French cyberwarriors ready to test their defense against hackers and malware during the Olympics

May 4 2024, by John Leicester

A cyber-security experts hold a tablet at the Yves du Manoir stadium, Friday, May 3, 2024 in Colombes, outside Paris. Cyber-security teams working to protect the Paris Games from hackers and other attackers aren't willing to divulge too much detail about their work. But they no doubt that cyber-criminals are going to keep them busy. Credit: AP Photo/Michel Euler

Just like the Olympic athletes, the cyberwarriors that will be crucial for the success of the Paris Games are deep into training for the big event.

They have turned to friendly hackers to probe their cyberdefenses, like boxers who use sparring partners to ready them for a championship fight. They have studied and analyzed the strengths, tactics and weaknesses of their opponents. Those could be anyone from teenage showoffs and ransomware gangs to Russian military hackers with a track record of malicious cyberattacks.

But unlike the 10,500 Olympians who will converge on France's capital in July, the cybersecurity engineers behind the Games are hoping to stay out of the spotlight. For them, the equivalent of a medal will be getting through the Olympics—and Paralympics—without a major incident. It would mean that their layers of digital defenses stand up to attempts to paralyze computer and information systems vital for the Games.

"My dream for the Olympics is that technology and cybersecurity aren't talked about, because that will mean it was a non-issue," said Jérémy Couture, who heads the Paris Games organizers' cybersecurity hub. Its job of spotting, analyzing and responding to cyberthreats is so sensitive and critical to the Games' success that event organizers keep its location secret.

While those in charge of fending off cyberattacks during the Games aren't willing to divulge much detail about their work, they have no doubt malicious hackers are going to keep them busy this summer. Those could range from cybercriminals to thrill-seeking teenage troublemakers to Russian military intelligence operatives with a track record of damaging cyberattacks.

Targets are not limited to the Games themselves but also infrastructure essential for them, such as transport networks or supply chains.

Attackers could include "hacktivists" seeking to make a political statement and cyberextortionists bent on lucre. And often these days, it can be difficult to distinguish a hacktivist from a state-sponsored cyber operator posing as one.

Among the most threatening cyberadversaries are countries who might want to embarrass and exact costs on France and the International Olympic Committee with proven offensive hacking chops. Russia tops the list of suspects.

Because of Russia's ongoing war in Ukraine, Olympic organizers have barred it from competing in team events at the Paris Games and will only allow some individual Russians to compete as neutrals. Russia also has beef with France for supplying Ukraine with weapons and military training and because it has become one of Moscow's fiercest critics in Europe.

Vincent Strubel, who heads France's national cybersecurity agency, known by its French initials, ANSSI, called the cyberthreats level facing the Games unprecedented.

Cyber-security experts work at the Yves du Manoir stadium, Friday, May 3, 2024 in Colombes, outside Paris. Cyber-security teams working to protect the Paris Games from hackers and other attackers aren't willing to divulge too much detail about their work. But they no doubt that cyber-criminals are going to keep them busy. Credit: AP Photo/Michel Euler

"There will be cyberattacks during the Games and the Paralympics," Strubel said at a briefing Friday. "Some won't be serious. Some will be serious but won't have an impact on the Games. And perhaps there will be some that are serious and liable to have an impact on the Games."

He said the agency has trained "enormously" and more than ever before, so things will go well. "I think we have managed to stay a step ahead of the attackers."

While Strubel named Russia as among the actors who attack France "a bit recurrently," he said it makes no sense to focus on one actor in particular. "We are preparing for everything."

An especially aggressive unit of Russia's GRU military intelligence agency dubbed Sandworm is blamed by Western nations for using malware dubbed "Olympic Destroyer" to disrupt the opening ceremony of the 2018 Winter Games in Pyeongchang, South Korea. It's the same unit accused of so-called wiper attacks on Ukraine's power grid and the 2017 NotPetya virus that caused over $10 billion in damage worldwide.

Paris' cybersecurity teams have sought to learn from those experiences, consulting technicians who also worked in Pyeongchang.

Sweden-based cybersecurity firm Outpost24 gave a broad thumbs-up to Paris' preparations in a report this week, but said its research still found gaps in the Games' online infrastructure. The rating it gave was "not quite a gold medal, but certainly a silver."

"Just as pickpockets and ticket touts target groups of tourists, cybercriminals will be conscious of increased online traffic towards the Paris 2024 games and will hope to capitalize," the report said.

Citation: French cyberwarriors ready to test their defense against hackers and malware during the Olympics (2024, May 4) retrieved 17 July 2024 from https://techxplore.com/news/2024-05-french-cyberwarriors-ready-defense-hackers.html