American Technology Services

2017-02 ATS Security Advisory

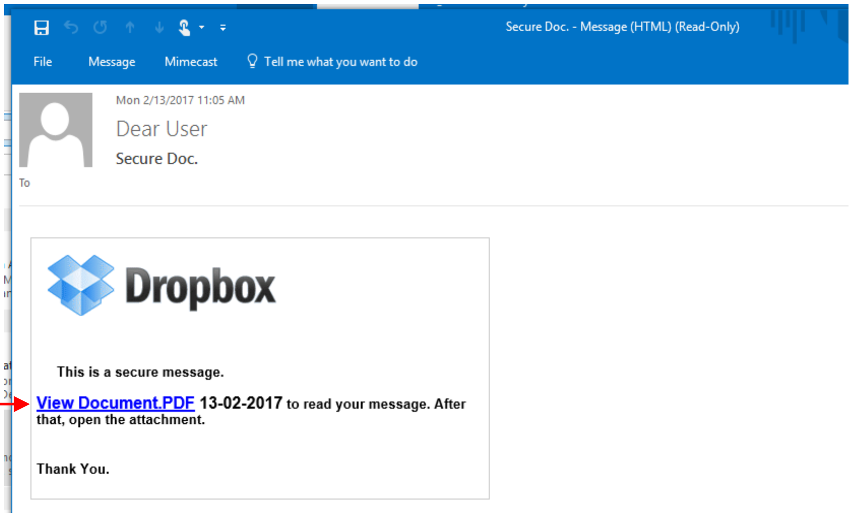
Phishing Attacks Simulating Federated Authentication Forms

Summary

Attackers are using phishing emails with links to landing pages that impersonate *federated authentication* pages from common providers such as Gmail, Office 365, Yahoo and Twitter. Typically, an attacker may send a link to a “secure” document or message hosted at one of these providers. The link leads to a landing page with a menu of service providers and fields to enter a username and password. Submitting any forms on this page simply gives the victim’s credentials to the attackers. The attackers may use these credentials to send spam or steal data. They may attempt to re-use the login and password combination on other services to broaden their attack.

Details

These phishing campaigns are sent in bulk and may have the branding or logo of a common and trusted platform, such as Dropbox, as seen below.


Secure Doc. - Message (HTML) (Read-Only)
File
Message
Mimecast
Tell me what you want to do
To
Dropbox

Mon 2/13/2017 11:05 AM

Dear User

Secure Doc.

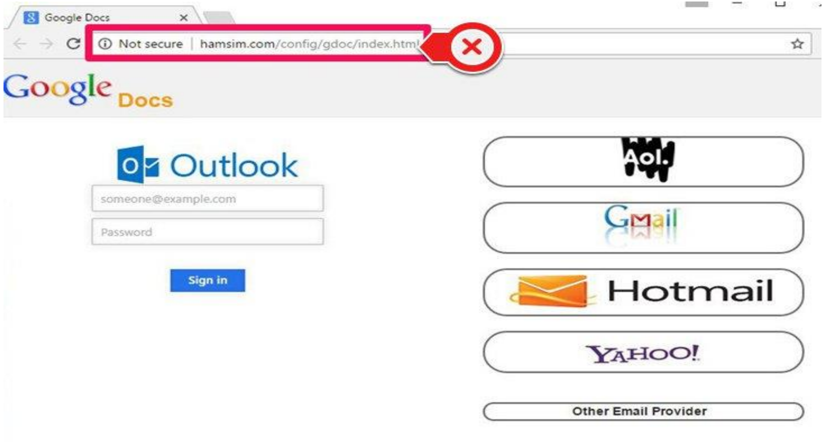
This is a secure message.

View Document.PDF 13-02-2017 to read your message. After that, open the attachment.

Thank You.

Not a link to Dropbox

When a victim clicks on the attacker’s link, they are directed to a landing page with various login options. The login options are designed to mimic federated logins offered by these various providers. However, the forms on the page submit directly to the attacker.



Google Docs

Not secure | hamsim.com/config/gdoc/index.html

Google Docs

Outlook

someone@example.com

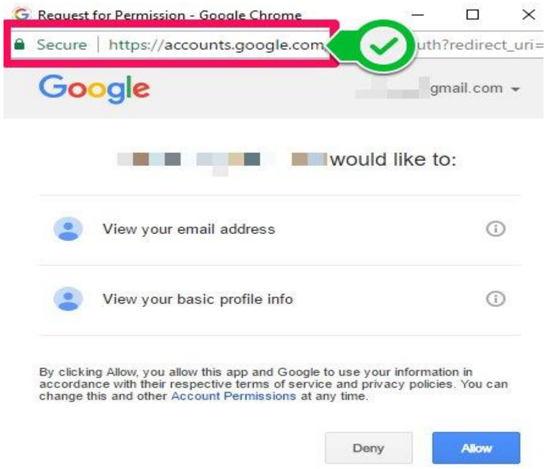
Password

Sign in

Attackers may immediately use the account to send spam email, steal information from the compromised account, or by using identical credentials on other service providers.

Guidance

Federated authentication from large providers such as Microsoft, Google, Twitter and Facebook are implemented for secondary services to simplify the authentication process for end-users and to speed up development. However, **federated logins never give actual credentials to these secondary services. Credentials are always submitted to the federated authentication provider, with granted permissions stated clearly.** An example, legitimate federated login form can be seen below.



Request for Permission - Google Chrome

Secure | https://accounts.google.com uth?redirect_uri=

Google gmail.com

would like to:

View your email address

View your basic profile info

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.

The most common method of avoiding these types of attacks is to Implement **Multifactor Authentication** for access to any tool where corporate data is stored. This will ensure that an attacker cannot access sensitive information even if they obtain a username and password combination. Checking the address bar for the “Secure” indicator (pictured above) before typing any password is also helpful, though it is possible for an attacker to spoof that in some cases.

If you have any concerns regarding security, 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.