Russian state hackers behind San Francisco airport hack

By Catalin Cimpanu

Published: 2020-04-14 · Archived: 2026-04-06 00:41:44 UTC

Hackers believed to be operating on behalf of the Russian government have hacked two websites operated by the San Francisco International Airport, cyber-security firm ESET said today.

The hacks took place last month, in March, according to a data breach notification [PDF] posted on the airport's website.

The attacks targeted SFOConnect.com, a website used by airport employees, and SFOConstruction.com, a portal used by airport construction contractors.

According to San Francisco airport officials, hackers breached both websites and planted code that exploited an Internet Explorer bug to steal login credentials.

But in a series of tweets today, ESET said that "the targeted information was NOT the visitor's credentials to the compromised websites, but rather the visitor's own Windows credentials."

"The intent was to collect Windows credentials (username/NTLM hash) of visitors by exploiting an SMB feature and the file:// prefix," the ESET research team said.

NTLM hashes can be cracked to obtain a cleartext version of a user's Windows password. If the hackers had access to the airport's internal network, they could have used credentials obtained from airport employees to spread laterally through the airport's internal network to conduct reconnaissance, data theft, or sabotage.

ESET links hack to Energetic Bear

ESET said the attack was carried out by a threat actor known as Energetic Bear (also known as DragonFly). The group has been active since 2010 and is believed to be operating on behalf of the Russian government.

The group is one of Russia's most active state-sponsored entities. Over the past decade, Energetic Bear hackers have been behind a widespread hacking campaign that targeted organizations all over the world.

The group's primary targets have been organizations in the energy sector -- hence its name of Energetic Bear -- primarily those located in the Middle East, Turkey, and the US.

However, Energetic Bear has also recently began targeting other types of organizations as well, including companies in the aerospace and the aviation sector, according to a report published by Kaspersky in April 2018, and an alert sent at the time by the US Department of Homeland Security.

In fact, the same Kaspersky report details a series of watering hole attacks carried out by Energetic Bear that used the same "*file:// prefix*" trick to obtain NTLM hashes from users visiting a compromised website.

> The recently reported breach of #SFO airport websites is in line with the TTPs of an APT group known as Dragonfly/Energetic Bear. The intent was to collect Windows credentials (username/NTLM hash) of visitors by exploiting an SMB feature and the file:// prefix #ESETresearch 1/2 pic.twitter.com/pDZMdb49lb
>
> — ESET research (@ESETresearch) April 14, 2020

"This technique has been used for years by Energetic Bear/DragonFly," Matthieu Faou, malware researcher at ESET, told *ZDNet* in an interview today.

We also asked Faou to expand on the company's tweets and inquired if this hack is part of a new campaign aimed at the US aviation sector.

"We don't have any information about the compromise of another airport website," Faou told us. "According to ESET telemetry, the other websites that were recently compromised are mainly media websites in Eastern Europe."

San Francisco airport reset all employee passwords

Faou said that when they detected the technique being used in the wild again, they "reported it immediately to the SFO airport team" who "quickly removed the malicious piece of code from their website."

Airport officials than followed through by forcing password resets for "all SFO related email and network passwords on Monday, March 23, 2020."

The password reset is enough to prevent hackers from using the stolen NTLM hashes for any future intrusions.

However, the two websites were also used by other users who were not airport employees. Through its public security breach announcement, the San Francisco airport is now urging users who recently visited the site to take similar actions and reset their Windows passwords.
