FINISHED INTELLIGENCE REPORTS

Tokyo 2021 Olympics: Potential Targets on the World Stage

TLP:WHITE

Jul 09, 2021

The international Olympics generate a myriad of international relations issues, political acts from local dissidents, and a novel opportunity for nation state actors to exploit and damage reviled entities upon an international stage. Japan's geopolitical relations with Eastern Eurasian entities, along with their physical location on the Sea of Japan and East China Sea, create a highly dynamic and clustered environment that is hosting one of the largest athletic events in the world. Any nation state that is not aligned with Japan may see an opportunity to try to embarrass Japan through a cyberattack or disruption of essential services.

Whether via direct attacks or by brand sponsor disruption, nation state actors will target any opening of any entity that has a direct connection to some aspect of the 2021 Summer Olympics. Brand sponsors, specifically, have large commercial environments, complex technical logistics systems, and monetary holdings that can be targeted due to their signaled support of the games. While the sponsor holds no political stances towards the geopolitical and regional issues of the host nation, APTs could readily target infrastructure of businesses that have indirect ties to the games.

Please the attached report for further analysis regarding the 2021 Tokyo Olympic Games.

Below is a collection of potential targets that geopolitical actors might scan, exploit or disrupt in a effort to halt the 2021 Summer Olympic Games:

Athletes:

Because the Olympics' popularity and money generation are mainly contingent on voluntary participation, athletes, especially those who are most well-known among fans, are high-value targets to threat actors.If athletes are targeted or even feel targeted by potential actors, via scanning, probing and attempted identity theft, overall participation declines and thus viewership declines, damaging a host nation economically.

Spectators:

Traveling abroad brings new potential targets for actors, as tourists often carry sensitive data on a variety of mobile devices. Public Wi-Fi networks, including those in hotels and event stadiums, are usually unencrypted and can be exploited by cybercriminals to steal sensitive data from spectators.

Anti-Doping Agencies:

As Russia remains banned from participating in the 2021 and 2022 Olympic Games due to doping, the agencies that contributed to decision remain a target for Russian APTs. In addition to World Anti-Doping Agency (WADA) having already been the target of a major data breach, Russians have also attempted to compromise other related organizations, including the US and UK Anti-Doping Agencies. Any nation-state that has been caught cheating or perceives it has been otherwise embarrassed on the international

stage could be motivated to carry out retaliatory cyber attacks towards Olympic anti-doping agencies.

Infrastructure Providers:

Threat actors could potentially disrupt spectators' ability to view the games both locally and internationally by taking down ticketing systems, Wi-Fi networks, or communications and broadcast operations, as they did during the 2018 Winter Olympics.

Reference(s)	wada-ama, BBC, si, cyber Threat Alliance

Release Date
Jul 09, 2021

Sources
CTA: Updating the 2020 Summer Olympics Threat Assessment

Alert ID 3335d74e

View Alert

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**