Jogos Olímpicos de 2024: quais os riscos em jogo?

dinheirovivo.pt/1398856832/jogos-olimpicos-de-2024-quais-os-riscos-em-jogo/

Bruno Castro

A tentação de perturbar os Jogos Olímpicos de 2024 em Paris, será sem dúvida, imensa para a comunidade cibercriminosa, que vai desde cibercriminosos à procura de sua oportunidade de “ganhar dinheiro fácil”, passando por hacktivistas a querer impor uma ideologia, até a intervenientes estatais com interesses geopolíticos de toda a espécie. Impõem-se a questão: que ameaças e riscos cibernéticos a França enfrentará durante os Jogos de Paris e se realmente estará preparada para um tsunami cibernético que se aproxima rapidamente das suas fronteiras digitais?

Um dos principais riscos está naturalmente relacionado com as atuais tensões geopolíticas e as suas implicações no evento mundial dos Jogos Olímpicos em Paris, cuja possibilidade de disrupção cibernética não pode ser ignorada - sendo o pior cenário, a coordenação entre um ciberataque e um ataque físico que traria certamente um impacto de larga escala em Paris.

Tal como observado nas edições anteriores dos Jogos Olímpicos, o contexto geopolítico tem um impacto enorme no cenário de ciberameaças, nomeadamente, pelo potencial inerente a este grande evento para conduzir operações, que vão muito além das questões desportivas. Tendo em conta a proibição de entrada na competição da Rússia e da Bielorrússia nos Jogos de Paris de 2024, devido à suspensão do Comité Olímpico Russo, uma vez que este colocou sob a sua autoridade várias organizações desportivas de quatro regiões ocupadas da Ucrânia, é altamente provável que os Jogos sejam alvo de operações cibernéticas russas e/ou bielorrussas como medida de retaliação para minar a reputação de França.

Em simultâneo, grupos cibercriminosos russos, supostamente categorizados como hacktivistas cibernéticos podem também tirar partido da cobertura mediática dos Jogos para promover narrativas de propaganda como uma contribuição para o esforço russo de minar a França. Estas operações consistem principalmente em ciberataques DDoS (Distributed Denial of Service) sobre organizações ou instituições de relevo que permitam, utilizando o sucesso dos ciberataques desenvolvidos, como meio para transmitir mensagens políticas.

Outra ameaça que estará certamente incluída na estratégia de ciberdefesa está relacionado com a espionagem individual para fins de inteligência. Os Jogos atraem personalidades de destaque, desde atletas famosos, CEO’s a diplomatas e inúmeras personalidades políticas - ora, temos reunidos num só espaço, os alvos preferidos dos serviços de inteligência que procuram informações estratégicas que possam vir a criar vantagem geopolítica nos conflitos mundiais da atualidade. Ao mesmo tempo, estas campanhas de ciberespionagem também podem tirar partido da atenção concentrada

nas ameaças mais visíveis durante os Jogos para permanecerem “fora do radar” e assim comprometerem alvos mais críticos. Discreta por natureza, é pouco provável que este tipo de operação tenha impacto imediato durante o evento, contudo e ainda assim, pode resultar em consequências a médio e longo prazo.

Uma outra ameaça a ter em conta, e esta é preponderante para os cibercriminosos, são as campanhas massivas de ciberataques com objetivos financeiros, desde scams através de websites falsos, phishing com oferta de “última hora” e até com o envolvimento de ações de engenharia social através de chamadas telefónicas enganadoras para suportar o scam.

Os temas mais recorrentes para este tipo de ameaças serão certamente em torno de apostas, bilhetes para entrada e viagens servindo-se de diferentes técnicas para roubar credenciais ou dados para posteriormente serem monitorizados, seja através da venda das informações roubadas ou de extorsão de dinheiro às próprias vítimas.

Em edições anteriores dos Jogos Olímpicos foi salientada a recorrência de ciberameaças que afetam este tipo de eventos e, infelizmente, os Jogos Olímpicos de Paris em 2024 certamente não serão a exceção – são um alvo de eleição preferencial para os principais intervenientes do cibercrime dispostos a atacar a reputação da França, como nação por si só mas também como membro da NATO, colocando em causa a sua capacidade de defesa, a recolher informações estratégicas, e a explorar vulnerabilidades para obter benefícios financeiros.

Sabe-se que a agência francesa de cibersegurança (ANSSI), juntamente com o governo, têm-se preparado em grande medida para todas as implicações inerentes à organização deste evento mundial, com particular atenção nos últimos dois anos, ao realizar por exemplo, diversos simulacros cibernéticos, ao aumentar também a sensibilização para os riscos em larga escala e ao tomar medidas preventivas para proteção de todas as entidades que estarão envolvidas nos Jogos, incluindo, as infraestruturas críticas como energia e transportes. Resta apenas saber se todos os esforços serão suficientes para evitar o tsunami cibernético que se avizinha.

Fundador & CEO da VisionWare e especialista em Cibersegurança e Investigação Forense