Microsoft Defender is Wrongly Detecting Malware in Lasernet Monitor

2024-01-17 - Kacper Dylewski - Comments (0) - Lasernet News

Since December 2023, Microsoft Defender has been flagging the LnMonitor.exe software (developed by Formpipe) as Trojan:Win32/Znyonm!pz or Phonzy malware. However, this is a "false positive", and Microsoft has confirmed that this is the case.

As a part of our rigorous release process for Lasernet, the Lasernet installer packages from Formpipe Software are scanned for viruses by VirusTotal and must be declared clean before release.

Microsoft Confirmation of False Positive

Formpipe has tracked the file hashes of the Lasernet Monitor 10 application (that Microsoft Defender has been flagging as malware), and has raised these detections with the Microsoft security team as false positive detections.

As shown below, that Microsoft team has confirmed that they are false positives, and the detection has been whitelisted from the Microsoft Defender threat database.

It is currently unclear why Microsoft Defender wrongly flagged Lasernet software as malware. During December 2023 and January 2024, Formpipe rebuilt Lasernet software multiple times, but Microsoft Defender flagged each build as malware. Microsoft (and other antivirus companies) intentionally do not publish information around how their antivirus solutions characterize malware, to prevent real malware creators from designing around those algorithms.

Current Status

We are currently still working with Microsoft to fully resolve this issue. From January 16th 2024, we can confirm that new builds of Lasernet software are no longer being flagged as malware by Microsoft Defender. Formpipe uses Microsoft build servers to build Lasernet software, and those build servers run Microsoft Defender.

However, we currently cannot be certain that Microsoft Defender will not subsequently repeat its mistake for these (and future) builds of Lasernet software. Also, Microsoft's work

to update Microsoft Defender (to fully resolve this issue) is still ongoing.

Before we release the latest software builds, we are further investigating the extent and efficacy of Microsoft's latest actions on this issue.

Workaround
While Formpipe customers are waiting for Microsoft to update Microsoft Defender, they can use the following workarounds:

- Use the web version of Lasernet Monitor.
- Remove LnMonitor.exe from quarantine in Microsoft Defender. See https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/restore-quarantined-files-microsoft-defender-antivirus?view=o365-worldwide.

Updating Microsoft Defender's virus definitions (https://www.microsoft.com/en-us/wdsi/defenderupdates) to clear cached detections and obtain the latest malware definitions will not resolve this detection issue until Microsoft distributes comprehensive and effective updates to the Microsoft Defender virus definitions.

Alternatively, customers can upgrade to Lasernet 10.7. The third-party software components that cause this issue have been removed from Lasernet 10.7. Consequently, the Performance and Transactions tabs are not present in Lasernet Monitor 10.7.

Long-Term Solution
Formpipe is working with Microsoft to find a long-term solution to this issue. We will update you with news in due course.

Thank you for your understanding during this time. If you have any questions, please contact us via the Create Ticket button in the support portal.