Previstos milhões de ciberataques aos Jogos Olímpicos em Paris. França é alvo para vários países

observador.pt/2024/06/12/previstos-milhoes-de-ciberataques-aos-jogos-olimpicos-em-paris-franca-e-alvo-para-varios-paises

Alcance mundial do evento e crescente digitalização da organização transforma-o num alvo apetecível para hackers. Ataques podem ter origem na Rússia, Azerbaijão, Irão ou até mesmo internamente.

Sistemas 100% digitalizados, desde cartões de acesso dos atletas, passando pela vigilância do recinto da aldeia olímpica até à transmissão das provas. A organização dos Jogos Olímpicos de Paris primou pela automatização do evento desportivo, mas esta não se separa do aumento da vulnerabilidade a **ciberataques**. As conclusões são do recente relatório do Visionware Threat Intelligence Center, que aborda as principais ameaças à maior competição desportiva do mundo e faz uma previsão do número de ciberataques relacionados com o evento — são esperados cerca de 3.5 mil miliões, um aumento significativo em relação às edições anteriores.

Uma das justificações apresentadas para a especial vulnerabilidade do evento e do país em que este decorre é o **apoio diplomático e financeiro de França à Ucrânia** e o facto de os atletas russos só poderem competir na qualidade de atletas neutros. Este ano, a Rússia e a Bielorrússia estão impedidas de participar em Paris 2024 devido à invasão da Ucrânia em fevereiro de 2022. É do Kremlin que parte uma fatia significativa dos ciberataques ao nível mundial.

O conflito israelo-palestiniano também pode vir a ser um fator que potencie o número de ameaças. A postura diplomática francesa pode ser vista pelos apoiantes da Palestina como pró-Israel e servir de fundamento para operações cibernéticas maliciosas. “O Irão, o lémen, as milícias do Hezbollah ou o próprio Hamas, podem também utilizar as suas capacidades ciberofensivas para afetar os Jogos Olímpicos”, destaca-se no documento.

Também o Azerbaijão é tido como um dos países que pode a tornar França num alvo enquanto decorrerem as provas olímpicas, de 24 de julho a 11 de agosto, já que tem lançado campanhas de desinformação sobre a alegada incapacidade de Paris em receber o evento. Além de ataques promovidos por países, também são esperados por parte de grupos de ativistas franceses para fins de **ativismo político, social ou ecológico**.

De acordo com a Visionware, que realizou o estudo em causa, o número de ataques aos Jogos Olímpicos têm aumentado progressivamente, uma vez que o sistema associado ao evento se tem vindo a digitalizar cada vez mais. Em 2012, em Londres, contabilizaram-se 212 milhões de ciberataques. Em 2021, nos jogos que se realizaram em Tóquio, o número subiu para 450 milhões. Agora, perante o **contexto geopolítico atual e toda a tecnologia envolvida** na organização, espera-se que o número aumente significativamente, para os tais mais de três biliões de ataques.

Gráfico do relatório “Jogos Olímpicos Paris 2024” da autoria da Vision Ware Threat Intelligence

“O evento terá um impacto mediático astronómico e com a imensa tecnologia em jogo – entre outros, os sistemas de captação de vídeo para a televisão ou para os árbitros, as câmaras CCTV, os sistemas de alarme, e os leitores de cartões e bilhetes, os riscos cibernéticos serão imensos”, destaca-se no relatório da empresa de cibersegurança.

Espetadores devem ficar atentos a campanhas de *phishing* e bilhetes falsos. Atletas famosos podem ser alvos para interferir no evento

Os ciberataques com propósitos lucrativos são, habitualmente, os mais frequentes durante os Jogos Olímpicos. Consistem na realização de **campanhas de *phishing* e esquemas de fraude** e falsificação de bilhetes ou apostas online e são frequentemente dirigidos aos espetadores, patrocinadores e indústrias associadas aos Jogos. A Visionware alerta para a vulnerabilidade dos espetadores, que muitas vezes são turistas, e que, por regra, “não utilizam boas práticas de cibersegurança e não estão bem informados sobre o cenário de ameaças”. As redes Wi-Fi públicas, incluindo as de

hotéis, cafés e estádios para eventos, não são normalmente encriptadas e podem ser exploradas por cibercriminosos que pretendem roubar informações sensíveis. Os turistas olímpicos tornam-se, assim, “alvos fáceis”.

São igualmente esperados ataques de “desestabilização/perturbação”, que incluem sabotagem informática, “hacktivismo” e comprometimento e divulgação de dados. Este tipo de interferências cumprem fins de **ativismo político ou social**, representando uma ameaça crescente, sendo provável que os Jogos Olímpicos sirvam de palco para reivindicações políticas, ainda mais num momento em que França atravessa uma crise política.

Como indica o relatório, este tipo de operações são mais complexas e, por isso, são normalmente promovidas por Estados, estando associadas a tensões geopolíticas que afetam os países anfitriões e os países participantes. Os atletas, especialmente os mais conhecidos, são alvos de elevado valor porque a popularidade dos Jogos Olímpicos e a geração de receitas depende, em grande medida, da sua participação e desempenho. A empresa de cibersegurança alerta mesmo para o facto de as agências e os peritos antidoping correrem um risco elevado de serem alvo de ataques informáticos.