June 10, 2024

Heightened Cyberthreats Loom Over Euro 2024 Amidst Global Geopolitical Tensions

The UEFA Euro 2024 takes place in Germany from June 14 to July 14, 2024. Poised to be a major international event, it attracts millions of spectators in person and online. Given the scale and global interest in the tournament, it is a high-value target for cybercriminals and nation-state actors. This threat was highlighted during the Tokyo 2021 Olympics, where reports of millions of cyberattacks were prevented, underscoring the scale of cyberthreats to large international events.

Key Cybersecurity Threats

Ticket Fraud and Phishing Attacks

Cybercriminals may exploit the excitement around ticket sales to deceive fans with fraudulent websites and phishing emails. This threat was evident during the 2022 World Cup, where phishing emails promising free tickets or streaming links were prevalent. Such incidents can result in financial losses for fans, stolen personal information and decreased trust in official ticketing platforms.

DoS (Denial of Service) Attacks

DoS and DDoS (Distributed Denial of Service) attacks pose a significant threat as they could disrupt live broadcasts, stadium operations and critical infrastructure. Recently, the e-sports industry in Korea has been grappling with DDoS attacks, causing disruptions in matches and practice time for teams. One of the most affected events is LCK, the premier league for Riot's popular online game League of Legends. In matches held last February, the games were interrupted by DDoS attacks. A best-of-three match, which typically lasts about two hours, unexpectedly extended over six hours due to the DDoS attacks. Due to the lengthy delays, matches were then forced to be played without spectators in the crowd. In response, the organizers set up their own offline servers and restored normal match operations within a month. Despite these fixes, the disruption had a significant impact, particularly on some teams like T1, which were heavily affected.

Deepfake Technology

The use of deepfake videos and voice cloning to impersonate athletes, officials or other public figures is a growing concern. Deepfake technology has become increasingly accessible with numerous repositories on platforms like GitHub and services offered on Telegram. This

technology helps to spread misinformation, cause reputational damage and potentially blackmail or defraud victims.

Nation-State Cyber Attacks

Nation-state actors may target critical infrastructure, such as power grids and public transportation systems, to cause widespread disruption and chaos. During the 2018 PyeongChang Winter Olympics in South Korea, the Olympic Destroyer worm targeted the event's IT infrastructure, causing service interruptions and widespread disruptions. It took down the official Olympics website and the Wi-Fi at the stadium and affected the event's broadcasts. The UK government confirmed that the Russian GRU's cyber unit attempted to disguise itself as North Korean and Chinese hackers when it targeted the opening ceremony of the 2018 Winter Games. It went on to target broadcasters, a ski resort, Olympic officials and sponsors of the 2018 games.

Hacktivist and Terrorist Attacks

The Euro 2024 tournament in Germany faces heightened security concerns, including the risk of terrorist threats. With the event drawing global attention, it presents a high-profile target for hacktivist and terrorist groups aiming to disrupt the proceedings and garner international media coverage. The ongoing geopolitical tensions, such as the active conflicts in Ukraine and Israel and potential threats in Taiwan, exacerbate these risks. The convergence of large crowds, critical infrastructure and the presence of international figures at Euro 2024 amplifies the potential for terrorist activities.

Reasons for Concern

Numerous organizations are involved with Euro 2024, engaging in advertising campaigns, sponsorships and selling apparel, tickets and services. The UEFA is surrounded by many such entities. Additionally, critical infrastructure and public transportation or logistics in Germany, the host of Euro 2024, face an elevated risk of cyberattacks from cybercriminals, hacktivists and nation-state actors. Current geopolitical tensions are heightened by ongoing conflicts in Ukraine and Israel, along with looming threats in Taiwan.

Recommendations

Fans should only purchase tickets from official UEFA channels and be cautious of emails or links offering free tickets, streaming or prize draws. It is important to use strong, unique passwords and enable multi-factor authentication where possible.

Organizations and government institutions should implement robust DDoS protection measures, including traffic monitoring and anomaly detection systems. They should also have a response plan in place to quickly address any disruptions.

Organizations that offer services to fans should ensure their stakeholders' awareness of deepfake technology. Use verification mechanisms for official communications and social media channels, and educate customers and the broader public on identifying deepfakes.

Collaborate with national cybersecurity agencies to protect from and respond to nation-state threats. Conduct security audits, tabletop exercises and red-teaming drills to ensure preparedness. Monitor online platforms for planning or chattering about potential attacks.

Additionally, vendor security is crucial. All third-party vendors must comply with stringent security standards to prevent supply chain attacks.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.