NAME: FABIHA TASNIM

ID: 20-43426-1

a. What was the time when this event occurred?
   Ans: Date: Mon, 28 Jan 2019, 21:49:19 GMT
b. What are the internal & external IP's?
   Ans: Internal IP address: 10.12.25.101
   External IP address: 128.199.64.235
c. What was NIC vendor info for the client?
   Ans: Cisco Systems, Inc. MAC : 00049A58EB0D. IP: 91.121.30.169, 216.239.94.252.
d. What was NIC vendor info for the host/attacker?
   Ans: Dell Inc. MAC: 14FEB5D415CA. IP: 172.17.9.109.
e. Name of the Malware that infected?
   Ans: Recorded traffic from several IP addresses, but 139.119.184.166 was by far the most active during the timeframe. Guessing, It's Trojan.emotet/dIve.
f. f. What was the MD5 hash generated for the malware?
   Ans:7872b5f2511c55d20af993114574d356
g. How did the malware get into the Victim's PC?
   Ans: The traffic seen from a web server, where someone is scanning or probing for a weakness/vulnerability. Traffic from many IP addresses were recorded, however the most active one at the time was 139.119.184.166.
h. What are the characteristics of the malware?
   Ans: There were no specific type of malware but some IP addresses were recorded. But I'm guessing it is Trojan.emotet/dlve. In this malware, be persistent, brute-force passwords, and get user credentials from widely used email and web applications.
i. Was there more than one malware at play in this scenario?
   Ans: No specific. Maybe Trojan, banker.
j. What is the malware group or family?
   Ans: As the malware was undefined so no group or family found. But as a predict, the group or family is emotet, dive,csri.
k. Summarize the whole event from how the victim got attacked and what data was stolen as per your research.
   Ans: As per research, this is an illustration of communication coming from a web server that is being probed or scanned for flaws. After setting up a fresh web server and letting it run for a few days, used dumpcap to record network activity from users attempting to browse or access the server. 139.119.184.166 was by far the most active IP address during the time that logged the data; however saw activity from other numbers as well. The majority of this is web activity, however some attempted TCP connections to the web server across TCP ports 8080 and 8983 can be seen if filter on!(tcp.port eq 80). To make it appear as though the server was hosted on a Digital Ocean IP address cleaned up the pcap. The identification of the webserver in the pcap is sanitized, but the probe/scan by

139.119.184.166 was certainly real. And as predict the malware, The trojan.emotet/dlve virus was present in the downloaded doc file. Sensitive information, including bank account details and login credentials, were lost when the client opened the file and the virus entered the client machine.