Incident Report: Suspicious File Detected in MicroDicom Viewer

1. Source of the File

The installer files were downloaded from the official MicroDicom website: https://www.microdicom.com.

2. Filename & Hashes

File	SHA256 Hash	Description	File Size
MicroDicom-2025.1-x64.exe	15ee7e246846a9c46aac53a855f4e2bc123de8c50cfa39dbffd9e3fcdac9b811	Installer from April 2025	12 MB
MicroDicom-2025.3-x64.exe	783af5c29ed89ae46bc62b5775729d46622e3ebcdba628eb85e3558074b22513	Current official installer	14 MB
~~VisusStarter.bin	058370b70c65c1764960ce0b3eaddcd789b473e90097d247b97dec63959cd4f6	Suspicious temporary binary	1.3 MB

3. Date & Time of Initial Detection

The suspicious file was first detected on June 5, 2025, approximately at 00:30.

4. Tools Used for Analysis

- Malwarebytes (up to date), performed a full system scan. The suspicious file was detected early during an 8-hour scan.
- Windows Defender (up to date), performed a full system scan (exact scan time not available).

- Additional scanning services used: VirusTotal (virustotal.com), FileScan.io, Dr.Web Virus Monitor (vms.drweb.com), IPQualityScore (ipqualityscore.com).

5. Findings & Behavior

Malwarebytes:

- Detection name: Malware.Sandbox.50
- Detection time: June 5, 2025, 00:30 (approx)
- File path: `C:\Users\49157\AppData\Local\Temp\~~VisusStarter.bin`
- Type: File

VirusTotal:

- The file ~~VisusStarter.bin was flagged as malicious by 4 out of 62 vendors, including Avira, GData, Cynet, and WithSecure.

FileScan.io Highlights (only suspicious/important findings):

- XOR decoding loop detected in entry point (Defense Evasion: Obfuscated Files or Information)
- PE imports APIs related to privilege modification, file attribute modification, code injection, and anti-debugging (Defense Evasion, Discovery, Impact)
- Presence of overlay and suspicious section names
- PE resources exceed 75% of total file size

Other results from VirusTotal, Dr.Web, and IPQualityScore showed no significant findings for the installer files.

6. Additional Files Affected

Only the temporary file ~~VisusStarter.bin was found to be suspicious.
The installer files themselves showed fewer signs of malicious behavior, with only FileScan.io flagging the current installer.

7. System Environment

Operating System: Windows 10, 64-bit, fully up to date.
Malwarebytes and Windows Defender were both updated to the latest versions before scans.

8. Context & Background

This analysis was conducted by **Darius Nasseri-Jafar**, a cybersecurity enthusiast preparing to start a formal IT training program in cybersecurity. The initial reason for investigation was to view X-ray images of his dog using MicroDicom Viewer.

9. Personal Conclusion

There is a strong suspicion of malicious behavior in the temporary file associated with the MicroDicom Viewer software, which is not typical for a legitimate image viewer. Further analysis by the software manufacturer is recommended.

10. Disclaimer

This report is based on personal analysis and available scan data as of June 2025. It does not constitute a definitive malware diagnosis. Users are advised to perform their own security checks and exercise caution when using the affected software.

Report created by Darius Nasseri-Jafar, Cybersecurity Enthusiast