Network Forensics Class Lab: Billie Went Nuclear

Prof. Josh Brunty
Cyber Forensics & Security
Marshall University

- At your DC-based company (Clinton, Inc.) Security Operations Center (SOC), an analyst received a call from Billie Gardner, who is an executive assistant for your Chief Executive Officer (CEO), William “Billy” Clinton at the UK Office.
- While searching for a tasty steak dinner location for his boss Billy, Billie described the computer as “acting funny” and “files inaccessible”. He also stated that the desktop wallpaper had been changed and said something about “ransom” and “paying up”

- At the same time One of the other analysts is investigating a snort alert that came in at the exact same time.
- Fortunately, that location has full packet capture, and the analyst retrieved a .pcap of network traffic (nuke.pcap) from the associated IP address.
- You’ve been asked to take a look and determine what exactly happened and what must be done to mitigate further damage to the company’s network.

- You review the pcap and check the other analyst's report. First, we need to double-check the following:
  - ✓ Date and time of the activity
  - ✓ IP address of computer
  - ✓ Host name of computer
  - ✓ MAC address of computer
  - ✓ IP address and domain name that generated the traffic