Severity

High

Analysis Summary

APT29 aka Nobelium and Cozy Bear are the group which were behind the infamous Solar Wind attacks in 2020. APT29 threat group has previously targeted commercial entities and government organizations in Germany, Uzbekistan, South Korea and the US, including the US State Department and the White House in 2014. They have also targeted several vaccine manufacturers in attempt to sabotage the process to combat the Coronavirus pandemic. This time they've come up with a current campaign to target government organizations in attempt to steal sensitive information.

Impact

- Information Theft and Espionage
- Exposure of Sensitive Data

Indicators of Compromise

MD5

- e3df714141a8fe07060e37a84ad69d23
- 454f59dc7d3d7f228bbd4ddd4c250ed8

SHA-256

- d5c84cbd7dc70e71f3eb24434a58b2f149d0c39faa7e4157552b60c7dbb53d11
- 23a09b74498aea166470ea2b569d42fd661c440f3f3014636879bd012600ed68

SHA-1

- 9f5645acf202623d1a1d56890ae560555c1222d5
- ad33bab4bc6232a6666c2190b3bf9fc2ab2a720a

Remediation

- Always be suspicious about emails sent by unknown senders.
- Never click on links/attachments sent by unknown senders.
- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.