ActiveFence

The Exploitation of VR Technologies

An ActiveFence Report

Contents

Executive Summary

Threat actor communities construct virtual places to meet, share ideas, and promote dangerous groups and activities. While this has up until now centered around message boards, forums, online games, and private servers, these communities are beginning to experiment with the possibilities presented by VR. ActiveFence has found an evolution in online behavior as each community tests how to migrate their current activity into VR spaces.

Key Findings

- ActiveFence has identified that VR technology is leveraged by various threat actors:
    - Foreign terrorist organizations (such as the IRGC);
    - White supremacist networks (linked to groups such as the Order of Nine Angels);
    - Large networks of child predators.
- These groups all take advantage (consciously or not) of the lack of moderation in this evolving technology.
- Well-established organizations create purpose-made VR applications to spread propaganda.
- Disparate networks and communities tend to create VR mods for their preexisting gaming activities. These VR mods are primarily used to glorify violence and strengthen communal ties.
- Child predator communities are also actively engaged in exploiting VR technologies. These communities are the pioneers in the exploitation of this technology. They create modifications to abuse features and produce their own applications, largely to simulate sexual experiences and produce custom content without the risk of exposure.

As VR technology becomes more available, these threat actor groups will likely be more proactive in their exploitation.

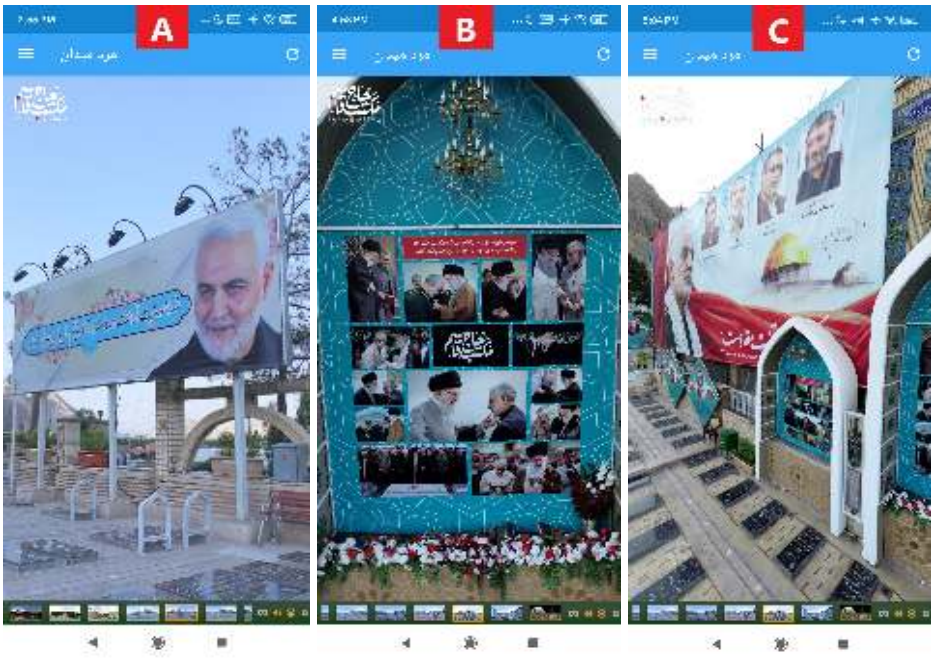
Foreign Terrorist Organizations (FTOs)

ActiveFence has identified multiple examples of VR applications produced by FTOs and their subsidiaries to create interactive propaganda experiences. These experiences glorify terrorists and promote the FTO's moral and religious legitimacy. These groups already use games and apps to initiate new accessible methods to spread their propaganda to young supporters and reach impressionable new crowds, so it is not surprising that they seek to gain a presence within the VR world. These apps are widely distributed and are uploaded to mainstream APK stores for the public to download.

Man of the Field: Qasem Soleimani - Haj Qasem Foundation

This app was created by the Haj Qasem Foundation[1] to commemorate Qassem Soleimani. The app venerates Soleimani and allows supporters of the IRGC, and its affiliated terrorist organizations, to make a virtual pilgrimage to his grave in Iran.

The VR experience presents 360° interactive panoramic images from Kerman Martyrs Cemetery, Iran.[2] These views are filled with religious posters that show Soleimani together with the Iranian Ayatollah and the Golden Dome of the Rock in Jerusalem. This application's function appears to be the same as the first example, providing religious legitimacy to this FTO's activities.



Screenshots from Man of the Field: Qasem Soleimani application

[1] The Iranian Islamic Revolutionary Guard Corps (IRGC) provides financial and military support to Islamist terrorist organizations around the world. The US designated the IRGC as an FTO in 2019, while Qasem Soleimani was designated a foreign terrorist by the US in 2005. He was killed in a US airstrike in 2020. Before his assassination, Soleimani was responsible for the IRGC's extraterritorial military operations and its provision of support to terrorist organizations worldwide.

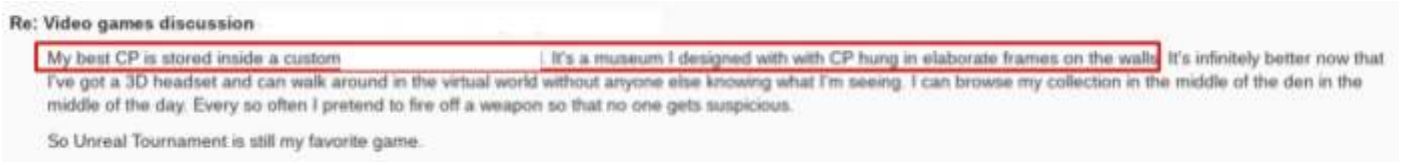
[2] Ayatollah Khamenei, founded the Haj Qasem Foundation to honor and build upon Soleimani's legacy. It operates through the website - soleimany.ir. It promotes Qassem Soleimani's thoughts and beliefs as well as preserves and publishes his works.

Child Predator Communities

ActiveFence has detected significant chatter from child predators exploring the opportunities presented by VR technologies. These communities were the earliest threat actor adopters of VR technology and are primarily engaged in modding games to create child exploitation imagery (CSAM). The communications indicate that child predators are mainly looking to abuse VR to build simulators to reenact sexual violence against minors, create places to store and view CSAM and make new content to share within larger child predator communities.

Storing and Viewing Child Exploitative Imagery

ActiveFence has uncovered communications between child predators about the potential to store and view child pornography in mainstream VR places. In the example below, a user claims to exploit the game display features of a tournament game, having built a virtual museum to store their child pornography collection.



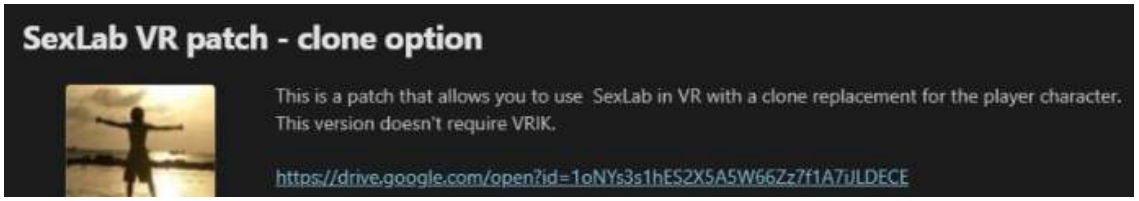
A user claims he holds a collection of child pornography within a custom level of a popular tournament game

Creating Bespoke VR Mods

Users within child predators communities share different tips, tools, and methods to exploit games and create various modifications to create CSAM. As VR technologies become more accessible, the chatter and activity related to bespoke VR mods are increasing in this context.

Tools and Patches

Predators share tools that allow users to clone and alter characters within different games. This activity has a long history, with chatter around this dating from 2019. There are websites and forums dedicated only to this purpose, producing different mods for public use.



Posts from CSAM-related forums discussing different mods of popular games

Virt-a-Mate

Virt-a-Mate is an “adults-only VR sex simulator sandbox game” that is widely discussed and shared amongst pedophile communities on the Darknet. In the game, users can build characters with whom they can engage in sex simulation experiences.

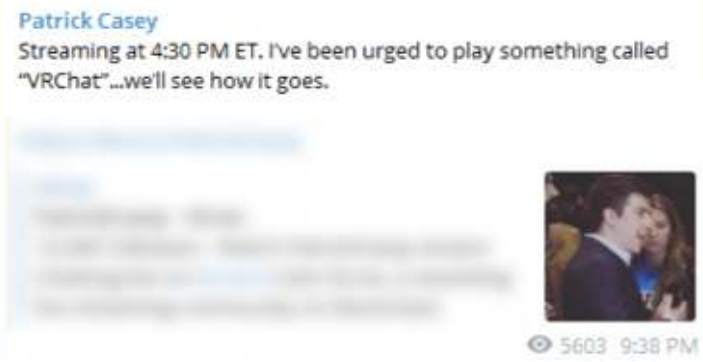
According to chatter within child predators' closed forums, Virt-a-Mate has been modified so that child predators can build and then simulate sexual acts with virtual minors. The images and recordings that are produced from this modded game are shared within child predator communities.

Chatter from a closed forum of child predators, in different threads, discussing ways to watch and produce CSAM; Users share their experience of Virt-a-Mate VR game and claim to have “cp mods”

White Supremacist Organizations

ActiveFence's investigations into the VR activity of white supremacist organizations found that this is composed mainly of converting their preexisting activities to be accessible in VR. White supremacist influencers such as Patrick Casey[3] broadcast hate events on VR platforms, while supporters of specific organizations construct virtual worlds for in-person meetings or to re-enact and plan for future acts of violence.

Fringe groups also exploit VR technology to elevate the experiences of joining white supremacist worlds that were constructed on gaming platforms. These worlds were already created on gaming platforms, but VR enables a more immersive experience for members. White supremacist organizations then use these spaces to deliver racist propaganda, plan the abuse of minorities and incite violence in increasingly radical echo chambers.



Patrick Casey promotes his streaming on an app called VRChat in a Telegram group dedicated to his supporters

[3] Patrick Casey is an alt-right, white nationalist activist who has led the American Identity Movement (AIM) between 2019 and 2020. AIM was a white nationalist, identitarian group that emerged from "Identity Evropa". The movement became one of the largest groups within the alt-Right. AIM focused on marches, rallies, protests and leaf-lifting on the streets and other public areas across the USA, promoting the idea of a white ethno-state and confronting "white genocide". While AIM is no longer active, Patrick Casey continues to be an important influencer amongst neo-Nazis online.

Inciting Violence in Games

The following are examples of white supremacists exploiting a major gaming platform to create experiences that promote dangerous organizations, ideologies, and racially motivated violence. While these are mainly re-enactments rather than instructional guides, ActiveFence is tracking multiple neo-Nazi groups that leverage the gaming ecosystem to radicalize their members for real-world violence.

Christchurch Shooting - Supporters of Brenton Tarrant

The Christchurch Shooting was a white supremacist terror attack against two mosques in Christchurch, New Zealand. The attack took place on March 15, 2019, during Friday prayers and left fifty-one people dead and another forty wounded. Brenton Tarrant, who perpetrated this violence, live-streamed the attack to audiences worldwide and became a cult figure for white supremacists.

The following example was created by supporters of Tarrant. It allows users to re-enact the Christchurch shooting. The game's name is deliberately ambiguous, but its true nature and content are shared directly in forums and private servers to bypass the abused platform's moderation work.

[Left] User uploads game; [Right] Users promote Hate Crimes Simulator Remastered: 2021

White supremacist communities frequently share recreations of mass-casualty racist and homophobic events. For example, ActiveFence has identified games where users can perpetrate the Pulse Shooting (Orland, 2016) and the Columbine Massacre (Colorado, 1999). These glorify violence and radicalize community members with playable training for future attacks. Below is a screenshot from another re-enactment of the Christchurch shooting that is playable in VR.

[Left] Tarrant's gun from the live-stream video [Right] User holds a gun mimicking Tarrant's weapon in the game

Order of Nine Angels - Agios O Vindex!

The Order of Nine Angels (O9A) is a neo-Nazi esoteric Satanic organization with many international branches ("nexions").[4] ActiveFence identified a group O9Aand the game Agios O Vindex![5] These were created by supporters of this dangerous organization in honor of the group's violent mythology. Members of this group display unique terminology and symbols to indicate their affiliation with O9A publicly.

[Lef] O9A group; [Middle] Agios o Vindex; [Right] Link to the Agios O Vindex! game shared within a neo-Nazi group

Raiding Attacks on Minorities

Neo-Nazis collaborate on forums to select targets before piggybacking off other VR spaces to abuse members of minority communities. For example, ActiveFence has collected information on raids against LGBTQ+ Hangouts. Users displayed images of Adolf Hitler, skull masks, and abused LGBTQ+ users calling them mentally ill and claiming that these "kids need beatings." Another detected incident, this time antisemitic, saw a user enter another game to engage in Holocaust Denial.

The user cl_ots writes, "The Holocaust didn't happen. World War II is almost all a lie.

[4] O9A has been linked to various rapes, killings, and acts of terrorism. It is closely associated with the terrorist organization Atomwaffen Division and other violent groups such as Temple of Blood which urges white supremacists to join organizations with "sinister potential" such as the armed forces and the police to perpetrate violence and bring about the apocalypse.
[5] Vindex (Latin for "avenger") is an entity from O9A mythos that the adherents believe will eventually incarnate as a human to overthrow the Judeo-Christian white society.

Conclusion

As the access to VR technologies expands, so will its exploitation by threat actors grow. While the abuse documented in this report is in its early stages, we see the rapid development of new risk areas from multiple directions. The work by terrorist groups to promote themselves, the construction of meeting places and incitement of racially motivated violence by racial supremacists, and the storing and viewing of CSAM video material indicate a conversion towards more sophisticated abuses in the months and years to come.

While VR's social penetration is in its infancy. However, threat actors are already migrating from gaming exploitation to extend their activities to these new platforms and the opportunities they present. This report has shown how threats are in their infancy but are growing in sophistication at a considerable pace. This is the moment for VR developers to take note and build safety by design, working to proactively prevent the harmful abuse of their technologies.

For more information on the threats posed to VR platforms by dangerous groups and organizations, please contact sales@activefence.com.

The proactive approach to online integrity.

ActiveFence is the leading tool stack for Trust & Safety teams, worldwide. By relying on ActiveFence's end-to-end solution, Trust & Safety teams – of all sizes – can keep users safe from the widest spectrum of online harms, unwanted content, and malicious behavior, including child safety, disinformation, fraud, hate speech, terror, nudity, and more.

Using cutting-edge AI and a team of world-class subject-matter experts to continuously collect, analyze, and contextualize data, ActiveFence ensures that in an ever-changing world, customers are always two steps ahead of bad actors. As a result, Trust & Safety teams can be proactive and provide maximum protection to users across a multitude of abuse areas, in 70+ languages.

Backed by leading Silicon Valley investors such as CRV and Norwest, ActiveFence has raised $100M to date; employs over 270 people worldwide; and has contributed to the online safety of billions of users across the globe.

ActiveFence