Executive Summary

Upon analysis, the pcap file provided shows that the Windows host in question host was infected with three separate viruses: Hancitor, Cobalt Strike, and Ficker Stealer. This machine, under the user Bill Cook, was infected around 4:00 PM on February 2, 2021. Extracting the HTTP from the uninviting.php packet and running that in a text environment reveals that the Hancitor infection occurred from a word document that was sent to the host, which contains macros for running the malware. Looking at the app.any.run report, the document can be seen opening multiple services that Word doesn't usually use. For Cobalt Strike, the target machine can be seen in multiple suspicious communications that hint at the virus communicating with its associated domains. Fickler Stealer does this as well, but also can be seen generating TCP traffic. Throughout the packets, the target machine is identified as DESKTOP-MGVG60Z signed in as bill.cook, which has a MAC address of 00:12:79:41:c2:aa and an IP address of 10.2.8.101.

IOCs

- Traffic associated with Hancitor: tonmatdoanminh.com and satursed.com over port 80.
- Traffic associated with Cobalt Strike: roanoakemortgages.com and 198.211.10.238 over ports 8080 and 443.
- Traffic Associated with Fickler Stealer: roanokemortgages.com and sweybllidian.com over port 80.