Olympics 2024 Threats.
Wifi honeypots, Phishing, Bec, Domain spoofing and fake apps

Millions will be flocking to Paris where the Olympics will be held over the next 16 days, starting yesterday. It will be the first in-person summer games since pandemic restrictions were lifted. **While the French capital will host over 10,000 athletes of various disciplines, there are fears that it could also become a hunting ground for cybersecurity threat actors.** As a security expert, I suggest cautioning people against possible threats.

An analysis of nearly 25,000 free Wi-Fi spots in Paris showed that almost 25 percent of these networks had weak or no encryption. This means that travelers using public Wi-Fi at large events like this face significant cybersecurity risks, such as data theft and identity fraud.

Additionally, almost one in five (20 percent) were configured with WPS, an outdated and easily compromised algorithm, rendering them highly susceptible to WPS attacks that could result in data loss. *Only six percent of the analyzed networks used the latest WPA3 security protocol.*

Wi-Fi threats are particularly concerning in such a densely populated event. Cybercriminals often exploit open and insecure Wi-Fi networks to carry out a variety of attacks. These threats include:

1. Man-in-the-Middle Attacks - In this type of attack, the hacker intercepts the communication between two parties, allowing them to capture sensitive data such as login credentials, credit card numbers, and personal information.

2. Evil Twin Attacks - Cybercriminals set up a rogue Wi-Fi network with a name similar to a legitimate network. When users connect to the fake network, their data can be intercepted, and malicious software can be injected into their devices.

3. Data Sniffing - Attackers use software to capture data being transmitted over unsecured Wi-Fi networks. This data can include emails, browsing history, and other personal information.

Like the athletes training for the summer of sport in France, cybercriminals have also prepared an unsavory welcome for the millions of people heading for Paris hotels, fan zones, and events. They might set up fake access points or compromise legitimate networks to intercept and manipulate data transfers. Open and misconfigured Wi-Fi networks are desirable to criminals, as they enable the theft of passwords, credit card details, and other sensitive user data.

Apart from Wi-Fi vulnerabilities, the global sporting event has also attracted the eyes of **phishing scammers**. A Cloudflare analysis points towards a rise in phishing and malicious emails related to the Paris Olympics. From January 2024 up to late July, the firm processed over half a million emails containing “Olympics” or “Paris 2024” in the subject, out of which 1.5 percent were spam, and 0.2 percent were malicious.

Further, there are possibilities of scams happening through a setup known as **Wi-Fi Honeypots**, which are fake Wi-Fi hotspots set up by attackers to lure unsuspecting users, say experts.
I think people must pay great attention to Free Public Wi-Fi or mimic legitimate networks (e.g., a coffee shop's Wi-Fi). Once you connect to a honeypot, attackers can easily monitor your traffic, steal your data, and even inject malware into your device.
To protect against these threats, users should avoid connecting to unknown Wi-Fi networks, use VPNs for secure browsing, and ensure their devices have updated security software.

Business Email Compromise (BEC) is another significant threat projected to occur leading up to the Games, during the Olympics, and even persist for several weeks after the Games.
BEC is a sophisticated cyberattack where criminals use email fraud to deceive and manipulate individuals within an organization into making unauthorized payments or revealing confidential information. Unlike traditional phishing attacks, BEC typically involves targeted attacks on specific

individuals, often executives or finance department employees, who have access to company finances and sensitive data.

BEC attacks usually start with extensive research. Cybercriminals gather information about the organization, its structure, and key personnel. They may use social engineering techniques to gain access to an employee's email account or spoof email addresses to appear as if they are coming from a legitimate source within the organization. Once they have access or have successfully spoofed an email address, they send carefully crafted emails that appear to be urgent requests from senior executives or trusted business partners.

There are several types of BEC attacks:

1. CEO Fraud - The attacker poses as the company's CEO or another high-ranking executive and sends an email to an employee in finance, instructing them to transfer funds to a fraudulent account.

2. Account Compromise - The attacker hacks into an employee's email account and uses it to request invoice payments to fraudulent bank accounts.

3. Attorney Impersonation - The attacker impersonates a lawyer or legal representative, often claiming to handle confidential or time-sensitive matters, and pressures the recipient to act quickly without verifying the request.

4. Data Theft - The attacker targets HR or finance departments to obtain personally identifiable information (PII) or tax statements, which can be used for future attacks.

The impact of BEC can be devastating, resulting in significant financial losses and damage to an organization's reputation. *According to the police authorities, BEC scams have cost businesses billions of dollars worldwide.*
To protect against this threat, organizations should implement robust security measures such as multi-factor authentication (MFA), advanced email filtering, and employee training programs to recognize and report suspicious emails. Additionally, establishing strict protocols for verifying significant financial transactions, such as confirming requests through multiple channels, can help prevent these attacks. Regularly updating and patching systems, as well as monitoring email accounts for unusual activity, are also crucial steps in safeguarding against BEC threats.

Further, **domains spoofing** the legitimate Olympics website. Just to be clear, domain spoofing is a cyberattack method where attackers create domain names that closely mimic legitimate ones to deceive users. They often use slight variations in spelling, added or omitted characters, or different top-level domains (TLDs) to trick people into believing they are interacting with a genuine website or email address.
In domain spoofing, attackers might set up fake websites that look almost identical to real ones, or send emails from addresses that appear to be from trusted sources. The goal is to steal sensitive information such as login credentials, financial details, or personal data. These spoofed domains can be used in phishing attacks to lure victims into clicking malicious links or downloading malware.
To protect against domain spoofing, organizations should implement email authentication protocols like SPF, DKIM, and DMARC, and regularly monitor for similar domain registrations.
Educating users about recognizing suspicious domain names and verifying website authenticity can also help. Ensuring websites use SSL/TLS certificates for secure connections adds an extra layer of protection.

And, one of the last threats planned for these Olympics are the **fake mobile apps** masquerading as transport, booking, or other planning apps are also certain to be leveraged by fraudsters during the event, cybersecurity firms say, which puts users at risk.

Travelers going to the Olympics event are equally vulnerable to these threats.

To stay safe, I recommend using secure networks, avoiding public Wi-Fi for sensitive transactions, and being cautious of emails and links related to the Olympics.

Author: Alessandro Civati.