Defensive Cyber Operations – National Guard (DCO-NG)

ARMY NATIONAL GUARD (ARNG)

Advisory

AD-17-13	**"Google Docs Phishing Scam"**	**12 June 2017**

RISK

Medium

AFFECTED SYSTEMS

ALL

ISSUE

Providing useful and relevant information to the National Guard and its personnel is one of the many goals of the DCO-NG. Highlighting cyber-incidents in addition to best practices not only protects our networks but also protects our users by keeping them well informed. Cloud collaboration sites such as Microsoft One Drive and Google Docs have become extremely popular over the past several years. This is mainly because the ease of which users can write and share documents with other individuals by giving permission to an item located within a user's account. Hackers have been known to target these applications, and now they are using a new attack vector.

This new attack vector involves an invite being sent to an unknowing participant to edit a Google document. The victim receives an email with the subject line stating a contact "has shared a document on Google Docs with you". When the individual clicks on the "Open in Docs" link in the email, it sends them to a legitimate Google sign-in screen that asks to "continue in Google Docs". Clicking on this link allows the fraudulent 3rd party app to obtain access to contacts, emails, and an opportunity for spam to be sent to those contacts. The reason this is harder to detect is that the malicious app actually uses the "Google Docs" name.

.

Defensive Cyber Operations – National Guard (DCO-NG)

ARMY NATIONAL GUARD (ARNG)

Advisory

MITIGATION

- Be suspicious of unsolicited email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security.
- If you are not expecting an email about editing or sharing a document or you do not know the sender, do not click on it.

REFERENCES

"Google Docs users hit with sophisticated phishing attack in their inboxes"

https://www.theguardian.com/technology/2017/may/03/google-docs-phishing-attack-malware

"Google Docs app spam goes phishing"

https://blog.malwarebytes.com/cybercrime/2017/05/google-docs-app-spam-goes-phishing/

If you have any questions about this report, contact:
Defensive Cyber Operations – National Guard
ng.ncr.ngb.mbx.dco-ng-cnd@mail.mil
703-607-8455