Cyberint

OLYMPICS 2024: When Cybercriminals Join the Arena

TABLE OF CONTENTS

INTRODUCTION 3

SETTING THE STAGE 4
- Olympics – Threat Actor Motives 4
- Olympics – Past Attacks 6
- Olympics 2024 – Main Threat Vectors 8
  - State-Sponsored Groups 8
  - Hacktivist Groups 10
  - Ransomware Attacks 11

BEHIND THE SCENES 12
- Phishing & Data Breaches 12
- Fraud Schemes 15
- WiFi Attacks 18
- Compromised Credentials 19
- Hacktivist Attacks 23

RECOMMENDATIONS FOR ORGANIZATIONS 25

RECOMMENDATIONS FOR INDIVIDUALS 26

CONCLUSION 27

SUMMARY 27

ABOUT CYBERINT 28

INTRODUCTION

As the Paris 2024 Summer Olympics approaches, concerns have surfaced over the heightened threat of cyberattacks during and preceding the games. The international attention makes it a prime target for malicious actors looking to engage in cyberespionage, make political statements, or generate profits.

Consequently, there is a widespread expectation of a significant increase in cyberattacks targeting Olympic-related organizations, sponsors, local infrastructure, high-profile individuals in France, payment systems, athletes, fans, and the local population.

Previous Olympics were targets of multiple cyber threats, including DDoS attacks, phishing campaigns, data breaches, and suspected cyberespionage operations among others. This year's Olympic Games are expected to face even more cyber threats due to escalating geopolitical tensions - notably between Russia/Ukraine and their allies, as well as the ongoing Israel/Hamas conflict. Recent advancements in artificial intelligence have provided cybercriminals with powerful tools, which heightens the risk of sophisticated cyberattacks.

Potential risks include phishing, credential theft, data breaches, ransomware attacks, DDoS attacks, and fraudulent schemes.

> ***Targets of concern include the International Olympic Committee (IOC), sponsors, local infrastructures, high-profile individuals, payment systems, and athletes, among others.***

While organizations and individuals have been widely advised to bolster their security awareness, many cyber incidents related to the Paris 2024 Summer Olympics have been reported in the wild, with further attacks anticipated. In this report, Cyberint sheds light into the challenges faced by organizations and individuals alike, highlighting cybercriminals' relentless efforts to win the game.

SETTING THE STAGE

Despite being a thrilling globally awaited sporting event, the Olympics have long been synonymous with concerns for the organizers and associated entities, given the high-profile nature of the event and the tumultuous history of cyberattacks sustained during the past iterations of the games.

OLYMPICS – THREAT ACTOR MOTIVES

Cyberespionage

The Olympics are a prime target for cybercriminals due to their global visibility and impact, and threat actors attempt to take advantage of the event's high profile. For instance, state-sponsored actors may exploit the Olympics to launch sophisticated phishing and cyber espionage operations with the aim of collecting strategic intelligence on enemy countries and governments.

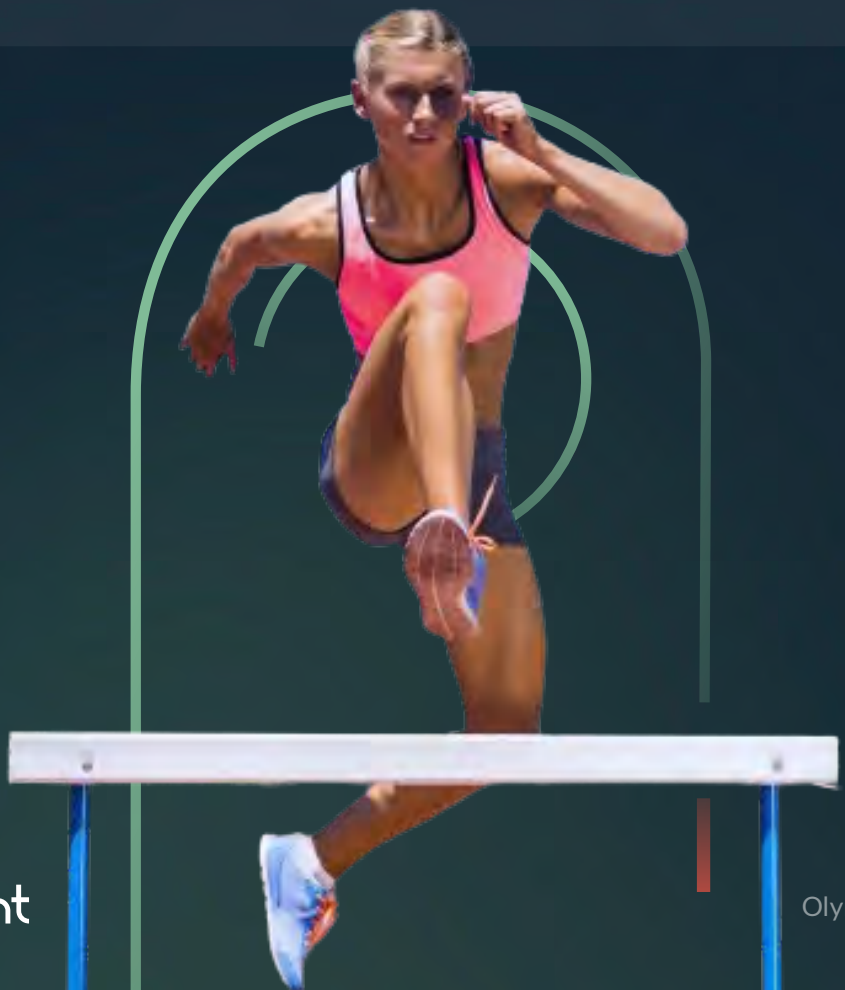
Political statements

Hacktivist groups, on the other hand, may take advantage of the Olympics to make political statements or to influence international relations. Indeed, hacktivists may aim to disrupt operations during the Olympics as an act of revenge against a country or an entity that they perceive as hostile. Disrupting critical infrastructure such as ticketing systems or broadcasting networks can cause widespread chaos and damage the event's reputation, affecting participants, spectators, affiliated organizations and the hosting country's government.

Financial gains

The Olympics present a prime opportunity for threat actors and ransomware groups to exploit and seek financial gain through ransom demands and fraudulent schemes. On the one hand, ransomware groups may likely capitalize on the extensive use of digital platforms for communication, transactions, and information dissemination during such high-profile events.

They may take advantage of the pressure on the organizations involved to ensure a smooth conduct of the event. Attackers are aware that organizations cannot afford to have their systems encrypted during this worldwide renowned sporting event and may specifically target them to extract substantial ransom payments. On the other hand, threat actors are likely to exploit the public's heightened enthusiasm around the games and related services to perpetrate scams and fraudulent activities. Indeed, they may take advantage of the public interest and the direct or indirect involvement of major organizations to deceive individuals and employees into sharing sensitive information or engaging in financial transactions.



OLYMPICS – PAST ATTACKS

Distributed Denial-of-Service (DDoS) Attacks

The threat of Distributed Denial-of-Service (DDoS) attacks is nothing new to the Olympics' attack surface. Indeed, an extended and widespread Distributed Denial-of-Service (DDoS) attack targeted the 2016 Rio Olympics' official website and affiliated organizations a few months before the games started. Additional waves of attempted DDoS attacks were also detected during the 2021 Tokyo Olympics, when security teams reported a staggering 450 million cyberattack attempts.

Nation-State Phishing Campaigns & Data Breaches

Nation-state actors have threatened many previous Olympic games. Indeed, the Russian state-sponsored Advanced Persistent Threat (APT) group Fancy Bear (aka APT28/Sofacy) attempted to attack the 2016 Rio Olympics, targeting the World Anti-Doping Agency through a phishing campaign. The attack resulted in a significant data breach and public disclosing of confidential information on medical treatments used by 41 athletes participating in the games.

Malware Attacks

Additional threats such as malware attacks impacted many of the previous Olympics games, especially during the 2018 Pyeong Chang Winter Olympics, when a sophisticated malware dubbed Olympic Destroyer disrupted operations of the Pyeongchang Organizing Committee. It caused heavy Internet disruptions, and rendered telecasts inoperative. The attack also disrupted ticketing systems and broadcasters' drones, shut down the event website, and prevented spectators from printing reservations, resulting in many empty seats.
Other malware attack attempts were detected during the 2021 Tokyo Olympics, including the infamous Emotet malware, as well as a wiper malware concealed within a counterfeit PDF document. The wiper malware targeted Olympic enthusiasts and upon opening the file, it infected the victims' computers and erased files.

Cyber-espionage

During the Beijing 2022 Winter Olympics, concerning reports emerged about the Covid-19 tracking app My2022, developed by a state-owned company for the Beijing organizing committee. Indeed, a reverse engineering analysis of the app allegedly revealed that Olympics athletes' data was collected, analyzed, and stored on servers in China.

Regarding the Paris 2024 Summer Olympics, the organizers are preparing to face an unprecedented surge in cyber threats, with attacks that will likely exceed the number observed during previous editions of the games. This is specifically due to the increase of geopolitical tensions globally and significant AI advancements that enable cybercriminals to leverage more sophisticated and automated methods for cyberattacks and disinformation operations.

OLYMPICS 2024 – MAIN THREAT VECTORS

State-Sponsored Groups

One of the top threats posed to the Paris 2024 Summer Olympics games are the state-sponsored groups. Among them, two prolific Russian groups dubbed Storm-1679 and Storm-1099 have been recently targeting the Paris 2024 Summer Olympics, the International Olympic Committee (IOC), and the French President Emmanuel Macron in extensive, AI-assisted misinformation campaigns.

The Russian groups' efforts to target the Olympics date back to June 2023, when Storm-1679 shared a fake documentary called "Olympics Has Fallen", featuring the voice of the iconic actor Tom Cruise in a fabricated discourse mocking the IOC.

Figure 1: Screenshot of the fabricated documentary "Olympics Has Fallen" made by Russian-affiliate threat group Strom-1679

In addition, Storm-1679 and Storm-1099 launched deceptive campaigns with the main goal to defame the reputation of the IOC, while instilling fear of violence in Paris. For instance, some of the videos shared by the Russian threat groups purported that "24% of the Olympics' tickets had been returned" and that "Parisians were allegedly purchasing property insurance ahead of the Olympics due to increased fear of terror attacks."

On the other hand, the French Computer Emergency Response Team (CERT) reported on June 19, 2024 that the Russian state-sponsored group Midnight Blizzard (previously known as Nobelium), was observed targeting French diplomatic entities, aiming to "exfiltrate strategic intelligence". Such an announcement just a month ahead of the beginning of the Paris 2024 Summer Olympics may suggest higher concerns about potential state-sponsored activities during the games.

Considering the historical context of Russia's use of international sports events to demonstrate their power and dominance, it is reasonable to assume that the upcoming event may be a target for attacks. Given the recent restriction on Russia's athletes participation in the Olympics, this event takes on additional significance.

> ***Russian state-sponsored actors have demonstrated historic willingness and capabilities to target the Olympics in the past, and the Paris 2024 Summer Olympics face an increasing risk of cyberattacks due to France's financial and military support of Ukraine since Russia's invasion in 2022.***

Asides from Russian threat actors, it is likely, at a lower extent, that Chinese and North Korean state-sponsored groups may see the Paris 2024 Summer Olympics as an opportunity to ramp up cyberattacks through social engineering, phishing campaigns and cyber-espionage operations against government officials. Moreover, Iranian state-sponsored groups may opportunistically conduct cyberattacks during the Paris 2024 Olympics for geopolitical objectives, ideological message spreading, and intelligence gathering. This interest could be heightened amidst the Israel-Hamas war and related hostilities towards Western countries.

---

[1] https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/

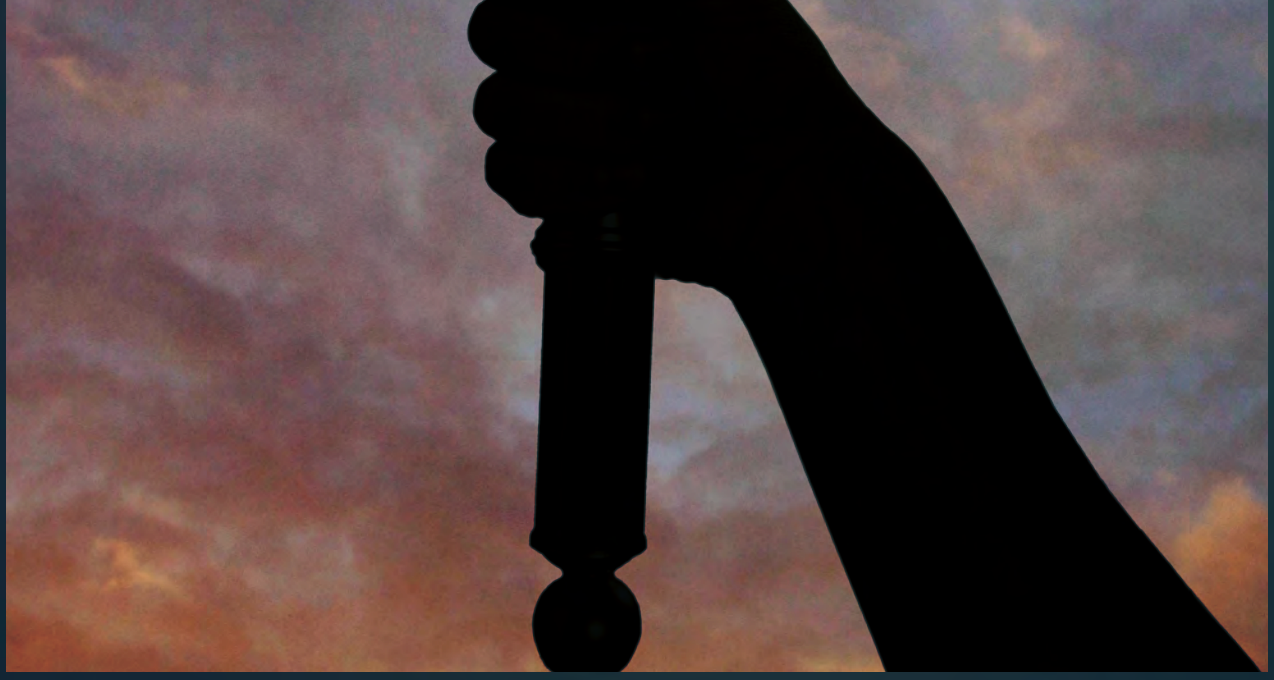
[2] https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/

[3] Rapport menaces et incidents - CERT-FR (ssi.gouv.fr)

Hacktivist Groups

Aside from state-sponsored entities, multiple Russian hacktivist groups like the infamous collectives HackNet, NoName057(16), Anonymous Sudan and People's Cyber Army, among many others, have consistently targeted pro-Ukrainian countries with website defacements, DDoS attacks and data breaches, and might take this opportunity to increase their attacks against the Olympics and France's critical infrastructures

As a reminder, during the globally followed Eurovision Song Contest 2022 in Turin, Italy, the Italian police cybersecurity department thwarted multiple cyberattacks on network infrastructure, which were attributed to Killnet and its affiliate Legion, the latter actively encouraging affiliates on Telegram to target the contest's final. While pro-Russian hacktivists have not explicitly expressed their intentions to disrupt the Paris 2024 Olympics and related entities yet, it is only a matter of time until first claims of attacks will be published on their underground communication channels.



Ransomware Attacks

Last but not least, the Paris 2024 Summer Olympics present an enticing opportunity for financially motivated cybercriminals to launch ransomware attacks. Indeed, the pressure on event-related companies to ensure smooth operations and maintain their reputation to the world makes them susceptible to ransomware attacks aimed at extorting significant payments.

In addition, and as Paris prepares for an influx of 15 million tourists, organizations in sectors such as hospitality, transportation, public services, and logistics appear as prime targets of ransomware attacks.

Among the potential attackers, sophisticated groups like Lockbit, Play and Clop might launch disruptive ransomware attacks on Olympics-related organizations and critical infrastructures in France, threatening to leak sensitive data in a double-extortion scheme to pressure victims into making payments. Some particularly aggressive ransomware groups such as ALPHV (aka BlackCat) and AvosLocker might also use the triple-extortion scheme, involving the launch of DDoS attacks after deploying ransomware on victims' systems to strengthen the pressure and maximize payouts.

> ***In the past 6 months, Cyberint detected around 200 claims of ransomware attacks on French organizations only, with 8base, Lockbit, Cactus, and RansomHub being the top attacking groups.***

Ransomware groups may rely on zero-day vulnerabilities to perform Remote-Code-Execution (RCE) and elevate privileges on victims' networks. Attackers could also exploit the interconnection between Olympics organizations and service providers, and deploy widespread ransomware in supply-chain attacks. Such a scenario happened in 2023 when the Clop ransomware group exploited a critical vulnerability in the widely used MOVEit Transfer component, resulting in widespread infections affecting over 2,000 organizations globally.

BEHIND THE SCENES

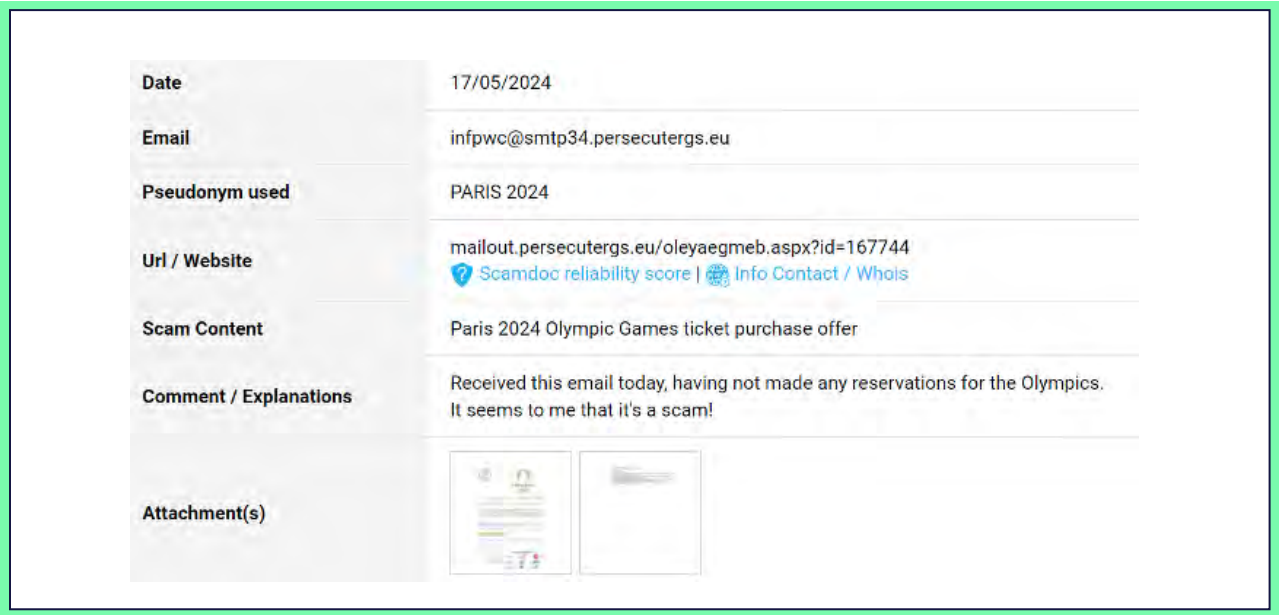
Cyberint recently observed and collected multiple intelligence items illustrating cybercriminals' attempts to perpetrate attacks, as well as sensitive data associated with the IOC and which could be misused by malicious actors.

PHISHING & DATA BREACHES

In the last six months, we have observed a number of phishing instances and campaigns that have the Olympics as a topic. One such instance is discussed below. The following screenshot displays an item collected by Cyberint's Argos Intelligence platform, involving a fraudulent email received by a French national and reported on May 17, 2024. The item was first shared on a fraud report website.

This phishing email exhibits classic social engineering tactics that exploit the public's enthusiasm in participating in the Paris 2024 Summer Paralympics' opening event and involves a sense of gratification. Indeed, the attachment of this email claims that the recipient won a free ticket for the Paris 2024 Paralympics opening ceremony and prompts the recipient to provide their financial information to cover a low delivery fee of €1.99 to receive the ticket at home. Once the victim provides their financial details, the cybercriminals will be able to reuse them on further platforms and perform fraudulent payments on the victim's behalf.

While the attachment mimics the design of an official and legitimate attachment, it turns out that this email is part of a widespread phishing operation that has been attracting significant attention among the French public.



Date	17/05/2024
Email	infpwc@smtp34.persecutergs.eu
Pseudonym used	PARIS 2024
Url / Website	mailout.persecutergs.eu/oleyaegmeb.aspx?id=167744 Scamdoc reliability score | Info Contact / Whois
Scam Content	Paris 2024 Olympic Games ticket purchase offer
Comment / Explanations	Received this email today, having not made any reservations for the Olympics. It seems to me that it's a scam!
Attachment(s)	

Figure 2: Report of a phishing email exploiting the Paris 2024 Summer Paralympics' event

Figure 3: Attachment of the phishing email

While the above example illustrates an instance of a mass phishing campaign, threat actors can also target their victims in spear-phishing attacks, which involve emails directed at a specific individual. These attacks are more targeted, and attackers initially gather enough Personal Identifiable Information (PII) about their victims to appear more credible. While these attacks may be less visible outside of the targeted organization, we have no doubt that IOC employees are experiencing these attacks.

In some cases, attackers source this information directly from cybercriminal forums, which host a myriad of compromised databases including citizens' PII such as full names, email addresses, physical addresses, phone numbers, birth dates and more. Threat actors can cross-reference these details with other sources of information in order to create a highly deceiving spear-phishing emails.

In early July 2024, Cyberint detected the following post from a highly active member of a Russian-speaking cybercriminal forum selling a huge database with information on French citizens. This example is just one of many databases related to France and Europe that Cyberint's Argos Platform collects.

The database allegedly contains over 3 million rows of data including full names, email addresses, physical addresses, zip codes, phone numbers and birth dates. The full database can be purchased by any threat actor for a bit more than $600, and would constitute a valuable source to conduct spear-phishing attacks and all kind of fraud schemes against the French public ahead of the Paris 2024 Summer Olympics.

Figure 4: A database containing information on French citizens offered on a Russian cybercrime forum

FRAUD SCHEMES

As with other attack vectors, fraud is an integral part of any big event. The following screenshot displays the homepage of a "secondary," malicious marketplace selling tickets for a range of sports events, including the Paris 2024 Summer Olympics. The domain associated with this malicious website (paris24tickets[.]com) was timely registered in mid-March 2024, and is hosted in Moldova. Interestingly, the WHOIS information for the domain is obscured, a tactic commonly employed by fraudulent websites' operators to conceal the identity of the domain owner.

The website lacks information regarding its entity and team, and fails to offer secure payment options typically expected from legitimate marketplaces. Despite its recent registration, the site strategically ranks among the top paid results in Google searches and therefore, has the potential to lure a large number of interested fans seeking tickets for the games.

Such fraudulent sites are widespread and aim to steal victims' money while collecting their financial data for further misuse in fraud schemes.

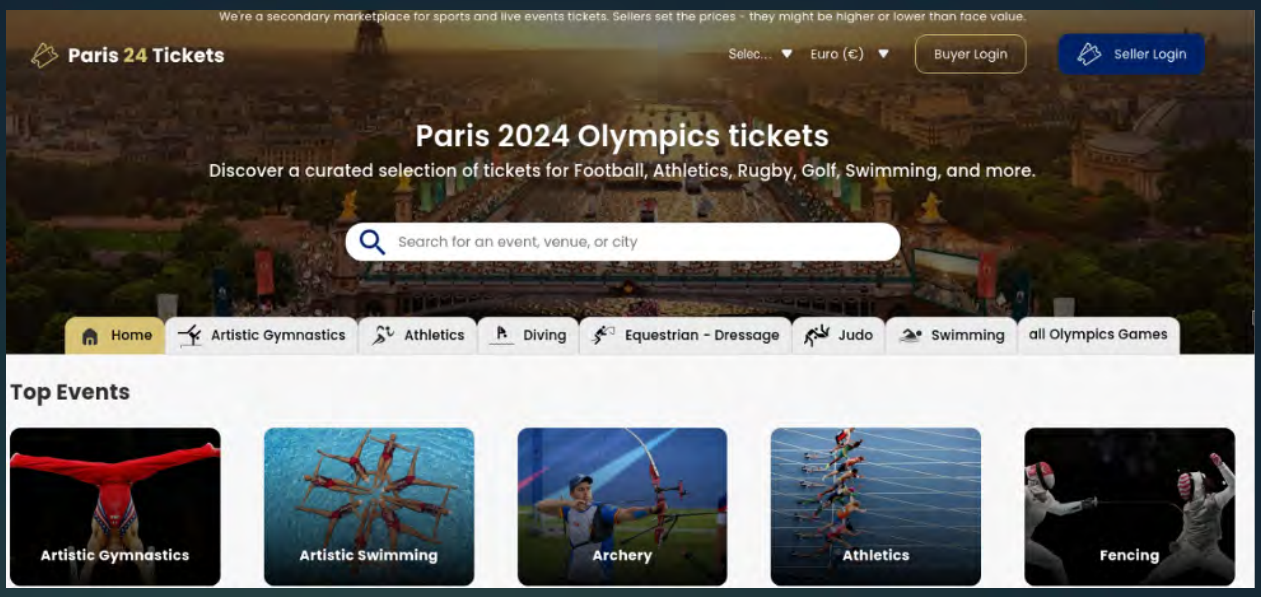


Figure 5: Screenshot of the paris24tickets[.]com fraudulent marketplace

The Forensic Canvas' screenshot below displays the connections between the paris24tickets[.]com domain and other indicators such as IP addresses, subdomains and related files, among others. For instance, the domain was found to be hosted on at least one IP address identified as malicious. In addition, several email subdomains were detected being related to the paris24tickets[.]com, suggesting that the operators of the fraudulent site may also engage with victims through direct phishing emails.

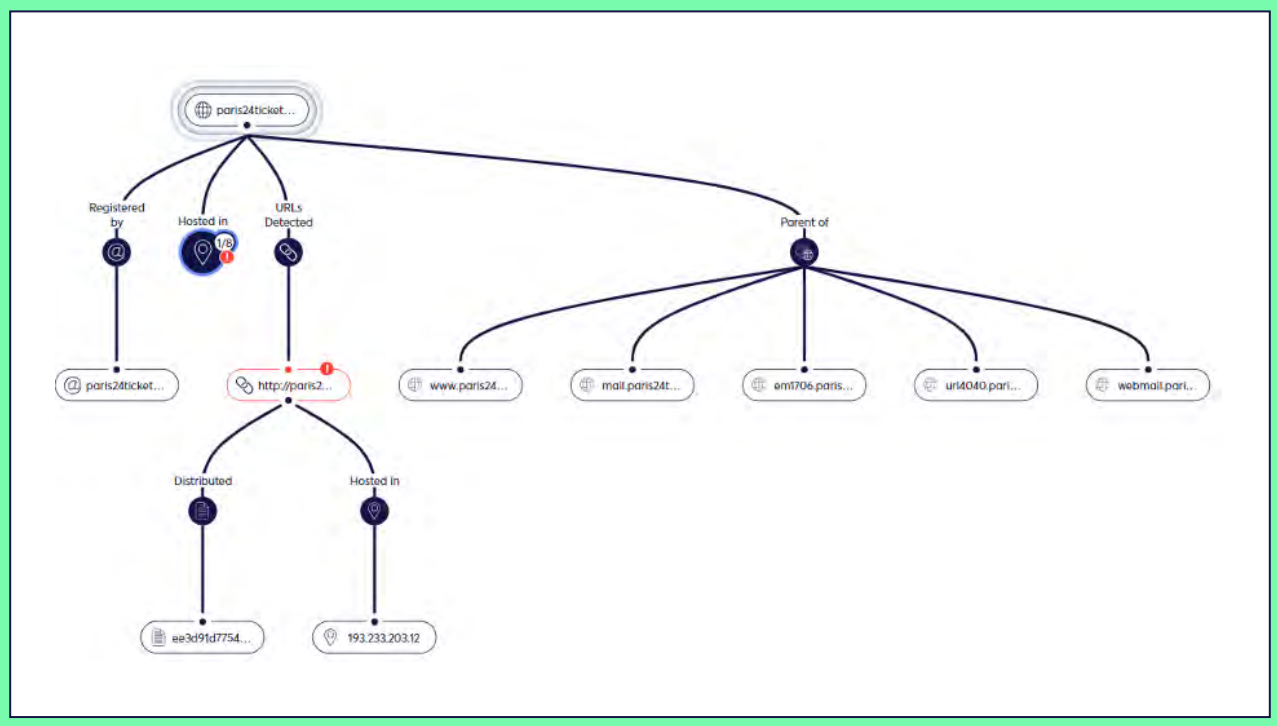


Figure 6: Cyberint's Forensic Canvas mapping the paris24tickets[.]com website's digital footprint

While this example illustrates an instance of a fake ticketing website, fraudsters may be highly imaginative and target the public with Olympics' sponsor fraud schemes, malicious live streaming sites, and fake mobile applications.

For instance, Cyberint detected many unofficial app stores advertising Olympics 2024 applications for download. These unofficial app stores are less supervised and controlled than official ones such as Google Play and Apple Store. Because applications can be uploaded by anyone on these unofficial app stores, the latter are considered less safe and less reliable. Some of these unofficial app stores may contain tampered contents impersonating official apps and potentially containing malicious components. Therefore, Olympics enthusiasts are advised to download applications from official mobile app stores only.

Generally, applications that have a low download number, an overall low score, as well as poor grammar in the application's description constitute a red flag and must be approached with caution. Also, it is advised to carefully check the kind of permissions required by the application and remain cautious with signs of possible attempts to abuse access to users' phone data.

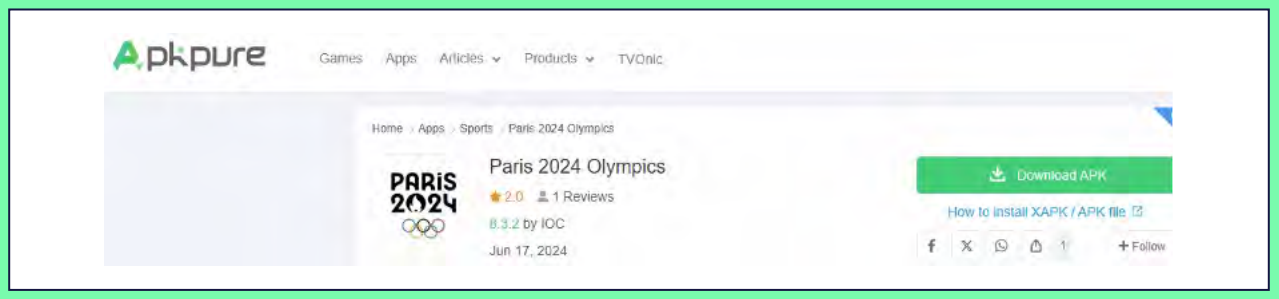


Figure 7: Suspicious Olympics 2024 app advertised on an unofficial app store

Fraud schemes could go beyond the targeting of Olympics ticketing websites and mobile applications. They could also impact organizations such as banks and insurance companies as well as their customers. For instance, malicious actors could misuse victims' financial details harvested through Olympics-themed phishing campaigns and request the victims' banks to initiate funds transfers, loans, and other financial transactions on the behalf of the banks' customers. These actions could result in significant financial losses for the affected individuals and erode their trust in their banks, potentially damaging the banks' reputation.

Also, threat actors could submit fraudulent claims to insurance companies, claiming fake insurance payouts for alleged losses or damages related to the Olympics. Such schemes could involve the falsification of documents or exaggerated claims of property damage, travel disruptions, or medical expenses allegedly incurred during the event period.

If successful, these scams could result in significant financial losses for targeted insurance companies and affect their capacity to maintain solvency and meet their commitments to policy holders.

It could also affect insurance companies' levels of regulatory compliance and impact their overall industry reputation.

In early July 2024, Cyberint observed a Telegram post where French threat actors were offering a variety of counterfeit documents, such as sick leave notes, medical prescriptions, and customizable documents, which threat actors could use to support their false insurance claims. While the threat actors did not explicitly encourage using their services during the Olympics period, sharing this post at this time could potentially encourage fraudsters seeking to exploit insurance companies with fake claims during the games.

Figure 8:
French threat actors offer multiple counterfeit documents on Telegram

WIFI ATTACKS

The large influx of tourists from around the world during the Olympic games is expected to increase the risk of public WiFi attacks, aiming to intercept traffic and hijack network sessions of unsuspecting victims. Indeed, during the Olympics, visitors and fans may want to check their emails, view their bank account balance, log in to their social media accounts, and conduct financial transactions, using the public WiFi offered in airports, hotels, restaurants, cafes, and even in the street.

What victims probably don't realize is that malicious actors may act as Man-in-the-Middle (MitM), exploiting public WiFi spots' lack of security to intercept traffic and steal their data such as PII, logins, passwords, and financial details. Moreover, threat actors could redirect the victims to malicious, spoofed websites, aiming to steal further information and installing malware on their devices.

In the end of June 2024, Cyberint detected a post from a member of the cybercriminal platform Carder Market sharing a full tutorial on how to successfully intercept traffic on public WiFi spots. The post's author shared a list of tools that would enable other cybercriminals to intercept victims' networks and capture passwords, messages and communications, among others. The author also included screenshots of a tool used to redirect users of the Russian social media VKontakte (vk.com) to a spoofed website, as an example.

The technique involved is an SSL-Strip MitM attack, where secured HTTPS connections are downgraded to unsecured HTTP, as the encryption provided by SSL/TLS protocols is bypassed or stripped away. This could allow an attacker to intercept and manipulate data exchanged between the user and the website, potentially exposing sensitive information like login credentials or financial details.

While the author included a disclaimer stating that the tutorial was intended for educational purposes, it could be a tactic to evade legal repercussions while enabling threat actors to exploit the information for malicious purposes, which may boost his own reputation on the platform.

The Carder Market member did not explicitly link the Paris 2024 Summer Olympics as an opportunity to carry out such attacks. However, the timing of sharing this tutorial could potentially inspire malicious actors seeking to exploit tourists' lack of awareness during the games.

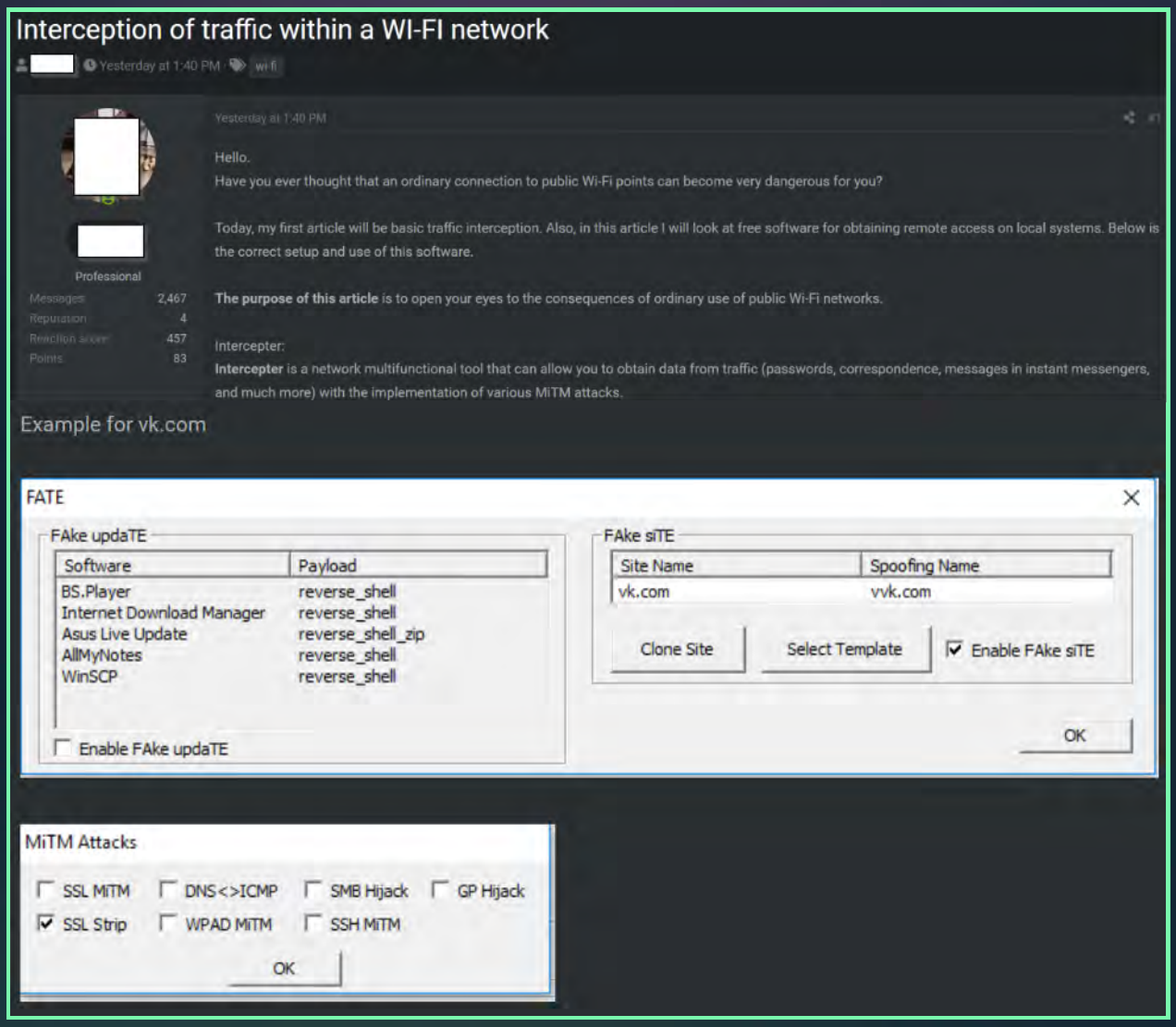


Figure 9: Public WiFi attack tutorial shared on Carder Market and collected by Cyberint's Argos platform

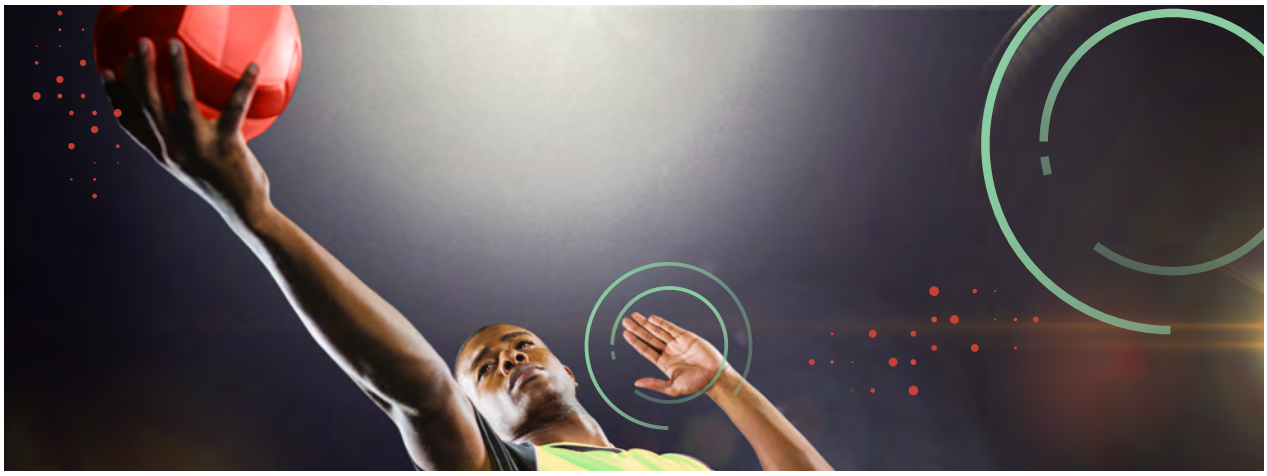
COMPROMISED CREDENTIALS

Cybercriminals employ several vectors to attack their victims' accounts and networks, and one of the most frequently used method is the use of compromised credentials. Indeed, using compromised credentials saves cybercriminals precious time as it eliminates the need to orchestrate phishing schemes or exploit vulnerabilities to gain a foothold into their victims' systems. This technique might also decrease detection on the systems as the attackers' log into their victims' login interfaces as "legitimate" users.

Cybercriminals could either use credentials sourced from several deep and dark web sources for free, or purchase credentials offered for sale as part of stealer malware logs or from Initial Access Brokers (IABs).

In the context of the Paris 2024 Summer Olympics, cybercriminals might target accounts associated with Olympics entities, French institutions, critical organizations, sponsors, athletes and more. For instance, if a cybercriminal successfully leverages an IOC employee's credentials, they could impersonate the affected individual. They could then launch convincing fraudulent operations, deploy harmful malware on the networks, disrupt the planning and supervision of the Olympics, and even gather strategic intelligence about officials and politicians.

On the other hand, cybercriminals could use credentials belonging to athlethes, fans and tourists. In such cases, attackers could launch fraudulent operations on their behalf, steal their identity, and perform illegal transacations, leading to financial losses and potential legal issues for the affected individuals.



To illustrate such threats, Cyberint's Argos Intelligence Platform collected the following post which was shared on a Telegram bot. This post was selected out of more than 50 intel items related to Olympics accounts' compromised credentials collected by Cyberint in the past 6 months. This specific bot acts like a search engine to look up compromised credentials, and any subscriber of this Telegram channel can query for credentials associated with a specific domain, and retrieve the data for free.

On April 10, 2024, a user requested to get credentials associated with the Paris Organizing Committee for the 2024 Olympic and Paralympic Games. As seen in the screenshot below, the query returned 11 results, including 9 sets of corporate credentials in clear text. By using these email credentials, cybercriminals could easily impersonnate legitimate members of the Committee, retrieve sensitive information related to the Olympic and Paralympic Games' planning and supervision, and potentially gather further intelligence on officials that could serve political and strategic agendas.

The use of these compromised credentials could have far reaching consequences, including heavy financial losses, legal penalties, and reputational damage for the Committee and the French government. Moreover, it could pose a potential threat for the national security and disrupt the smooth operation of the games.

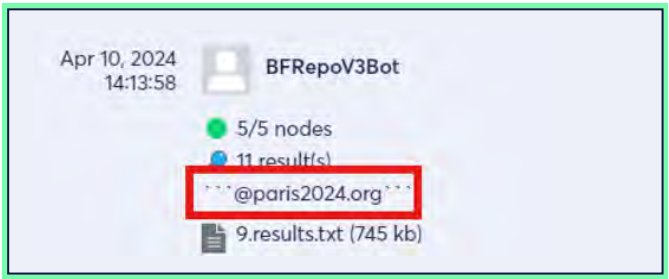


Figure 10:
Credentials related to the Paris Organizing Committee for the 2024 Olympic and Paralympic Games shared on Telegram monitored by Cyberint's Argos Platform

In another example, Cyberint collected the following intel item, involving a list of compromised credentials harvested at the beginning of June by the infamous Redline stealer malware. According to the logs, and after further investigation, it seems that the impacted individual has been a member of the IOC for more than 10 years and is particularly in charge of overseeing a data-centric project related to the Olympics. The nature of this role implies that the individual may have access to a broad spectrum of sensitive information related to various aspects of the Olympics and its third parties, which could be accessed by an attacker.

In addition, the technical details of the log indicate that the affected computer is a corporate machine. Stealer malware infecting a corporate machine not only reflects less-than-optimal security hygiene but also poses substantial risks such as data theft, potential network compromise, and operational disruptions.

In this specific case, the harvested credentials are associated with the Doodle free meeting scheduling tool. Cybercriminals could use these credentials to gather information and notes related to past and planned meetings and discover valuable details about the planning and implementation of the games, among other useful insights. Moreover, cybercriminals could try the same password on other login portals to exploit the victim's potential reuse of their password on multiple platforms.

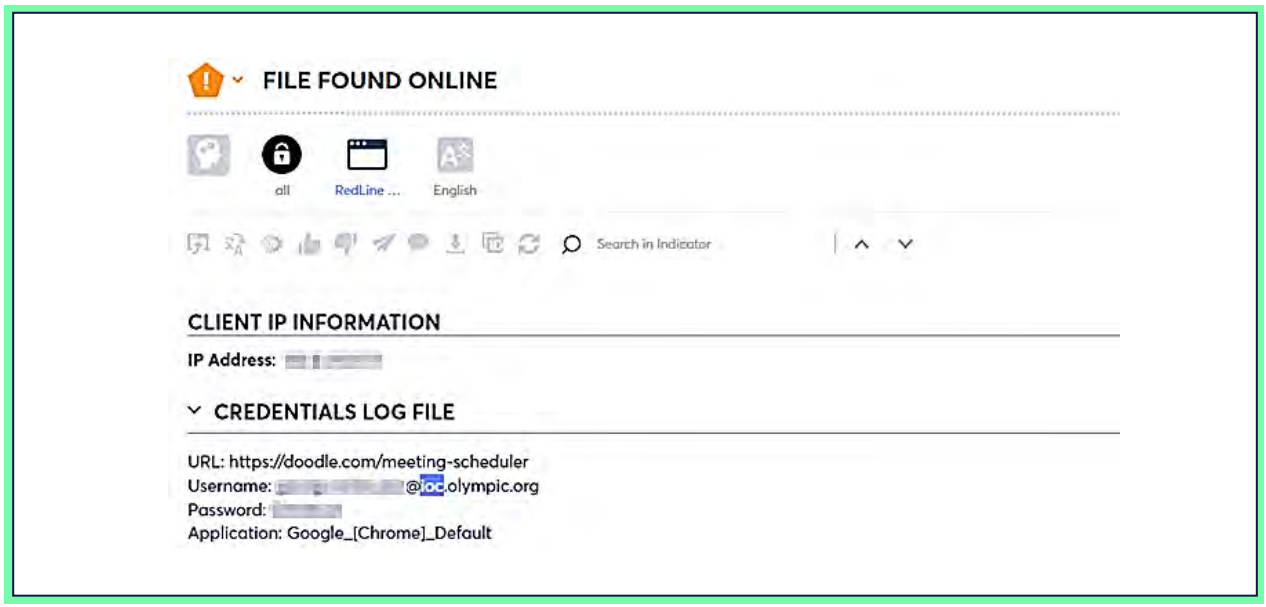


Figure 11: IOC member's credentials harvested by Redline stealer malware, collected by Cyberint's Argos platform

In early July, Cyberint collected the following post on a Russian-speaking cybercriminal forum. The threat actor was actively looking for initial access to the networks of organizations related to the Olympics, among other items. Specifically, the threat actor expressed his willingness to purchase “anything related to the 2024 Olympics”, strongly indicating his intention to conduct a wide range of cyberattacks imminently.

No public responses were observed in the thread of the post, however, threat actors could have contacted the post's author privately to share valuable information or attack methods.

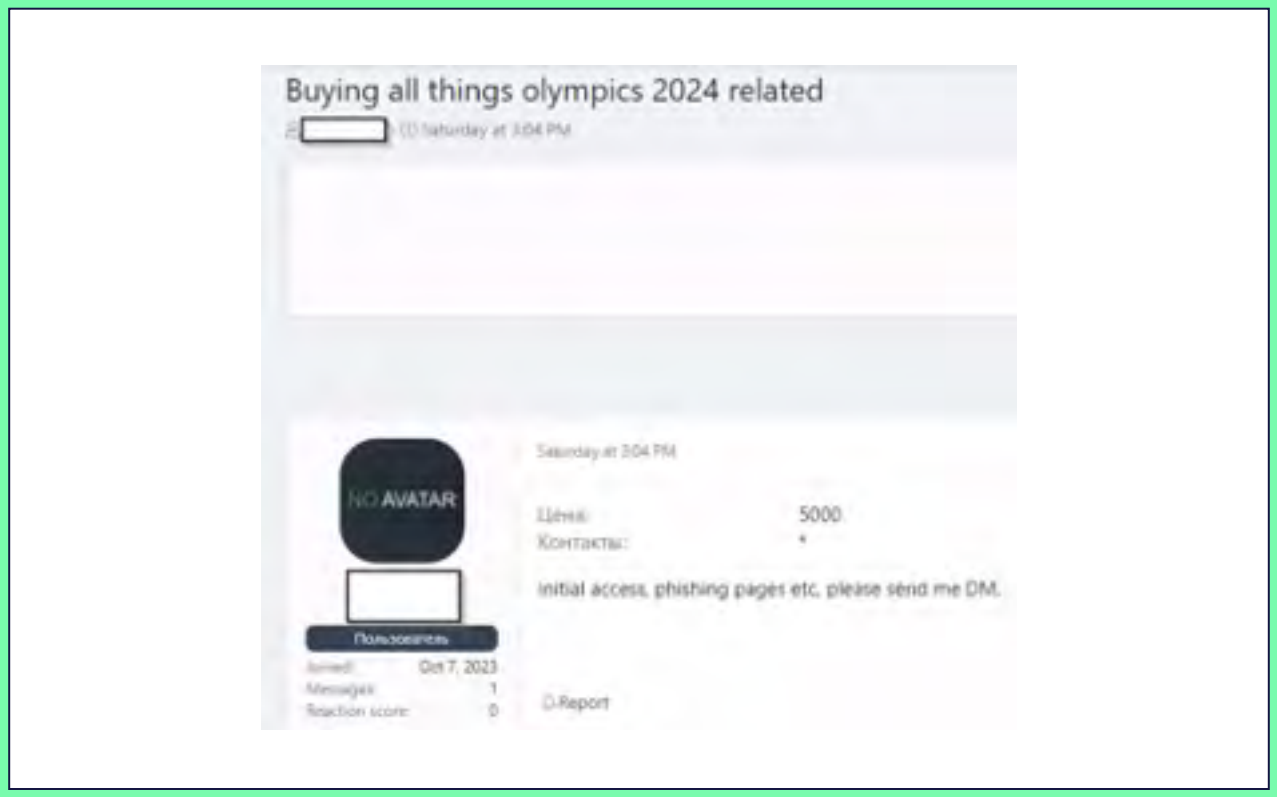
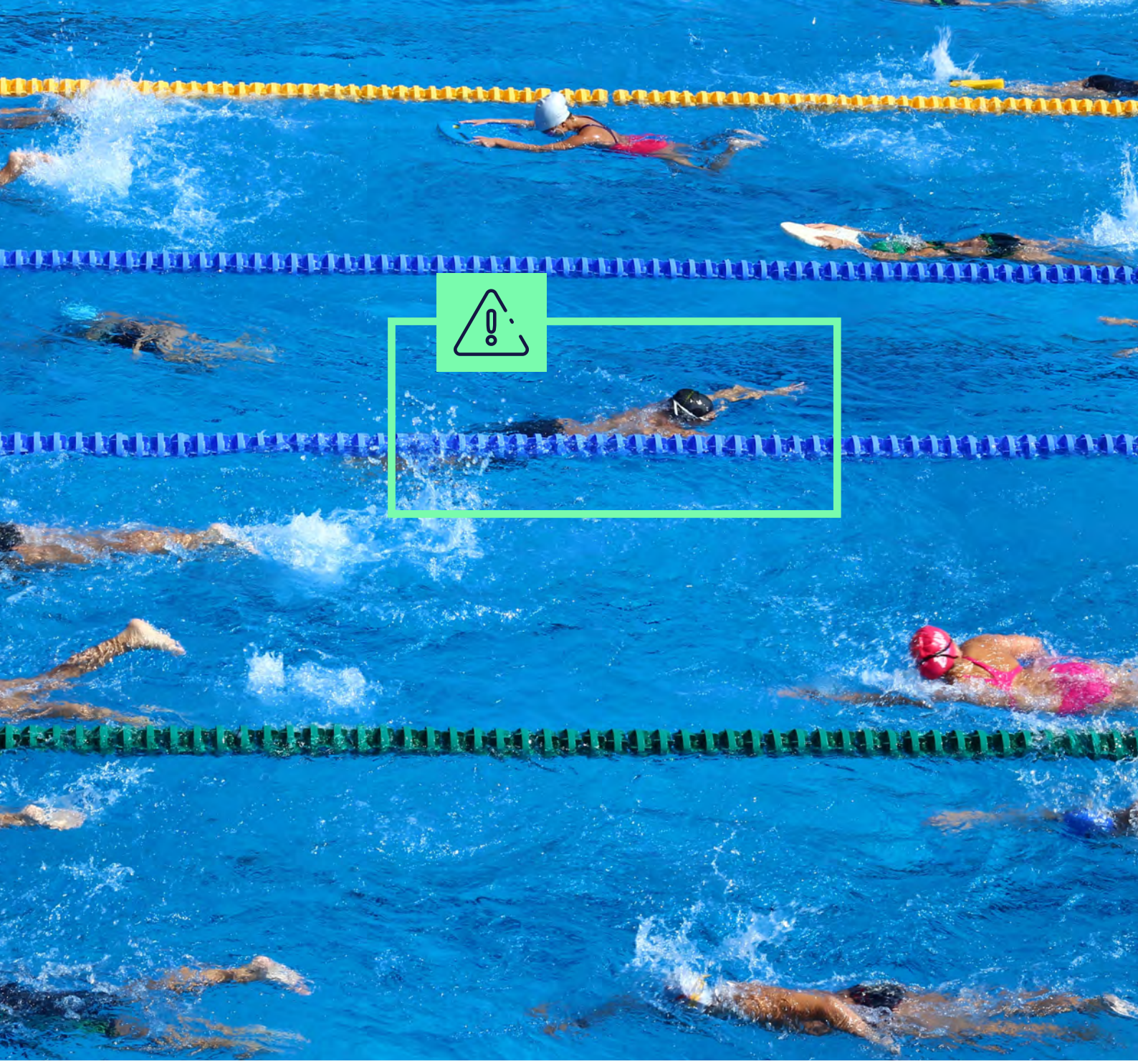


Figure 12: A threat actor seeks initial access to organizations linked with the Olympics, among other items, on a Russian cybercriminal forum



HACKTIVIST ATTACKS

As mentioned earlier in this report, hacktivists groups love to capitalize on events like the Olympics, due to their global spotlight. They do this to advance their political and ideological agendas and/or to gain recognition within the cybercriminal industry and among the public.

Pro-Russian hacktivist are usually the most active groups during significant global events and take the opportunity to disrupt entities that they perceive as hostile to Russia, especially since the war against Ukraine. As such, hacktivist groups often partner with like-minded collectives to gather forces and have already launched hundreds of DDoS attacks against NATO countries' critical infrastructure, along with website defacements and data breaches.

Recently, some hacktivist groups also announced their own ransomware programs such as GhostLocker, the new Ransomware-as-a-Service (RaaS) program launched by several pro-Palestinian hacktivist groups led by the infamous hacktivist collective GhostSec. These new TTPs could be employed during the Olympics to both disrupt targets and draw attention to the gangs' political causes.

As early as February 2023, Cyberint observed the pro-Russian hacktivist group NoName057(16) claiming successful DDoS attacks on Estonian institutions in retaliation for Estonia's Prime Minister's discourse expressing disappointment with the proposal of allowing Russian athletes participating to the Paris 2024 Olympic Games.

During the upcoming Paris 2024 Summer Olympics, hacktivist groups like NoName057(16), Anonymous Sudan, and members of HackNet, could launch disruptive attacks on Olympics-related network infrastructures, ticketing systems, credentials scanners, broadcasting networks, timing and scoring systems, as well as smartphone applications sharing essential information related to the games.

This year, amidst the Israel-Hamas war, pro-Russian groups may likely be followed by pro-Palestinian hacktivists who may direct attacks at the French government and critical infrastructures in Paris.

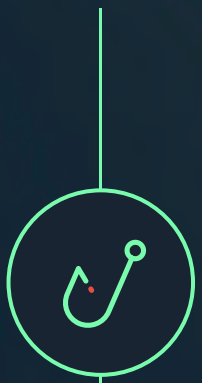
This will maximize the chaos during the Olympics and promote their political agenda. Specifically, organizations that directly or indirectly have relations with Israel must enhance their security measures, as they may face direct targeting by pro-Palestinian hacktivists.

A couple of months ago, Cyberint detected this Telegram post from the pro-Palestinian LulzSec hacktivist group. Active since 2011, LulzSec started their hacktivist operations sowing chaos online, before switching to more sophisticated attacks targeting high-profile organizations like Sony, PBS, and the CIA, mainly through website defacement and data leaks. While some of the group's original founding members were arrested in 2012, LulzSec have resumed their malicious activities against a range of worldwide organizations, conducting disruptive DDoS attacks and data breaches.

In March 2024, the group conducted a poll within their Telegram community to determine the next target country for their attacks. France emerged as the top choice, garnering 42% of all votes. In the same timeframe, a French member of the LulzSec group, going by the moniker Kizarush, sarcastically claimed to have joined the Olympic games and announced to have hacked the Paris 2024 Summer Olympics' admin panel.

Figure 13: LulzSec member claims to be actively targeting the Paris 2024 Summer Olympics

RECOMMENDATIONS FOR ORGANIZATIONS



PHISHING & FRAUD SCHEMES

TTo thwart phishing campaigns and fraud attempts, Olympics' staff and employees of organizations directly or indirectly tied to the Olympics should exercise added caution with unsolicited communications and verify the legitimacy of email senders.

Banks, insurance companies and organizations that manage a wide range of sensitive data should remain vigilant with solicitations and action requests that appear suspicious and that urge them to perform an operation on behalf of a customer or a colleague.

ACCOUNT TAKEOVER & MALWARE INSTALLATION

Organizations should strengthen their security posture by implementing Multi-Factor-Authentication (MFA) to introduce an additional layer of security and complicate threat actors' attempts of account takeovers and malware dissemination.

Organizations should instruct their employees to choose long, complex and unique passwords, and should systematically deactivate login credentials associated with former employees. It is also highly recommended to regularly monitor deep and dark web sources to proactively detect compromised credentials shared by cybercriminals and mitigate the threat.

DDoS ATTACKS

Critical infrastructures and institutions at risk of DDoS attacks should make sure to rely on valuable intelligence to remain aware of hacktivist groups' next moves, and invest in robust DDoS mitigation strategies, including scalable network infrastructure and real-time network monitoring.

RANSOMWARE ATTACKS & VULNERABILITY EXPLOITATION

Finally, organizations could lower the impact of potential ransomware attacks by creating and regularly maintaining data backups isolated from the main networks, and establishing a robust incident response plan to promptly mitigate attack attempts. Organizations are also highly advised to keep all their software and products up to date, and immediately mitigate any vulnerable component to prevent exploitation by attackers.

RECOMMENDATIONS FOR INDIVIDUALS

FRAUD SCHEMES

Olympics fans and the public should opt for official, secure payment methods when purchasing tickets or Olympic-related items, and make sure to download mobile applications from trusted and official sources only, to safeguard against fraud schemes.

PHISHING ATTACKS

The public should also exercise caution regarding any unexpected emails claiming to be from an official source and demanding urgent action. If in doubt, it is advisable to contact the official service provider directly to verify the email's authenticity. Following this practice will help prevent the installation of malware and the harvesting of sensitive data by malicious actors.

ACCOUNT ATTACKS

If there is suspicion of account intrusion by a threat actor, it is recommended to force log out from all devices and immediately change the password, opting for a long, complex and unique one.

WIFI ATTACKS

Tourists, Olympics fans, and the public at large are advised to avoid conducting sensitive mobile and/or web operations using unsecured public WiFi spots. Instead, it is recommended to log in from a password-protected WiFi network or use a VPN, which adds an extra layer of encryption and security. This will help safeguard sensitive data from potential interception by malicious actors.

DISINFORMATION CAMPAIGNS

Lastly, it is recommended that the public rely on official governmental sources for updates and alerts, especially with the proliferation of AI-driven disinformation aimed at spreading fear. This will avoid unnecessary panic and ensure proper information dissemination and smooth conduct of the games.

CONCLUSION

The Paris 2024 Summer Olympics are expected to face an unprecedented rise in cyber threats, including DDoS attacks, fraud and phishing, WiFi attacks, data breaches, account intrusions and malware installation.

Cyberint's investigation underscores a growing threat landscape, driven by motives like cyberespionage, political agendas, and financial gain. Advancements in AI also heighten concerns, as they enable sophisticated cyberattacks that are harder to detect and facilitate fraud and operations disruption.

Potential targets include the IOC, Olympic organizers, sponsors, local infrastructure, high-profile individuals in France, payment systems, athletes, tourists, and fans. Financial institutions, insurance companies, and data-driven sectors are also particularly vulnerable to targeted attacks.

In essence, the collective enthusiasm and widespread digital engagement of millions create a favorable environment for a wide range of cyberattacks before and during the games, highlighting the need for increased cybersecurity measures and vigilance.

SUMMARY

By combining optimal security hygiene with reliable, impactful intelligence, organizations, stakeholders and the public could better protect themselves from cyber threats during the Paris 2024 Summer Olympics, enabling them to fully enjoy the games without being get offside by unwanted security incidents.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972 3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House
14-18 Great Titchfield Street,
London, W1W 8BD

USA – TX

Tel: +1-646-568-7813
7250 Dallas Pkwy STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform's patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://Cyberint.com.

© Cyberint, 2024. All Rights Reserved.