Olympics – Cyber Threats to Paris 2024

Written by Tim West

July 2024

WITH secure

Table of Contents

Executive Summary

- WithSecure assesses with HIGH confidence that due to geopolitical turbulence and low international relations with Russia, the Paris Olympic games will face an increased risk of malign cyber activity compared to previous Olympics.

- The Olympics offers an attractive opportunity for cyber-enabled scams, and fraud on a wide scale.

- WithSecure assesses with HIGH confidence that a MODERATE to HIGH threat to the Olympic games originates from Russian state sponsored intrusion sets who have both the capability and intent to undermine both the International Olympic Committee and France.

- WithSecure assess with moderate confidence that other nation-state sponsored intrusion sets (China, Iran, DPRK) may have objectives that can be achieved by capitalising on the topic of the Olympics, however the threat posed from these to the Olympics itself is LOW.

- WithSecure assess that state aligned Hacktivists operating with a pro-Russian mandate will ALMOST CERTAINLY seek to disrupt the execution of the games. WithSecure assess these groups pose MODERATE threat to the games.

- WithSecure assess that the risk to Olympics core networks from capable Ransomware actors is MODERATE TO LOW, however the risk to other networks operating externally, but still in the sphere of the Olympics is MODERATE.

- It is POSSIBLE that due to the proximity of significant elections in France, the Olympics will be used as a lever to undermine and influence future elections in the build-up.

- Network defenders involved in Paris 2024 are almost certainly well equipped and prepared to mitigate Computer Network Exploitation (CNE) and Computer Network Attacks (CNA) operations. The cyber security operation will be able to draw on lessons learned from previous campaigns targeting previous Olympic games.

Background

In 2021, the International Olympic Committee approved a change in the official motto of the Olympic games from "Faster, Higher, Stronger" to " Faster, Higher, Stronger **- Together**". This change was intended to reflect and highlight the need for solidarity in order to make the world a better place.

There is no greater world stage than the Olympic games. Over 500 million more people watched the 2022 Beijing Winter Olympics than the 2022 football World Cup, and a further billion people watched the 2020 Summer Olympics in Tokyo. This makes it an extremely attractive target for a wide range of malignant actors operating inside and outside of cyberspace. Couple this with recent geopolitical events that have demonstrated the world is now more polarised than it has been over the last two decades, it is clear why the chief of Paris 2024 has claimed an "unprecedented security operation" will be in place. While this will be heavily concerned with terrorism and physical security, this strategy will also almost certainly consider malicious cyber dependant actors as a priority threat to the games with expectations that the number of cyber security events will be ten-fold that of Toyko 2020.

A History of Targeting

There is a precedent of cyber-attacks seeking to impact the Olympic games, the most famous example being the deployment of 'Olympics Destroyer' malware in 2016, almost certainly as an act of retribution by the Russian government in response to their suspension from competing at international sports events for four years following the exposure of their comprehensive state-sponsored doping programmes. This attack was a blatant sabotage event, deliberately timed to coincide with the opening ceremony.

London 2012: The London 2012 CIO claimed the games were hit by DDoS attack every day they were running. Some attacks were orchestrated, and some were automated (low sophistication and not adaptive to security efforts). While these were mitigated due to the level of preparedness of network defenders it does highlight adversary intent, even during a period of (relative) geopolitical stability.
Rio 2016: #OpOlympicHacking was an operation launched by the hacktivist group Anonymous. Where they claimed that their actions took a number of Brazilian city and start web pages down, along with hack-and-leak actions targeting Brazil's sporting associations.
PyeongChang 2018: We have covered Olympic Destroyer campaign in brief, this marked the start of more deliberate and overt Russian targeting of the Olympic games.
Tokyo 2020: The United Kingdom took quite a significant step when it publicly attributed the aforementioned series of Russian cyber-attacks against the PyeongChang 2018 games, however it also noted a campaign of cyber reconnaissance against officials and organisations of Tokyo 2020 games, including its logistics services and sponsors. Organisers of Tokyo 2020 also reported facing '450 million' cyber-attacks - although this is quite a vague statistic as it is hard to quantify a single unit of 'cyber-attack'.

Wider Context in France

Each hosting country is responsible for the success of their games and there will a certain pressure to ensure they live up to the spectacle that is expected of the Olympics. Therefore, it is highly likely any incidents impacting upon this spectacle will be perceived as a source of international embarrassment. The Olympics will almost certainly be seen as an opportunity for France's adversaries to undermine France on the world stage. France is currently at the epicentre of several geopolitically significant events, all of which will affect the cyber threat France, and by extension, to the games.

Hacktivism

In March 2024, France's government found itself targeted with cyberattacks of "unprecedented intensity", which was claimed by the hacktivist group Anonymous Sudan. This group overtly operates with a pro-Russian political mandate, and while they are very active, this was the first time they were seen wielding a capability strong and coordinated as such to impact multiple French government departments simultaneously, until a crisis cell was deployed and able to contain the attack. While Anonymous Sudan took responsibility for the hack, a reason was never communicated – another unusuality of the incident. It is possible this was launched as a method to test French reaction, or in response to the (at the time) imminent announcement that France will begin manufacturing weapons inside Ukraine.

Upcoming Elections

France is a key global power, with the seventh largest global economy, and a permanent seat on the UN (United Nations) security council. In their national elections in 2022, amid reports of interference by Russian influence operations, France's far-right party led by Marine Le Pen made significant gains over their 2017 performance. It is almost certain that Putin's Russia supports French far-right political parties and sees them as a useful tool in polarising European powers and eroding the mechanisms that enable cohesion and unity in Russia's geopolitical opponents.

The far-right momentum has continued, and following an embarrassing defeat in the European elections, with only 46 days before the Olympic games opens, France's president (at the time of writing) has called a snap legislative election. This will finish less than three weeks before the start of the games and decide who will sit as members of the French parliament [this is not a presidential election]. A louder pro-isolationist voice in parliament would undermine France's ability to continue to support both the European Union, and Ukraine to the extent it currently is. While a far-right majority in parliament isn’t the most likely outcome, any fragmentation of the status quo would make it harder for Macron to deliver on his agenda. For this reason, there will almost certainly be a high intent towards undermining Macron and influencing upcoming elections wherever possible. Macron himself has called agitators [*almost certainly referring to Russia*] a threat to France, Europe, and France's place in the world.

Tensions with Russia

Franco/Russian relations are strained as a result of France's condemnation of the illegal invasion of Ukraine, and the continued military support to Ukraine's defensive efforts. There have been examples of 'stunts' which aim to insult, embarrass or undermine the other. Following the shock defeat of Macron's centralist party by Le-Pen's far right party, many pro-Russian spokespeople spoke out in support of the result, and against Macron. This comes only days after Russian commentary that they were 'still waiting for their invite' to France to commemorate the 80th anniversary of the D-Day landings, criticising France for using World War II as the subject of political games.

The Russians themselves were accused in June 2024 of making conflict the subject of political games when they were forced to deny involvement in a stunt around the Eiffel Tower in which five coffins covered in the French flag were placed with the inscription "French Soldiers of Ukraine". It was claimed this came in response to France's suggestion that French soldiers could be deployed in a training capacity to Ukraine and/or allow French weapons to strike targets within Russia.

Threats to the games

Before we discuss threats 'to' the Olympic games, we will first briefly discuss the threats coming 'from' the Olympic games. This anthesis is deployed more as a linguistic device than a suggestion that the games themselves are a threat in cyberspace, however there will be actors seeking to utilise the Olympic games to achieve other illicit objectives outside the sphere of the games' operation. The games are already acting as a catalyst for financially motivated fraudsters undertaking ticket scams, phishing campaigns and email fraud.

There have also been misinformation campaigns utilising the celebrity of the games to advance an agenda. In the month of June, Microsoft released a report detailing how Tom Cruise's likeness was used with deepfake technology to narrate a documentary targeting the organisation of the Olympic games in order to criticise both the International Olympic Committee, and France.

Misinformation campaigns targeting the games and fraud/scam events catalysed by games are cyber-enabled, and do not contain an element of CNE/CNA (Computer Network Exploitation/Attack). Therefore, they are technically out of scope of this report, however, should be considered no less serious.

Threat Actors

The most famous and significant example of vindictive Olympic targeting (Olympic Destroyer 2016) came in response to events surrounding state-sponsored doping. This time, geopolitical tensions are higher, events carry more significance, and the Olympic games comes at a year when approximately half of the planet go to the polls in various elections. Primary threats to the Olympics will align to one of three themes: State, Hacktivist and Criminal.

State - Russia

Russian state actors almost certainly pose the greatest threat to a successful and seamless Olympic Games, wielding both capability and intent to undermine both the Olympics and France.

Intent

Russia almost certainly wields a level of hostility towards France, and the reasons why they may target the games to embarrass and undermine Macron have been documented in this report. Russia will also almost certainly feel acrimony to the Olympics as an institution.

In Paris 2024, Russia has served its four-year ban (2019) for its systemic doping campaign, however following the illegal invasion of Ukraine in 2022, a ban on Russian and Belarusian athletes was recommended by the International Olympic Committee (IOC). This has since been relaxed, allowing Russian and Belarusian athletes to compete under a set of circumstances, all of which will be perceived as insulting to Russia and Belarus. Athletes can only enter as neutrals, must not compete under their national flag or colours, and must not support the invasion of Ukraine. Furthermore, Russian and Belarusian athletes are also banned from participating in the opening ceremony. In response, Russia said it was "outraged", and even went as far as to say the IOC was slipping "into racism and neo-Nazism". Russian state actors have set a precedent for targeting the Olympics, being responsible for the 2018 Olympic Destroyer campaign where it attempted to launch a destructive campaign on PyeongChang 2018 networks, deliberately timed to perfectly coincide with the opening ceremony.

Capability

Russia has a demonstrable ability to enact its objectives in cyberspace including, but not limited to, complex and coordinated operations involving false flag events, influence operations, espionage events and destructive attacks. Russia is well able to deploy human operations in conjunction to cyber-attacks, and is able to target all types of networks, including Operational Technology (OT). Russian state actors will be capable of launching targeted and sophisticated attacks against both the games' networks, and that of France's supporting infrastructure (travel, hospitality etc).

It is unlikely that Russian state actors will conduct any offensive cyber operation against the Olympic games, or disruptive attack against national or local (Parisian) infrastructure without a level of deniability. The Russian state almost certainly has the capability to influence and direct hacktivist collectives, along with operating 'hacktivist collectives' as a thin false cover for their own operations. This obfuscation technique is commonly deployed by Russian state-sponsored threat actors.

Likely Objectives

Russia will likely have several objectives that will be furthered through successful targeting of Paris 2024.

- **Embarrass / Discredit France:** As noted in the introductory paragraph to this report, the organisers of the games will feel a high level or responsibility for the success of the games. If this success is prevented, Russia could use this as an opportunity to discredit France on the international stage.

- **Embarrass / Discredit IOC:** In a throwback to 1984, in 2023 Russia announced they will put on an event named the 'Friendship games'. This, while denied, is almost certainly intended as a competitor to the Olympic games. The concept was first introduced in 1984 following the Soviet Union's boycotting of Los Angeles 1984. Russia has often been cited as deploying cyber-attacks in a vindictive manner, often asymmetrically for perceived slights. Therefore, a likely objective of Russia, either directly, or through intermediaries will be to embarrass or discredit the Olympic games and encourage nations Russia is courting (namely Brazil, India, China, South Africa), to support the secessionist event.

- **Espionage opportunity:** As with any mass gathering of people, dignitaries and statesmen, the Olympics will almost certainly offer an attractive opportunity for information gathering campaigns.

- **Amplify a message:** Particularly as they continue to spend people and resources in Ukraine, Russia will be keen to demonstrate their potency and position as a global power. It is possible they will see force projection using Olympics as a viable means to achieve this objective. Russia may use this as a platform with which to criticise France, the IOC and NATO.

- **Influence over Elections:** If there is an opportunity to undermine Macron and/or influence the French population in a particular direction when they go to the polls, it will almost certainly be explored. The perceived inability to conduct and organise a successful event may make for an effective political lever for Macron's opponents. In the weeks preceding the Olympics, Russia may explore leveraging the Olympics in order to influence upcoming parliamentary elections. The outcome of this election may weaken Macron's position in the French presidential elections (2027).

State – China

With moderate to strong confidence, we assess PRC threats pose a low threat to the operations of the games, however, they will likely seek to use the games to target high value individuals and/or organisations that may hold intelligence value.

Intent

We assess that it is highly unlikely Chinese state will seek to jeopardise the smooth operation of the games with destructive or disruptive operations. A strong medal position in the games is likely a source of national pride and China will highly likely not wish to undermine this.

With moderate confidence we assess China will likely see the games as an opportunity to target high profile/value individuals and organisations attending the games. It is a realistic possibility Chinese state actors will seek to capitalise on the games to harvest PII of global citizens.

The projection of Nazi ideals and power in Belin 1936, and events surrounding Russia's systemic state sponsored doping are two clear pieces of evidence which prove the reputation boost that success in the Olympics (as organisers or participants) can provide to nations. Unlike Russia, China is able to use the Olympics as a stage to project its soft power. As with industrial espionage, it is possible PRC will seek to gain a competitive advantage over rival participants by compromising specific sporting federations to harvest relevant and valuable information. This activity will have occurred prior to the opening ceremony and will almost certainly not impact the running of the games.

Capability

People's Republic of China (PRC) is arguably among the most capable and well-resourced state operating in cyberspace. PRC intrusion sets have demonstrated the ability to conduct sophisticated espionage operations and it is almost certain that the mature and well-resourced intelligence infrastructure of PRC will mean they are capable of processing and exploiting data/PII collected at scale. China state may not necessarily use offensive cyber means to achieve this goal. Chinese state sponsored intrusion sets are demonstrably capable of utilising overly invasive legitimate services, such as mobile applications or, as many speculate; infrastructure.

Likely Objectives

- **Espionage opportunity:** As with any mass gathering of people, dignitaries and statesmen, any Olympics offer an attractive opportunity for information gathering campaigns. There is a realistic possibility PRC has historically targeted rival sporting associations in order to gain a competitive advantage.

State – Iran

We assess with moderate confidence that Iran is a low threat to the Olympic games. There will be a risk that Iranian, or Iranian aligned hacktivists may wish to use the Olympics as a stage to project an anti-Israel sentiment. It is unlikely Iran will attempt to deploy destructive malware against core Olympic systems, however there is a realistic possibility Iran will utilize the games to target high value individuals that may hold intelligence value to them.

Intent

In April 2024, Iran/Israel tensions escalated to the point where Israel bombed an Iranian consulate in Syria. Iran and Israel then traded retaliatory kinetic attacks. This escalation was reflected in cyberspace with several hacktivist groups emerging, each almost certainly will be see the Olympics as a powerful platform with which to push their message. This situation could be further exacerbated in the event Iranian athletes refuse to compete against Israeli athletes, a policy which has been the norm for Iran for some time. Kinetic attacks within sovereign territory is a drastic escalation, so Iran may be willing to exploit any and all anti-Israel sentiment on one of the world's biggest stages.

Approximately 40% (14 of 36) athletes competing in the IOC Refugee Olympic Team are/were Iranian. At the previous summer Olympic games in 2020, Iran's only female medallist deflected from Iran. This came after a spate of Iranian athletes seeking asylum in various countries. High profile deflections are an embarrassment for any nation, and Iran will keen to avoid this, having a known precedent of targeting dissidents in cyberspace.

France's involvement in a joint statement criticising Iran for its non-compliance of the JPCOA (Joint Comprehensive Plan of Action) in late 2023 and the number of 'political emigrants' now residing in France, including Iran's pre-revolution Empress Farah is unlikely to significantly drive Iranian intent to target the Olympic games.

Capability

Iran is very active in cyberspace and operates several capable intrusion sets. It is highly likely they have the capability to deploy destructive malware, and coordinate hacktivist groups. Many Iranian intrusion sets will be capable enough to successfully target individual sporting federations. Iran has a precedent of targeting individuals, particularly dissidents and influential people, with spyware campaigns impacting both personal computers and mobile devices.

Possible Primary Objectives

- **Espionage opportunity:** As with any mass gathering of people, dignitaries and statesmen, any Olympics offer an attractive opportunity for information gathering campaigns. It is likely Iran will seek to target dissidents, and a realistic possibility Iran will seek to target high value individuals and organisations.

- **Amplify a message:** Iran may seek to capitalise on both the Olympic stage, and a perceived decrease of public support for Israel to attempt to amplify an anti-Israel message.

State – DPRK

With moderate to high confidence, we assess that North Korean threat actors pose a low risk to the Olympic games. It is possible that actors in DPRK will seek to utilise the celebrity of the games to catalyse their financially motivated attacks. It is a likely that DPRK are involved in 'commercial' ransomware operations which may impact the games [discussed in a later segment].

Intent

Sporting events, and the Olympic games historically have been a unifying force for North and South Korea, with unified march in the opening ceremony and a unified ice hockey team in Pyeongchang. Relations between DPRK and IOC may have somewhat chilled with DPRK's ban from competing at Beijing 2022 as a result of their refusal to participate in 2020, however this is unlikely to be sufficient motivation to wish to significantly undermine the Olympics.

As ever, the Olympics will be seen as an opportunity to enhance cyber dependant crime with a view to raising revenue for the state – such as scams and fraud for a plethora of actors. It is a realistic possibility that intrusion sets domiciled in North Korea will be among these, seeking to use the Olympics as a lure and capitalising on the sheer number of financial transactions that occur as part of any Olympic games.

Capability

Actors associated with DPRK are capable cyber-criminals and have built effective money laundering machinery. It has been estimated that DPRK has stolen billions of dollars in the form of cash and cryptocurrency over the past decade. The required capability barrier to launching social engineering attacks is low, and the Olympics theme will be effective lure material.

Likely Objectives

- **Revenue Generation:** Most globally significant events are utilised by threat actors to generate leads for cyber dependant crime.

Hacktivist Threat

The treat from hacktivists is not new, but since the 2022 illegal invasion of Ukraine, hacktivist collectives have been galvanised. These hacktivist groups typically form around Telegram channels where targets and the respective attack outcomes are announced. Hacktivist groups have arisen around all poles of current conflicts. Pro-Russian, Pro-Ukrainian, Pro-Palestinian and Pro-Israeli groups are conducting near constant denial of service (predominantly), and hack-and-leak operations.

Hacktivist collectives typically have two objectives. 1.) Cause disrupt/destroy or undermine a target's information systems, and/or 2.) Amplify the message or the operation/cause, and the celebrity of the actor.

It is almost certain these 'typical' hacktivists will be little more than a 'thorn in the side' of Olympic organisers who will almost certainly have employed significant DDoS mitigation capabilities. WithSecure assesses the threat to the Olympics from hacktivists operating with state support, however, is moderate. This is due to the following factors: 1.) Recent examples of capability enhancements in certain pro-Russian hacktivist groups and 2.) Russian state involvement with, or oversight of, hacktivist collectives.

Intent

The size of the platform of the Olympics will tempt hacktivist collectives pursuing all causes. Hacktivists will be aiming to gain notoriety and amplify their message. A key metric of success will be the media attention of their campaigns, and not necessarily direct impact caused.

It is likely that any events at the Olympics that are related to geopolitical tumult will be exploited by activists. To give an example of this - Iran and some other Arab and/or Muslim competitors avoid competing against Israeli participants. In Toyko 2020, an Algerian athlete and coach were suspended by the International Judo Federation for refusing to compete against an Israeli opponent. With many news outlets reporting a drop in public sentiment and support for Israel, any similar events that could be perceived as unjust to or unfairly supportive of a particular social cause will almost certainly be amplified in cyberspace.

It is most likely that Hacktivists with a pro-Russian mandate will attempt to disrupt the games. It is possible actors with an anti-Israel sentiment will also be active over the course of Paris 2024.

It is almost certain that Russian state sponsored intrusion sets would utilize a hacktivist cover in the event that they seek to launch an offensive campaign against the Olympics in cyberspace.

Pro-Russian Hacktivism

Pro-Russian hacktivists pose one of the biggest hacktivist threats to the Olympic games. Over the previous two years there have been a number of concerning hacktivist events where certain DDoS events suggest advancements in the capability available to certain pro-Russian hacktivist groups.

- **February 2022** – Numerous DDoS attacks on Ukraine financial sector prior to invasion by Russian forces
- **March 2023** – DDoSia multi-architecture toolkit released by NoName057 and DDoSia project
- **April 2023** - KillNet hack-and-leak operation against NATO networks.
- **June 2023** - Anonymous Sudan impacting Microsoft networks with DDoS attacks.
- **January 2024** – NoName057 impacting Switzerland government services with DDoS attacks.
- **March 2024** – Anonymous Sudan impacting many French government services with DDoS attacks.

State sponsored hacktivism

Many Pro-Russian hacktivist collectives very extremely closely with Russian strategic goals. In April 2024, Mandiant reported that three pro-RU hacktivist groups are a front for an intrusion set tracked as Sandworm (APT44). These three hacktivist groups have been observed attacking networks including, but not limited to, those supporting elections, utilities and Ukranian power. It is likely these groups are methods used to offer a veil of plausible deniability by Russian state actors enacting offensive action against civilian industry. Russia previously utilised hacktivist covers when targeting Ukraine targets in the lead up to the campaign seeking to disrupt the 2018 Olympics in the 'Olympic Destroyer' campaign.

It is a realistic possibility that Russian state is able to exert influence over other hacktivist groups in such a manner that it able to coordinate other hacktivist groups to bolster the efficacy of a campaign.

Insider threat

There is a remote chance that an insider threat may seek to take extreme measures in support of a social cause they believe in, however this is not likely at such an event that promotes global peace and unity.

Capability

Hacktivist groups are often thought of as less capable than state sponsored actors, or even organised cyber criminals. To consider an operation a success, Hacktivists do not necessarily need to cause any real impact to a target's network if the campaign or operation is amplified by media. Hacktivist collective's capability improves as their cohesion improves. Under a unifying objective, it is a realistic possibility that hacktivists will be able to temporarily impact some network services of the Olympic games.

Denial of service attacks

Distributed denial of service attacks utilises computing power from several disparate, networked, devices in order to send volumes of network traffic intended to consume the available resources of a service, rendering it unusable for legitimate purposes.

Hacktivist groups typically utilise 'botnets for hire', often advertised as 'stresser' services. Hacktivist collectives may also call upon individuals, supportive of their cause to supplement the 'firepower' of their DDoS capability. Typically, volumetric based attacks are relatively easy to mitigate though specialist services, and in the event of successful disruption, recovery is often simple. This being said, there have been some concerning examples over the previous years when hacktivist groups appeared to wield more potent capability to cause notable impact against harder targets.

More advanced DDoS attacks do not solely utilise volumetric methods, but also can shape the attack traffic in a way that exploits the way a target protocol or application operates. Furthermore, particularly advanced, and coordinated attacks can also quickly cycle through both attack methods and attack sources, making remediation particularly difficult.

Likely Objectives

- **Attain celebrity:** Hacktivists typically seek to build and develop a 'brand' that they seek to project.

- **Amplify a message:** Where Hacktivists will support social causes with differing levels of zeal, hacktivists will certainly look to utilise events at the Olympics to propagate and amplify their message.

- **Support state objectives:** Where hacktivists groups are either influenced by state powers, or under direct control they may seek to launch attacks that directly correlate with state objectives or operations. Hacktivist collectives may be simply a cover for nation-state intrusion sets.

Organised Crime

With high confidence we assess that organised cyber-criminal groups pose a moderate to low threat to core Olympic networks. Ransomware actors pose a moderate threat to networks in the sphere of the Olympics, but not necessarily core networks.

Intent

Ransomware actors will attempt to target networks that may have to prioritise uptime over integrity (such as a hospital network, or prominent sporting event) as they will believe it is more likely that the victim will be increasingly receptive to paying a ransom in order to resume operation as soon as possible.

Capability

Financially motivated criminals, particularly ransomware actors and affiliates have become increasingly capable over recent years. This is due to a greater number of criminals entering the criminal space, increases in available resources to threat actors, and an evolved cybercrime ecosystem and marketplace.

Typically, ransomware actors will target vulnerabilities in order to obtain access to networks or exploit the human in the form of a social engineering attack. Due to the emphasis put into cyber security at Paris 2024, It is unlikely the core networks underpinning the games will carry any known or unmitigated vulnerabilities exposed to the internet. Most ransomware actors are inherently opportunistic, targeting vulnerabilities and capitalising on leaked, exposed or easily guessable authentication material.

Some ransomware affiliates have the capability to exploit zero-day vulnerabilities, and by definition it is very difficult to ascertain whether these exist in any network and are known by threat actors before compromise. This being said, it is almost certain that robust defence in depth practises are employed, and rapid recovery processes will be documented, tested and drilled. Core Olympic networks will likely be too hard of a target for typical ransomware actors.

Ransomware actors are likely to represent a moderate threat to satellite services that support the Olympics. These may include services such as ticketing, hotels and hospitality or the networks of individual sporting confederations. It is highly likely that ransomware actors will feel that the Olympics will offer a bigger lever with which to pull to extort such network owners.

Overlap with Hacktivism

As with hacktivism, there have been examples of state actors operating under a false ransomware flag. It is almost certain that, as with Hacktivism, Ransomware actors will seek to over-exaggerate effect in the event that they are able to successfully, but insignificantly, cause impact.

Likely Objectives

- **Revenue Generation:** Ransomware actors will believe a heavy ransom will be extortable if they manage to successfully disrupt a network, or system that will impede the smooth running of the games.

The Defensive Perspective

As noted throughout this report, there are lots of services that need to be defended (Ticketing, Power, Communications etc), and even more surrounding private and civil networks that also will be relied upon to contribute to a successful Olympics (hospitality, accommodation, transport etc). There are numerous threats to the Olympics, each with varying levels of motivation and capabilities and a successful cyber security operation will be a great challenge for the Olympic authorities. This being said, information system administrators will be well resourced, prepared and drilled. It is almost certain that specialist tooling, software and personnel will be ready to deploy upon commencement of malign cyber events, and previous lessons from previous Olympics will have been learned.

About WithSecure™

WithSecure™, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies. Committed to the European Way of data protection, WithSecure prioritizes privacy, data sovereignty, and regulatory compliance.

Boasting more than 35 years of industry experience, WithSecure™ has designed its portfolio to navigate the paradigm shift from reactive to proactive cyber security. In alignment with its commitment to collaborative growth, WithSecure™ offers partners flexible commercial models, ensuring mutual success across the dynamic cyber security landscape.

Central to WithSecure's™ cutting-edge offerings is Elements Cloud which seamlessly integrates AI-powered technologies, human expertise, and co-security services. Further, it empowers mid-market customers with modular capabilities spanning endpoint and cloud protection, threat detection and response, and exposure management.

WithSecure™ Corporation was founded in 1988, and is listed on the NASDAQ OMX Helsinki Ltd.