MS-ISAC™ **Intel Paper**

Olympics-Related Malicious Activity Likely to Impact SLTT Governments

February 5, 2018 - IP2018-0104

TLP: WHITE Malicious cyber threat actors (CTAs) have historically used high-profile events, such as the Olympic Games, to disseminate malware and conduct scams, fraud, and cyber-espionage. As employees are likely to view Olympics related content at work, these activities will have direct implications for state, local, tribal, and territorial (SLTT) government networks. Furthermore, there is a distinct cyber threat against SLTT government devices brought to PyeongChang by employees, as it is almost certain that cybercriminals and foreign intelligence agencies will monitor and intercept communications at the Games.

TLP: WHITE It is highly likely that malicious actors will recycle old tactics such as Olympic-themed phishing emails, malvertising, and malicious mobile apps, as well as develop new methods to compromise target devices and accounts. The Multi-State Information Sharing and Analysis Center (MS-ISAC) observed similar campaign tactics in response to former high-profile events, including the 2014 and 2016 Olympics Games in Sochi, Russia, and Rio de Janeiro, Brazil, the 2013 Boston Marathon bombing, and Hurricanes Harvey and Irma in 2017.

- **Phishing** – It is highly likely that malicious actors will capitalize on the 2018 Winter Olympics to send phishing emails with links to malicious websites advertising relevant information such as live coverage, news stories, or ticket sales. These websites often contain malware or attempt to steal login credentials. Based on historic trends, this method is almost certain to be opportunistic in nature, reaffirming that SLTT government employees are likely to receive these emails as part of larger campaigns. Users who follow phishing links or open malicious attachments risk compromising SLTT government networks by disclosing their credentials or downloading malware.
- **Olympic Coverage** – Malicious actors will likely recycle the tactic of creating malware laden websites, masquerading as legitimate platforms, for users to find out information about the Olympic Games. Previously, CTAs have leveraged social media as a platform to spread links to malicious websites. Malicious actors are actively domain squatting, registering domains similar to legitimate ones. Evidence of this tactic has already surfaced with the registration of several suspect domains with themes relevant to live streaming the 2018 Olympic Games. The MS-ISAC has already observed the registration of several domains containing “Olympics”, “winter”, “games”, “PyeongChang”, or “2018” such as winterolympics2018live[.]com, nbcolympics-live[.]com, and statsolympics[.]com. These websites are not confirmed as malicious, although they are not the official domains some of them purport to be.
- **Mobile Apps** – Malicious actors are likely to upload Olympics themed mobile apps with collection capabilities that are likely to cause data breaches if downloaded to SLTT government endpoints. During the Rio Olympics, Proofpoint researchers identified over 4,500 mobile apps pertaining to the Games that also performed risky or malicious activities such as hijacking social media accounts or collecting data

Figure 1 - unofficial application using official Olympics branding

from devices to which the phone connects. In 2018, actors with unknown intentions have uploaded apps to the Google Play Store that claim to be official apps and use the official 2018 Olympic branding. However, these apps appear suspect, as at least one publisher has a poor reputation, and they do not have an official association with the Olympics.

- **Travel to the Olympics** – Nation-state actors are almost certain to conduct cyber-espionage operations against visitors to the Olympics. In addition, the Olympics often attract cybercriminal gangs who travel to high-profile events to conduct Wi-Fi spoofing, packet sniffing, card skimming, and other profit-motivated cyberattacks against visitors. Employees traveling to the 2018 Winter Olympics should avoid bringing government devices or credit cards, or doing government work while traveling as there is a high risk of compromise.
- **Fraudulent Ticket Websites and Free Trips** – During previous Olympics malicious actors established fake ticket websites offering large discounts to draw curious users to the site and other actors used spam emails to lure victims into paying taxes and fees associated with purportedly winning trips to the Olympics. It is likely that this financially-motivated trend will remerge for the 2018 Winter Olympics.

RECOMMENDATIONS:

TLP: WHITE The MS-ISAC recommends that technical administrators adhere to the following guidelines when protecting their networks and users during the 2018 Winter Olympics:

End User Awareness

- Use this opportunity to warn users of the threats associated with scams, phishing, and malware associated with the Olympics and train users about social engineering attempts.
- Disseminate the MS-ISAC Monthly Newsletter on Olympic-themed cyber threats to end users.
- Consider conducting a phishing exercise against your organization with an Olympic theme to increase awareness about this particular threat.
- Remind employees they should only visit trusted websites for information regarding the Olympics and that official coverage will be provided by the Olympics website and NBC Olympics.

Email Security

- Flag emails from external sources with a warning banner.
- Implement filters at your email gateway to filter out emails with known phishing attempt indicators.
- Implement DMARC filtering on email servers. For more information consult the Global Cyber Alliance Guide to Implementing DMARC.

Mobile Device Security

- Remind employees to only install apps on government issued devices in accordance with the agencies' mobile device policy and to thoroughly screen app permissions before downloading. Users should be wary of apps that request permissions outside of what is expected and pay close attention to the publisher to ensure the app originates from a trusted or official organization.
- If permissible, within the confines of organizational Internet use policies, consider providing employees with guest wireless access.

Travel to the Olympics

- Restrict employees from bringing government devices to the Olympics and do not allow remote connections. Do not connect a device or transfer data from a device to SLTT government networks until the device has been scanned and preferably reimaged;
- Direct employees to the State Department's travel recommendations for general security information before traveling to the Olympics and urge them to consult the MS-ISAC Security Primer on Cybersecurity While Traveling.

TLP: WHITE The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information, as well as 24x7 cybersecurity assistance for SLTT governments, is available by contacting the MS-ISAC at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/.