Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

31 January 2022

PIN Number

20220131-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Potential for Malicious Cyber Activities to Disrupt the 2022 Beijing Winter Olympics and Paralympics

Summary

The FBI is warning entities associated with the February 2022 Beijing Winter Olympics and March 2022 Paralympics that cyber actors could use a broad range of cyber activities to disrupt these events. These activities include distributed denial of service (DDoS) attacks, ransomware, malware, social engineering, data theft or leaks, phishing campaigns, disinformation campaigns, or insider threats, and when successful, can block or disrupt the live broadcast of the event, steal or leak sensitive data, or impact public or private digital infrastructure supporting the Olympics. Additionally, the FBI warns Olympic participants and travelers of potential threats associated with mobile applications developed by untrusted vendors. The download and use of applications, including those required to participate or stay in country, could increase the opportunity for cyber actors to steal personal information or install tracking tools, malicious code, or malware[1]. The FBI urges all athletes to keep their personal cell phones at home and use a temporary phone while at the Games. The National Olympic Committees in some Western countries are also advising their athletes to leave personal devices at home or use temporary

[1] For more information on the malware risk associated with government-mandated software, please see FBI FLASH AC-000129-TT, disseminated on 23 July 2020, titled "Tactics, Techniques, and Procedures Associated with Malware within Chinese Government-Mandated Tax Software."

phones due to cybersecurity concerns at the Games. The FBI to date is not aware of any specific cyber threat against the Olympics, but encourages partners to remain vigilant and maintain best practices in their network and digital environments.

Threat

As we mentioned in PIN 20210719-001, large, high-profile events provide an opportunity for criminal and nation-state cyber actors to make money, sow confusion, increase their notoriety, discredit adversaries, and advance ideological goals. Due to the ongoing COVID-19 pandemic, no foreign spectators will be allowed to attend the Olympics or Paralympics. Spectators will be reliant on remote streaming services and social media throughout the duration of the Games. Adversaries could use social engineering and phishing campaigns leading up to and during the event to implant malware to disrupt networks broadcasting the event. Cyber actors could use ransomware or other malicious tools and services available for purchase to execute DDoS attacks against Internet service providers and television broadcast companies to interrupt service during the Olympics. Similarly, actors could target the networks of hotels, mass transit providers, ticketing services, event security infrastructure or similar Olympic support functions.

For example, during the 2020 Tokyo Olympics and Paralympics, the NTT Corporation—which provided its services for the Tokyo Olympic & Paralympic Games—revealed there were more than 450 million attempted cyber-related incidents during the event, though none were successful due to cybersecurity measures in place. While there were no major cyber disruptions, the most popular attack methods used were malware, email spoofing, phishing and the use of fake websites and streaming services designed to look like official Olympic service providers.

In addition, the use of new digital infrastructure and mobile applications, such as digital wallets or applications that track COVID testing or vaccination status, could also increase the opportunity for cyber actors to steal personal information or install tracking tools, malicious code, or malware. Athletes will be required to use the smartphone app, MY2022, which will be used to track the athletes' health and travel data.

During the 2018 PyeongChang Winter Olympics, Russian cyber actors conducted a destructive cyber attack against the opening ceremony, enabled through spearphishing campaigns and malicious mobile applications.

Recommendations

The FBI encourages service providers and other relevant partners to maintain business continuity plans to minimize essential service interruptions. Given the increase in remote work environments and increased use of digitalized infrastructure, to include the use of Virtual Private Network (VPS) services, the FBI encourages regularly monitoring networks and employing best practices. The FBI also suggests reviewing or establishing security policies, user agreements, and patching plans to address current threats posed by malicious cyber actors.

Network Best Practices

- Patch and update operating systems, software, and firmware as soon as manufacturer updates are available.
- Regularly change network system and account passwords, and avoid re-using passwords for multiple accounts.
- Utilize multi-factor authentication when possible.
- Monitor remote access/Remote Desktop Protocol (RDP) logs and disable unused remote access/RDP ports.
- Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
- Regularly audit administrative user accounts and configure access controls under the concept of least privilege.
- Regularly audit logs to ensure new accounts are legitimate users.
- Scan network for open and listening ports, and mediate those that are unnecessary.
- Identify and create offline backups for critical assets.
- Implement network segmentation.
- Automatically update antivirus and anti-malware solutions and conduct regular virus and malware scans.

Remote Work Environment Best Practices

Given the increase in remote work environments and use of Virtual Private Network (VPN) services due to COVID-19, the FBI encourages regularly monitoring these networks and employing best practices.

- Regularly update VPNs, network infrastructure devices, and devices used for remote work environments with the latest software patches and security configurations.
- When possible, implement multi-factor authentication on all VPN connections. Physical security tokens are the most secure form of multi-factor authentication, followed by authenticator applications. When multi-factor authentication is unavailable, require employees engaging in remote work to use strong passwords.
- Monitor network traffic for unapproved and unexpected protocols.
- Reduce potential attack surface by discontinuing unused VPN servers that may be used as a point of entry for attackers.

Ransomware Best Practices

The FBI does not recommend paying ransoms. Payment does not guarantee files will be recovered and may embolden malicious cyber actors to target additional organizations, encourage other criminal actors to engage in the distribution of malware, and/or may fund illicit activities. Regardless of whether the ransom was paid, the FBI urges organizations to report ransomware incidents to a local FBI field

office or file a report with the FBI's Internet Crime Complaint Center (IC3) at IC3.gov. In addition to the above network best practices, the FBI also recommends the following:

- Maintain offline, encrypted backups of data. Regularly test those backups and keep them current.
- Create, maintain, and exercise a basic cyber incident response plan that includes procedures for response and notification in a ransomware incident and plans for the possibility of critical systems being inaccessible for a period of time.

User Awareness Best Practices

- Provide end user awareness and training. To help prevent targeted social engineering, ransomware, and phishing scams, ensure that employees and stakeholders are aware of potential cyber threats and how they are delivered. Also provide users with training on information security principles and techniques.

- Employee knowledge of reporting procedures. Ensure that employees are aware of what to do and who to contact when they see suspicious activity or suspect a cyberattack, to help quickly and efficiently identify threats and employ mitigation strategies.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.