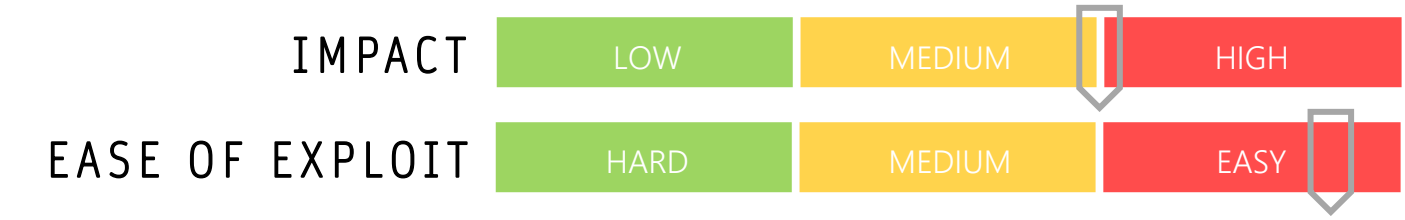
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00064

GOOGLE DRIVE EMPLOYED BY ATTACKERS

DATE ISSUED: 10th November 2020



OVERVIEW

Using the collaboration features available in Google Drive, attackers are using push notifications and emails to lure victims into opening malicious links and documents.

BREAKDOWN

Using an invitation to a shared document, attackers are leveraging Google Drives collaboration features which allow push notifications or emails to be sent to victims using the no-reply email address, making them appear to be legitimate. In a spray attack hundreds of thousands of Google users have been targeted by notifications prompting users to log in to accounts, threatening deletion of accounts, shared documents or important notices of financial transactions association with their account. Others contain prize scams leading to malicious websites.

REMEDIATION STEPS

- Use caution when accessing Google Drive notifications and emails, particularly if you are not expecting documents to be shared.
- Use common phishing visual identification of scams as reports suggest the language used is poor
- Be wary of any "Personal Notification" messages, as these are recognized as a primary vector
- Change passwords immediately if there is belief the account has been compromised
- Use web and email filtering to prevent users accessing known suspicious links

REFERENCES & RESOURCES

Threatpost https://threatpost.com/scammers-google-drive-malicious-links/160832/
Wired https://www.wired.co.uk/article/google-drive-spam-comments-phishing
Tripwire https://www.tripwire.com/state-of-security/security-data-protection/phishers-using-google-drive-to-trick-people-into-visiting-malicious-websites/