Key Points

- Research suggests CommandoVM is trustworthy and malware-free, developed by Mandiant, a reputable cybersecurity firm now owned by Google.
- It seems likely that CommandoVM is safe for use, given its open-source nature and lack of reported security issues.
- The evidence leans toward Mandiant, and thus CommandoVM, being owned by Google following their 2022 acquisition.

Ownership

CommandoVM is developed by Mandiant, which was acquired by Google in 2022 for $5.4 billion, integrating it into Google Cloud. This makes CommandoVM indirectly owned by Google.

Trustworthiness and Malware-Free Status

CommandoVM is designed for penetration testing and red teaming, with over 140 tools, and is actively maintained, with recent updates noted in 2023. Its open-source availability on GitHub allows community auditing, enhancing trustworthiness. No significant security concerns or malware reports were found, supporting its safety for intended use.

Survey Note: Detailed Analysis of Mandiant CommandoVM Trustworthiness and Ownership

This survey note provides a comprehensive examination of Mandiant CommandoVM's trustworthiness, malware-free status, and ownership, based on extensive research conducted as of 07:51 PM CDT on Friday, May 23, 2025. The analysis aims to address the user's query with detailed insights, ensuring a thorough understanding for both technical and non-technical audiences.

Background on CommandoVM

CommandoVM, or the Complete Mandiant Offensive VM, is a Windows-based virtual machine distribution specifically tailored for penetration testing and red teaming activities. It was first introduced by Mandiant in early 2019 at Black Hat Asia Arsenal, featuring over 140 tools in its initial release, with subsequent versions adding features like Kali Linux

integration, Docker containers, and package customization. The VM is designed to support internal penetration tests, offering native support for Windows and Active Directory, making it a go-to platform for cybersecurity professionals assessing such environments.

The distribution is built using tools like Boxstarter, Chocolatey, and MyGet packages, automating the installation of software and utilities necessary for offensive security tasks. This automation, combined with its open-source nature on GitHub, allows for community contributions and regular maintenance, with recent updates noted in 2023, indicating active development.

Ownership by Google

The ownership question centers on Mandiant, the developer of CommandoVM. Research confirms that Google acquired Mandiant in March 2022 for $5.4 billion, with the acquisition completed by September 2022, as reported in various sources, including the Google Cloud blog

.

Given this acquisition, it is reasonable to conclude that CommandoVM falls under Google's ownership through Mandiant, aligning with the corporate structure where subsidiaries and their products are integrated into the parent company's ecosystem.

Trustworthiness and Malware-Free Status

Assessing CommandoVM's trustworthiness and malware-free status involves evaluating its development, community feedback, and reported issues. Mandiant, known for its expertise in cybersecurity, particularly in incident response and threat intelligence, lends significant credibility to CommandoVM. The company's reputation, now bolstered by Google's acquisition, suggests a high standard of security practices in its products.

CommandoVM's open-source nature, hosted on GitHub

. This issue appears to be mitigated in later versions, as GitHub hosting ensures HTTPS access, reducing the risk of man-in-the-middle attacks.

No significant reports of malware or security vulnerabilities were found in searches for "CommandoVM security concerns" or "CommandoVM malware." Blog posts and tutorials, such as those on Kali Linux Tutorials

, focus on installation and usage, with no mention of malware. The absence of issues on the GitHub issues page, when searched for security-related topics, further supports the conclusion that CommandoVM is malware-free.

It's worth noting that CommandoVM's installation process requires disabling Windows Defender, as mentioned in the GitHub documentation. This is a common practice for penetration testing tools, as many offensive tools trigger antivirus alerts, but it does not imply the VM itself is malicious. Instead, it reflects the environment's need for running potentially flagged software, which is expected in red teaming scenarios.

Community and Expert Opinions

Community discussions provide additional insights into CommandoVM's reliability. A YouTube review titled "Red Teaming from Windows | Commando VM Review"

.

However, some users expressed concerns about the lack of antivirus in the VM, as noted in a 2022 LinkedIn post, suggesting it could be a drawback for certain use cases

. This is consistent with its purpose as an offensive toolset, where security measures like antivirus might interfere with functionality, but it underscores the importance of using CommandoVM in isolated, controlled environments.

Comparative Context

Compared to other penetration testing distributions like Kali Linux, CommandoVM fills a niche for Windows-based environments, offering tools not typically found in Linux distributions. Its design for Active Directory assessments and native Windows support makes it particularly valuable, and its development by Mandiant, now backed by Google, positions it as a credible option. The lack of reported malware, combined with active maintenance and community engagement, suggests it is safe for its intended purpose.

Table: Summary of Key Findings

Aspect	Details
Ownership	Developed by Mandiant, acquired by Google in 2022, operated under Google Cloud.

Trustworthiness	High, given Mandiant's reputation, open-source nature, and community auditing.
Malware-Free Status	No reported malware; designed for penetration testing, requires disabling antivirus for functionality.
Recent Updates	Version 3.0 noted in 2023, indicating active maintenance.
Community Feedback	Mostly positive, with some concerns about initial HTTP downloads (mitigated in later versions).

Conclusion

Based on the research, CommandoVM appears trustworthy and malware-free, suitable for its intended use in penetration testing and red teaming, given its development by Mandiant, now part of Google, and its open-source, community-reviewed status. The ownership by Google, through the acquisition of Mandiant, is confirmed, aligning with corporate integration into Google Cloud. Users should ensure isolated environments for deployment, given the need to disable antivirus, but this is standard for such tools.

Key Citations

- Mandiant Wikipedia page
- Google completes acquisition of Mandiant Google Cloud Blog
- GitHub mandiant commando-vm repository
- Commando VM 2.0 Customization Containers and Kali Google Cloud Blog
- r/netsec Reddit post on Fireeye Commando VM
- CommandoVM Complete Mandiant Offensive VM Kali Linux Tutorials
- Commando VM Installation 0xdf hacks stuff
- Red Teaming from Windows Commando VM Review YouTube
- Daily REDTeam LinkedIn post on Commando VM 3.0
- George Litvinov LinkedIn post on Commando VM 3.0

- Chang Tan LinkedIn post on Commando VM concerns
- Google closes 5.4B Mandiant acquisition TechCrunch