Source : www.thehindu.com Date : 2021-06-29

MICROSOFT SAYS NEW BREACH DISCOVERED IN PROBE OF SUSPECTED SOLARWINDS HACKERS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Microsoft later said the group had compromised its own employee accounts and taken software instructions governing how Microsoft verifies user identities. | Photo Credit: AP

(Subscribe to our Today's Cache newsletter for a quick snapshot of top 5 tech stories. Click here to subscribe for free.)

Microsoft said on Friday an attacker had won access to one of its customer-service agents and then used information from that to launch hacking attempts against customers.

The company said it had found the compromise during its response to hacks by a team it identifies as responsible for earlier major breaches at SolarWinds and Microsoft.

Microsoft said it had warned the affected customers. A copy of one warning seen by Reuters said the attacker belonged to the group Microsoft calls Nobelium and that it had access during the second half of May.

"A sophisticated Nation-State associated actor that Microsoft identifies as NOBELLIUM accessed Microsoft customer support tools to review information regarding your Microsoft Services subscriptions," the warning reads in part. The U.S. government has publicly attributed the earlier attacks to the Russian government, which denies involvement.

When Reuters asked about that warning, Microsoft announced the breach publicly.

After commenting on a broader phishing campaign it said had compromised a small number of entities, Microsoft said it had also found the breach of its own agent, who it said had limited powers.

Also Read | 78% companies expect another SolarWinds-style hack, survey finds

The agent could see billing contact information and what services the customers pay for, among other things.

"The actor used this information in some cases to launch highly-targeted attacks as part of their broader campaign," Microsoft said.

Microsoft warned affected customers to be careful about communications to their billing contacts and consider changing those usernames and email addresses, as well as barring old usernames from logging in.

Microsoft said it was aware of three entities that had been compromised in the phishing campaign.

It did not immediately clarify whether any had been among those whose data was viewed through the support agent, or if the agent had been tricked by the broader campaign.

Microsoft did not say whether the agent was at a contractor or a direct employee.

A spokesman said the latest breach by the threat actor was not part of Nobelium's previous successful attack on Microsoft, in which it obtained some source code.

In the SolarWinds attack, the group altered code at that company to access SolarWinds customers, including nine U.S. federal agencies.

At the SolarWinds customers and others, the attackers also took advantage of weaknesses in the way Microsoft programs were configured, according to the Department of Homeland Security.

Also Read | Microsoft, Darktrace team up to counter cyber threats

Microsoft later said the group had compromised its own employee accounts and taken software instructions governing how Microsoft verifies user identities.

A White House official said the latest intrusion and phishing campaign was far less serious than the SolarWinds fiasco.

"This appears to be largely unsuccessful, run-of-the-mill espionage," the official said.

Scott McConnell, a spokesman for Homeland Security's Cybersecurity and Infrastructure Security Agency, said the defensive group “is working with Microsoft and our interagency partners to evaluate the impact. We stand ready to assist any affected entities.”

A SolarWinds spokesperson said, "The latest cyberattack reported by Microsoft does not involve our company or our customers in any way."

Bengio is expected to lead a new AI research unit at Apple under John Giannandrea, senior vice president of machine learning and AI strategy, two people familiar with the matter said.

END