TECH HIVE ADVISORY

SECURITY ADVISORY SERIES

Cybersecurity, News, Events and Threat Advisories. Volume 1. Issue 5.

THREAT ADVISORY

RANSOMWARE ATTACK HITS COLONIAL PIPELINE IN THE US

TLDR: a ransomware attack hit colonial Pipeline company, an American pipeline organisation that transports diesel, gasoline and other natural gas from Texas to New Jersey. The ransomware attack impacted the organisation's IT network. The notorious hacker group named Darkside has claimed credit for the attack.

See detailed information here.

SEVERITY **HIGH**

What is the issue?

On 7 May 2021, Colonial Pipeline company, a critical infrastructure provider, detected that it had been hacked when an employee found a ransom note on a control room computer. DarkSide, known for its Ransomware-as-a-service (RaaS) operation, stole the company's data and, after that, encrypted the data to make it inaccessible. The encryption made operation impossible for the company, and to prevent further infection, the company moved some of its operations offline and halted its pipeline operations. This slowed down operation and its productivity.

The attackers stole about 100 gigabytes of data and threatened to publish them if a ransom of 5 million USD or 75 bitcoins was not paid. The CEO of Colonial Pipeline confirmed that a ransom of 4.4 million USD was paid, and the decryption of data has commenced, albeit very slow.

Impact

The attack has an impact on everyday Americans. The shutdown led to a shortage of fuel and consequently panic buying by citizens. Some flights were also temporarily rescheduled due to the fuel shortage. The company has been unable to run its customer billing system since the attack.

A potential risk is that DarkSide may publish the stolen data online, notwithstanding that the ransom has been paid. They have a history of doing so. Similar ransomware attacks have hit the United States quite frequently, and it shows that they are not going away anytime soon.

Lessons for Nigeria Business

- **Organisations should deploy the use of two-factor authentication (2FA) or multi-layered authentication (MLA)**
- **Keep data secured even at the storage level with an immutable backup copy. Attackers will not be able to change this data form, hence rendering malicious encryption impossible for some time.**
- **Use spam filters to block spam emails and prevent phishing emails.**
- **Implement URL blocklists to prevent employees from accessing malicious websites.**
- **Always update software to fix patches that may be existing.**

Curated by Tojola Yusuf
@tojolabilqis Tojola Yusuf

contact@techhiveadvisory.org.ng
www.techhiveadvisory.org.ng
@Hiveadvisory