THREAT BULLETINS

New NOBELIUM Activity Compromises Microsoft Support Agent

TLP:WHITE

Jun 28, 2021

On June 25, 2021, Microsoft publicly disclosed that threat actor group NOBELIUM compromised a machine belonging to one of their support agents. According to investigation, information-stealing malware was detected on the machine which provided access to basic account information for a small number of their customers since the second half of May. After gaining unauthorized access to customer information, the actor used the data in some cases to launch password spray and brute-force attacks as part of their broader campaign. Currently, three entities have been compromised as a result of the breach.

According to the Microsoft Security Response Center blog post, Microsoft maintains that the recent activity was mostly unsuccessful and the majority

of targets were not successfully compromised. The customers that were compromised or targeted are being contacted through Microsoft's nation-state notification process.

Health-ISAC will continue to monitor the situation for new developments and share the information accordingly. In coordination with efforts to encourage continued vigilance as NOBELIUM continues to launch attacks, please revisit a prior Health-ISAC report highlighting active exploitation techniques used by the threat actor available here.

The recent activity was targeted at specific customers, primarily IT companies (57%), followed by government (20%), and smaller percentages for non-governmental organizations and think tanks, as well as financial services. The activity was largely focused on US interests, about 45%, followed by 10% in the UK, and smaller numbers from Germany and Canada. In all, 36 countries were targeted.

As part of their investigation into the ongoing activity, Microsoft detected information-stealing malware on a machine belonging to one of their customer support agents with access to basic account including billing contact information and purchased services, amongst other things. It has been determined that the recent breach by the threat actor was not part of Nobelium's previous successful attack on Microsoft in which it obtained some source code.

Microsoft has since responded to the breach by removing access and securing the device in addition to advising affected customers to be careful about communications to their billing contacts and consider changing usernames and email addresses, as well as barring old usernames from logging in. As the investigation continues, Microsoft confirms that their support agents were configured with a minimal set of permissions required as part of their Zero Trust "least privileged access" approach to customer information.

Reference(s)	Microsoft, Microsoft, Microsoft, Reuters, Ars Technica, Microsoft

Recommendations

The recent activity reinforces the importance of best practice security precautions such as Zero Trust architecture and multi-factor authentication in addition to the significance of their implementation.

For additional information, please see the following for best practice security priorities:

- Identity Access Management
- Zero Trust
- Implementing Least-Privilege Access Models

Sources
Microsoft Says New Breach Discovered in Probe of Suspected SolarWinds Hackers

SolarWinds Hackers Breach New Victims, Including a Microsoft Support Agent

Microsoft Security Response Center: New NOBELIUM Activity

Alert ID 2e6b813a

View Alert

Tags NOBELIUM, Microsoft

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.