The Hacker's Mindset

What you don't know can hurt you

> Future and past blurred; what he had already experienced and what he would eventually experience blended so that nothing remained but the moment.

Philip K. Dick,
Do Androids Dream of Electric Sheep?

Embracing the metaverse

The metaverse is no longer the stuff of science fiction. A subtle shift to the metaverse is already taking place as we speak, as consumers embrace the metaverse where it makes sense for them – from attending virtual concerts and auctions to using augmented reality furniture apps.

The word "metaverse" is a new word created from combining the word "meta," which means "to go beyond," and the word "verse" from the word "universe." It is a combination of augmented reality and virtual reality – an alternate digital reality where people can work, play, and socialize.

The metaverse is essentially the next iteration of the internet. It is an exciting ecosystem for businesses to engage with customers in new ways and take the digital economy to the next level. In fact, there are already plenty of businesses who are building parts of the metaverse and others with a solid vision for what it should look like to function.

Eventually, the metaverse will blend the physical and digital world seamlessly.

Virtual reality (VR):
fully artificial environment; full immersion in virtual environment

Augmented reality (AR):
virtual objects overlaid on real-world environment; the real world is enhanced with digital objects

Mixed reality (MR):
virtual environment combined with the real world; interact with both

Extended reality (XR) / metaverse:
a mix of all the above

However, the sheer complexity and number of moving parts involve in expanding organizations beyond the physical world brings a whole host of new security concerns.

The question we need to ask is: How can we prepare for this shift?

What is clear is that every organization's attack surface will greatly expand as we move into the metaverse. Although we can use existing protection techniques, it may not stop new attacks that have never been seen before.

As we move towards a metaverse, financial transactions will cover not just virtual goods, but also real-world goods and services sold through a broader range of channels that may include AR/VR interactions.

In today's social selling, goods are sold and paid through a social media platform with the seller linking their system to the platform via an API. The metaverse opens near-infinite virtual storefronts – making data privacy and authentication a bigger challenge.

In addition, today's fraudulent transactions can be reversible if acted upon soon enough. However, commercial transactions on the metaverse are built on blockchain and are irreversible.

There is also the interoperability aspect of the metaverse. Even in today's gaming world, you cannot take game items from one game to the other. The metaverse, on the other hand, is trying to be open and interoperable.

Security in the metaverse era requires security of content created in the virtual world and protection of personal data. The role of an edge platform company like Akamai with the highest edge platform coverage worldwide is very important.

Jonathan Singer of Akamai shared some of the challenges we can expect the metaverse to deliver for CSOs and their teams based on the definition by venture capitalist Matthew Ball.

The metaverse essentially enables a digital version of "you" in a virtual space that can perform various activities and conduct financial transactions. Unlike one-dimensional social media profiles, the metaverse version is intended to be your digital replica.

It will gradually establish itself in your daily life – like smartphones – which is inevitable. Someday, it will just become a part of our lives without us even noticing it.

What are your organization's plans as we go into the metaverse?

> *Commercial transactions on the metaverse are built on blockchain and are irreversible.*

Definition	Challenges
The metaverse is a massively scaled	authentication, access policies, malware, encryption and secure traffic, DNS security, web app attacks
and interoperable network	uptime, DDoS attacks, flash crowds
of real-time	security vs. performance trade-offs, API security, stream protection, anti-piracy
rendered **3D virtual worlds**	fraud, physical/access security, hardware/IoT security, content integrity
which can be experienced synchronously by an effectively **unlimited number of users**, each with an individual sense of presence	flash crowds, MFA, security at scale
and with continuity of data such as identity,	secure registration, credential provisioning, authorization
history,	encryption, PII
entitlements,	encryption, PII, fraud prevention, intellectual property rights, payment security
objects, communications,	encryption, PII, fraud prevention, intellectual property rights
and payments.	encryption, PII, fraud prevention, PCI compliance, tokenization, payment risk

Gaming security – our metaverse security blueprint?

To prepare for the metaverse, and everything that comes between then and now, we recommend that all CISOs, regardless of industry, become familiar with the audience and security challenges of the gaming industry.

Gaming is already providing and influencing a significant portion of the metaverse's foundational technology.

As multitudes of technologies continue to converge into a connected social/technological landscape, it's clear that video games are one of the key driving industries paving the way forward. The gaming industry has pioneered technologies and interactive models that would be used not only for video games themselves.

Gaming is already providing and influencing a significant portion of the metaverse's foundational technology. Beyond technology, its business models are being adapted and leveraged across industries.

> *Gaming is already providing and influencing a significant portion of the metaverse's foundational technology.*

Ten years ago, the primary value of any account was in credit card numbers, and any information that could help a criminal get into a bank account.

Now, gaming accounts themselves have value in the form of a player's time and in-game items. Accounts that have put in time playing and racked up gear can allow purchasers of stolen accounts to play at a high level without putting in the effort. In-game goods can also be sold in third-party markets for real cash.

This form of virtual value is already being reflected in the investment community with people buying up NFTs. As the world, and your business, move toward operating in the metaverse, securing accounts and access will continue to be a top priority.

Understand the risk scale of today's authentication models and how traditional MFA solutions can still be compromised:

Akamai MFA

click to read

As every company moves to do business in the metaverse, partnership with your users and employees around account security will become a larger part of the customer experience and the brand relationship, expanding security's role in the enterprise.

At Akamai, we have strong visibility into the problems in the gaming space. Reports published include how and why criminals attack the gaming industry, and two recent "State of the Internet" reports on gaming security: You Can't Solo Security and Gaming in a Pandemic.

Each of these examines several aspects of what it takes to keep systems online and running despite the relentless efforts of attackers.

The You Can't Solo Security report also features the survey results of hardcore gaming players. Akamai undertook this survey exercise in partnership with the international gaming conference organization DreamHack (now ESL Gaming) to better understand how players feel about the security of their games and how much personal responsibility they believe is warranted when it comes to securing their own gaming accounts.

No discussion of the metaverse and gaming during the pandemic would be complete without talking about Roblox. While children and parents were at home with a pandemic raging across the globe, Roblox was there as a social, creative, and educational outlet for children and teens. Estimates point to there being anywhere from 520,000 to 40 million published games on Roblox. If that seems like a bit of a wide range to choose from — it is.

Roblox was trying to grow into a global entity and needed to deliver secure, consistent experiences for developers and players alike, regardless of where they were in the world. Poor user experiences, such as slow load times or disconnects, could mean lost revenue for the business.

Roblox came to Akamai for help ensuring they were successful in enabling high-performing online multiplayer games and game creation experiences.

Using Akamai, the company was able to deliver secure, consistent experiences for developers and players around the world.

Find out more:

Roblox delivers high-performing, global games

click to read

Securing online retail during the holidays

Retailers worldwide breathed a collective sigh of relief after the holiday season.

Global supply chain issues, skyrocketing shipping costs, inflation, and domestic labor shortages have rapidly compounded problems within a sector already slammed by the COVID-19 pandemic.

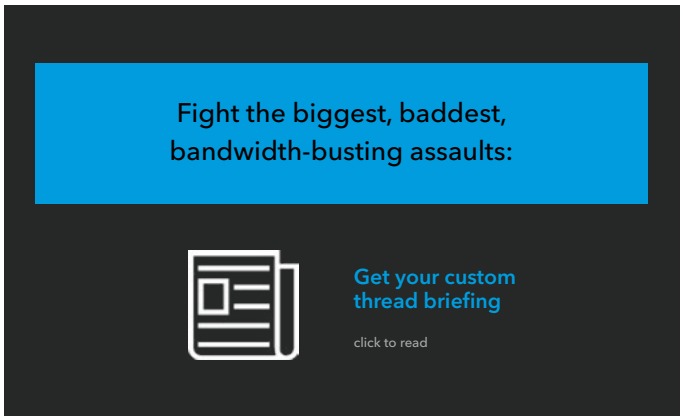
Threat actors are aware of the increased pressure facing retailers (and consumers) globally and stand ready to take advantage of the industry's "make or break it" time of year.

While cybercriminals have an arsenal of attack vectors, tools, and exploits to leverage, malicious bots can pose a significant threat to online retailers – and their bottom line.

Bots can be broken down into two buckets – good bots and bad bots. Good bots, like Googlebot and Bingbot, crawl and index retailer websites to help improve search results. These types of bots are not built with bad intentions, and they respect rules as defined by the webmaster's robots.txt file.

However, malicious bots are purpose-built for a variety of nefarious activities like credential abuse for account takeover (ATO) attacks, grabbing limited inventory ahead of real customers, Layer 7 application DDoS attacks, price scraping, gift card fraud, and more. Juniper Research estimated that ecommerce fraud – oftentimes associated with bad bots – increased 18% in 2021 to reach $20 billion in losses for retailers globally.

With so much on the line, it comes as no surprise that Akamai observed bot operators out in full force, causing significant upticks in malicious bot activity leading up to and during the most recent online shopping mega-holidays like Christmas and Lunar New Year.



Here's what businesses can do to help ensure bots don't ruin holiday cheer.

Be alert to evidence of an attacker moving through the ATO kill chain. For example, threat actors often start preparing for full-scale attacks with some testing, so you might see a small spike in failed logins in the days before Singles Day or Black Friday.

Keep in mind that discovering and stopping bot attackers early in the weaponization and delivery phases of the ATO kill chain means organizations can better defend against fraud and abuse.

Tune your bot solution if you see more bots coming through. Note: Not all bot management solutions need manual tuning; check if yours does.

This is an edited version of a blog post written by *Susan McReynolds, Akamai*

If you would like to understand more about Akamai and the solutions we offer, please do

Contact Us