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

- 2f712cdae87cdb7ccc0f4046ffa3281d
- 4ae0b6be7f38e2eb84b881abf5110edc
- 6ac740ebf98df7217d31cb826a207af6
- a0b4e7622728c317f37ae354b8bc3dbb
- e031c9984f65a9060ec1e70fbb84746b
- 363a95777f401df40db61148593ea387

SHA-256

- 207132befb085f413480f8af9fdd690ddf5b9d21a9ea0d4a4e75f34f023ad95d
- 538d896cf066796d8546a587deea385db9e285f1a7ebf7dcddae22f8d61a2723
- 2f11ca3dcc1d9400e141d8f3ee9a7a0d18e21908e825990f5c22119214fbb2f5
- 8bdd318996fb3a947d10042f85b6c6ed29547e1d6ebdc177d5d85fa26859e1ca
- 95bbd494cecc25a422fa35912ec2365f3200d5a18ea4bfad5566432eb0834f9f
- 8cb64b95931d435e01b835c05c2774b1f66399381b9fa0b3fb8ec07e18f836b0

SHA-1

- bf088d12a823ec49f4746773466f48d98f07a0ea
- de3500353ff9c7f2be60b83bfe453cc6791bfaf9
- 6bf6fc77b10f6700fa0b868f6d3515b495d1e1e0
- bdfd9f8371e683e9013b74cc61a3583acf9206ad
- b01950ed9b1929fee04a9c23ac49e3de89e37228
- fa63b1a711c807d807ab3d9681a7efd5ac978e67

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.