Chinese hackers breached US govt email accounts: Microsoft

July 13 2023, by Chris Lefkow

China-based hackers seeking intelligence information breached the email accounts of a number of US government agencies, Microsoft said.

Chinese-based hackers seeking intelligence information breached the email accounts of a number of US government agencies, computer giant Microsoft said.

"The threat actor Microsoft links to this incident is an adversary based in China that Microsoft calls Storm-0558," the company said in a blog post late Tuesday.

Microsoft said Storm-0558 gained access to email accounts at approximately 25 organizations including government agencies.

Microsoft did not identify the targets but a US State Department spokesperson said the department had "detected anomalous activity" and had taken "immediate steps to secure our systems."

"As a matter of cybersecurity policy, we do not discuss details of our response and the incident remains under investigation," the spokesperson said.

According to The Washington Post, the breached email accounts were unclassified and "Pentagon, intelligence community and military email accounts did not appear to be affected."

But the paper reported Wednesday evening, quoting US officials, that State Department email accounts and that of Commerce Secretary Gina Raimondo were hacked. Raimondo's agency has angered China by imposing tough export controls on Chinese technologies.

CNN, citing sources familiar with the investigation, said the Chinese hackers targeted a small number of federal agencies and the email accounts of specific officials at each agency.

In the blog post, Charlie Bell, a Microsoft executive vice president, said "we assess this adversary is focused on espionage, such as gaining access to email systems for intelligence collection.

"This type of espionage-motivated adversary seeks to abuse credentials

and gain access to data residing in sensitive systems," Bell said.

US National Security Adviser Jake Sullivan addressed the hack in an appearance on Wednesday on ABC's Good Morning America, and said it had been detected "fairly rapidly."

"We were able to prevent further breaches," Sullivan said.

"The matter is still being investigated, so I have to leave it there because we're gathering further information in consultation with Microsoft and we will continue to apprise the public as we learn more," Sullivan said.

Espionage and data theft

Microsoft said Storm-0558 "primarily targets government agencies in Western Europe and focuses on espionage, data theft, and credential access."

The Redmond, Washington-based company said it had launched an investigation into "anomalous mail activity" on June 16.

"Over the next few weeks, our investigation revealed that beginning on May 15, 2023, Storm-0558 gained access to email accounts affecting approximately 25 organizations including government agencies as well as related consumer accounts.

"They did this by using forged authentication tokens to access user email using an acquired Microsoft account consumer signing key," the company said. "Microsoft has completed mitigation of this attack for all customers."

US Senator Mark Warner, chairman of the Senate Select Committee on Intelligence, said the panel is "closely monitoring what appears to be a

significant cybersecurity breach by Chinese intelligence."

"It's clear that the PRC is steadily improving its cyber collection capabilities directed against the US and our allies," Warner said in a statement.

Disclosure of the Chinese hacking comes on the heels of trips to China by US Secretary of State Antony Blinken and Treasury Secretary Janet Yellen and the shooting down by the United States of a Chinese surveillance balloon.

In May, Microsoft said state-sponsored Chinese hackers called "Volt Typhoon" had infiltrated critical US infrastructure networks.

Microsoft highlighted Guam, a US territory in the Pacific Ocean with a vital military outpost, as one of the targets in that attack, but said "malicious" activity had also been detected elsewhere in the United States.

"Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises," the company said at the time.

Microsoft's May statement coincided with an advisory released by US, Australian, Canadian, New Zealand and British authorities warning that the hacking was likely occurring globally.

China denied the allegations, describing the Microsoft report as "extremely unprofessional" and "scissors-and-paste work."

"It is clear that this is a collective disinformation campaign of the Five Eyes coalition countries, initiated by the US for its geopolitical

purposes," foreign ministry spokeswoman Mao Ning said, referring to the security alliance of the United States and its Western allies that wrote the report.