Securing Smart Cities releases guideline to protect The Olympic Games

Without the Olympics, there would be no means of fostering the quick growth of various technologies. Multiple technological areas have witnessed growth because of these elite Games including; cyber security, smart cities, smart transportation systems, big data revolution, waste recycling, and player tracking and monitoring systems. The Games are the catalyst that make scientists, engineers, and other experts come up with improved products that can be displayed to millions of people and that lead to healthy and more productive lifestyles. With extensive cyber security planning, the Olympics are being kept safe and the framework is in place to ensure that it matches global deployment requirements. Can the Olympics keep up with the challenges and keep the technological evolution going?

Research shows that there is much at stake, from critical infrastructure to healthcare or environmental issues. All of these should be properly managed in the pursuit of a bright future. Figures support this concern. At the 2008 Beijing Games, around 190 million cyber-attacks were reported (12 million per day). At the 2012 London Games, cybercriminals made over 200 million failed attacks on the event's official website. At the 2014 Sochi Olympics, 322 million attacks were reported, followed by 570 million at the 2016 Rio Olympics.

What are the most likely attack vectors at the upcoming Olympics? Here is what the Securing Smart Cities experts think:
• Cyber-attacks on online services for ticketing, reservations, seating, hotels, transport services and food orders (compromise or denial of service)
• Cyber-attacks on authentication and authorization systems (onsite access control accuracy)
• Attacks on robotic machinery, by disabling them or controlling them remotely.
• Attacks on cyber physical operational technologies: Heating, ventilation, and air conditioning (HVAC), elevators, emergency lighting, traffic signals, water treatment facilities, sewage pumps, monitoring drones and cameras…
• Attacks on employees and attendees of the games (phishing, hacking, remote monitoring or data manipulation, blackmailing…)
• Attacks on country infrastructure, water treatment/distribution, power/electricity, transport/airlines, banking, e-government services
• Attacks and manipulation of judges/judging systems, data and/or scoring decisions
• Attacks and manipulation of athlete monitoring (performance enhancement drugs) or monitoring sensors (which are used to enhance their exercising programs and their results)
• Manipulation of data analytics systems and algorithms (which help predict traffic, population density, weather, water/power/storage demands…)
• The spreading of rumors on social media can also significantly impact the Olympics. Fake profiles can post fake messages that can start crowd panics or similar troubles.

Mohamad Amin Hasbini, Senior Security Researcher at Kaspersky Lab, comments: "At every Olympic event, we usually witness a showcase of amazing and futuristic technologies to channel communications, enhance the user experience, and ensure the success of every event. Because of the extensive use of technology at the games, it has attracted a high number of hackers trying to find a way of breaking the systems and causing havoc. This creates a situation where cyber security

challenges are not only an issue of safety, but also provide the opportunity to demonstrate to the world that we are able to successfully combat the threats around us.”