American
Technology Services

2017-03 ATS Security Advisory

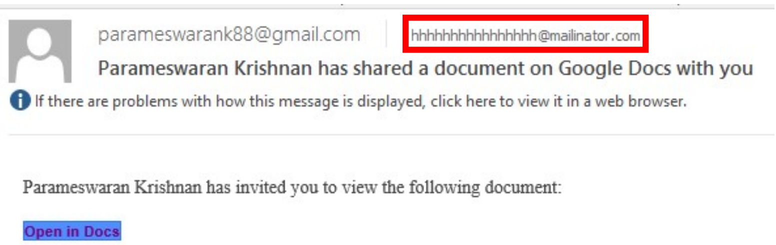
Google Docs Phishing Attack

Summary

Yesterday afternoon a unique phishing attack impersonating Google Docs quickly began spreading via email. The email appeared to be sharing a Google Doc and contained a link to a legitimate Google webpage, requesting permissions to your account. If you granted the permissions, the attacker had the ability to read and send from your email account as well as manage your contacts.

Details

The scam starts with an email from someone that has sent you an email before, who had likely been recently compromised. This email looks legitimate but you can see it includes an unexpected ‘To:’ address as shown below. This is an indicator of an illegitimate email.



parameswarank88@gmail.com hhhhhhhhhhhhhhhh@mailinator.com

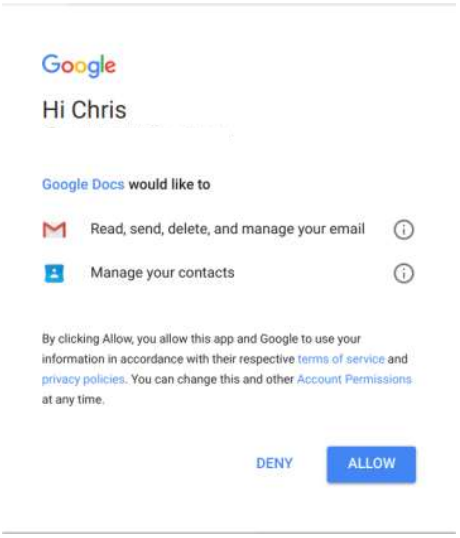
Parameswaran Krishnan has shared a document on Google Docs with you

If there are problems with how this message is displayed, click here to view it in a web browser.

Parameswaran Krishnan has invited you to view the following document:

Open in Docs

The link leads to a legitimate Google page requesting full permissions for an extension called ‘Google Docs’ to your email and contacts. **This extension is malicious** and **is not** the real Google Docs. Granting these permissions will result in your account immediately sending the same email to everyone you have ever emailed. Additionally, the attacker has permissions to your account which can be used for further attacks.



Google

Hi Chris

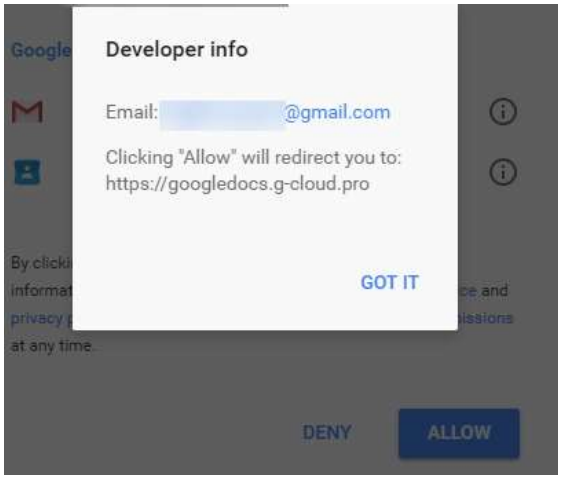
Google Docs would like to

Read, send, delete, and manage your email

Manage your contacts

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

Clicking on the 'Google Docs' link on this permissions page reveals that the web app was developed by a miscellaneous Gmail account. Clicking 'Allow' will grant that Gmail user access to your account.



Developer info

Email: [redacted]@gmail.com

Clicking "Allow" will redirect you to: https://googledocs.g-cloud.pro

What makes this attack significant is the malicious use of a real web app developed for Google accounts. You were not directed to a page *impersonating* Google, as is typical for these types of attacks. Instead, you were being asked by Google to give permissions to an attacker.

While Google quickly reacted to shut down this scam and disable the affected accounts, this method is likely to be seen again. Attackers now have a blueprint for more effective phishing attacks in the future.

Guidance

If you granted access to this malicious extension, Google suggests going to this site: http://g.co/SecurityCheckup and removing any apps you do not recognize. If you see one called 'Google Docs' **remove it** immediately. The real Google Docs has access to your account by default.

General best practices to protect your account from similar attacks include:

- Keeping a 'think before you click' mentality with links and attachments in email. Taking a second look before clicking could save you or your organization a lot of time and money. Do not be afraid to ask for help if you are not sure if a link is safe.
- Performing the Security Checkup, linked above, on a regular basis. This is a great way to keep tabs on what has permissions to your account and where your account is being accessed.
- Implementing **Multifactor Authentication** on your account. This requires access to your phone as well as your password to log in to your account and can be implemented for personal and business Google accounts.

If you have any questions on the above, please reach out to your ATS Account Manager. If you have an email that you suspect to be fraudulent, please forward it to security@networkats.com for investigation.