NetApp Knowledge Base

Why are we receiving mimikatz cyber security alerts using Snapmirror

https://kb-stage.netapp.com/on-prem/ontap/DP/SnapMirror/SnapMirror-KBs/Why_are_we_receiving_mi…
Updated: Wed, 24 Jun 2026 06:07:04 GMT

Applies to

- ONTAP OS
- Snapmirror
- Kerberos

Answer

NetAppsCyber Security Team has never taken a report of malware that runs on ONTAP. There is a Microsoft Utility that flagged a customer's ONTAP system as possible Mimikatz, apparently due to the use of Kerberos. This report was not focused on Snapmirror ports, and it was inaccurate.

'NetApp provides no representations or warranties regarding the accuracy or reliability or serviceability of any information or recommendations provided in this publication or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS and the use of this information or the implementation of any recommendations or techniques herein is a customers responsibility and depends on the customers ability to evaluate and integrate them into the customers operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.'

Additional Information

Our Cyber Security Team has never taken a report of malware that runs on ONTAP. If such a malware existed, it would require manual installation on a ONTAP node by someone authorized as an admin. I f such a malware existed, it would require manual installation on a ONTAP node by someone authorized as an admin

© 2023 NetApp.No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner. For more information, see Legal Notices.