CSCI 301 SCRIPTING LANGUAGES PRESENTATION

THOMAS HAMILTON

INITIAL ATTACK

- The attack took place on May 6-7 when the attackers, DarkSide, where able to get access to an unsecured VPN account
- The VPN was their way to access the server in a “secured” way
- The DarkSide got the password in a different data theft
- This means that the password was most likely used somewhere else

SECOND PART

- After stealing over 100 GB of data DarkSide then planted ransomware into the IT network
- This forced the Colonial Pipeline to shutdown to prevent the spread of the ransomware
- The Pipeline was then forced to pay 75 bitcoins to DarkSide

WHAT HAPPENED

- DarkSide was able to get access to a VPN account as the employee used the same password in a different account
- They were then able to then log into the VPN and access the network and download ransomware
- There was no firewall to prevent it as it was just someone logging into an account
- The ransomware then made it impossible to use the systems
- Colonial Pipeline then had to pay 75 bitcoins to DarkSide to get the decryption key to regain control of their systems

DAMAGES

- Colonial Pipeline was forced to pay 75 bitcoins ($4.4 million) as ransom to DarkSide
- The Department of Justice was able to recover 63.7 bitcoins ($2.3 million)
- The pipeline had to shutdown for 5 days
- The loss of revenue for both the pipeline and the companies that bought from it
- The people buying the refined oil had to pay more to buy products

HOW IT COULD HAVE BEEN PREVENTED

- By not using the same password in two different accounts
  - Especially one as important as a work account
- By using two-step verification