Policinginsight

ANALYSIS:

Patrolling the metaverse: Next generation cyber-terror threat

1st November 2022 | Andrew Staniforth | Policing Insight

Yesterday was the final day of the EU's European Cybersecurity Month, a four-week long initiative of awareness-raising and learning opportunities across Europe; Policing Insight's Andrew Staniforth looks at the current cybersecurity landscape, the potential threats for the public and some of the probable challenges for law enforcement moving forwards.

As the 10th European Cybersecurity Month (ECSM) drew to a close at the end of October, cyber security policymakers and practitioners across Europe will have been reflecting on the challenges that lie ahead and the enormity of their task to keep citizens and businesses safe online.

> “Simple endpoint attacks became complex, multi-stage operations. Ransomware attacks hit small businesses and huge corporations alike. Crypto mining attacks gave cyber criminals an easy foothold into company networks.”

Despite major government developments across the world involving billions of dollars of investment to strengthen cybersecurity measures, the undeniable truth is that cybercrime is booming.

Between 2008 and 2021, the Federal Bureau of Investigation (FBI) recorded a 207% increase in cybercrime reports, with losses hitting almost $7bn last year. This continued rise in cyber threats is being driven by an increasingly professionalised, specialised, and collaborative underground supply chain that is harming individuals and businesses alike.

According to the Cisco Umbrella 2021 Cybersecurity Threat Trends Report, cyber criminals last year delivered a wave of cyber attacks that were not just highly co-ordinated, but far more advanced than ever seen before.

Simple endpoint attacks became complex, multi-stage operations. Ransomware attacks hit small businesses and huge corporations alike. Crypto mining attacks gave cyber criminals an easy foothold into company networks. 2022 continues to be a year of massive data leaks, expensive ransomware pay outs, and a vast, new, complicated threat landscape.

But the current attack surface is set to grow exponentially in Europe with the recent launch of Meta’s platform Horizon Worlds in France and Spain, the company bringing its immersive world or metaverse experience to Europe for the first time.

Metaverse

The cyber domain is a human-made environment and is fundamentally shaped by human behaviour. It amplifies such behaviours for better or worse, the impacts of which are usually also felt in the physical world.

> “The metaverse will provide new opportunities to commit old crimes and an even greater opportunity to commit an abundance of new crimes. Policing the metaverse will be a huge challenge.”

The new metaverse has been described as the next iteration of the internet and, as was the case with the emergence of the internet, cybersecurity experts do not know what direction the metaverse is going to take. Moreover, like the internet, it will likely keep evolving, periodically taking new directions.

The Europol Innovation Hub has revealed that increasing adoption and functionality of metaverse technology means digital identities, and access to them, will become more valuable.

Europol suggests that as the virtual representation of users in the metaverse becomes more realistic and permanent, this provides opportunities to convincingly copy user appearance in so-called deepfakes.

The metaverse will provide new opportunities to commit old crimes and an even greater opportunity to commit an abundance of new crimes. Policing the metaverse will be a huge challenge.

A large responsibility will fall on the organisations that provide the platforms to monitor and moderate what happens on their platforms, and to provide law enforcement with the tools to do their job on these platforms.

As with current online activities, this will not be easy, and the challenges will be amplified and exacerbated with new issues to overcome.

Cyber terror

A major concern is the new cyber terror threat that will emerge from the proliferation of the metaverse. Terrorists will always try to exploit new technological options to facilitate their activities; in the case of the metaverse, this may lead to new opportunities for terrorist organisations, primarily for propaganda, recruitment and training.

With more immersive technology and related generated data at their disposal in the metaverse, it will become easier for terrorists to select and target vulnerable people and tailor their messages to their biases. That will enable them to more effectively target their propaganda and recruitment campaigns.

> “These virtual worlds may even allow them to impose their extremist rules on anyone entering their ‘state’. This would create a truly parallel world for these people to live in, acting out scenarios that undermine general acceptance of rule of law.”

The added realism of virtual environments may provide an increasingly useful platform for training, both in generally available applications and in specifically created environments and scenarios. As an increasingly accurate and complete digital twin of reality becomes available, it may provide real-time information on planned targets which could be countered by law enforcement agency metaverse surveillance operations.

The metaverse may allow users to create a virtual world which reflects their own ideologies, enabling them to create a virtual caliphate or white supremacist state for example. Members of such places could live their virtual lives according to rules that may contradict fundamental laws and values of the real physical society they live in.

These virtual worlds may even allow them to impose their extremist rules on anyone entering their ‘state’. This would create a truly parallel world for these people to live in and act out scenarios that undermine general acceptance of rule of law. Moreover, such spaces would provide a perfect environment for recruiting for terrorist activities in other virtual worlds – and even the physical world.

Law and order

Examining the metaverse for future security challenges from a police investigator's perspective reveals a set of vulnerabilities to ensure virtual lawlessness does not transfer into the real physical world. As an example, current legislation is already woefully lacking for present-day cybercrime and online interactions, and we see the challenges of bringing new cyber powers with the continued dither and delay of the UK's Online Safety Bill.

With new types of experiences and possibilities in the metaverse, legislation will be found even more inadequate. Therefore, it will be important to raise awareness with legislators of these issues and the tools law enforcement will need to fulfil their duties in these new virtual worlds.

And of course, cyberspace transcends national borders; technology supply chains and critical dependencies have become increasingly global, with cyber criminals, cyber terrorists and state-based actors operating from around the world. Cyberspace is also continually evolving as technology and the ways people use it change, requiring all in authority to adopt an agile and responsive approach.

The next generation of the internet will rapidly and exponentially amplify all manner of cyber threats; those in authority are seemingly ill-prepared to meet the magnitude of policing the metaverse.

Link to online article at Policing Insight: https://policinginsight.com/features/patrolling-the-metaverse-next-generation-cyber-terror-threats/

Andrew Staniforth is Director of Innovation at SAHER (Europe), a security research, training and consultancy operating at a global level, participating in the NOTIONES (*iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS*) network, funded by the European Commission Horizon 2020 Programme (No. 101021853). Andrew is also an active Researcher of Cyber Threats at the Hillary Rodham Clinton School of Law and Criminology, University of Swansea. As a former Counter-Terrorism Detective, he has worked across the world and supported missions of the United Nations Terrorism Prevention Branch. **Contact:** Andy@saher-eu.com
To learn more about NOTIONES visit: https://www.notiones.eu