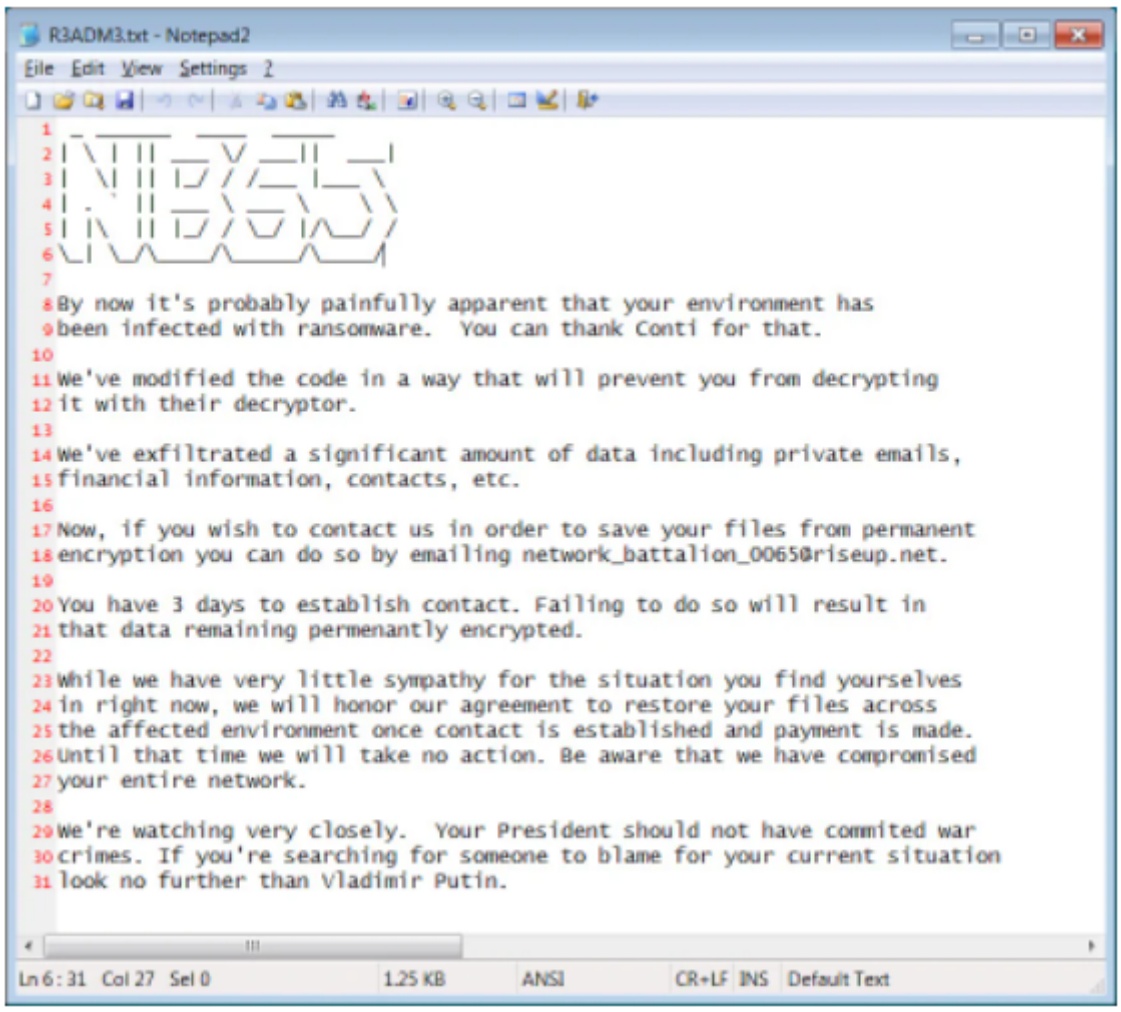
Severity

High

Analysis Summary

Conti ransomware was discovered in December 2019 and is delivered via TrickBot. It's been utilized against large companies and government institutions across the world, especially in North America. Conti steals important files and information from targeted networks and threatens to disseminate it unless the ransom is paid. Conti ransomware enhances performance by utilizing "up to 32 simultaneous encryption operations," and is very likely directly controlled by its controllers. This ransomware can target network-based resources while ignoring local files. This feature has the noticeable impact of being able to create targeted harm in an environment in a way that might hinder incident response actions.



Impact

- Sensitive File Theft
- File Encryption

Indicators of Compromise

MD5

- f746ea39c0c5ff9d0a1f2d250170ad80

SHA-256

- 7f6dbd9fa0cb7ba2487464c824b6d7e16ace9d4cd15e4452df4c9a9fd6bd1907

SHA-1

- dac28369f5a4436b2556f9b4f875e78d5c233edb

Remediation

- Search for IOCs in your environment.
- Block all threat indicators at your respective controls