/VR/MR/XR), the internet of things (IoT), artificial intelligence & machine learning (AI/ML), distributed ledger technology (DLT), IPv6, and the Spatial Web, a new interactive application layer was needed to provide a foundation for integrating all of these technologies and build the Internet of Experiences (IoX).

While the metaverse marketing hype is making everyone excited about the future, the reality is that the metaverse is not a single product that one company can build alone.[4] Optimistically, the promised metaverse dream is estimated to be at least five to ten years away from becoming reality. Metaverse-like applications already exist today, such as the popular *Decentraland* and *Cryptovoxels*, games like *Flight Simulator*, and some of the MMORPGs mentioned previously. However, the latter applications primarily cater to gamers and not everyday users. Over the next three to five years, we expect to see the introduction of more metaverse-like applications. These next-generation applications will likely be used in daily activities such as remote work, entertainment, education, and shopping.

We anticipate that at some point in the future when the technology has reached its maturity in terms of hardware, software, network infrastructure, and ubiquity, there will be a natural convergence of the many metaverse-like applications. The convergence will become a shared cyberspace that will eventually become the metaverse. In this shared cyberspace, users will be able to transition seamlessly from one application to the next, with a wide variety of hardware options for accessing the metaverse. Until then, there will be a pile of technical and design problems to solve.

What is the Metaverse?



What is the metaverse? There seems to be no single answer to this question. Everyone has a different opinion about what the metaverse is and how it fits into the bigger picture of the internet. No idea is wrong, given that the metaverse concept is not well defined. To aid in our research, we created a working definition for it that we fully expect to evolve as the metaverse concept itself evolves.

This working definition is a good starting point for exploring all the upcoming technologies and predicting what types of cyberthreats will arise in the metaverse:

The metaverse is a cloud distributed, multi-vendor, immersive-interactive operating environment that users can access through different categories of connected devices (both static and mobile). It uses Web 2.0 and Web 3.0 technologies to provide an interactive layer on top of the existing internet. As proposed, it is an open platform for working and playing inside a VR/AR/MR/XR environment. This concept is comparable to existing MMORPG platforms, but while each MMORPG represents a proprietary single virtual world, the metaverse will allow players to seamlessly move between virtual spaces together with their virtual assets. The metaverse is not merely a platform for human users; it will also be a communications layer for smart city devices through which humans and AI can share information.

Metaverse Threats

It is difficult to predict cyberthreats for a product space that doesn't exist yet and may or may not exist in the form that we envisioned. With that in mind, we brainstormed ideas to refine our understanding of the metaverse and identify threats against it and inside it. The result is a comprehensive list of threats that include some that are applicable today and others that will be applicable in three to five years. We sorted the threats into nine broad categories outlined in the succeeding sections.

I. NFTs

A non-fungible token (NFT) is a unique unit of data that is stored in a blockchain and can be sold and traded.[5] NFT data can include hashes or links to digital files of text, photos, videos, audio, and more. NFTs provide a public certificate of authenticity or proof of ownership of the data, although there is no legal foundation for this type of ownership yet. They are uniquely identifiable and governed by smart contracts.[6]

NFTs have become very popular and lucrative in recent years — the most expensive NFT ever sold was of digital artwork that netted the artist US$69.3 million.[7] NFTs are (for now) the main candidate for a system of owning digital property in the metaverse.

Threat scenarios and security concerns:

- There are integrity issues. NFTs regulate ownership of assets, but do not provide storage for the assets. This may lead to ransoming or other criminal attacks. If NFT data files are encrypted in a ransomware attack, the user will still retain ownership but they can be blocked from accessing the assets if they do not pay the ransom.
- While NFTs can, in principle, be used to verify ownership of digital assets, a lot of things can still go wrong. For example, NFT ownership is verified using blockchains so they are susceptible to blockchain hijacking attacks. NFTs that rely on smaller blockchains could be susceptible to a Sybil attack.[8] This is where the attacker gains control of more than 50% of the peer nodes that verify transactions and thus can manipulate NFT ownership verification. Finally, a metaverse space may not honor the ownership asserted in the NFT as there is no legal reason to do so.
- The assets certified by NFTs are mostly stored on the InterPlanetary File System (IPFS).[9] The owner of an NFT pays a fee to "pin" the asset, so it does not disappear. But the "pin" service provider might not pin it forever, and the asset could be removed if a recurring fee is not paid.
- Security researcher Moxie Marlinspike demonstrated how to falsify NFT artwork by showing art that changed depending on the viewer's IP and user agent.[10] The assets were stored in centralized storage, but he managed to make an NFT that looked different based on who was looking at it.
- There will likely be a cost for moving digital assets between different metaverse spaces, and incompatible assets will need to be "converted" to move from one space to another. Malicious actors may take advantage of people who use asset brokers, or scammers can claim to be legitimate

brokers and defraud people. Virtual trade routes across virtual worlds could be like the wild west before customs and rules were established.

- NFT content cannot be changed but download links for data files can be used in phishing and spear phishing attacks.
- If NFTs become more popular, an inherent trust will develop and that trust can be exploited to victimize metaverse users. Malicious actors can use phishing tactics, drive-by-downloads, redirections, and other types of attacks.
- Forged NFT data files could also be sold to new buyers if a few bits of data are changed from the original. If the hash value of the original is similar to that of the counterfeit, the false artwork might appear nearly identical.

II. The Darkverse

The darkverse is like the dark web, except it exists inside the metaverse. In some ways, it is more dangerous than the dark web because of the pseudo-physical presence of the users. It mimics clandestine physical meetings versus the purely online open discussion threads in dark web criminal forums. The darkverse lives inside the deepverse, which is unindexed like the deep web.

Threat scenarios and security concerns:

- The darkverse was created for facilitating and conducting illegal or criminal activities. Conversely, the space could also be used for free speech against oppressive entities or governments.
- It could be a space for underground marketplaces in the metaverse. The marketplaces will be used for illegal or criminal activities and users would probably need authentication tokens for access. Even if law enforcement agencies (LEA) are aware of these spaces, they would be unable to infiltrate them without authentication tokens. This means that a darkverse safehouse could be sitting in plain sight and be inaccessible to LEA.
- One possibility is that users can only access a darkverse space if they're inside a designated physical location. This provides an additional level of protection for closed communities in the metaverse.
- Users of the darkverse could also implement location-based messages as well as proximity messages for metaverse spaces. This would make it extremely difficult for LEA to intercept exchanged communications.
- Because LEA do not have a way to monitor child pornography or sexual assault in the darkverse, these types of crimes will gradually grow. LEA will have difficulty tracking down offenders.

III. Financial Fraud

Criminals and criminal groups will be drawn to the metaverse because of the huge volume of e-commerce transactions that will occur in these worlds. There will be many who try and take advantage of users, steal their money, and capture their digital assets.

Threat scenarios and security concerns:

- The metaverse may introduce a new heterogenous digital economy (involving Bitcoin, Ethereum, real money, PayPal, e-transfers, etc.). This economy will operate in the metaverse, where the exchange rates will be controlled by the free (and possibly deregulated) market. This will become a prime target for finance-savvy criminals who will try to manipulate and exploit the market.
- Money laundering may happen using metaverse real estate. The valuation of virtual "land" is highly dependent on perception. It can be influenced by many parameters, and is open to manipulation.
- A company that exists only in the metaverse may lack a logical jurisdiction and, for example, could effectively avoid paying income taxes.
- Metaverse real estate investors could become victims of Ponzi schemes and securities fraud.
- Metaverse publishers will likely create their own in-world digital currencies and digital assets, and also maintain direct control of the supply. The intertwined systems of different digital currencies, digital assets, and fiat money could create a need for complicated arbitration, or cause collapses like what has happened to the Luna cryptocurrency in 2022.[11]
- Digital currencies are convenient for receiving funds. However, if a user is defrauded or there are transaction issues, the publisher of the digital currency will have to deal with complex financial issues, possibly even at the regulatory levels.
- If a user is defrauded or robbed, then getting help, filing complaints, or filing legal actions will be very difficult. The user will also be using decentralized digital currencies, which adds to the complexity of the situation.
- In the metaverse, we will likely see more pump-and-dump schemes. Malicious actors will boost the value of digital assets through fake recommendations, endorsements, and investments; and then dump the assets for a profit.

IV. Privacy Issues

The metaverse will likely be a collection of virtual worlds primarily created and hosted by big corporations, free to use for all interested persons. But we all know there is no such thing as a free lunch. Metaverse publishers will control all aspects of their meta spaces, collect vast amounts of user data, and monetize the collected data. Even if there are open-source metaverse worlds that users can host, the publisher who hosts them will still be able to collect and monetize user data. Privacy issues will become a major concern in the metaverse.

Threat scenarios and security concerns:

- There will be a ubiquitous wiretap in the metaverse. Everything a user does will be subject to unlimited surveillance. Privacy and tracking will be even more extreme. It will be the wild west, a free-for-all until laws are put in place.
- Metaverse operators will have unprecedented visibility into user actions. Essentially, when you are using the operator's metaspace, there will be little privacy. It will be similar to today's social media, where the service is seemingly free but the users pay for it with their data. Metaverse operators will collect vast amounts of user data and commoditize it.
- Data sovereignty is a major problem we are going to face in the metaverse because the servers, assets, and users will be in many different locations. The cloud-distributed nature of the metaverse means that data will be processed and stored in multiple locations separate from the user.
- The application programming interface (API) economy will become a critical component of the data supply chain. User data will be shared and accessed by third-party vendors, in different locations, and in an uncontrolled manner. This makes data sovereignty very hard to enforce. Any issues in the data supply chain will rest squarely with the API owners. As more and more third-party vendors are added to the data supply chain, the risk of data leakage or vulnerability exploitation greatly increases. Data accuracy is also critical for metaverse applications and as data supply chains increase in length, ensuring data accuracy becomes more difficult.
- AR devices have iris tracking, so it may be possible to steal the iris patterns of users. According to a study published in Nature, users' body motions can also be identifiable.[12]
- A lot of data processing happens at the user endpoints (e.g., AR/VR headsets) that are becoming powerful computing platforms. User identity data, biometrics, location data, credentials, payment information, avatar data, and more, will be stored locally in user endpoints, making them a lucrative hacking target.
- Metaverse platforms (e.g., Meta, Mesh, etc.) will still know a lot about the user even if the user moves between different metaverse spaces.

- Is your real identity tied to your virtual identity in the metaverse? Users can have multiple identities, like in social media platforms, which are not tied to a real identity. However, the platforms themselves may be able to accurately identify the real person behind the avatar using parameters such as body motion data and user behaviour.
- There may also be identity confusion in these spaces. Individuals will often have multiple identities in the same space and across metaverse worlds, leading to trust issues.
- Stalking may also be an issue. Malicious individuals can stalk a victim using an invisible avatar. The victim will not even know that someone is tailing them, monitoring them, or eavesdropping on their conversations. Invisible avatars will typically need a user account with a higher privilege, which may be bought or acquired by exploiting some vulnerability in the metaverse publisher's code.

V. Cyber-Physical Threats

The metaverse is going to be an interactive application layer for the Spatial Web.[13] The Spatial Web is a computing environment that exists in 3D space – a twinning of real and virtual realities enabled via billions of connected devices and accessed through VR/AR/MR/XR interfaces.[14] This integration of IoT and cyber worlds could give rise to cyber-physical threats.

Threat scenarios and security concerns:

- Entity-user interactions will happen via the metaverse. For example, smart city infrastructure can communicate with users who are wearing metaverse-enabled AR glasses. This can lead to interesting new threat avenues (e.g., man-in-the-middle (MitM) attacks, unlawful access to ICS/SCADA infrastructure, unauthorized access to digital twins, etc.) and new ways to exploit the cyber-physical space, especially if smart city data can be forged and used to trick users into making incorrect decisions.
- Critical infrastructure (CI) facilities will have physical equipment connected to digital twins, and these spaces will be accessible via the metaverse. This improves operations and enables remote work, but it also potentially exposes CI to external cyberattacks via the metaverse.
- The cyber-physical presence is a big part of the metaverse – how will this affect crimes like sexual assault, romance scams, or bullying? Because assailants can create multiple avatars without revealing their identity, these crimes will become a pervasive problem in the metaverse. The cyber-physical nature of the metaverse means these crimes will impact the victim's emotional and mental health, much like the way these crimes affect victims in the physical world.
- Most companies will have some presence in the metaverse, and some companies might be 100% located in the metaverse. It is important to make sure metaverse HQ buildings are secure, and data is protected. Some type of cyber-physical security will be needed to protect such buildings and prevent sabotage or attacks.

- New classes of IoT and IIoT devices will be connected to the metaverse, exposing a bigger attack surface.
- Location-based pricing may become an issue. For instance, Steam, a popular video game distribution service, has cheaper offers in some countries. This is attractive for users, especially if they can purchase things for lower prices in certain metaverse spaces. Criminals will take advantage of this and try and entice users to shop in obscure metaverse spaces (that they control) to get discounted prices. Users may end up just getting scammed.
- Many metaverse automations will be built using smart contracts. Purchases made in a virtual store could be automatically delivered to a physical address. Criminals will find ways to hack smart contracts or create fraudulent contracts to steal from users.
- Location-based services (LBS) will evolve to virtual LBS. Criminals will sell teleportation services to access parts of the darkverse or other restricted parts of the metaverse.

VI. Virtual/Augmented/Mixed/Extended Reality Threats

The metaverse is going to exist as both a VR and an MR world — user interactions will occur inside the 3D virtual worlds, or with 3D objects augmented in the real world. We expect that VR metaverse-like spaces will arrive within two to three years, while AR/MR metaverse spaces are at least four to five years away.

Threat scenarios and security concerns:

- Users can create a new identity and life in the metaverse — what are the implications of this dual identity in the real world? Criminals can pretend to be LEA in the metaverse to gather intelligence about targets from legitimate organizations.[15]
- Bad actors will use a virtual world to plan and rehearse real-world crime. Maps and building plans that mirror the real world can be used to preplan actual crime.
- Criminals will attempt to block user avatars from accessing services they paid for. One example is preventing them from accessing or leaving a building or a virtual space. As mentioned in the NFT section, the malicious actors will ask for a ransom to grant user's access to the services they paid for.
- Businesses will create digital replicas of their real-world stores in the metaverse. Criminals will copy these digital stores in a different metaverse space to scam shoppers. For example, they could create a fake Gucci store that looks identical to the real one and have users think they are buying real Gucci merchandise. The fake Gucci store could be used to sell counterfeit products, undercutting Gucci's sales.

- Criminals could set up metaverse spaces to spread fake news — these can be turned into VR honeypots for intelligence services. Criminals or even LEA can create fictitious metaverse spaces in order to gather intelligence from targeted groups.
- The physical aspect of sexual assault is not present in the metaverse, but sexual attacks in the virtual world have taken place and will be repeated in the future.[16, 17] These events often cause trauma to the victims.
- VR/MR/AR/XR applications depend on location data to access localized services. If the GPS data is spoofed or a third-party application is sending incorrect location data, then users or programs can be tricked into behaving incorrectly. For example, spoofing location data in the AR game *Pokémon GO*[18] allows users to access Pokémon gyms outside their immediate vicinity — which the game developer considers as cheating and can result in account bans.[19] A criminal ecosystem, such as LBS-spoof-as-a-service, may also emerge.

VII. Social Engineering

The term "social engineering attacks" is used to describe a broad range of malicious activities accomplished through human interactions. Social engineering uses psychological manipulation to trick users into making security mistakes or give away sensitive information.[20]

Threat scenarios and security concerns:

- Metaverse operators will be able to perform precise sentiment analysis, such as those used by politicians to sway public opinion during elections. This is done by analyzing personal data collected in the metaverse — eye tracking, body tracking, location and movement tracking, voice tonality, etc.
- Criminals or state actors will look for vulnerable groups of people who are sensitive to certain topics and then drop targeted narratives to influence them. These narratives could be used to amplify current global issues.
- Deep fakes can be leveraged to commit crime. Speech combined with visual elements is a powerful method of expression (and tool of influence). The metaverse is the perfect platform for this type of manipulation.
- Criminals can infiltrate a metaverse space to impersonate official avatars and then misdirect users in that space. Conversely, they can enter a competitor's metaverse space (in their impersonated avatar skin) and create mischief which will then reflect badly on the company they are impersonating.
- Criminals can also potentially impersonate service providers like doctors and give false medical advice to patients in return for payment. Impersonation to commit fraud is an age-old crime.

- People will be exposed to the global scammers relatively easily because the metaverse transcends physical boundaries — any crimes involving social engineering will be exacerbated.
- As mentioned in the previous section, fake news spaces can be created. These can be turned into VR honeypots for intelligence gathering.
- Malicious advertisers can scam users, sell fakes of a digital product, or sell products that end up being a trojan.

VIII. Traditional IT Attacks

These are the traditional IT attacks that Trend Micro and other security vendors provide protection against daily. Since metaverse worlds will run on regular IT hardware, they are susceptible to these IT attacks.

Current IT threat scenarios will very likely keep happening in the metaverse:

- Distributed-denial-of-service (DDoS) for extortion is a major problem. The metaverse is very expensive to run, so organizations will pay to stop these DDoS attacks (and also pay for protection against them).
- Bad actors may encrypt the servers that store user or corporate data and hold it hostage for ransom.
- Once APIs for metaverse applications are made public, bad actors will attempt to write malicious code or phish people by exploiting those APIs.
- If the metaverse uses existing technology when calling or executing API calls, then there is a good chance that current cloud specific attacks would also work against it.[21]
- Metaverse applications will communicate with a wide range of IoT devices to enable cyber-physical AR interactions. This opens the possibility of discovering exposed and vulnerable devices on the metaverse-internet using an internet scanning engine like Shodan.[22]

IX. Miscellaneous Threats and Issues

Some of the metaverse threats and security concerns that we conceptualized did not fit neatly into any of the previous eight categories, so we created a miscellaneous category to organize these threats. They are an interesting mixture that touch on many disparate topics.

Miscellaneous threats and issues:

- LEA will struggle in the first couple of years because of the high cost of intercepting crimes and criminals at scale in the metaverse. They will also have difficulty because jurisdiction is hard to establish. They will need time to build their metaverse expertise, which will leave it largely unpoliced in the initial years.

- Aside from threats to users, the environmental impact of running the metaverse is also an issue. Bitcoin mining uses huge amounts of electricity, and a graphics-heavy metaverse space will consume even more power compared to bitcoin mining.
- In a distributed metaverse architecture, network partitioning due to uplink or power failures need to be handled securely. If e-commerce transactions are not tokenized, users could lose money because of a sudden outage. This is especially true with some blockchain technologies that do not handle partitioning securely.
- The metaverse can hardly be disassociated from large tech companies. We might address the issue in two different ways: be independent of metaverse infrastructure of big tech companies, or prevent big tech companies from collecting user data.
- How will copyright infringements be policed and enforced in the metaverse? If there are too many fake products, will this dissuade genuine companies from joining the metaverse economy or encourage them to leave?
- How will users know if they're interacting with a real person or a bot? Will there be a Turing Test to validate if an entity is AI or human? The ethics, responsibilities, and accountability of interacting with AI are open for debate.
- User-to-user interactions are the cornerstone of the metaverse — these spaces are essentially platforms where anybody can say anything to anyone. This is exacerbated by the fact that users are communicating with each other via their avatars and not talking in-person, so typical societal rules for interactions quickly disappear. Moderation of activities and speech will become a massive, but necessary, undertaking to keep the metaverse safe. If users feel harassed, bullied, or cheated, they will simply stop using the metaverse application, which translates to losses for the companies. But moderation at such a massive scale is easier said than done. We only have to look at the current state of social media to see how challenging moderation is and how woefully moderation is failing to curb hate, fake news, extremism, racism, bullying, etc. in existing platforms.

Metaverse Use Cases and Threats

Metaverse use case	Threats
Critical infrastructure Workers at a hydroelectric plant (or any critical infrastructure facility) use the metaverse to virtually move inside a digital twin of the power plant. All the important equipment and sensors in the plant are network connected. Their values/states can be visually read in the metaverse digital twin, and corrective or maintenance actions taken. The digital twin gives the workers a physical sense of the actual plant and its equipment placement versus simply viewing readings on a control panel and looking at CCTV images. Third-party contractors can also remotely work inside the digital twin of the hydro plant, which significantly reduces travel and increases efficiency.	**Cyber-physical threats** – Criminals who get access to a power plant's digital twin can exploit it to gain unlawful access to the plant's internal systems and/or the ICS/SCADA environment. **Traditional IT attacks** – Criminals leverage everyday IT attacks because the digital twin is running on IT infrastructure. Brute forcing, vulnerability exploitation, and ransomware are examples of IT attacks that we see every day. **VR/AR/MR/XR threats** – Criminals can use digital blueprints of the site to plot their attacks or plan entry/exit vectors.
IIoT Some jobs can move from the real world into the metaverse, where cyber-physical interaction exists. For example, industrial equipment can now be operated by specialist operators thousands of miles away without needing special simulators because all the equipment is connected and accessible via custom metaverse space interfaces.[23] Another example: security guards can do their job monitoring a physical world facility via the metaverse. The guards can use sensors and CCTVs built into the physical space by interacting with a digital twin in the metaverse. The digital twin gives them the physical feel of the facility and reduces the need for hourly foot patrolling.	**Cyber-physical threats** – Criminals can launch MitM attacks between industrial equipment and the remote operators. **Traditional IT attacks** – Traditional IT attacks, such as vulnerability exploitation, can be used to gain access to industrial equipment. Because everything in the metaverse is connected, lateral movement will also be easy after initial entry. **VR/AR/MR/XR threats** – Criminals can preplan physical attacks if they can get access to a digital twin of the site. This can happen via avatar takeovers, or accessing raw information exposed to the metaverse.
Social media Social media influencers are already a major force in today's internet. In the metaverse, influencers will take on an even greater role. Fans will be able to follow influencers in real-time inside the metaverse and interact with them at special events. Influencers can record VR videos of their experiences that fans can directly interact with, and the fans can even virtually go through the same experiences. Fans can even interact with objects and go places inside the interactive VR videos. Product placements, small purchases, advertisement, and endorsement revenues are expected to skyrocket with influencer VR videos.	**Privacy** – Operators will have an unprecedented view of user actions inside their metaverse space. Avatars can be used to track a person's virtual location. **Financial fraud** – Criminals can hide behind avatars, making it easy for them to commit fraud (this is similar to the current state of social media platforms). **Social engineering** – Someone using an avatar can impersonate a social media influencer and scam the influencer's fans and damage the influencer's reputation.

Metaverse use case	Threats
Advertising Advertisers will heavily use the metaverse. We have already seen a vision of this future in games like Cyberpunk 2077 and movies like Blade Runner, where ads are everywhere. This will be especially true in metaverse worlds. Since real-world physics don't apply, companies can fill the virtual sky with advertisements. Users' real identities may not matter, but their avatars can be profiled. A person can be anonymous but be precisely targeted by advertisers based on the actions and interests of their avatar.	**Privacy** – User data, including personal information, will likely be shared and accessed in an unregulated manner across the metaverse. **Financial fraud** – In the metaverse, pump-and-dump schemes will occur. The value of digital assets will be inflated by fake ads, endorsements, and recommendations. **VR/AR/MR/XR threats** – Unmanaged adverts can invade the metaverse and drive users to unsafe sites. **Social engineering** - Advertisers can sell scams or cheats of a digital product that ends up being malware.
Shopping Shopping experiences will be redefined in the metaverse. For instance, we expect that most major stores will have a virtual overlay on top of their physical stores. The overlay will provide customers with extra information such as sales promos, item stocks, customization options, etc. In addition to physical stores, there will also be fully virtual stores where customers will be able to look at products from all angles, interact with them (the avatars can try on clothes and accessories), and order items for either delivery or pickup. E-commerce retailers like Amazon and Alibaba, or even traditional brick-and-mortar retailers like Walmart and Target, will create massive digital storefronts where users can walk around, browse, interact with products, and make purchases. There will be mega malls in the metaverse where all the major brands will be present. Users from around the world will be able to visit, browse, and shop in these malls.	**NFTs** – There will be a fee for moving digital assets across metaverse worlds, and users will also need a broker to handle asset exchanges. Criminals can pretend to be brokers and steal payment/banking information from users. **Financial fraud** – Fake businesses can pose as legitimate vendors and offer counterfeit goods. **VR/AR/MR/XR threats** - Businesses will have digital twins of their real-world stores, which criminals will duplicate in a different metaverse space and use to defraud customers.
Art In the metaverse, artists will be able to create extraordinary art pieces. Physical laws that govern the real world do not exist in the metaverse (unless programmed), and this gives artists the liberty and means to create multi-dimensional artwork that is unlike anything we can enjoy today.	**NFTs** – Ransomware operators in the metaverse will target and try to ransom NFTs. **Financial fraud** – Scammers will facilitate the sale of counterfeit or stolen artwork in the metaverse. **VR/AR/MR/XR threats** – There will be fake metaverse galleries displaying and selling counterfeit art.

Metaverse use case	Threats
Education Simulation, training, and education will be enhanced in the metaverse. The UX will be very good, which will lead to more precise simulation of topics or incidents. Users will not have to sit inside a simulator; instead, they can work like they are dealing with a real incident. Education in the classroom will take on a whole new visual dimension with students able to explore concepts in 3D. For example, they can explore the pyramids of Giza, study the internal structure of an organ, do hands-on training on assembling a car engine, etc.	**Privacy** - Privacy and tracking will be more invasive, and operators of the metaverse space can monitor users indefinitely. **Social engineering** - Criminals will seek out vulnerable groups of people who are sensitive to certain issues, then use targeted narratives to sway them. Visuals and speech in a cyber-physical world can have profound effects.
Publishing industry Libraries will make a major comeback in the metaverse. The internet made information easily available, which greatly reduced trips to traditional libraries and bookstores. In the metaverse, there will be massive digital library buildings that users can explore. These will store digital versions of books, audio files, video files, even VR books and videos. These libraries can be curated collections or free form data.	**VR/AR/MR/XR threats** – Visual elements and speech in a cyber-physical world can project powerful messages. Fake news, which is a major problem today, will be further exacerbated in the metaverse. **Miscellaneous** – Copyright infringements in the metaverse will be an issue, especially if we do not have a strong mechanism for enforcing copyright across metaverse spaces and copyright jurisdictions.
Experiences industry Full-body actuator suits will be developed, giving users the ability to physically feel things inside the metaverse. They can touch an object, sense a push, feel a jump, experience the elements, and more. This full-body suit concept paired with an omni-directional treadmill was explored in the movie version of the book Ready Player One. These could be an extension or a replacement for theme parks and other similar entertainment industries.	**Cyber-physical threats** – Malicious code embedded in body suits can cause them to malfunction, endangering the user. E.g., bypassing the cooling mechanism of a body suit and making it uncomfortably hot; intensifying the feeling of a burn or increasing the pain level threshold of a full body actuator suit; stroboscopic light effects played in the headset triggering epilepsy or seizures, etc. **VR/AR/MR/XR threats** – Criminals can gain access to body suits and monitor the user's actions. **Privacy** – The suits will have access to a wide range of biometric data that could be misused, akin to health data.

Conclusion

The metaverse concept is constantly evolving. In the early 1990s, a science fiction writer came up with the concept of a virtual reality world, and today this idea has transformed into a multi-billion-dollar ambition for big tech companies. While the metaverse promises to be a game changer, the reality is, it will face pushback from the globally entrenched smart phone ecosystem, which has a user base of more than six billion people and is still growing.[24] In the beginning, we expect the metaverse to be adopted by developed countries with well-established telecommunications networks and a user base that can afford the expensive hardware. As the technology becomes more accessible and universally supported, adoption will increase similar to what happed with smart phones.

In previous sections, we discussed a wide range of uses cases and compiled a comprehensive list of threats against the metaverse. If we were to focus on the top five metaverse security issues, these would be:

- NFTs are an important component of the metaverse and will be used to regulate ownership of digital assets. They will be susceptible to phishing, ransom, fraud, and other threats.
- Illegal or criminal activities are likely to flourish in the darkverse since it will be difficult to track and monitor. LEA will also have a difficult time infiltrating these spaces.
- Expensive metaverse real estate and NFTs will be used to launder money.
- Criminal or state actors will look for vulnerable groups of people who are sensitive to certain topics and then drop targeted narratives to influence them.
- In the metaverse, privacy will be a key concern because metaverse-like space operators will have unprecedented access to user actions. Data sovereignty will also be a major issue.

We fully expect that there will be numerous issues to resolve on the road to making the metaverse a reality. No single company has the resources to build the metaverse alone, and it will take the concerted effort of many industries to realize the metaverse dream. It is realistic to expect that somewhere down the line, we will see that the metaverse we envisioned is not feasible nor attainable, and the whole metaverse idea train changes course in a new direction.

Large investments are pouring into the metaverse, so now is an excellent time to start developing security models for it. This is challenging because we are exploring a constantly evolving concept and trying to create security guidelines for products and services that don't currently exist. Anticipating threats and acting early will help us protect both metaverse-like applications and the future metaverse.

References

1 Rabindra Ratan and Yiming Lei. (Nov. 1, 2021). *Down to Earth*. "What is the metaverse? 2 media and information experts explain." Accessed on July 4, 2022 at https://www.downtoearth.org.in/blog/science-technology/what-is-the-Metaverse-2-media-and-information-experts-explain-79993.

2 Meta. (Oct. 28, 2021). *FB*. "Introducing Meta: A Social Technology Company." Accessed on July 4, 2022 at https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

3 Meta. (Oct. 28, 2021). *FB*. "Introducing Meta: A Social Technology Company." Accessed on July 4, 2022 at https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

4 Jonathan Greig. (Sept. 27, 2021). *ZDNet*. "Facebook announces $50 million investment in 'responsible' metaverse development." Accessed on July 4, 2022 at https://www.zdnet.com/article/facebook-announces-50-million-investment-in-responsible-metaverse-development/.

5 Shane Brunette. (April 7, 2022). *CryptoTax*. "What is an NFT?." Accessed on July 4, 2022 at https://cryptotaxcalculator.io/blog/what-is-an-nft/.

6 Melanie Kramer, Stephen Graves and Daniel Phillips. (Jan. 12, 2022). *Decrypt*. "Beginner's Guide to NFTs: What Are Non-Fungible Tokens?." Accessed on July 4, 2022 at https://decrypt.co/resources/non-fungible-tokens-nfts-explained-guide-learn-blockchain.

7 Stephen Graves, Daniel Phillips and Andrew Hayward. (Feb. 22, 2022). *Decrypt*. "The 15 Most Expensive NFTs Ever Sold." Accessed on July 4, 2022 at https://decrypt.co/62898/most-expensive-nfts-ever-sold.

8 Binance. (Oct 4, 2021). *Binance*. "Sybil Attacks Explained." Accessed on July 4, 2022 at https://academy.binance.com/en/articles/sybil-attacks-explained.

9 IFPS. (n.d.). *IFPS*. "IPFS powers the Distributed Web." Accessed on July 4, 2022 at https://ipfs.io/.

10 Moxie Marlinspike. (Jan. 7, 2022). *Moxie*. "My first impressions of web3." Accessed on July 4, 2022 https://moxie.org/2022/01/07/web3-first-impressions.html.

11 Zeke Faux and Muyao Shen. (May 19, 2022). *Bloomberg*. "A $60 Billion Crypto Collapse Reveals a New Kind of Bank Run." Accessed on July 4, 2022 https://www.bloomberg.com/news/articles/2022-05-19/luna-terra-collapse-reveal-crypto-price-volatility.

12 Mark Roman Miller et al. (Oct. 15, 2020). *Nature*. "Personal identifiability of user tracking data during observation of 360-degree VR video." Accessed on July 4, 2022 https://www.nature.com/articles/s41598-020-74486-y.

13 Gabriel Rene. (Oct. 2, 2019). *Medium*. "An Introduction to The Spatial Web." Accessed on July 4, 2022 https://medium.com/swlh/an-introduction-to-the-spatial-web-bb8127f9ac45.

14 Peter H. Diamandis, MD, (Nov. 16, 2018). *SingularityHub*. "The Spatial Web Will Map Our 3D World—And Change Everything In the Process." Accessed on July 4, 2022 https://singularityhub.com/2018/11/16/the-spatial-web-will-map-our-3d-world-and-change-everything-about-it-in-the-process/.

15 José Adorno. (March 30, 2022). *9to5mac*. "Apple and Facebook reportedly provided personal user data to hackers posing as law enforcement." Accessed on July 4, 2022 https://9to5mac.com/2022/03/30/apple-and-facebook-reportedly-provided-personal-user-data-to-hackers-posing-as-law-enforcement/amp/.

16 Angus Crawford and Tony Smith. (Feb 23, 2022). *BBC*. "Metaverse app allows kids into virtual strip clubs." Accessed on July 4, 2022 https://www.bbc.com/news/technology-60415317.

17 Tanya Basu (Dec. 16, 2021). *MIT Technology Review*. "The metaverse has a groping problem already." Accessed on July 4, 2022 https://www.technologyreview.com/2021/12/16/1042516/the-Metaverse-has-a-groping-problem/.

18 Ruheni Mathenge. (June 1, 2022). *Privacy Savvy*. "How to spoof Pokemon GO location in 2022 (quick and easy)." Accessed on July 4, 2022 https://privacysavvy.com/geoblocking/censorship/spoof-pokemon-go-location/.

19 Niantic. (n.d.). *Niantic*. "Three-Strike Discipline Policy." Accessed on July 4, 2022 https://niantic.helpshift.com/hc/en/6-pokemon-go/faq/39-three-strike-discipline-policy/.

20 Imperva. (n.d.). *Imperva*. "Social Engineering." Accessed on July 4, 2022 https://www.imperva.com/learn/application-security/social-engineering-attack/.

21 Morton Swimmer et al. (April 8, 2022). *Trend Micro*. "Exploring Common Threats to Cloud Security." Accessed on July 4, 2022 https://www.trendmicro.com/vinfo/ph/security/news/virtualization-and-cloud/exploring-common-threats-to-cloud-security.

22 Shodan. (n.d.). *Shodan*. "Search Engine for the Internet of Everything." Accessed on July 4, 2022 https://www.shodan.io/.

23 David Edwards. (Feb. 25, 2022). *Menafn*. "Caterpillar claims 'world's largest' number of autonomous trucks." Accessed on July 4, 2022 https://menafn.com/1103764554/Caterpillar-claims-worlds-largest-number-of-autonomous-trucks.

24 S. O'Dea. (Feb. 23, 2022). *Statista*. "Number of smartphone subscriptions worldwide from 2016 to 2027." Accessed on July 4, 2022 https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research