TO: MWCCDC

FROM: Team 6

DATE: January 27, 2024

SUBJECT: Extraction of NTP Log File

Dear MWCCDC,

Based on the information provided from the packet capture, the NTP packet does not show adequate analysis to make the ruling that the packet captured is a potential malware beacon. Seeing as though the input information offered was only one packet instead of additional context, for example logging network behavior over a span of time which would be very useful in building a conclusion. Whether or not a packet capture may have seen unusual or possibly suspicious malware falls in the context of the amount of information to make the defense.

Judging only on the details provided in the single packet sample, it appears to be a typical NTP packet because every detail matches those of a client requesting time synchronization from the server that hosts the NTP service. Looking further into the fields in the packet capture, we found that the parameters of NTP such as leap indicator, version, mode, and various date and time do not specify any malicious activity. Since it aligns with what is expected this packet capture is ruled to be normal activity.

Nevertheless, a single packet tracer can not be fully concluded and concise to make a full conclusion, so it is recommended to log and audit any further suspicious behavior.

Please let us know if you would like further assistance in the future, we would be honored help secure any patches.

Sincerely,

Team 6