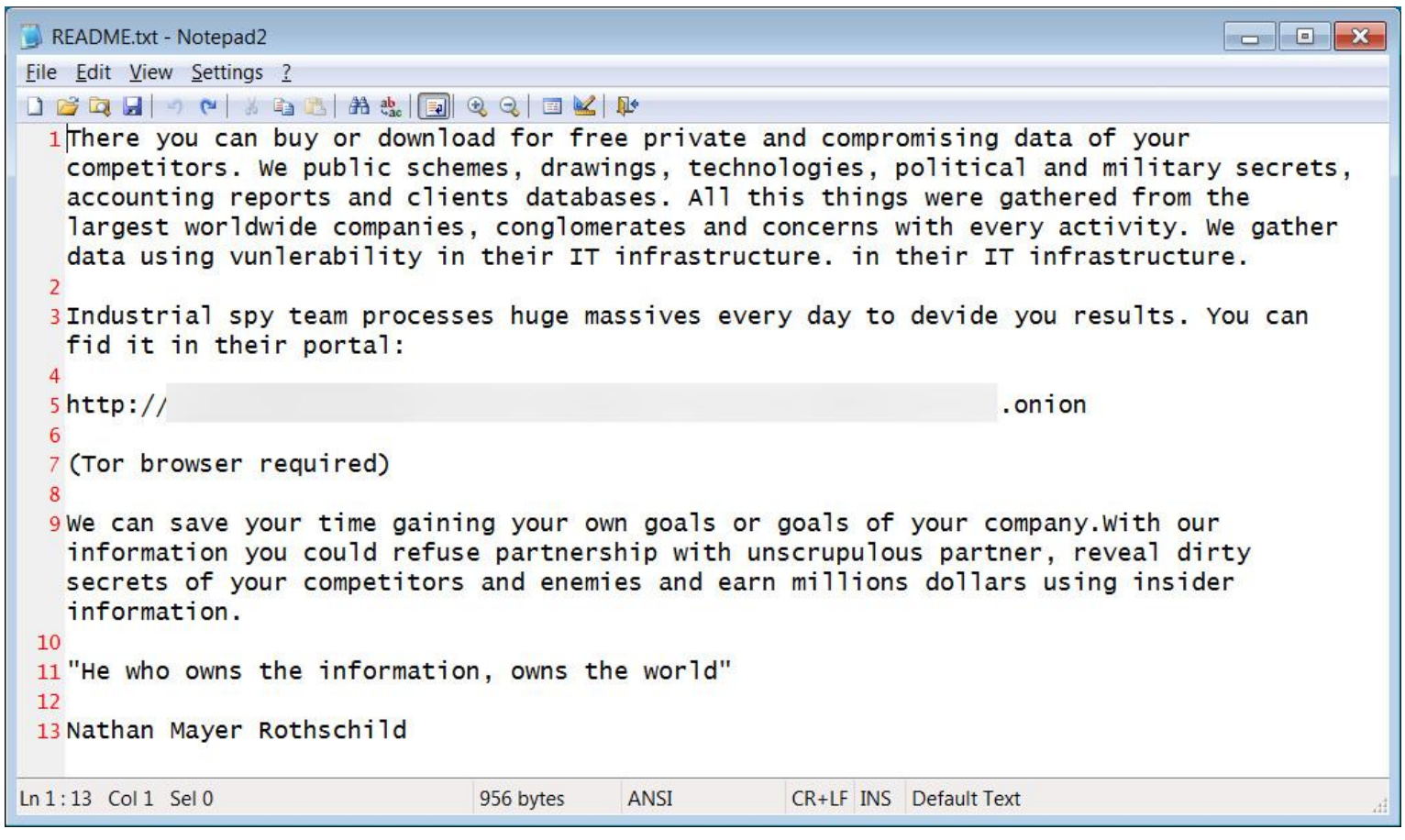
Severity

Medium

Analysis Summary

A new marketplace for purchasing leaked and breached data has emerged called “Industrial Spy.” The gang behind the marketplace also uses adware and cracks to spread further. Once the Industrial Spy executable is downloaded on a device, it creates a README.txt file in every folder on the victim device. The text file contains a description of the company, their vision, and a promotional campaign regarding the marketplace.



The marketplace has three services: Premium, General, and free. And individual files can be bought for as low as $2. The filenames of the malware’s executable are:

- tools.exe
- DEA2.exe
- 2bd1.exe
- F0EA.exe
- DE41.exe
- 49DD.exe
- 367C.exe
- F14E.exe
- 5206.exe
- 46C2.exe
- 61af.exe
- 822a.exe
- FA9D.exe
- 79F0.exe
- d661.exe
- B3D9.exe
- bc8b.exe
- E399.exe
- F2B0.exe
- BC09.exe
- B31D.exe
- 9391.exe
- 92D1.exe

- 7773.exe
- 56a7.exe
- 69FB.exe
- 5262.exe
- CFE3.exe
- 4BF9.exe
- 6308.exe
- 3A89.exe
- CC8E.exe
- 176B.exe
- 4DE7.exe
- 20F.exe
- 2603.exe
- 6542.exe
- EA6F.exe
- 6793.exe
- F6B4.exe
- 77be.exe
- F225.exe
- DF15.exe
- 9FF4.exe
- EF37.exe
- 3d1f.exe
- 9395.exe
- D565.exe
- FE84.exe
- 23B4.exe
- 350C.exe
- C8A4.exe
- 97DF.exe
- 9ba2.exe
- BBEC.exe
- 61e2f011274d734599209767ab76cad136e8a94f.bin
- 9932.exe
- D640.exe
- b0a9.exe
- BD59.exe
- 7C92.exe
- README.txt
- toolsnpd.exe
- B871.exe
- ac65.exe
- CC9B.exe
- 8F15.exe
- D2B6.exe
- 9fe.exe
- 2C20.exe
- D527.exe
- 90EA.exe
- E488.exe
- A131.exe
- D1EB.exe
- C73C.exe

- 953.exe
- AC2E.exe
- toolsnpd.exe

Impact

- Information Theft
- Financial Loss
- Misuse of Data
- Cyber Espionage

Indicators Of Compromise

MD5

- 95d4d597b3065359e471890fc166abfc
- 333d29ffe93e71b521057698adf722e3

SHA-256

- c96b098cab47c0a33d0b6d8f14b24e7c9ba897b0c59a2ac1f3dc608ca7a2ed7e
- 5ed4ffbd9a1a1acd44f4859c39a49639babe515434ca34bec603598b50211bab

SHA-1

- 51a2437cadd422446b0bc6bd59cd5fe467eed26a
- 61e2f011274d734599209767ab76cad136e8a94f

Remediation

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