New Nobelium activity

msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

The Microsoft Threat Intelligence Center is tracking new activity from the NOBELIUM threat actor. Our investigation into the methods and tactics being used continues, but we have seen password spray and brute-force attacks and want to share some details to help our customers and communities protect themselves.

This recent activity was mostly unsuccessful, and the majority of targets were not successfully compromised – we are aware of three compromised entities to date. All customers that were compromised or targeted are being contacted through our nation-state notification process.

This type of activity is not new, and we continue to recommend everyone take security precautions such as enabling multi-factor authentication to protect their environments from this and similar attacks. This 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 our investigation into this ongoing activity, we also detected information-stealing malware on a machine belonging to one of our customer support agents with access to basic account information for a small number of our customers. The actor used this information in some cases to launch highly-targeted attacks as part of their broader campaign. We responded quickly, removed the access and secured the device. The investigation is ongoing, but we can confirm that our support agents are configured with the minimal set of permissions required as part of our Zero Trust “least privileged access” approach to customer information. We are notifying all impacted customers and are supporting them to ensure their accounts remain secure.

This activity reinforces the importance of best practice security precautions such as Zero-trust architecture and multi-factor authentication and their importance for everyone. Additional information on best practice security priorities is listed below: