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

- 110c4ae194e7b49ed3e3b254d599f7f4
- 9ec1fcb11b597941bec03078cccab724
- 7e44d94813b6100ca296aa91d321020c

SHA-256

- 4c68c840ae1a034d47900ebdc291116726fd37b3ab0b7e026fad90eaab84d820
- 7f96d59cb02229529b14761f979f710bca500c68cc2b37d80e60e751f809475e
- 6fc54151607a82d5f4fae661ef0b7b0767d325f5935ed6139f8932bc27309202

SHA-1

- c9a5314eb247c7441a5262a7cd22abbe1fcba7b6
- 489c36c9ea3fb90f61209d43efffd8d997a362c6
- 9ef9a6ba386a2728b6f2ddb78e18c517a597a3cd

Remediation

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