Russian hackers 'Fancy Bear' likely breached Olympic drug-testing agency and DNC, experts say

ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-agency-dnc-experts-say-1577508

Hyacinth Mascarenhas August 23, 2016

People walk out of the Russian Olympic Committee headquarters in Moscow Reuters/Maxim Shemetov

The same hackers who infiltrated the World Anti-Doping Agency (WADA) website after its damning report on the Russian government's major cover-up of doping during the 2014 Sochi Games is likely the team behind the breach of the Democratic National Committee in July, cybersecurity experts said. WADA's nearly 100-page report resulted in a ban on Russian athletes from this summer's Rio Olympics.

Researchers at Arlington-based cybersecurity firm ThreatConnect believe that the cybercriminals behind the breach were part of the decade-old Russian hacking group "Fancy Bear." Last week, WADA and the Court of Arbitration for Sport (CAS) said they were targeted by hackers with so-called phishing emails sent to users of the database claiming to be official WADA communications requesting their login credentials.

After reviewing the two domains provided in the WADA alert, the researchers found that "the sites were recently registered and their registration and hosting information are consistent with Russian Fancy Bear tactics, techniques and procedures (TTPs)". They also identified another domain registered by the same threat actors that spoofs the official CAS domain.

ThreatConnect director of research operations Toni Gidwani told The Guardian that the cybersecurity team believes the attack was also a form of retaliation against Yuliya Stepanova, the Russian runner and doping whistleblower who helped uncover the state-sponsored doping scandal. The middle-distance runner, whose WADA and email accounts were hacked on 13 August, was called "Judas" by Vladimir Putin. Stepanova was then forced to go into hiding in the United States with her husband Vitaly, a former Russian anti-doping official.

"They attacked her email, they got her records out of WADA," Gidwani said. "There's very much a retaliatory aspect to it and a way of intimidating anybody who might be thinking about speaking out."

The firm also noted that both the phishing and Stepanova's compromise are likely a part of "targeted activity by Russian actors in response to the whistleblower and the WADA's recommendation to ban all Russian athletes from the Olympic and Paralympic games" in Rio.

"Successful operations against these individuals and organisations could facilitate Russian efforts to privately or publically intimidate them or other potential whistleblowers," ThreatConnect researchers wrote in a blog post. "At this time, we are skeptical of @anpoland's origins but cannot determine the extent to which, if any, they are a Russian platform similar to Guccifer 2.0 or DCLeaks."

ThreatConnect added that the recent hack highlights the strong, long-running connection between sports and Russian political figures, saying they expect to see more Russian cyberattacks targeting Professor Richard McLaren and Dr Grigory Rodchenkov who were key sources in the doping scandal investigation.

"Russian activity targeting these organisations is an important example of how Russia responds to wide-reaching current events that have negative implications for Moscow," the firm noted. "Organisations involved in such events can reasonably expect to experience targeted Russian cyber operations that ultimately facilitate retaliatory influence or propaganda efforts against them. Knowledge of this TTP, and others associated with Russian APT activity, can help those organisations augment their security posture and defend against such retaliation."

Multiple cybersecurity firms including CrowdStrike and ThreatConnect have provided evidence linking the Russian government to the DNC infiltration reportedly carried out by hacker groups Cosy Bear and Fancy Bear. Following a brief Twitter suspension, 'lone wolf'

hacker Guccifer 2.0, who also claimed responsibility for the DNC hack, recently released more files, memos and dossiers from the Democratic Congressional Campaign Committee (DCCC).

The Kremlin, on the other hand, has vehemently denied playing any role in the hacks.

Rio 2016 Olympics