2020 SUMMER OLYMPICS THREAT ASSESSMENT

CYBER THREAT ALLIANCE

The Cyber Threat Alliance (CTA) is the industry's first formally organized group of cybersecurity practitioners that work together in good faith to share threat information and improve global defenses against advanced cyber adversaries. CTA facilitates the sharing of cyber threat intelligence to improve defenses, advance the security of critical infrastructure, and increase the security, integrity, and availability of IT systems.

We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared amongst its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operational collaboration to enable a more secure future for all.

For more information about the Cyber Threat Alliance,
please visit: https://www.cyberthreatalliance.org.

OLYMPICS CYBERSECURITY WORKING GROUP MEMBERS

Cisco Talos:
Kendall McKay (Lead Author), Ryan Pentney

Fortinet:
Val Saengphaibul, Kenichi Terashita

NEC Corporation:
Ryusuke Ichimiya, Tomoomi Iwata, Takaki Utsuda

NTT Security:
Jeremy Scott, Shinji Abe, Hiroki Hada, Syogo Hayashi

Palo Alto Networks:
Karou Hayashi, Ryan Olson, Brittany Ash

Radware: Daniel Smith

Cyber Threat Alliance:
Neil Jenkins

This report also leverages shared data and published analysis from CTA members Alien Labs, Check Point, Dragos, Telefonica's ElevenPaths, IntSights, Juniper Networks, Lastline, McAfee, NETSCOUT Arbor, Panda Security, Radware, Rapid7, Reversing Labs, SecureBrain, SK Infosec, Sophos, Symantec, and Verizon. CTA members reviewed the document throughout its development and the report reflects our shared consensus.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Cyber Threat Alliance (CTA) has established an Olympics Cybersecurity Working Group to bring members together to share information and prepare for any cybersecurity events that may impact the 2020 Summer Olympics in Tokyo, Japan. As a part of our preparation for this event, CTA members have jointly developed CTA's first Threat Assessment. This document provides a high-level summary of the threat environment facing the 2020 Olympics and recommendations for the Tokyo Organizing Committee to use as they prepare for the Games. This Threat Assessment also focuses CTA members' information sharing around the Games and enables us to develop planning scenarios based off the cybersecurity threat landscape.

CTA assesses that nation-state actors will pose the highest threat to the Olympics and Olympics-affiliated entities based on their sophisticated capabilities and past operations. Russian, North Korean, and Chinese state-sponsored adversaries likely pose the most significant threats to the Games given their prior attack history, reputations as formidable actors, and geopolitical tensions. Comparatively, CTA judges that Iran is less likely to conduct Olympics-related cyber threat operations. Despite Iran's history of conducting offensive cyber campaigns globally, we assess that it is not in Tehran's strategic interest to compromise the Tokyo Games or affiliated entities.

As with any global event, geopolitics plays an important role in understanding the threat landscape. Current events, territorial disagreements, and historical tensions will further motivate these actors to conduct cyber operations against Japan. Japan is at the center of several regional conflicts, and its role as Olympics host is likely to make the country a high-priority target for longtime adversaries looking to embarrass Tokyo on the international stage.

While nation-state actors have the potential to carry out a variety of different types of operations, we judge that disruptive attacks and disinformation campaigns are the most likely. Specifically, actors may try to conduct targeted data leaks, attempt to disrupt the 2020 Olympics through Distributed Denial of Service (DDoS) attacks, compromise systems through ransomware attacks, or affect physical critical infrastructure. CTA assesses that anti-doping agencies and experts, along with services supporting the Games' operations and logistics, such as Wi-Fi networks and ticketing systems, are at the highest risk of being compromised. Other potential targets include tourists and spectators, Japanese officials and partner governments, Olympic partners and sponsors, and supply chain and infrastructure providers.

In addition to nation-state threats, CTA members assess that the 2020 Summer Olympics will be a prime target for cyber criminals due to the large number of potential victims leveraging online systems and tourists' poor cybersecurity awareness. The 2020 Organizing Committee is already facing scams and other criminal activity in the lead up to the Olympics.

Japan faces many cybersecurity challenges leading up to the Games but has implemented several positive changes in recent years. While Japan's efforts are encouraging, CTA notes that the underlying cybersecurity problems in corporate and government environments are not easy to fix in a short amount of time. These problems are not unique to Japan and they are common problems in many countries that rely on information technology to deliver services and drive the economy. CTA recommends that the Organizing Committee and Japanese government focus their current efforts on implementing best practices, information sharing, coordinated planning around cybersecurity incidents, and regular examination of critical systems.

INTRODUCTION

The Cyber Threat Alliance (CTA) provides a forum for members to share information on cybersecurity threat indicators, intelligence, and defensive measures and to collaborate on cybersecurity issues. CTA members are committed to working together to protect end-users, disrupt malicious actors, and elevate overall cybersecurity. CTA members routinely identify significant events that may be the target of malicious cyber activity. We then establish working groups to focus our sharing activities around threats to those events.

CTA established the Olympics Cybersecurity Working Group in the fall of 2019 to begin sharing information about Olympics-related activity and working internally with members and externally with various stakeholders to prepare for the Summer Games. To support our collective efforts and assist the Tokyo Organizing Committee, the Working Group has developed CTA's first Threat Assessment. This document provides an overview of prior threat activity targeting past Olympics and organizations related to the Olympics, reviews of the potential threat actors that may target the games, the organizations and stakeholders that may be targeted, the potential threat activity that may occur, an overview of Japan's security posture, and lessons learned and recommendations to address these issues. This document is being provided to the Tokyo Organizing Committee for their review and use in preparing for the 2020 Summer Olympics.

PRIOR THREAT ACTIVITY

Cyber threat actors have been targeting the Olympics for at least a decade, with their attacks growing more complex and effective with each iteration of the Games. Since 2008, Olympics-related cyber threat activity has increased in frequency and sophistication, with disruptive attacks being among the most common. In several cases, the threat activity started before the Olympics began but increased in intensity once the Games officially got underway, highlighting the potential for months-long sustained campaigns. Adversaries used an array of tactics, techniques, and procedures (TTPs) to carry out their campaigns, the most common being phishing, spearphising, domain spoofing, and botnets-for-hire. Based on prior threat activity, anti-doping organizations and officials are at increasingly high risk of being compromised, as are operational and infrastructure-related targets such as power utilities, broadcast systems, and stadium Wi-Fi networks.

The following summary of threat activity from prior Olympics is not intended to be an all-inclusive list; rather, it highlights some of the major or highly reported incidents from each respective event.

2008 BEIJING

Malicious cyber threat activity prior to and during the 2008 Beijing Olympics was relatively limited. While officials reportedly responded to 11 to 12 million cyber alerts per day, none of those incidents resulted in any successful attacks.[1] Some ticket scams were also detected, with the United States shutting down two websites that stole users' credit card information after fraudulently promising to sell tickets.[2]

2012 LONDON

Overall, cybersecurity incidents during the 2012 London Olympics were low-level and did not result in any successful high-impact events. The most significant event involved evidence of a credible cyber threat against the electrical infrastructure

1 https://www.infosecurity-magazine.com/magazine-features/securing-the-2012-olympics/

2 https://www.scmagazine.com/home/security-news/beijing-olympic-ticket-scam-shut-down/

supporting the Games. There was reportedly a 40-minute Distributed Denial of Service (DDoS) attack on the Olympic Park's power systems that was likely intended to disrupt the opening ceremony.[3] While the attack failed, organizers had installed backup systems in the event the stadium lost power. Separately, for about five days after the Olympics began, hacktivists promoted the #letthegamesbegin social media campaign urging people to conduct timed DoS attacks against the Olympics IT infrastructure. The effort resulted in virtually no impact.[4]

2016 RIO DE JANEIRO

Prior to and during the 2016 Rio de Janeiro Olympic Games, Olympics-affiliated organizations were targeted by a large-scale DDoS attack carried out by a known IoT botnet, LizardStresser. Brazilian and International Olympics Committee (IOC) officials mitigated the threat activity and were able to keep systems up and running despite peak attack traffic registering at a staggering 540 Gbps.[5] Many of these attacks occurred before the Games started, but the adversaries increased their efforts significantly after the Olympics got underway, according to research published by Arbor Networks' Security Engineering & Response Team (ASERT), a division of CTA member NETSCOUT Arbor, who has been actively involved in enabling DDoS detection and mitigation at major events.[6] There were also threats from a hacktivist movement, the #OpOlympicHacking campaign, in response to perceived Brazilian government overspending during the 2014 World Cup.[7]

2016-2017 CAMPAIGN AGAINST ANTI-DOPING ORGANIZATIONS

Between 2016 and 2017, Russian state-sponsored cyber actors conducted a massive influence campaign against multiple anti-doping agencies in revenge for a disparaging report accusing Russia of orchestrating a state-run drug testing subversion program. The report, known as the McLaren Report, was released in July 2016 by the World Anti-Doping Agency (WADA) and described systemic efforts by the Russian government to undermine the drug testing process prior to, during, and after the 2014 Sochi Winter Olympics. The findings resulted in the IOC levying harsh sanctions against Russia, including banning over 100 Russian athletes from participating in the 2016 Rio Olympics.

The threat activity began in mid- to late-2016, when adversaries stole sensitive information from WADA and posted it online in a series of September releases. The data included medical records of numerous well-known athletes from multiple countries, including, in many cases, evidence that they had been cleared to participate in the Rio Games despite testing positive for banned substances. Subsequent to the WADA data breach, Russian actors compromised officials at several other anti-doping organizations, including the United States Anti-Doping Agency (USADA), the Canadian Centre for Ethics in Sport (CCES), the International Association of Athletics Federations (IAAF), Fédération Internationale de Football Association (FIFA), and approximately 35 other anti-doping agencies or sporting organizations.[8] Ultimately, the attackers released private or medical information on approximately 250 athletes from

3 https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2395/RAND_RR2395.pdf

4 https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2395/RAND_RR2395.pdf

5 https://news.softpedia.com/news/ddos-attacks-during-rio-olympics-peaked-at-540-gbps-507822.shtml

6 https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec- ddos-attack-failed-to-spoil-the-rio-olympics/

7 Booz Allen and Cyber4Sight, 2016 Rio Summer Olympic Games Cyberthreat Environment, May 26, 2016. Available at https://docplayer.net/50042593-2016-rio-summer-olympic-games-cyberthreat-environment.html

8 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

almost 30 countries.[9] In preparation for these attacks, the adversaries procured spoofed domains mimicking those belonging to WADA and other anti-doping organizations, probed those entities' networks, and sent spearphishing emails to employees.[10]

2018 PYEONGCHANG

On February 9, 2018, attackers targeted networks prior to the opening ceremony of the Pyeongchang Winter Olympics in what was likely an attempt to cause chaos and confusion. The attackers used a malicious worm, called Olympic Destroyer, that took the official Olympics website offline, interrupted Wi-Fi access at the stadium, and disrupted broadcasts of the event. The attack prevented many spectators from accessing and printing tickets to the ceremony.

Based on analysis conducted by Cisco Talos on multiple malware samples used in the attack, the adversaries were solely intent on disrupting the games, not exfiltrating data. According to Talos, the malware renders the victim machine unusable by deleting shadow copies, event logs, and trying to use native operating system functions, such as PsExec[11] & Windows Management Instrumentation (WMI),[12] to further move through the environment.[13]

The 2018 Pyeongchang Olympics saw another campaign that received relatively little media attention. One attack leveraged a Rich Text Format (RTF) file utilizing CVE-2012-0158 as an exploit vector, discovered by Clearsky Security.[14] CVE-2012-0158 is a Microsoft Office buffer overflow vulnerability in the ListView/ TreeView ActiveX controls in the MSCOMCTL.OCX library. A specially crafted malicious DOC or RTF file can be used to arbitrarily execute remote code in MS Office versions 2003, 2007, and 2010.

This campaign appeared to target individuals at an unidentified organization who were possibly interested in the Olympics. The lure was a malicious Word document titled "Russian figure skater won the Pyeongchang Winter Olympics in South Korea. doc" (translated from Russian). Once the user opened the document, the sample dropped a backdoor component that appeared to be related to the Icefog APT backdoor, which has been used in the past to target various sectors in the APAC region, with a focus on Japan and South Korea. The Icefog group also has been observed leveraging CVE-2012-0158.

SEPTEMBER 2019 ANTI-DOPING ORGANIZATIONS

In the most recent Olympics-related threat activity, there is evidence that APT28/Fancy Bear is again targeting anti-doping organizations. According to Microsoft (who refers to the actor group as Strontium), the threat actor began targeting at least 16 related entities in mid-September 2019, days before WADA announced that Russia could face additional Olympics bans. [15] [16] Most of the attacks were unsuccessful.

9 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

10 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

11 https://attack.mitre.org/software/S0029/

12 https://attack.mitre.org/techniques/T1047/

13 https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

14 https://twitter.com/ClearskySec/status/968104465818669057?s=20

15 https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

16 https://www.bbc.com/sport/athletics/49805296

HISTORICAL ADVERSARIES AND POTENTIAL THREAT ACTORS

Nation-state actors will likely pose the highest threat to the Olympic Games and Olympics-affiliated entities based on their sophisticated capabilities and proven ability to conduct highly effective operations. Nation-state actors often enjoy the tacit support of their host government and, in many cases, operate with assistance from or under the direction of state intelligence services, which affords them a range of resources and benefits unavailable to lower-level actors or cybercriminals. Relatedly, geopolitics are likely to play a significant role in influencing Japan's threat landscape leading up to the Olympics, as the country is at the center of several regional and historical disputes that could prompt cyber threat activity.

While well-known Russian, North Korean, and Chinese state-sponsored adversaries pose significant threats to the Games based on their prior attack history and reputations as formidable actors, we judge that current events, territorial disagreements, and historical tensions will further motivate these actors to conduct cyber operations against Japan. Furthermore, regional disputes will possibly motivate other nation-state actors from countries typically unassociated with cyber threat activity, such as South Korea, to conduct operations in support of the government's national interests. Japan is at the center of several regional conflicts, and its role as Olympics host is likely to make the country a target for longtime foes looking to embarrass Tokyo on the world stage.

RUSSIA

We assess that Russia poses the most significant threat to the Tokyo Games and affiliated entities based on APT28's prior Olympics-related threat activity and WADA's most recent anti-doping penalties levied against Moscow. In December 2019, WADA banned Russia from competing in international sporting events for four years for manipulating laboratory data handed over to investigators in January 2019.[17] As part of the sanctions, the Russian anthem will not be allowed at the 2020 Olympics and Russian athletes will have to compete under a neutral flag. This is the second time Russia has been banned from the Olympics. The first incident, which is well-documented in this report, prompted Russia-backed cyber actors to carry out an attack campaign against WADA, suggesting Moscow is likely to react similarly in response to this latest ban.

There are multiple examples of Russian state-sponsored actors carrying out prior cyber attacks against Olympics-affiliated entities and individuals, a further indication that future threat activity against similar targets is highly likely. As previously mentioned, APT28, a Russian nation-state cyber threat actor group, was responsible for the 2016-2017 campaign against WADA and other anti-doping agencies. The U.S. Department of Justice (DOJ) indicted seven Russian GRU officers for their involvement in the crimes.[18] The threat activity carried out during the 2018 Pyeongchang Olympics was rumored to have been carried out by Russia as well, with several U.S. intelligence officials claiming as much.[19] Most recently, Microsoft attributed a new round of attacks on anti-doping organizations in September 2019 to APT28, as previously mentioned.[20]

Based on prior threat activity, Russia has the

17 https://www.wada-ama.org/en/media/news/2019-12/wada-executive-committee-unanimously-endorses-four-year-period-of-non-compliance

18 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

19 https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html

20 https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

propensity to conduct targeted operations in retaliation for embarrassment or perceived unfairness. In addition to Russia's known history of targeting Olympics-related organizations and individuals, the latest WADA development makes it even more likely that Moscow will conduct attacks in advance of or during the Tokyo Games. While many of APT28's previous attacks have been brazen, Russian state-sponsored threat actors are also known to obfuscate their operations -- either as a way to imitate other nation-state groups or avoid attribution altogether -- suggesting that future Olympics-related threat activity could take either form.[21]

On the geopolitical front, Russia and Japan have an ongoing territorial dispute over the Kuril Islands, a cluster of four land masses northwest of Japan's mainland. The disagreement further complicates Japan's threat environment vis-à-vis Russia and will possibly further motivate Moscow to conduct cyber operations during the Tokyo Games.

NORTH KOREA

While there have not been any reported incidents linking Pyongyang to potential 2020 Olympics-related cyber attacks, North Korean state-sponsored cyber actors pose a possible threat to the Games based on their hostile relationship with Japan and demonstrated ability to conduct highly sophisticated and targeted operations. North Korean state-sponsored cyber actors have carried out some of the most notorious and lucrative attacks in recent years, including stealing hundreds of millions of dollars from banks and cryptocurrency exchanges.[22] In addition to financially motivated operations, Pyongyang has also used its cyber capabilities to conduct espionage, such as in the 2013 campaign against South Korea dubbed Operation Troy, and carry out disruptive and destructive campaigns, including the 2017 WannaCry ransomware attacks and 2014 Sony Pictures compromise. These operations have targeted an array of industries in multiple countries, highlighting the actors' sophistication and global reach.

Tense North Korea-Japan relations, driven by both pre- and post-World War II disputes, heighten Tokyo's threat environment leading up to the 2020 Olympics. Over the last 20 years, sporadic attempts have been made between the two countries to normalize relations, but such efforts have been largely unsuccessful.

North Korean state-sponsored cyber actors use a variety of infection methods, including email spoofing with decoy documents, watering hole attacks, and supply chain compromises. In recent years, they have reportedly developed custom tools for targeting MacOS and mobile applications to broaden their capabilities. These threat actors, particularly North Korea-linked Lazarus Group, are also highly skilled in obfuscation techniques to prevent network defenders and security software from identifying nefarious activity.

CHINA

Chinese state-sponsored cyber actors also pose a threat to the Games based on their known history of targeting Japanese companies, highly sophisticated cyber capabilities, and tense China-Japan relations. Several China-linked groups are known to routinely carry out operations against Japanese entities, indicating that Japan is a top target for China-sponsored cyber threat actors. APT10, in particular, has been publicly blamed by multiple countries for such activity. In December 2018, the FBI indicted two Chinese individuals linked to APT10 for cyber espionage, which included operations against

21 https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html

22 https://www.forbes.com/sites/leemathews/2019/03/11/north-korean-hackers-have-raked-in-670-million-via-cyberattacks/#7a674c807018

Japanese companies.[23] [24]

China and Japan have several historical and territorial disputes that motivate much of the ongoing cyber threat activity and which adds to the heightened threat environment leading up to the 2020 Olympics.

Chinese state-sponsored threat actors have the capabilities to use an array of malware, including both custom and open-source tools, to compromise hosts and establish persistence on victim networks. They conduct reconnaissance on victims' networks prior to the start of their campaigns, enabling their operations to be highly targeted and well-thought-out. Many groups, such APT10, compromise victims through spearphishing emails and accessing victims' networks through managed service providers. Like most state-sponsored actors, those linked to Beijing are highly sophisticated and pose significant threats to entities globally.

IRAN

Iran has continued to improve its offensive cyber capabilities over the last several years and has engaged in activities ranging from website defacements to DDoS attacks, theft of personally identifiable information (PII), and destructive wiper malware attacks.[25] Several of the most well-known APTs and threat actor groups emanate from Iran and are tracked closely by the U.S. government and cybersecurity researchers monitoring their latest campaigns. Despite Iran's reputation, though, we assess that it is not in Iran's strategic interest to conduct cyber operations against the Olympics or affiliated entities. Iran and Japan lack the historical tensions that underpin so many of Japan's other geopolitical relationships outlined in this report and Iran-Japan relations are relatively friendly.[26]

Moreover, Iran has no obvious advantage to gain from carrying out such operations. While CTA assesses that Iranian Olympics-related threats are low, we note the heightened tensions between the U.S. and Iran–stemming from late 2019 and early 2020 incidents—and acknowledge the possibility for this to cause Tehran to rethink its global offensive strategy vis-à-vis the United States and its allies. CTA urges the Organizing Committee to remain vigilant regarding possible Iranian cyber operations.

SOUTH KOREA

South Korea has a tenuous relationship with Japan fueled by a complicated past and ongoing diplomatic disputes, but we assess that Seoul is unlikely to conduct cyber operations against the Olympics or related entities. While South Korea is not known for launching offensive cyber operations or supporting state-run cyber threat groups, international relations often effect cyber threat activities, and it is worth noting the countries' conflicts. Much of the tension dates back to the pre-WWII era. Currently, the two countries are embattled in a trade dispute as well as a longstanding disagreement over territorial claims.

HACKTIVISTS AND CYBERCRIMINALS

Hacktivists and cybercriminals are also likely to conduct operations before, during, or after the Olympics for many of the reasons that were previously outlined in earlier sections of this report. Opportunistic hacktivists may perceive the Olympics to be an effective platform through which to advance their causes given the event's media coverage and global interest. Any nefarious social media campaign or related threat activity is likely to garner much more publicity than a similar operation carried out during a lower-profile event. Similarly,

23 https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

24 https://www.scmp.com/news/asia/east-asia/article/2179072/japan-condemns-china-based-cyberattacks-urges-beijing-take

25 https://www.us-cert.gov/ncas/alerts/aa20-006a

26 https://www.reuters.com/article/us-iran-japan-abe-explainer/explainer-why-is-japans-abe-going-to-iran-what-can-he-accomplish-idUSKCN1T80U9

cybercriminals almost certainly will take advantage of the large victim pool of unsuspecting tourists employing poor cybersecurity practices.

POTENTIAL TARGETS

ATHLETES

Athletes, particularly those who are most well-known among fans, are high-value targets because the Olympics' popularity and revenue generation is largely dependent on their participation. There is also precedent for such attacks, as was witnessed during the 2016 WADA compromise. In the summer of 2016, Russian cyber threat actors stole drug test results from WADA and leaked the data onto the internet. The breach included sensitive and potentially embarrassing information about Olympic athletes. Some of the data, for example, included evidence that U.S. tennis stars Serena and Venus Williams and U.S. gold gymnast Simone Biles received waivers to participate in the 2016 Rio Olympics despite testing positive for banned substances. The operation was almost certainly in retaliation for WADA's July 2016 report condemning Russia for running a drug-testing subversion scheme before, during, and after the 2014 Winter Olympics. As a result of the report's findings, over 100 Russian athletes were banned from the 2016 Summer Games in Rio de Janeiro. Therefore, the data leak was likely intended to discredit or embarrass other non-Russian athletes.

ANTI-DOPING AGENCIES AND EXPERTS

Relatedly, anti-doping agencies and experts are at high risk of being targeted in cyber attacks. In addition to WADA having already been the target of a major data breach, the Russians also attempted to compromise other related organizations, including the U.S. and U.K. Anti-Doping Agencies and the Canadian Centre for Ethics in Sport. The threat actors also targeted anti-doping officials at sporting federations like the IAAF and FIFA. Any nation-state that has been caught cheating or perceives it has been otherwise embarrassed on the international stage is highly likely to be motivated to carry out retaliatory cyber attacks.

OPERATIONS, LOGISTICS, AND INFRASTRUCTURE PROVIDERS

Adversaries may seek to compromise targets affecting the operations and logistics of the Games. By shutting down ticketing systems, Wi-Fi networks, or communications and broadcast operations, as threat actors did during the 2018 Winter Olympics, adversaries could easily disrupt viewers' ability to watch the games both in-person and globally. Critical infrastructure, particularly the energy and transportation sectors servicing the Olympic Village, Olympic Venues, and the general population of Japan are also vulnerable targets. A successful compromise could cause mass chaos and significantly disrupt, if not altogether shut down, Olympic events. While there is no known nexus to the Olympic games, we note recent reporting of a major security breach at Mitsubishi Electric, one of Japan's biggest defense and infrastructure contractors.[27] Cybersecurity breaches and incidents such as these could be leveraged for disruptive attacks during the Olympic games.

Adversaries are also likely to compromise point-of-sale (POS) systems, which are key targets for cybercriminals seeking to steal credit or debit card information. While such attacks have increased in recent years, we judge that they are particularly more likely to occur at the 2020 Games given the high number of merchants and sales transactions during a major global event like the Olympics. A disruption to any of these operations would be embarrassing to the host nation, particularly considering the immense amount of global scrutiny and national pride that comes with hosting the Olympics.

27 https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/

Another potential target includes companies that provide infrastructure support during the Olympics. For example, ATOS is a managed security service provider (MSSP) of cloud services that has been the IOC's Worldwide IT Partner for years. As an Olympics provider of IT and managed infrastructure solutions, ATOS became a target during the 2018 Pyeongchang Games and was subsequently compromised by the same actors behind the Olympic Destroyer malware months before the Olympics began.[28] It is unknown whether the actors gained access to the Games' infrastructure through ATOS. Nevertheless, cyber incidents that access the target's supply chain partners have been on the rise recently and it is important to work closely with infrastructure providers on security. Several CTA members that worked on this report are also providing infrastructure for the Organizing Committee and are aware of the threat to their systems. We remain vigilant and are prepared to share information with each other and the Organizing Committee related to threats to our systems.

Depending on the threat actor's motivation, an overt attack would possibly be timed to occur during events that would attract the most media coverage to maximize impact. The opening and closing ceremonies are two of the most watched Olympics events, with the last Summer Olympics (Rio 2016) ceremonies drawing around 30 million and 15 million viewers, respectively.[29] [30] There is also precedent for such activity, as threat actors strategically chose to disrupt the Pyeongchang opening ceremony at the start of the 2018 Winter Olympics.

TOURISTS AND SPECTATORS

Unsuspecting tourists and event spectators are often easy targets, especially for cybercriminals, because they typically do not employ good cybersecurity practices and are not well-educated about the threat landscape. Traveling abroad brings unique challenges, as tourists often carry sensitive data on a variety of devices, including smartphones, tablets, and laptops. Public Wi-Fi networks, including those in hotels, cafes, and event stadiums, are usually unencrypted and can be exploited by cybercriminals to steal personal account information or other sensitive data from victims. This situation is especially problematic considering that tourists typically use public Wi-Fi more frequently when traveling to avoid data overage fees.

Similarly, Bluetooth connectivity can be exploited to carry out eavesdropping, data theft, and even complete device takeover. Travelers also face a heightened risk of data breaches at customs checkpoints, as governments typically increase security measures at those locations. Security services, for example, can confiscate devices for inspection then install malicious software, such as spyware, to gather information.

JAPANESE AND PARTNER CYBERSECURITY ORGANIZATIONS AND OFFICIALS

Another category of potential targets includes entities and individuals in the host country, particularly organizations charged with providing and overseeing cybersecurity efforts and high-ranking government officials. We assess that these targets are less likely to be the subject of a cyber attack, as it would be easier for an adversary to target many of the other previously mentioned victim groups employing poor cybersecurity practices. Japanese and partner country cybersecurity agencies are ostensibly harder targets, but a successful attack would therefore likely have a greater payoff. Likewise, government officials, particularly those with cybersecurity related positions, are less likely to become victims but might be targeted if an adversary was intent on

28 https://www.cyberscoop.com/atos-olympics-hack-olympic-destroyer-malware-peyongchang/

29 https://variety.com/2016/tv/news/olympics-opening-ceremony-ratings-rio-fall-london-1201831995/

30 https://variety.com/2016/tv/news/tv-ratings-olympics-closing-ceremony-ratings-down-1201842009/

carrying out a highly targeted attack that was meant to embarrass particular individuals. A nation-state actor would be the most likely adversary to carry out this type of attack since it would require more sophistication.

One such incident occurred during the 2016-2017 Russian campaign against anti-doping organizations, when adversaries stole keylogs and an array of documents and sensitive information from top officials at IAAF and FIFA. The actors targeted computers and accounts used by each organization's top anti-doping official.[31] They were almost certainly targets due to their high rank and subsequent access to data that adversaries perceived to be valuable.

OLYMPIC SPONSORS AND ASSOCIATED BUSINESSES

Lastly, adversaries will possibly target official Olympic sponsors and associated businesses. We expect that hacktivists would be the most likely culprit behind these types of attacks, as such entities would be good targets for groups or individuals seeking to advance their cause or draw attention to a particular issue or grievance. Malicious cyber operations are likely to come in the form of social media or disinformation campaigns rather than direct attempts to compromise a specific organization, although we do not rule out the latter possibility. Such operations could include campaigns to boycott a specific company. This type of activity has been observed in the past against U.S. businesses, including the 2017 social media push to boycott NFL sponsors in response to the league's standing over players' rights to kneel during the national anthem. We assess that Olympic sponsors and partners would be particularly high-value targets because of the global nature of the Games, as any attack or social media campaign against affiliated businesses would have the potential to draw international attention.

POTENTIAL THREATS

DATA LEAKS AND DISINFORMATION

Data leaks are an effective way for threat actors to cause embarrassment. The impact can be devastating for victims. Malicious cyber actors have conducted "hack and leak" operations numerous times over the recent past to embarrass victims and try and win concessions, either through blackmail or extortion, or to simply sow discontent in a population. Some of the more notable data leak operations include the leaking of diplomatic cables from the U.S. State Department that led to the exposure of sensitive, confidential information,[32] the leaking of emails from Sony Pictures Entertainment in 2015 in an attempt to prevent *The Interview* from being released,[33] and the 2016 hack of John Podesta's emails which led to embarrassing insights and private discussions among the Clinton Presidential Campaign and the Democratic National Committee.[34]

Disinformation, or false information that is intended to mislead, has become another real threat in recent years. Disinformation and propaganda operations are often seen in tandem with data leaks. During the 2016-2017 Russian campaign against anti-doping agencies, some of the WADA documents were modified prior to being leaked. According to the DOJ, some of the stolen, leaked information was accompanied by posts supporting themes that the Russian government had used in response to the anti-doping agencies' findings.[35] The threat actors conducted an outreach campaign on social media to

31 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

32 https://en.wikipedia.org/wiki/United_States_diplomatic_cables_leak

33 https://en.wikipedia.org/wiki/Sony_Pictures_hack

34 https://en.wikipedia.org/wiki/Podesta_emails

35 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

push the stolen data to reporters, then recirculated published articles about the breach to maximize exposure. In this instance, the threat actors were engaging in an organized effort to push a narrative intended to embarrass athletes and anti-doping officials while attempting to cast Russia in a more positive light.

Given the increasing use of disinformation campaigns and data leaks, both in Olympics- and non-Olympics-related incidents, we judge that these types of threats will likely occur before, during, or after the 2020 Games. Russia's latest WADA infraction, which has the country facing another Olympics ban, is likely to compel Moscow to carry out such attacks. In addition to Russia, other countries have undoubtedly observed the efficacy of such operations, and we judge it is plausible for any nation-state to perceive disinformation campaigns and data leaks as a viable attack option.

DISRUPTIVE ATTACKS

The 2018 Pyeongchang Olympics cyber threat activity is the most recent example of the type of disruptive attack we could expect to see during the Games. Such operations would aim to interrupt frequently used services, such as ticketing systems, POS systems, Wi-Fi and broadcast networks, or even critical infrastructure in the region, such as public transportation, electric power, gas, or water. These incidents would have the potential to cause massive slowdowns, confusion, and chaos. Ransomware may also be used by cyber criminals to disrupt operations for financial gain. High profile ransomware operations targeting government organizations have been prevalent in the US recently and may also be leveraged against government organizations and Olympic entities in Japan. Such an attack could render Olympics-related IT systems non-operational at critical points.

Finally, several of our examples from previous Olympics noted the use of Distributed Denial of Service (DDoS) attacks against the games specifically or against organizations affiliated with the Olympics. Historically, other major international sporting events, such as FIFA's World Cup, the Commonwealth Games, and the Rugby World Cup, have also seen significant DDoS attacks, often from hacktivists attempting to send a message. In keeping with observations from previous events, CTA members assess that actors are likely to leverage DDoS attacks and may target the Olympics directly, affiliates, or even common cloud services,[36] leading to disruptions in dependent applications.

CYBERCRIME

In addition to the specific cybersecurity incidents outlined above, common, low-level threats were also present at most, if not all, of the Olympics outlined in this report. Cybercrime threats, including ATM card skimming and point-of-sale (POS) malware, were constant, particularly in countries like Brazil with high levels of online criminal activity. In late 2019, the well-known banking malware Emotet resurfaced and infections were particularly concentrated in Japan.[37] In November, the government warned entities involved in the 2020 Olympics about the heightened threat, highlighting Tokyo's concern over a potentially devastating Emotet-related incident leading up to the Games.[38]

SCAMS

Ticket scams were a common occurrence at previous Olympics, many of which relied on fraudulent websites to steal payment credentials and PII from unwitting victims. Threat actors also routinely spoof popular Olympics-themed websites to trick users into visiting malicious sites intended to steal victims'

36 https://threatpost.com/massive-ddos-amazon-telecom-infrastructure/150096/

37 https://www.darkreading.com/threat-intelligence/trickbot-expands-in-japan-ahead-of-the-holidays/d/d-id/1336510

38 https://www.japantimes.co.jp/news/2019/11/28/national/emotet-computer-virus-spreading-japan-warns-official/#.Xe_bAZNKh3k

data or download malware onto victims' machines. Other common scams include fake awards or offers, such as the promise of free cash, travel, and hotel deals, which could be distributed via phishing emails or Olympics-themed pop-up advertisements. These scams are intended to lure victims into conducting fraudulent transactions so that threat actors can steal their information. The 2020 Olympics have already seen phishing campaigns that delivered emails designed to look like they were coming from the Organizing Committee and related organizations, such as the Special Olympics of New York, which has seen its email server compromised to send phishing emails to previous donors.[39]

HACKTIVISM

While most hacktivist activity is typically unsophisticated, such campaigns may still have a high impact if successful. Hacktivist campaigns often come in the form of organized boycotts against a particular company, website defacements, DDoS attacks, or compromises that can result in high-profile, high-impact data breaches.

WIRELESS NETWORKS

The influx of tourists and attendees to the Games will increase the demand for mobile data access in and around Tokyo, creating more opportunities for threat actors to compromise victims. As Japan's telecommunications providers prepare to accommodate a surge of mobile device usage, which could include additional mobile access points in geographic areas previously known for poor service, adversaries will likely be motivated to set up fake Wi-Fi networks to steal PII or conduct man-in-the-middle (MitM) attacks. These networks would possibly have names mimicking venue names, tourist locations, or other Olympics-affiliated monikers. Tourists are more likely to join local, potentially unsecured, Wi-Fi networks to avoid data or roaming fees, making them more vulnerable targets.

We have already seen examples of this happening in the leadup to other global events. The DOJ's indictment of Russians for the WADA threat activity mentioned that two GRU officers traveled to Rio de Janeiro to target Wi-Fi networks used by anti-doping officials. The actors captured an IOC official's credentials and used them to gain unauthorized access to an account in WADA's database containing medical and anti-doping related information.[40]

In a related incident in 2016, a senior USADA anti-doping official, who was in Rio for the Olympics, connected to hotel Wi-Fi to remotely access USADA's computer systems. While he was in Rio, threat actors compromised his USADA email account credentials, which included summaries of athlete test results and prescribed medications. That same year, as part of the same Russian campaign, threat actors compromised a hotel's Wi-Fi network in Switzerland, where WADA was hosting an anti-doping conference. They leveraged that access to compromise a senior CCES official's laptop and credentials and used the stolen data to compromise CCES's networks in Canada.[41]

MOBILE MALWARE

It is a common occurrence for particular large-scale sporting events such as the Olympics to produce mobile apps that provide a detailed schedule of the events, live streams of events and tracking of results, ticket and merchandise purchasing, and directions and tips for spectators. Malicious actors may take this as an opportunity to spread malicious apps that masquerade as official apps or attempt to compromise official apps.

39 https://www.bleepingcomputer.com/news/security/special-olympics-new-york-hacked-to-send-phishing-emails/

40 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

41 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

In the past, malicious apps have been used to steal personally identifiable information from victims, credit card information, and login credentials, run advertisements on the infected device to generate revenue for the attacker, or infect other apps on the mobile device or spread to other contacts on the device. Mobile malware can also be used to track the location or sensitive communications of the user. Often, the best defense against mobile malware is to spread awareness of malicious apps, encourage users to only download apps from official App Stores, and to work with the various App Stores to identify and eliminate malicious apps when they appear.

JAPAN'S SECURITY POSTURE

Japan faces many challenges to securing the 2020 Olympics from a range of sophisticated and complex cyber threats, many of which stem from a general lack of preparedness and failure to implement necessary cybersecurity practices. While these problems are not faced by Japan alone, Japan's private sector lags behind its U.S. and European counterparts in cybersecurity readiness, according to government statistics.[42] Many Japanese companies lack security governance, business processes, and proper IT architecture support,[43] deficiencies that are fueled by the country's cybersecurity skills gap.

Despite these challenges, Japanese Prime Minister Shinzo Abe appears to be using the country's role in hosting the Games as an opportunity to renew urgency on developing Tokyo's cybersecurity capacity. In 2018, the government published an outline of its next cybersecurity strategy, which focuses on improving cybersecurity in the private sector, among other things. The strategy also encourages industry to invest more in cybersecurity for business operations, risk management, and innovation.[44]

On a more tactical level, the Japanese government in January 2019 announced plans to survey 200 million domestic internet-connected devices to check for potential vulnerabilities in routers, webcams, and smart home appliances. The initiative includes efforts to examine hardware that uses physical cables to access the internet and requires researchers to notify internet service providers (ISPs) of vulnerable users. The plan is part of a larger push to improve security as the country prepared to host several major global events, including the Rugby World Cup (fall 2019) and the G20 Summit (summer 2019), in addition to the 2020 Summer Olympics.

The Japanese government also amended its 2014 Basic Act on Cybersecurity, paving the way for the country to set up a dedicated council to address Olympics-related cybersecurity matters. The council consists of national and local government agencies, critical infrastructure providers, academia, and private sector entities.[45] Japanese press has also reported that the country is strengthening its cooperation with the European Union ahead of the Olympics, although specific details of the partnership have not been widely reported.[46]

Japan's positive efforts at change are encouraging, but the underlying problems are deep-rooted in both corporate and governmental approaches to cybersecurity that will be difficult to change in just a few short years. These problems are not unique to Japan; in fact, they are common in many countries that rely on information technology to deliver services and drive the economy. Still, Japan's cybersecurity shortfalls may affect its ability to

42 https://www.cfr.org/blog/how-japans-new-cybersecurity-strategy-will-bring-country-par-rest-world

43 https://www.accenture.com/_acnmedia/pdf-87/acenture-comptia-eng.pdf

44 https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

45 https://govinsider.asia/connected-gov/japan-sets-up-cybersecurity-council-to-secure-the-2020-olympics/

46 https://www.japantimes.co.jp/news/2018/07/16/national/japan-strengthens-cybersecurity-cooperation- eu-ahead-olympics/#.XbhNpJNKh3k

detect, defend against, and respond to cyber threats during the Games. Adversaries may see the 2020 Games as an even more attractive target because of Tokyo's cyber challenges.

LESSONS AND RECOMMENDATIONS

With the Summer Olympics just around the corner, cybersecurity preparations are already well underway and many stakeholders have action plans in place. However, CTA recommends that anyone with responsibility for Olympics-related cybersecurity review this section for actions to further improve their security posture. These recommendations apply not just to Olympics planning but also to any major event in which governments, companies, and corporate sponsors are involved and which heads of state, executives, and network defenders must plan for and support.

FOCUS ON THE BASICS

There is no good substitute for ensuring basic cybersecurity practices are being followed and executed as efficiently as possible. Stakeholders should ensure they know what systems are on their network, regularly patch those systems, segment networks, and enable multi-factor authentication (MFA). Not only will this significantly raise defenses against less-sophisticated threat actors, but more sophisticated nation states will be forced to expend more resources to accomplish their goals.

INFORMATION SHARING

Engaging with key stakeholders on a regular basis is essential to ensuring that communication channels are established and information flows to and from all parties on a regular basis. Information should be shared with relevant stakeholders from government, industry, corporate sponsors, public transportation, broadcast networks, and the general public. Building relationships with commercial providers, such as energy companies, telecommunications companies, and internet service providers (ISPs), is particularly important, since these entities are often attractive cyber targets. Establishing such information-sharing channels will help provide cohesive coverage and advance threat warning while also helping to facilitate faster incident response. Without the relationships built during normal times, responders are much less effective during a crisis.

Organizations should consider nominating a primary cybersecurity facilitator (e.g., a federal agency or internal "tiger team") for the event to act as the de facto lead. This action will help streamline communications, information sharing, and decision-making. This actor could also deliver regular public briefings and status updates to build trust and share information. However, keep in mind both in spirit and practice that there is no single "owner" of the cybersecurity program and that regular information sharing and collaboration is key.

When possible, encourage cybersecurity providers, both public and private sector, to designate some analysts to be co-located at other partner agencies and organizations. Combining representatives from different teams and agencies fosters information sharing and teamwork.

COORDINATED CYBERSECURITY PLANNING

Start planning early and allocate all necessary resources, including personnel and equipment, as soon as possible. A good starting point is to conduct an in-depth risk assessment of potential threats and vulnerabilities well before the start of the event so that organizers and cybersecurity providers have time to make recommendations and stakeholders can get action plans in place. This risk assessment could include a cybersecurity capabilities matrix that maps the potential threats to their mitigation solutions.

Stakeholders should review incident response capabilities and plans across partner agencies and organizations. This review should include creating

standard operating procedures so that all parties have clear expectations of mitigation actions and response times in the event of an incident. Response plans should clearly define and assign responsibilities so that participants have no confusion about their roles. Running threat simulations, such as tabletop and war game exercises, is an effective way to test this structure and practice responding to threat events.

REGULAR EXAMINATION OF CRITICAL SYSTEMS

On the tactical front, stakeholders should be sure to regularly examine critical systems before, during, and after the event. This examination should include monitoring deployed security tools, shutting down any services that are unnecessarily exposed to the web, and ensuring centralized logging capabilities. Organizations should also implement network segmentation to segregate servers that contain sensitive information. Teams should establish what is normal activity for those environments so that anomalies can be detected and investigated as quickly as possible. Regular testing and red-team exercises will also help to identify potential security gaps. In addition, organizations should have security training for personnel so that they are educated on how to identify and respond to specific threats that might be targeting the event they are working.

2020 SUMMER OLYMPICS
THREAT ASSESSMENT

CYBER THREAT ALLIANCE

POWERED BY CTA