Cyberthreats to Paris 2024

June 2024

Background

Unit 42® is committed to protecting customers in their best moments and in sensitive situations. These include one of the most high-profile events in the world, the Olympics. For this year's 2024 Paris Summer Olympic Games, Unit 42 has orchestrated a cyber vigilance program to protect critical enterprises involved in the organisation and roll out of the Games.

Understanding the most likely threats and anticipating the worst impacts to the most sensitive assets is the first step for a truly resilient Olympic cybersecurity program. This paper is therefore meant to give an understanding of the cyberthreats the 2024 Summer Olympics are likely to face, and to highlight relevant essential services that could be impacted.

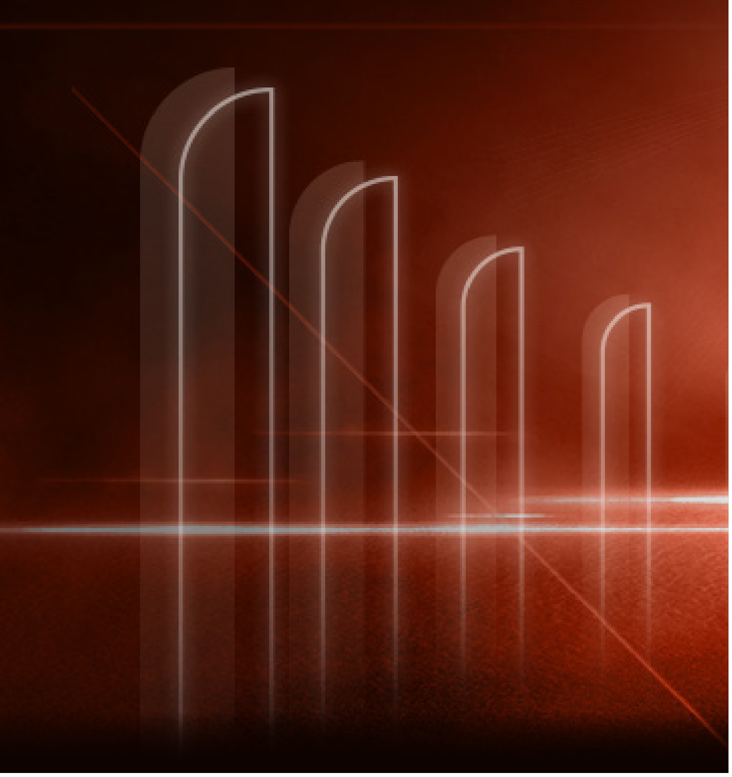


Table of Contents

Executive Summary

Key findings

Cyberattacks targeting critical Olympic services, such as transportation, hospitality, event management, telecommunications, media, payment processing, utilities, and safety and security have the potential to erode the event's reputation. They can also disrupt the attendee experience and inflict financial losses on organisers and sponsors. As the Olympics approach, heightened concerns arise over the risks posed by financially motivated cyber-enabled fraud, politically driven sabotage by state-sponsored actors and hacktivists, alongside the ever-present covert espionage activities—all posing substantial threats to the event's security and integrity.

Overall, Unit 42 makes the following assessments:

- Financially motivated crime is likely to present the highest and most sustained threat throughout the event, with cyber-enabled fraud being a particularly prevalent means to obtain illicit funds from enterprises and individuals alike.
- Politically motivated sabotage by both state-sponsored threat actors and hacktivists is likely a top concern, given previous incidents at past games. The potential for geopolitical tensions surrounding the event and the ability for such an attack to cause severe disruption or even physical harm is high.
- Espionage, although less overt, remains a concern, particularly regarding state-sponsored threats conducting surveillance on dissidents, activists, or persons of interest.

Cybercriminal fraud with its impact on revenue and reputation is likely the most relevant threat for Paris 2024:

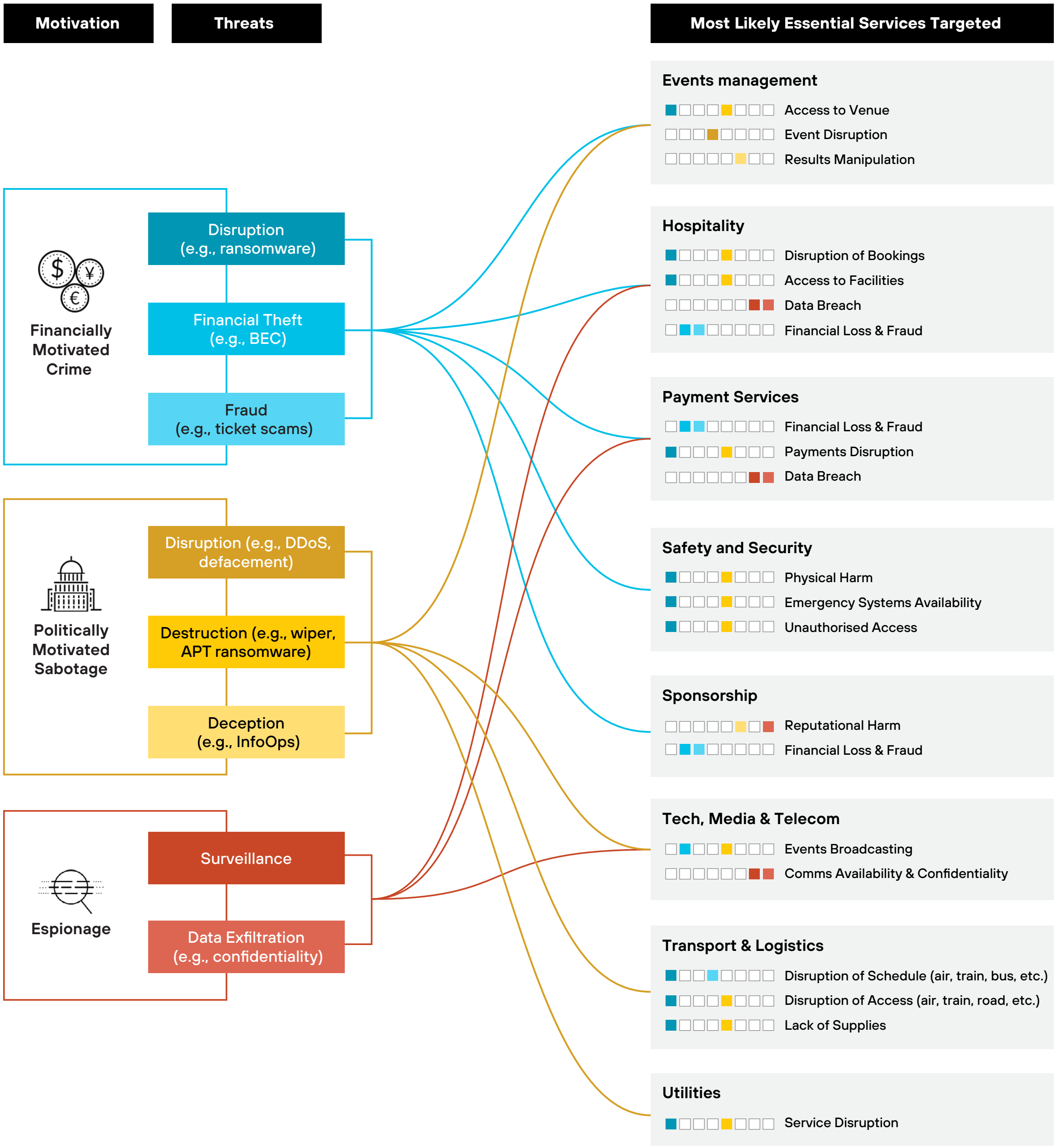
- Threat actors conducting both business email compromise (BEC) and cyber-enabled fraud are assessed to have a high intent to target the Olympics and use its brand to further the success of their fraudulent activities.
- Ransomware operators are less likely to target the Olympics directly. Although an attack on a widely used third party could cause significant disruption to the Games or local services.

Disruptive or destructive operations by Russia-based threat actors remain highly relevant:

- Russian state-sponsored threat actors are assessed to have a high intent to target the Olympics, with a high capability to conduct destructive, disruptive, and deceptive attacks, such as information operations.
- Pro-Russia hacktivists are also assessed to have a high intent to target the Olympics, albeit with lower technical capabilities usually limited to distributed denial-of-service ("DDoS") attacks or website defacements.
- In the last two years, we have observed increased collaboration between so-called hacktivists and known state-sponsored Russian groups, blurring the line between political activism and state-sponsored sabotage and disinformation.

Dodging Disaster to Craft Success

International sporting events function as intricate machinery, requiring various components to synchronise for a seamless and unforgettable experience for both on-site spectators and remote viewers. However, should any part falter, the repercussions can be extensive. Outlined below are the most critical services necessary for the successful execution of the Olympics, along with the perceived motives driving threat actors to potentially target them. Additionally, we explore the potential ramifications of such attacks on essential services.



Motivation | Threats | Most Likely Essential Services Targeted

Financially Motivated Crime
- Disruption (e.g., ransomware)
- Financial Theft (e.g., BEC)
- Fraud (e.g., ticket scams)

Politically Motivated Sabotage
- Disruption (e.g., DDoS, defacement)
- Destruction (e.g., wiper, APT ransomware)
- Deception (e.g., InfoOps)

Espionage
- Surveillance
- Data Exfiltration (e.g., confidentiality)

Events management
- Access to Venue
- Event Disruption
- Results Manipulation

Hospitality
- Disruption of Bookings
- Access to Facilities
- Data Breach
- Financial Loss & Fraud

Payment Services
- Financial Loss & Fraud
- Payments Disruption
- Data Breach

Safety and Security
- Physical Harm
- Emergency Systems Availability
- Unauthorised Access

Sponsorship
- Reputational Harm
- Financial Loss & Fraud

Tech, Media & Telecom
- Events Broadcasting
- Comms Availability & Confidentiality

Transport & Logistics
- Disruption of Schedule (air, train, bus, etc.)
- Disruption of Access (air, train, road, etc.)
- Lack of Supplies

Utilities
- Service Disruption

Figure 1: Overview of threats, motivations, most likely targeting of essential services, and potential effects

Exploring essential services and deciphering the reasons behind their targeting

As the world converges on the global stage of the Olympics, the event serves not only as a celebration of athletic prowess but also as a prime target for cyberthreats. In this section, we touch on essential services supporting the Olympics, while seeking to unravel the likely motivations driving cyberthreat actors to target these critical assets. Our selection of essential services and motives are largely driven by Unit 42's previous work protecting global sporting events, such as the Qatar World Cup 2022, but also by our threat intelligence investigations analysing the motives, intents, and capabilities of threat actors.

Every threat actor has an ultimate motive that drives their capabilities to achieve their objectives. The motivations behind threat actors can vary, but concerning the context of the 2024 Summer Olympics, the primary driving forces for cyber activity are summarised in the table below.

	State-sponsored	Hacktivist	Criminals
Financially motivated crime			X
Politically motivated sabotage	X	X	
Espionage	X		

Financially motivated crime is rather self-explanatory; it's the act of obtaining money via illicit means, spanning from traditional fraud tactics enabled by cyber means, such as online sales of fake tickets, to modern cybercrimes like ransomware attacks. **Politically motivated sabotage** is the aim to disrupt availability of systems, deceive society with influence campaigns, or even compromise the integrity of data. This motive is often perpetrated by either state-sponsored threat actors or hacktivists looking to further their cause or political objective. In contrast, **espionage** is almost exclusively perpetrated by states seeking to acquire strategic information for various purposes, such as national security, economic decisions, or tracking of high-value targets.

Threats affect various services and systems underpinning the Olympics in different ways. These are like crown jewels in an enterprise environment, so let's look at what such services are.

Essential services

Essential services contribute to creating a memorable and successful Olympics, indispensable for the experience of participants, spectators, and stakeholders alike. Cyberattacks on these essential services would undoubtedly generate media exposure and could result in various effects, ranging from logistical challenges and inconvenience, to financial losses and safety concerns, ultimately impacting the overall success and reputation of the 2024 Summer Olympics and its sponsoring organisations.

Event management

Event management oversees the planning, organisation, and execution of the entire event. This includes coordinating schedules, managing venues, staffing, ticketing, and ensuring compliance with regulations. A cyberattack on event management systems could disrupt ticketing processes, scheduling, and communication channels, leading to chaos and confusion in managing the event and potentially affecting attendance and revenue.

Case study: A major cyberattack occurred during the opening ceremony of the 2018 Winter Olympics. It caused disruptions across televised feeds within the Olympic stadium, RFID-based security gates systems, and the official Olympics app for digital ticketing.[1] The malware used was dubbed Olympic Destroyer, which would later be attributed to the Russian General Staff Main Intelligence Directorate (GRU), particularly the threat actor known as Razing Ursa (a.k.a., Sandworm).[2]

Hospitality

Hospitality services cater to the needs of guests attending the event. This includes accommodations, catering, entertainment, and ensuring a pleasant experience for attendees. A cyberattack on hospitality services could compromise guest information, disrupt hotel reservations, or disrupt entertainment services, leading to loss of revenue, dissatisfied guests, and tarnishing the event's reputation.

Leading up to Eurovision 2023, attendees were targeted with phishing attacks and general scams around fake hotel bookings.[3] Similar tactics have been observed in anticipation of the upcoming Olympics, as scammers are advertising inexpensive accommodations for the event, but the listings are fake and do not exist.[4]

Payment services

Payment services facilitate transactions for ticket sales, concessions, merchandise, and other purchases during the event. Providing secure and convenient payment options enhances the overall experience for attendees and helps maximise revenue for organisers and vendors. A cyberattack targeting payment systems could compromise financial transactions, leading to unauthorised access to sensitive payment information, fraudulent activities, and loss of trust among attendees and vendors, impacting revenue and reputation.

Safety and security

Safety and security services are paramount to protect participants and spectators alike. This includes crowd control, emergency medical services, surveillance, and implementing security protocols to prevent potential threats. A cyberattack on safety and security systems could compromise surveillance cameras, access control systems, or emergency communication channels, increasing the risk of unauthorised access, crowd control issues, or delayed response to emergencies.

Sponsorship

Sponsorship is vital for funding major sporting events. Sponsors provide financial support in exchange for branding opportunities, advertising exposure, and association with the event, which helps cover the high costs associated with organising and hosting the event. A cyberattack targeting sponsors could lead to reputational damages and undermine sponsors' confidence in future investments in sporting events, leading to financial losses for organisers.

Tech, media, and telecommunications

Technology, media, and telecommunications (TMT) are essential for broadcasting events to a global audience, providing real-time updates, managing online ticketing, and enhancing the overall fan experience through apps and social media engagement. A cyberattack on TMT infrastructure could disrupt live broadcasts, online streaming services, and communication channels, depriving fans of access to real-time updates and coverage of the event and impacting linked businesses like betting.

Transport and logistics

Efficient transport and logistics ensure that athletes, officials, spectators, and equipment can move in and out of the event venues, and Paris in general, smoothly. This includes coordinating transportation modes, train scheduling, and handling the logistics of equipment and supplies. A cyberattack on transport and logistics systems could disrupt transportation schedules or access to transport systems, leading to delays in the arrival of athletes, officials, and spectators, or causing a shortage of supplies.

Utilities

Utilities such as electricity, water, and sanitation are essential for the functioning of the event venue and facilities. Ensuring reliable access to these utilities is crucial for the comfort and well-being of attendees and participants. A cyberattack on utility systems could disrupt essential services such as electricity, water, or sanitation, leading to operational disruptions, safety concerns, and discomfort for attendees and participants.

Unveiling the threats and forecasting their potential effects

Drawing upon an analysis of emerging trends and past incidents, we aim to provide actionable insights into the specific threats confronting the 2024 Summer Olympics. This section details the type of threats and their typical attack types. The focus is uncovering the motivations driving malicious actors and forecasting the potential consequences of their actions. Threats are considered a combination of an actor's motivation and willingness to conduct an attack (intent) and their resources and technical know-how (capabilities).

Financially motivated cybercrime

Disruption (e.g., ransomware)

The most frequent cause of financially motivated disruption tends to be ransomware. In 2023, Unit 42 observed nearly 4,000 posts from ransomware leak sites, marking a 49% increase from the previous year.[5] Supporting this observed increase, in 2023 over 28% of all Unit 42 Incident Response cases were ransomware with data encryption.[6] Ransomware attacks on third parties can have a particular impact on supply chains, a scenario that could have a dramatic impact on the Olympics.

Ransomware operators are unlikely to have high intent for targeting the 2024 Summer Olympic Games and its related organisations. Targeting such a high-profile event is likely to cause immediate and strong law enforcement consequences that most criminals wish to avoid. A more likely scenario is a ransomware event on a third party that disrupts the Games or local services, such as a financial service provider that is unable to process payments, or a distributor that cannot ship perishable and necessary goods.

Case study: In 2023, financial trading services firm ION fell victim to LockBit ransomware, resulting in disruptions to its cleared derivatives platform. The attack had a cascading impact on prominent institutions such as banks, brokerages, and hedge funds leveraging ION's services.[7] In February 2024, another ransomware incident targeted EquiLend, a market utility firm, temporarily leaving Wall Street unaware of trading risks and causing a rise in capital costs for banks.[8] These examples serve to highlight how disruptions to third-party service providers can reverberate across wider industries, such as essential services that the Olympics are dependent on.

Financial theft (e.g., business email compromise [BEC])

Financial theft is a broad category of criminal operations aimed at illicit transfer of funds, targeting both individuals and organisations. According to Unit 42 Incident Response experience, BEC is the most common attack of this type affecting enterprises. The term BEC is considered synonymous with CEO fraud and vendor email compromise, all of which attempt to impersonate an organisation or its personnel as a means to illicit financial transfers. Since the Olympics have numerous parties involved and a complex supply chain, there are a large number of potential victims for fraudsters to impersonate and target.

BEC threat actors are highly likely to impersonate a sponsor or target business directly involved in the 2024 Summer Olympics. These types of attacks are lucrative, with Unit 42 research and investigations suggesting the average payout per successful incident exceeds USD 500,000. Financial theft is likely to occur leading up to the Games, during the Olympics, and even persist for several weeks after the Games. For example, BEC threat actors will likely use fear, uncertainty, and doubt of a "missed" payment to entice victims into paying a fake invoice after the Olympics have finished.

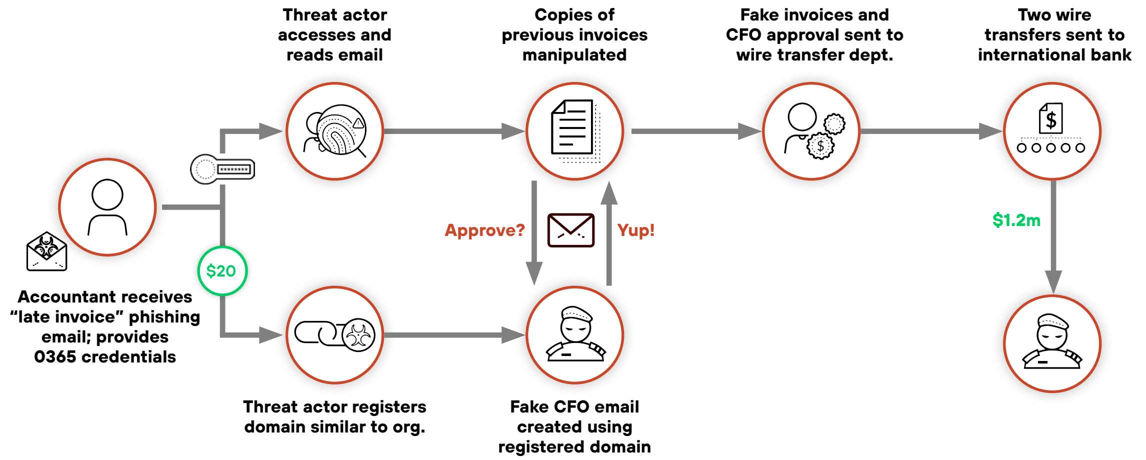

Threat actor accesses and reads email
Copies of previous invoices manipulated
Fake invoices and CFO approval sent to wire transfer dept.
Two wire transfers sent to international bank
Approve?
Yup!
$1.2m
$20
Accountant receives "late invoice" phishing email; provides 0365 credentials
Threat actor registers domain similar to org.
Fake CFO email created using registered domain

Figure 2: Common BEC attack flow based on Unit 42 IR experience

Fraud (e.g., ticket scams)

Fraud is an act of deception by a malicious actor targeting victims for financial gain. Cyber-enabled fraud allows threat actors to conduct these malicious acts remotely, and often reach a wider audience. The aim is usually to target individuals and steal their money, but often businesses are also impacted via reputational harm or loss of revenue to the scammers. Significant events like the Olympics attract tourists, meaning more payment card data is available to steal from hotels, restaurants, and retailers. It also means fraudulent websites selling fake tickets and merchandise. Indeed, Unit 42 has begun to observe domains spoofing the legitimate Olympics website, while fake mobile apps masquerading as transport, booking, or other planning apps are also certain to be leveraged by fraudsters.

It is highly likely that fraud, or specifically cyber-enabled fraud, is to occur before and during the 2024 Summer Olympics. Sponsors are assessed to be some of the most vulnerable organisations with regard to fraud causing reputation harm. Instead, payment processors or online businesses are likely to suffer from web-skimming attacks seeking to steal customer data and payment card data.

Case study: In May 2022, the French Ministry of the Interior claimed that more than 40,000 fake tickets were presented for the 2022 UEFA Champions League final match.[9] The scale of the fraudulent activity reportedly contributed to disrupting fans' access to the stadium, highlighting the potential chaotic impact that mass fraud can have on real-life sport events.

Politically motivated sabotage

Disruption (e.g., DDoS)

A disruptive cyberattack is an offensive action aimed at causing the loss of availability to computer systems, networks, or critical data. Both state-sponsored threat actors and hacktivists have been observed committing disruptive attacks. Cyber hacktivists target institutions or individuals that support governments, economic systems, or ideologies the attacker opposes. Hacktivist attacks may take the form of denial-of-service (DoS) or distributed denial-of-service (DDoS) operations, defacing websites, or data theft, and leaks. A theme with hacktivist activity is that it's often event-driven, with the Olympics and those involved being potential targets. Given the rising frequency of hacktivists' actions since Russia's invasion of Ukraine, and polarisation around the war in Gaza, hacktivism is likely to represent a potential threat to the 2024 Olympics. More local politics about hosting the Olympics in France, such as perceived environmental impact or anticapitalist sentiments, are also likely to play a role in driving hacktivism.

Case study: The hacktivist group known as Anonymous Brazil conducted a wave of DDoS attacks on state and city websites in regard to the Rio de Janeiro Olympics in 2016.[10] Some of the victims included Rio de Janeiro's military police department, the Institute for Public Security, and municipal garbage disposal organisations. They also reportedly hacked and leaked personal and financial details from various Brazilian sporting associations.

Disruptive incidents conducted by either state-sponsored actors or hacktivists, such as DDoS attacks or website defacing, are likely to occur against one or more essential services during the 2024 Summer Olympics. A similar incident occurred during the Qatar World Cup 2022 semifinal match between France and Morocco, in which customers of an internet broadcaster reportedly experienced issues accessing their accounts as a result of a cyberattack.[11] Assessed effects of a DDoS attack are likely to include loss of availability but for a limited duration, which could cause disruption to the broadcasting of an event or, in the most serious scenario, disruption to transportation services scheduling.

Destruction (e.g., wiper)

Destructive attacks impact the integrity of data, extending beyond the sole loss of availability caused by disruptive attacks. State-sponsored threat actors are typically the most common threat actors conducting destructive attacks, which can delete data on business-critical systems, such as the Olympic Destroyer malware used against the Olympics in 2018.[12]

There is a realistic probability that a targeted destructive attack backed by a state-sponsored actor could occur at the 2024 Summer Olympics. Past activity aimed at the Olympics support this assessment. Furthermore, both Russian and Belarusian athletes are barred from competing under their respective flags, lending to an increased likelihood that certain states could be motivated to use destructive methods as a retaliation. The effects of a wiping attack almost certainly result in the loss of critical data but also longer-term disruption, which has the potential to impact a wide range of essential services.

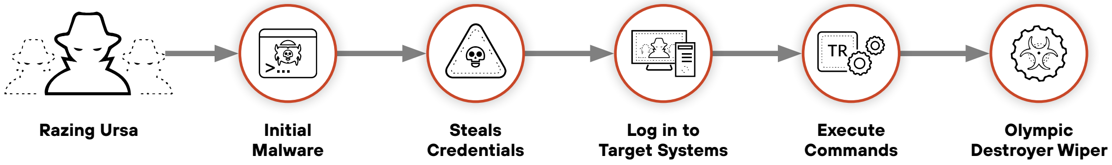


Figure 3: An overview of Razing Ursa's attack chain for Olympic Destroyer

Perpetrators often need to prepare their destructive attacks well in advance. The intrusion in Ukrainian telecommunication company Kyivstar, for instance, started at least six months ahead of the wiper deployment that crippled its network in December 2023.[13] This suggests that network intrusions with a destructive goal against the Paris Games would have to be already ongoing by the time this paper is published in June 2024.

Deception (e.g., information operations)

Deceptive tactics have been leveraged primarily by state-sponsored threat actors to amplify their sabotage objectives. An information operation is an umbrella term including tactics that are intent on influencing people and society by exploiting or controlling information. For example, an army of fake bots spreads disinformation about a hot-button political topic on social media, or a threat actor hacks and leaks information from an organisation, followed by a social media campaign to amplify the perception act. Deception operations can also be conducted in parallel with disruptive or destructive attacks to further amplify the perceived impact of an attack.

Case study: In July 2023, French security services uncovered a disinformation campaign on X, formerly known as Twitter, which reportedly emanated from Azerbaijan.[14] The objective appeared to harm France's reputation in its capacity to host the 2024 Olympic and Paralympic Games. Threat actors were likely motivated by France's support of Armenia, with which Azerbaijan has been fighting a war in the contested Nagorno-Karabakh region.

Deception tactics are likely to occur leading up to and during the Olympics. These tactics include information operations spreading disinformation or misinformation about the Games, the host country, or sponsors. Indeed, we have already seen organised social media information operations using unauthentic accounts to spread disinformation about the 2024 Paris Olympics (see case study above).

There's also a realistic probability that a hack-and-leak operation could occur by a state-sponsored threat actor, similar to the previous operation with a Russia state-sponsored threat actor targeting the World Anti-Doping Agency (WADA) in 2016.[15] Reputational harm is the most plausible effect of deception campaigns, with many sponsors likely to be impacted.

Espionage

Surveillance

States often attempt to conduct surveillance on people, or more specifically dissidents, activists, and persons of interests, like public officials. Tracking of individuals could include understanding patterns of movement, payment patterns, or close contacts. Given the diverse requirements for surveillance, multiple organisations may become targets for acquiring insights into individuals and their activity patterns, with the Olympics presenting an opportune environment for gathering such information and monitoring high-value targets expected to attend.

It is highly likely that surveillance operations by state-sponsored threat actors will occur during the 2024 Summer Olympics. These operations are clandestine and it is highly unlikely that their effects will be overtly observed by the public. However, the intentions of surveillance operations could result in physical harm, such as kidnappings, which then increase the likelihood of exposure. While individuals are most likely to be the ultimate target, organisations operating in hospitality and telecommunications are assessed to be at a heightened likelihood of being targeted.

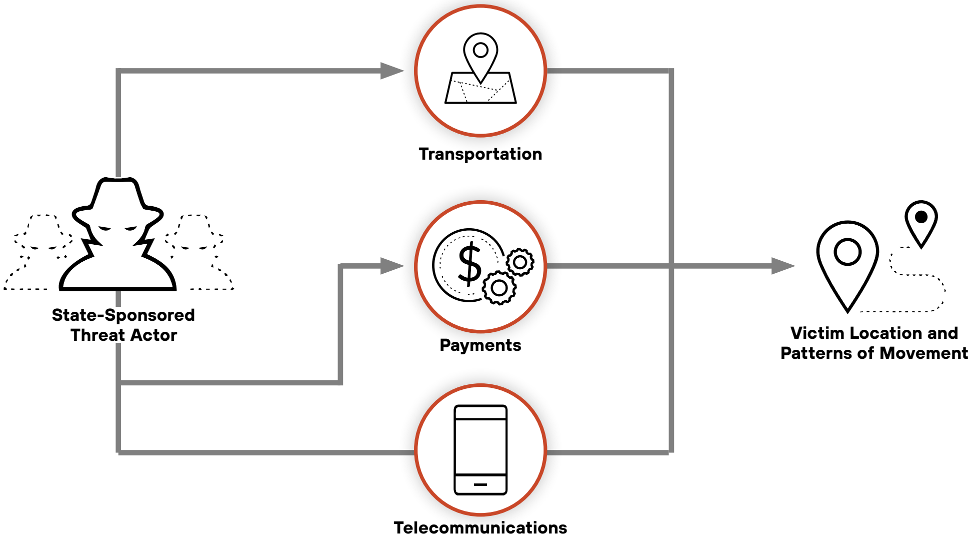

Transportation
State-Sponsored Threat Actor
Payments
Victim Location and Patterns of Movement
Telecommunications

Figure 4: State-sponsored threat actors target certain industries to track individuals

Data exfiltration

A primary focus of espionage attacks is the theft of sensitive data, ranging from customer data to intellectual property. The increased presence of people attending the Olympics likely means some essential services, such as hospitality or payment processing organisations, will hold and process more data. This may boost the intent for state-sponsored threat actors to increase their operational tempo during the event.

There is a realistic probability that a data breach by a state-sponsored threat actor could occur during the Olympics, although this could happen explicitly due to the Olympics or simply coincide with the Games. The increase in data for essential services is likely to correlate with the increase in motives by some threat actors, with the hospitality and telecommunication sectors being assessed as having the richest datasets to attempt to exfiltrate.

A closer look at the threat actors

After having reviewed essential Olympics services and potential threats to them, below is a list of threat actors illustrating some of the most recent or pertinent threats to the 2024 Summer Olympics. Each section contains a chart which details possible attack types on the left-hand side, mapped to threat actors and their historic use of these attack types on top. Some threat actors include a case study or a potential scenario detailing the actors' capabilities and intentions with respect to the Olympics.

While not exhaustive, this section aims to provide network defenders with an outline of some of the potential threat actors with perceived intent and capabilities to target the 2024 Olympics.

Cybercriminal threats

	Ransomware	Business Email Compromise	Cyber-enabled Fraud
	Play BlackBasta	Syndicate Orion	Magecart
Skimming			X
Phishing	X	X	X
Malvertising	X		X
Extortion	X		

Ransomware

Unit 42 assesses that ransomware operators have a low intent of targeting the 2024 Summer Olympic Games, but maintain a high capability for conducting disruptive attacks that could impact essential services either directly or indirectly. Indeed, successful targeting of a key supplier could have a significant impact on companies relying on it for their supply chain.

- **BlackBasta** is one of the most active ransomware groups in 2024. Unit 42 has observed a dwell time from initial access to BlackBasta ransomware deployment in less than 14 hours.[16] [17]
- **Play** is another highly active ransomware group at present. Unit 42 has observed an increase in Play ransomware incidents since 2023, affecting a wide variety of sectors.[18]

Unit 42 case study: In 2023, Unit 42 incident responders observed BlackBasta threat actors possessing a dwell time from initial access to ransomware deployment of less than 14 hours. The initial entry was made via a phishing email, then privilege escalation within two hours, and by hour eight data was exfiltrated. Shortly after the 12th hour, ransomware was staged and deployed across the network impacting hundreds of systems.[19]

Business email compromise

BEC threat actors are assessed to have a high intent of targeting essential services involved in the 2024 Summer Olympic Games. Overall, their technical know-how is low but the ability to operate at scale and increasingly sophisticated social engineering techniques increase their likelihood of successful campaigns.

- **Syndicate Orion** is a prolific network of West African cybercriminals that have been active since 2014.[20] They rely heavily on social engineering to trick their victims into making payments.

Cyber-enabled fraud

Threat actors conducting cyber-enabled fraud are assessed to have a high intent to target the 2024 Summer Olympic Games and use its brand to further the success of their fraudulent activities. Similar to BEC groups, fraud-focused threat actors have a low capability but operate at scale leading to large payouts. This type of activity is likely wide-ranging from web-skimming to selling fake event tickets.

- **Magecart** is a collective term used to describe nearly a dozen groups of threat actors specialising in digital credit card-skimming attacks.

Possible scenario: Magecart malware is injected into the HTML or JavaScript source code of a popular third-party service widget that is embedded on numerous e-commerce and hospitality websites. These websites are selling either souvenirs for the Olympics or providing bookings for hotels and restaurants in Paris. The malware is able to scrape the details inputted into the website, with emphasis on collecting credit card details and other personally identifiable information. The scale of this kind of attack affects hundreds of thousands of website customers. In 2018, a similar Magecart attack placed skimmers on over 800 websites' checkout pages via a compromised third-party service impacting more than 400,000 people.[21]

State-sponsored threats

	RUSSIA	BELARUS	IRAN	CHINA
	Fighting Ursa Razing Ursa	White Lynx	Agonizing Serpens	Towering Taurus
Espionage	X	X	X	X
Info-Ops	X	X	X	X
DDoS	X			
Wiper	X		X	
Defacement	X			
Hack-and-Leak	X		X	

Russia

Russia state-sponsored threat actors are assessed to have a high intent to target the 2024 Paris Olympics, with a high capability to conduct sabotage operations. Russia's exclusion from the Olympics, and statements by the French government perceived by the Kremlin as increasingly hostile informed our assessment.[22] Historically, Russian General Staff Main Intelligence Directorate (GRU) aligned actors have been responsible for sabotage attacks on the Olympics and closely related organisations.

- **Fighting Ursa** (a.k.a. APT28) is publicly attributed to the GRU and previously targeted the World Anti-Doping Agency (WADA) in 2016 via a hack-and-leak operation.[23] [24]
- **Razing Ursa** (a.k.a. Sandworm) is publicly attributed to the GRU and previously targeted both the 2018 Pyeongchang and 2021 Tokyo Olympics with wipers or with intent to deploy wipers.[25]

Belarus

Belarus state-sponsored threat actors are assessed to have a medium intent to target the 2024 Summer Olympics, with high capabilities to conduct information operations. Belarusian athletes have to compete as individual neutral athletes for their country's support of Russia in the Ukraine war, and Belarus has a long history of conducting cyber operations that support both Belarusian and Russian interests.

- **White Lynx** (a.k.a. Ghostwriter) is assessed to be a Belarus state-sponsored threat actor that has supported both Belarusian and Russian interests via espionage and information operations.

Possible scenario: Motivated by the exclusion of Belarus from the Games, and by French President Macron's vocal support for Ukraine war efforts, Whyte Lynx is tasked to target the Olympic Games in a retaliatory operation. White Lynx is known for conducting information operations by leveraging compromised websites or spoofed email accounts to disseminate fabricated content. Those sources could be used to send falsified news articles about the Olympics in an attempt to damage their reputation.

Iran

Iran state-sponsored threat actors are assessed to have a low intent to target the 2024 Summer Olympics, but possess high capabilities to conduct both sabotage and surveillance operations. Iran has significant capabilities to conduct sabotage, although potential motivations for such an attack on the Olympics are lacking. Tracking of dissidents or activists, on the other hand, is more likely. Iran has a long history of monitoring dissidents abroad with attempted kidnappings of individuals, and in some cases, the sanctioning of physical harm.[26]

- **Agonizing Serpens** (a.k.a. Agrius) is publicly attributed to Iran's Ministry of Intelligence and Security (MOIS), which has deployed wipers and conducted information operations.[27] [28]

China

China state-sponsored threat actors are assessed to have a low intent to target the 2024 Paris Olympics, with a high capability to conduct espionage operations focused on surveillance. In past Games, there have been espionage operations likely intent on tracking or surveilling people.[29] [30] This motive and objective is likely to persist into the current Games and extend to other high-value targets, ranging from political officials, dissidents, or organisations speaking against China.

- **Towering Taurus** (a.k.a. APT31) is publicly attributed to China's Ministry of State Security (MSS) and conducts espionage operations against political officials, dissidents, and activists.[31]

Hacktivists Threats

	PRO-RUSSIA	PRO-PALESTINE	OTHER
	NoName057(16) Cyber Army of Russia Anonymous Sudan	Seething Phoenix	Anonymous France
Info Ops		X	
DDoS	X		X
Wiper		X	
Defacement	X		X
Hack-and-Leak	X		X

Pro-Russia

Pro-Russia hacktivists are assessed to have a high intent to target the 2024 Paris Olympics, with low overall capabilities ranging from DDoS attacks to website defacements. Analysis of hacktivist incidents is complicated by the fact that state-sponsored threat actors may attempt to hide their activities behind the guise of hacktivist activity, and hacktivist groups have increasingly collaborated directly with state actors.

- **NoName057(16)** is the most active pro-Russia hacktivist group that Unit 42 observed since the start of the Ukraine conflict. In Q1 2024, NoName057(16) accounted for nearly 58% of hacktivist activity that Unit 42 is tracking.[32]
- **Cyber Army of Russia** is assessed to be operating in support of Russia state-sponsored threat actor Razing Ursa, and has claimed responsibility for cyberattacks on water utilities in 2024.[33]
- **Anonymous Sudan** in early 2023 heavily supported other pro-Russia hacktivists, but as of late has targeted organisations in light of pro-Palestinian sentiments. They are assessed to be closely aligned with Russia state-sponsored activity similar to that of the Cyber Army of Russia.

Case study: In March 2024, French state services were targeted by Anonymous Sudan via a DDoS attack with "unprecedented intensity." The threat actor is alleged to have targeted the State Interministerial Network, which connects thousands of websites. The attack impacted 177,000 IP addresses and over 300 web domains. The attack required a dedicated team to be stood up to counter the attack and restore web services to normal within 24 hours.[34] The scale of the attack and the swift response highlight the importance of incident response plans to counter the most likely threats an organisation could face, during and after the 2024 Paris Games.

Pro-Palestine

There has been a surge of pro-Palestine hacktivist activity since the Israel-Hamas conflict in October 2023. The upcoming Olympics are considered a high-profile event that provides a global audience for hacktivists, who could attempt to display their pro-Palestine or anti-Israel views. Pro-Palestine hacktivists are assessed to have a medium intent to target the 2024 Summer Olympics, with low-to-medium capabilities to conduct DDoS attacks, information operations, wiper attacks, or website defacements.

- **Seething Phoenix** is assessed to be a threat actor acting in the interests of Hamas, the Sunni militant group. The threat actor has historically focused on espionage operations against Israel but is likely capable of conducting sabotage campaigns in the form of wipers or information operations.[35]

Potential scenario: Given recent geopolitical events between Israel and Hamas, it's possible that Seething Phoenix seizes on this opportunity to conduct a sabotage attack against the Games, particularly focused on Israeli athletes and their delegation. The threat actor could attempt to disrupt the broadcasting of the opening ceremony when the Israeli athletes enter by displaying political messages. They could then further amplify the effects of this sabotage attack via an information operation on social media platforms. Historically, they have used social media accounts to spread propaganda and political messages following a disruptive attack.

Other hacktivism

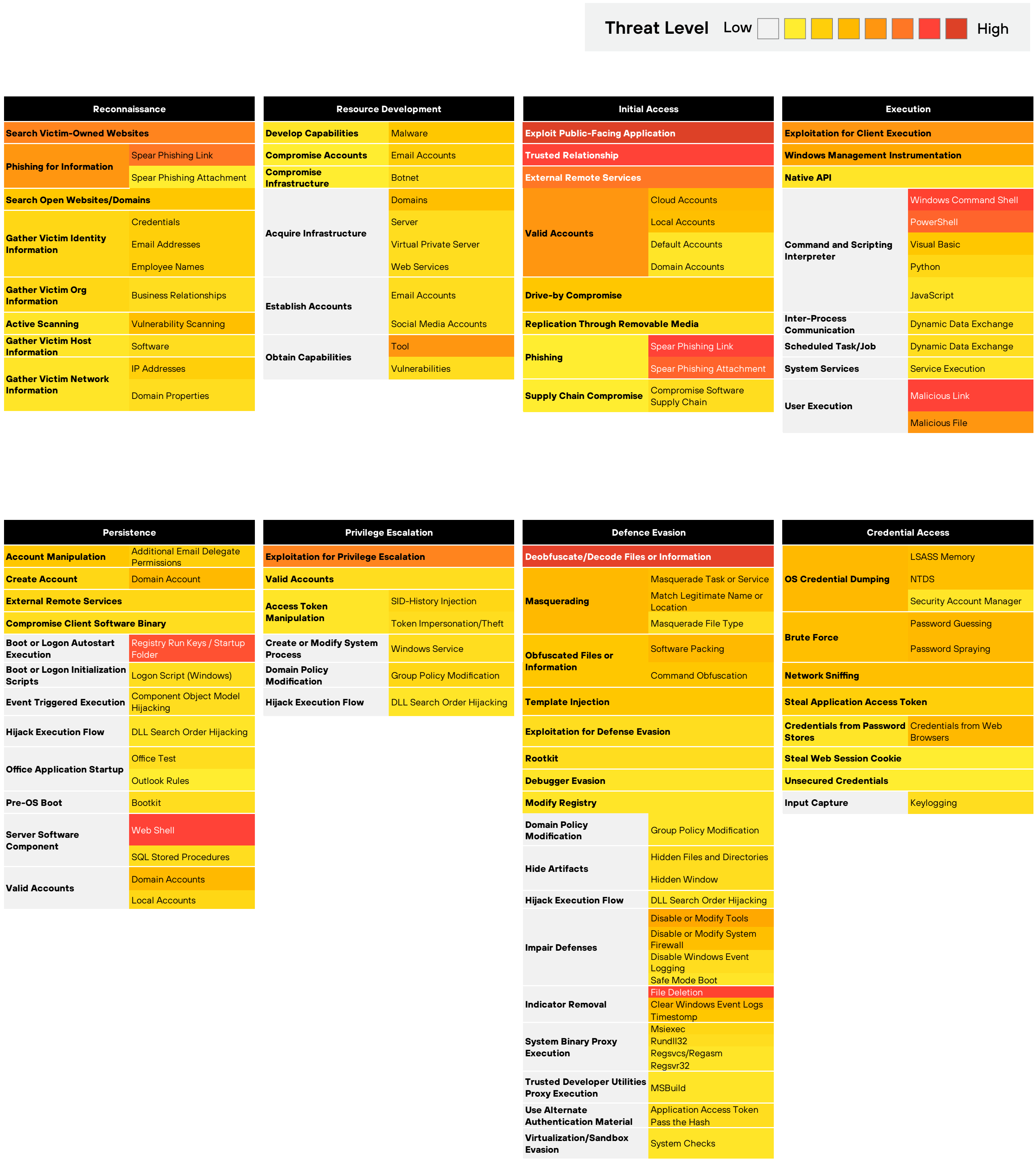
Other types of hacktivists, such as those against governments, capitalism, or even the Olympics themselves are assessed to have a high intent to target the 2024 Summer Olympics, with low capabilities to conduct DDoS attacks or website defacements. There is a precedent for hacktivists, like Anonymous, to target the upcoming Olympics similar to the anti-government hacks that occurred during the 2016 Rio de Janeiro games.

- **Anonymous France** is a loose collective of hackers based in France or that identify with French interests. Anonymous France has used tactics such as DDoS attacks, website defacements, and leaking of stolen data; for example, from the French Police Union.[36] However, the threat actor has been limited in its activities in recent months.

Tactics, techniques, and procedures

Unit 42 collated known tactics, techniques, and procedures (TTPs) known to be exploited by threat actors mentioned in this report. The TTPs have been aggregated and prioritised based on the threat that each threat actor is assessed to pose to the event. Below, we provide the resulting top 10 TTPs that organisations involved in the Olympics should ensure prioritising mitigation against, or detection of. In the following pages, a MITRE ATT&CK® heatmap shows the full range of known exploited TTPs.

#	Tactics	Techniques	U42 Recommendations
1	Initial Access	T1190: Exploit Public-Facing Application	Implement the appropriate mitigating controls against Exploit Public-Facing Application. Keep all internet-facing systems updated, regularly scan for vulnerabilities, enable application isolation and sandboxing.
2	Exfiltration	T1041: Exfiltration Over C2 Channel	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control (C2) signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.
3	Defence Evasion	T1140: Deobfuscate/Decode Files or Information	Monitor for the execution of certutil.exe within the environment. Monitor for the use of PowerShell to perform base64 decoding within the environment.
4	Command and Control	T1105: Ingress Tool Transfer	Implement network intrusion detection and prevention systems to block traffic on known C2 channels.
5	Initial Access, Persistence	T1133: External Remote Services	Disable or block remotely available services that may be unnecessary, especially alternate configurations for critical services. Unit 42 also recommends removing or denying access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
6	Execution	T1059.003: Command and Scripting Interpreter: Windows Command Shell	Use application control where appropriate. Limit user access to the Windows command shell to only authorised users and processes. Implement strong authentication mechanisms, such as multifactor authentication (MFA), to prevent unauthorised access to the command shell. Regularly monitor and review command shell activity logs for suspicious behaviour or unauthorised access. Regularly update and patch the operating system and command shell to protect against known vulnerabilities.
7	Collection	T1005: Data from Local System	Implement comprehensive data loss prevention (DLP) policies and procedures. DLP can restrict access to sensitive data and detect sensitive data that is unencrypted. Use role-based access controls (RBAC) to further protect sensitive data and monitor local systems for API calls that search for filenames and databases.
8	Initial Access	T1199: Trusted Relationship	Implement the appropriate mitigating controls against Trusted Relationship. Implement MFA for all delegated administrator accounts to enhance security.
9	Command and Control	T1071.001: Application Layer Protocol: Web Protocols	Utilise network intrusion detection and prevention systems with advanced signatures to identify and neutralise web protocol-based adversary activities.
10	Defence Evasion	T1070.004: Indicator Removal: File Deletion	Monitor executed commands and arguments for actions that could be utilised to unlink, rename, or delete files.



Reconnaissance	
Search Victim-Owned Websites	
Phishing for Information	Spear Phishing Link
	Spear Phishing Attachment
Search Open Websites/Domains	
Gather Victim Identity Information	Credentials
	Email Addresses
	Employee Names
Gather Victim Org Information	Business Relationships
Active Scanning	Vulnerability Scanning
Gather Victim Host Information	Software
Gather Victim Network Information	IP Addresses
	Domain Properties

Resource Development	
Develop Capabilities	Malware
Compromise Accounts	Email Accounts
Compromise Infrastructure	Botnet
Acquire Infrastructure	Domains
	Server
	Virtual Private Server
	Web Services
Establish Accounts	Email Accounts
	Social Media Accounts
Obtain Capabilities	Tool
	Vulnerabilities

Initial Access	
Exploit Public-Facing Application	
Trusted Relationship	
External Remote Services	
Valid Accounts	Cloud Accounts
	Local Accounts
	Default Accounts
	Domain Accounts
Drive-by Compromise	
Replication Through Removable Media	
Phishing	Spear Phishing Link
	Spear Phishing Attachment
Supply Chain Compromise	Compromise Software Supply Chain

Execution	
Exploitation for Client Execution	
Windows Management Instrumentation	
Native API	
Command and Scripting Interpreter	Windows Command Shell
	PowerShell
	Visual Basic
	Python
	JavaScript
Inter-Process Communication	Dynamic Data Exchange
Scheduled Task/Job	Dynamic Data Exchange
System Services	Service Execution
User Execution	Malicious Link
	Malicious File

Persistence	
Account Manipulation	Additional Email Delegate Permissions
Create Account	Domain Account
External Remote Services	
Compromise Client Software Binary	
Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder
Boot or Logon Initialization Scripts	Logon Script (Windows)
Event Triggered Execution	Component Object Model Hijacking
Hijack Execution Flow	DLL Search Order Hijacking
Office Application Startup	Office Test
	Outlook Rules
Pre-OS Boot	Bootkit
Server Software Component	Web Shell
	SQL Stored Procedures
Valid Accounts	Domain Accounts
	Local Accounts

Privilege Escalation	
Exploitation for Privilege Escalation	
Valid Accounts	
Access Token Manipulation	SID-History Injection
	Token Impersonation/Theft
Create or Modify System Process	Windows Service
Domain Policy Modification	Group Policy Modification
Hijack Execution Flow	DLL Search Order Hijacking

Defence Evasion	
Deobfuscate/Decode Files or Information	
Masquerading	Masquerade Task or Service
	Match Legitimate Name or Location
	Masquerade File Type
Obfuscated Files or Information	Software Packing
	Command Obfuscation
Template Injection	
Exploitation for Defense Evasion	
Rootkit	
Debugger Evasion	
Modify Registry	
Domain Policy Modification	Group Policy Modification
Hide Artifacts	Hidden Files and Directories
	Hidden Window
Hijack Execution Flow	DLL Search Order Hijacking
Impair Defenses	Disable or Modify Tools
	Disable or Modify System Firewall
	Disable Windows Event Logging
	Safe Mode Boot
Indicator Removal	File Deletion
	Clear Windows Event Logs
	Timestomp
System Binary Proxy Execution	Msiexec
	Rundll32
	Regsvcs/Regasm
	Regsvr32
Trusted Developer Utilities Proxy Execution	MSBuild
Use Alternate Authentication Material	Application Access Token
	Pass the Hash
Virtualization/Sandbox Evasion	System Checks

Credential Access	
OS Credential Dumping	LSASS Memory
	NTDS
	Security Account Manager
Brute Force	Password Guessing
	Password Spraying
Network Sniffing	
Steal Application Access Token	
Credentials from Password Stores	Credentials from Web Browsers
Steal Web Session Cookie	
Unsecured Credentials	
Input Capture	Keylogging

Threat Level Low ⬜ 🟨 🟨 🟧 🟧 🟧 🟥 🟥 High

Discovery	
System Information Discovery	
System Network Configuration Discovery	
System Owner/User Discovery	
Process Discovery	
File and Directory Discovery	
Query Registry	
System Time Discovery	
Peripheral Device Discovery	
Remote System Discovery	
System Network Connections Discovery	
Debugger Evasion	
Network Share Discovery	
Account Discovery	Domain Account
	Email Account
	Local Account
vare Discovery	Security Software Discovery

Lateral Movement	
Lateral Tool Transfer	
Exploitation of Remote Services	
Exploitation of Remote Services	
Internal Spear Phishing	
Remote Services	SMB/Windows Admin Shares
	Remote Desktop Protocol

Collection	
Data from Local System	
Archive Collected Data	Archive via Utility
Automated Collection	
Data from Information Repositories	Share Point
Screen Capture	
Data from Network Shared Drive	
Data from Removable Media	
Browser Session Hijacking	
Email Collection	Local Email Collection
	Remote Email Collection
	Email Forwarding Rule
Data Staged	Local Data Staging
	Remote Data Staging
Input Capture	Keylogging

Command and Control	
Ingress Tool Transfer	
Proxy	External Proxy
	Multi-hop Proxy
Remote Access Software	
Communication Through Removable Media	
Non-Standard Port	
Encrypted Channel	Symmetric Cryptography
	Asymmetric Cryptography
Protocol Tunneling	
Application Layer Protocol	Web Protocols
	Mail Protocols
	File Transfer Protocols
Data Encoding	Standard Encoding
Web Service	Bidirectional Communication

Exfiltration	
Exfiltration Over C2 Channel	
Exfiltration Over Web Service	Exfiltration to Cloud Storage
Data Transfer Size Limits	
Automated Exfiltration	
Exfiltration Over Alternative Protocol	Exfiltration Over Unencrypted Non-C2
	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Impact	
Endpoint Denial of Service	Service Exhaustion Flood
Data Encrypted for Impact	
Data Destruction	
Financial Theft	
Service Stop	
Network Denial of Service	Direct Network Flood
Data Manipulation	
Disk Wipe	Disk Structure Wipe
	Disk Content Wipe
Inhibit System Recovery	
System Shutdown/Reboot	
Defacement	External Defacement

Recommendations for CISO's and SecOps Teams

As the Paris 2024 Summer Olympics approach, the need for robust cybersecurity measures has never been more critical. The "Cyberthreats to Paris 2024 Report" by Unit 42 highlights the significant threat posed by financially motivated cybercrime, hacktivism, and espionage activities targeting this global event. CISOs and their teams play a pivotal role in safeguarding the integrity and success of such high-profile events. The following recommendations are designed to enhance their preparedness and resilience, ensuring the safety of critical services and the protection of sensitive assets during the Olympics.

- **Preparation.** One of the best ways to get ahead of attackers is to truly get ahead. Deploy advanced threat detection solutions to identify and block surveillance activities by state-sponsored entities and conduct regular training and simulation exercises for incident response teams to ensure preparedness.
- **Ensure complete visibility of your attack surface.** 75% of ransomware attacks and breaches fielded by Unit 42's Incident Response Team result from a common culprit–internet-facing attack surface exposures. Deploying solutions that provide centralised, near real-time visibility can help organisations identify and mitigate vulnerabilities before they can be exploited.
- **Monitor abnormal activity.** Strengthen monitoring systems to detect and respond to suspicious activities in real time. Don't forget to monitor for unusual access to your cloud environments, as threat actors are increasingly exploiting them. Launch awareness campaigns to educate employees, vendors, and contractors about common cyberthreats, what to look for, and how to avoid them, and provide clear guidelines on identifying and reporting suspicious activities.
- **Protect Your Supply Chain.** Prevent vendor cybersecurity gaps from disrupting operations and impacting your customers. Start by evaluating your cybersecurity supply chain risk management strategy, capabilities, and controls. Implement stringent security requirements for all vendors and third-party suppliers. Regularly audit and monitor vendors' cybersecurity practices to ensure they comply with security standards and are not vulnerable to exploitation.
- **React quickly.** Moving quickly to address security alerts can significantly limit damage. Security teams take an average of about six days to resolve a security alert, and over 60% of organizations take longer than four days to resolve security issues. Establish communication channels with relevant stakeholders, including government agencies, law enforcement, and other organisations involved in the event and participate in threat intelligence sharing initiatives to stay informed about emerging threats and best practices.
- **Maintain an incident response plan.** Develop and regularly update incident response plans tailored to the specific threats identified in the report. Organisations that continuously review, update, and test their incident response plans—ideally with input from cybersecurity experts–are much more likely to respond effectively to and contain an active attack.

References

1. Andy Greenberg, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," Wired, October 17, 2019.
2. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," U.S. Department of Justice Office of Public Affairs, October 19, 2020.
3. Daniel Rosney, "Eurovision 2023: Hotel phishing scam targets song contest fans," BBC, 7 March 2023.
4. Colin Clapson, "Beware of fake ads if you're looking online for a place to stay in Paris!," flandersnews.be, 12 September 2023.
5. Doel Santos, "Ransomware Retrospective 2024: Unit 42 Leak Site Analysis," Palo Alto Networks, February 5, 2024.
6. Unit 42, Incident Response Report, Palo Alto Networks, February 2024.
7. Harry Robertson, "ION brings clients back online after ransomware attack - source," Reuters, February 7, 2023.
8. Ionut Arghire, "EquiLend Ransomware Attack Leads to Data Breach," SecurityWeek, March 12, 2024.
9. Jonathan Wilson, "Fake tickets on 'industrial scale' caused Paris chaos, says French minister," The Guardian, May 30, 2022.
10. Nathan B. Thompson and Robert Muggah, "With Anonymous' latest attacks in Rio, the digital games have begun," openDemocracy, 12 August 2016.
11. "Statement From FuboTV Regarding December 14, 2022 Cyber Attack," Fubo, December 15, 2022.
12. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," U.S. Department of Justice Office of Public Affairs, October 19, 2020.
13. Tom Balmforth, "Exclusive: Russian hackers were inside Ukraine telecoms giant for months," Reuters, January 5, 2024.
14. "French report flags Azeri-linked disinformation campaign targeting 2024 Olympics," Reuters, November 13, 2023.
15. "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Department of Justice Office of Public Affairs, October 14, 2018.
16. Unit 42, "2024 Unit 42 Incident Response Report: Navigating the Shift in Cybersecurity Threat Tactics," Palo Alto Networks, February 20, 2024.
17. Amer Elsad, "Threat Assessment: Black Basta Ransomware," Palo Alto Networks, August 25, 2022.
18. Based on internal data.
19. Incident Response Report, February 2024.
20. Unit 42, "SilverTerrier (a.k.a. Syndicate Orion)", Palo Alto Networks.
21. Zach Whittaker, "Ticketmaster breach was part of a larger credit card skimming effort, analysis shows," ZDNET, July 10, 2018.
22. Cécile Ducourtieux et al., "War in Ukraine: Not all European countries view Russia as top threat," Le Monde, February 26, 2024.
23. "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Department of Justice Office of Public Affairs, October 4, 2024.
24. Unit 42, "Fighting Ursa AKA APT28: Illuminating a Covert Campaign," Palo Alto Networks, December 7, 2023.
25. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," U.S. Department of Justice Office of Public Affairs, October 19, 2020.
26. Eric Tucker, Didi Tang, and Nathan Ellgren, "As China and Iran hunt for dissidents in the US, the FBI is racing to counter the threat," AP, May 6, 2024.
27. "Iran and Hezbollah behind an attempted cyber attack on an Israeli Hospital," Gov.il, 18 December 2023.
28. Or Chechik et al., "Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors," Palo Alto Networks, November 6, 2023.
29. Dmitri Alperovitch, Revealed: Operation Shady RAT, McAfee, August 8, 2011.
30. Shaun Walker, "Russia to monitor 'all communications' at Winter Olympics in Sochi," The Guardian, 6 October 2013.
31. "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians," U.S. Department of Justice Office of Public Affairs, March 25, 2024.
32. Based on internal data.
33. Andy Greenberg, "A (Strange) Interview With the Russian-Military-Linked Hackers Targeting US Water Utilities," Wired, May 8, 2024.
34. "French state services hit by cyberattacks of 'unprecedented intensity'," France 24, March 11, 2024.
35. "HAMAS-LINKED SAMECOIN CAMPAIGN MALWARE ANALYSIS," Inside the Lan, 14 February 2024.
36. Catalin Cimpanu, "Three Anonymous Hackers Are Facing Trial in France After Targeting Local Police," Softpedia, February 26, 2016.

Tim Erridge
VP and Managing Partner
Unit 42
terridge@paloaltonetworks.com

Andre Reichow-Prehn
VP and Managing Partner
Unit 42
areichowpreh@paloaltonetworks.com

Under attack?

If you think you may have been compromised or have an urgent matter, please contact Unit 42 Incident Response team:

unit42-investigations@paloaltonetworks.com

+1.866.486.4842 (1.866.4.UNIT42)

+31.20.299.3130 (EMEA)

+65.6983.8730 (APAC)

+81.50.1790.0200 (Japan)

3000 Tannery Way
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com

Cyberthreats to Paris 2024 Report 06/2024