

A hacking group “sponsored” by Iran’s government is launching disruptive cyberattacks against a wide range of U.S. companies, including healthcare providers and transportation firms, according to a cybersecurity alert published by the U.S. Homeland Security Department (DHS) on Wednesday.

The warning, jointly authored by the FBI and DHS’ Cybersecurity and Infrastructure Security Agency, said the hackers were exploiting old software vulnerabilities in products made by Microsoft and Fortinet to break into victim computer networks. While the vulnerabilities were patched, some customers haven’t updated their networks.

On Tuesday, Microsoft said in a blog post that it had observed six different Iranian hacking groups deploying ransomware since September 2020.

Ransomware typically functions by encrypting a computer’s data, leaving it inaccessible until an extortion payment is sent to the hackers.

“As Iranian operators have adapted both their strategic goals and tradecraft, over time they have evolved into more competent threat actors capable of conducting a full spectrum of operations,” the Microsoft analysis reads.

A spokesperson for Iran’s mission to the United Nations did not immediately respond to a request for comment.

*Reporting by Christopher Bing Editing by Chris Reese and Gareth Jones*

*The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team*

Facebook Comments