Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

19 July 2021

PIN Number

20210719-001

Please contact the FBI with any questions related to this Private Industry Notification at your local **Cyber Task Force or file a report with the FBI's Internet Crime Complaint Center (IC3)**.

Local Field Offices: www.fbi.gov/contact-us/field-offices **FBI Internet Crime Complaint Center: ic3.gov**

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 has been coordinated with DHS-CISA.

This PIN has been released **TLP: WHITE** Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Potential for Malicious Cyber Activities to Disrupt the 2020 Tokyo Summer Olympics

Summary

The FBI is warning entities associated with the Tokyo 2020 Summer Olympics that cyber actors who wish to disrupt the event could use distributed denial of service (DDoS) attacks, ransomware, social engineering, phishing campaigns, or insider threats to block or disrupt live broadcasts of the event, steal and possibly hack and leak or hold hostage sensitive data, or impact public or private digital infrastructure supporting the Olympics. Malicious activity could disrupt multiple functions, including media broadcasting environments, hospitality, transit, ticketing, or security. The FBI to date is not aware of any specific cyber threat against these Olympics, but encourages partners to remain vigilant and maintain best practices in their network and digital environments.

Threat Overview

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. The Tokyo 2020 Summer Olympics may attract additional attention from these actors, as they are the first to be viewed solely through broadcast and digital platforms due to the prohibition on in-person spectators. Adversaries could use social engineering and phishing campaigns in the lead up to the event to obtain access or use previously obtained access to implant malware to disrupt affected networks during the event. Social engineering and phishing campaigns continue to provide adversaries with the access needed to carry out such attacks.

For example, the FBI indicted Russian cyber actors for intrusions into computers supporting the 2018 PyeongChang Winter Olympics, which culminated in the 9 February 2018 destructive cyber attack against the Opening Ceremony. Prior to the event, the actors targeted South Korean citizens and officials, Olympic athletes, partners, visitors, and International Olympic Committee officials with spearphishing campaigns and malicious mobile applications. The Russian actors obfuscated the true source of the malware by emulating code used by a North Korean group, creating the potential for misattribution.

Cyber actors could use ransomware or other malicious tools and services available for purchase on the Internet to execute DDoS attacks against Internet service providers and/or 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 Olympics support functions.

Criminal or nation-state actors—with different motivations—could hack and leak or hold for ransom sensitive data stolen from a variety of Olympics or Olympics support entities. In late May 2021, Japanese information technology equipment and service company Fujitsu disclosed a breach that compromised data from several of its corporate and government clients, including the Tokyo 2020 Organizing Committee and the Japanese Ministry of Land, Infrastructure, Transport, and Tourism.

Recommendations

The FBI encourages service providers and other relevant partners to maintain business continuity plans to minimize essential service interruptions, as well as preemptively evaluate potential continuity and capability gaps. Given the increase in remote work environments and use of Virtual Private Network (VPN) 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 cyber-attack, 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. Information on ransomware can be filed with the FBI's Internet Crime Complaint Center at IC3.gov. 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, **TLP: WHITE** information may be distributed without restriction.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey