Barracuda®

Solution Brief

How Cybercriminals are Impersonating Google Docs, Outlook and DocuSign to Steal Your Credentials

When you receive an email from a trusted web service such as Microsoft Outlook or DocuSign informing you of unread messages, you might blindly follow the directions to retrieve those messages. Unfortunately, cybercriminals are taking advantage of these trusted brands to convince you to log in to fake website portals and give up your login credentials. In this solution brief, we will examine how attackers are cunningly impersonating popular web services such as Microsoft Outlook, DocuSign and Google Docs to entice victims into giving away their credentials to these services. Criminals then use these credentials to either commit fraud or to launch targeted spear phishing campaigns within an organization to steal the crown jewels.

Highlighted Threat

Phishing attack by impersonation of popular web services.

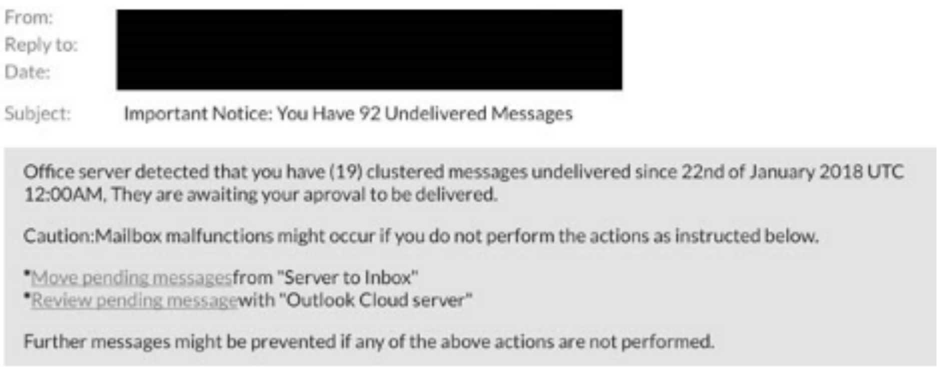
Web Service Spoof Directing to Fake Login Page

In these examples, Microsoft Outlook, DocuSign, and Google Docs are being impersonated or spoofed by email that contains a link that directs recipients to a fake login page on a legitimate website. There is no malicious attachment and cybercriminals are hoping victims will not recognize the web service web portal login page, and freely enter their credentials, giving attackers full access to their email accounts. In addition, the links used in these emails are typically "zero-day", meaning they have not been used before in other emails, and therefore don't appear in any bad link blacklists. Some of these links are legitimate small business websites that have been compromised and will appear to have a high reputation to traditional email security systems, which helps them evade detection.

Cybercriminal's simple yet very cunning tactics

This rise in web service impersonation attacks involves a few simple but effective tactics on behalf of cybercriminals:

- Including a link to a web page that prompts employees to log in. Here are several examples of these phishing emails:



From:
Reply to:
Date: [redacted]

Subject: Important Notice: You Have 92 Undelivered Messages

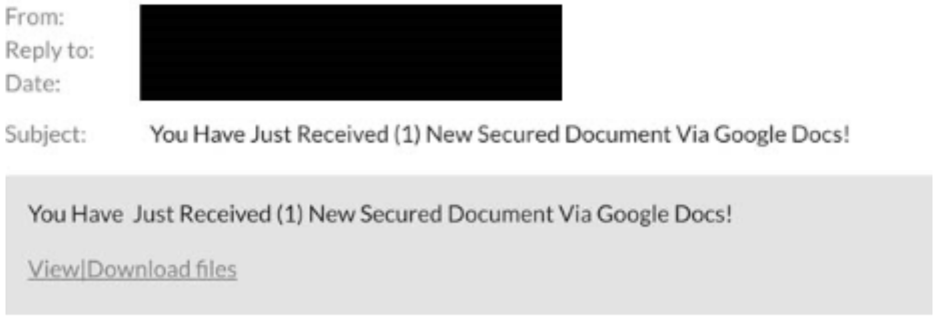
Office server detected that you have (19) clustered messages undelivered since 22nd of January 2018 UTC 12:00AM, They are awaiting your aproval to be delivered.

Caution:Mailbox malfunctions might occur if you do not perform the actions as instructed below.

*Move pending messagesfrom "Server to Inbox"
*Review pending messagewith "Outlook Cloud server"

Further messages might be prevented if any of the above actions are not performed.

~~



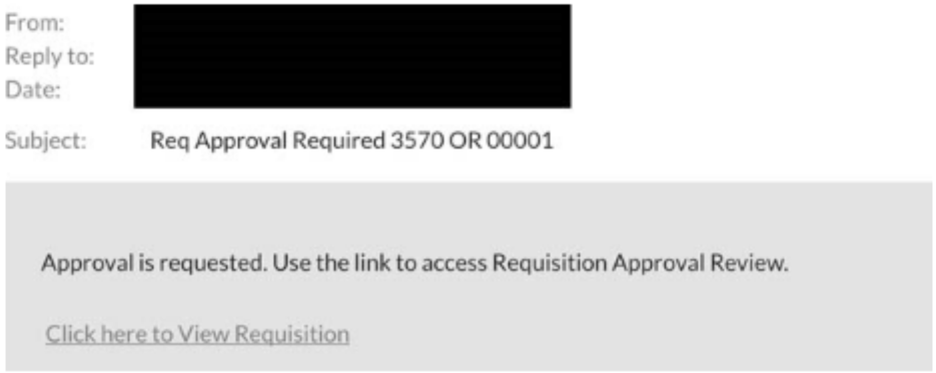
From:
Reply to:
Date:
[redacted]

Subject: You Have Just Received (1) New Secured Document Via Google Docs!

You Have Just Received (1) New Secured Document Via Google Docs!

View|Download files

~~



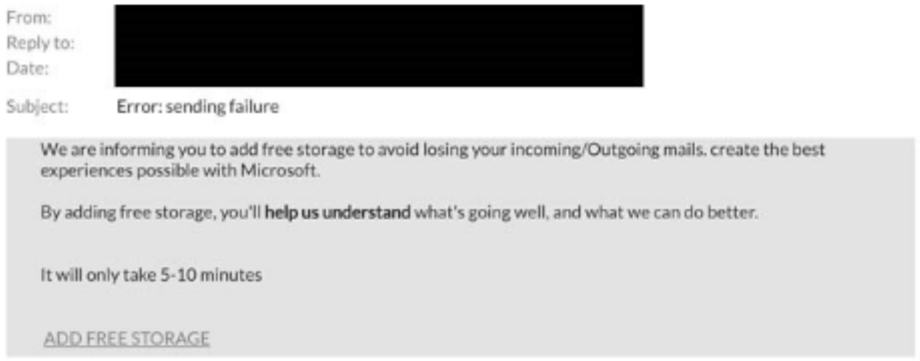
From:
Reply to:
Date:
[redacted]

Subject: Req Approval Required 3570 OR 00001

Approval is requested. Use the link to access Requisition Approval Review.

Click here to View Requisition

~~



From:
Reply to:
Date:
[redacted]

Subject: Error: sending failure

We are informing you to add free storage to avoid losing your incoming/Outgoing mails. create the best experiences possible with Microsoft.

By adding free storage, you'll **help us understand** what's going well, and what we can do better.

It will only take 5-10 minutes

ADD FREE STORAGE

- From there, when the unsuspecting victim clicks on the link and is directed to a fake sign-in page, they will provide attackers with their username and password without knowing they had done anything out of the ordinary.
- After stealing the victim's credentials, the attacker will typically use them to remotely log into the user's Office 365 or other email accounts and use this as a launching point for other spear phishing attacks.
- At this point, it becomes even more difficult to detect attackers at work because they will send additional emails to other employees or external partners, trying to entice those recipients to click on a link or transfer money to a fraudulent account.

Traditional email security solutions will not detect this attack!
This evolving attack will not be detected by existing email security solutions on the market for a host of reasons:

- This links included in the email attacks are typically zero-day in which a unique link is used in each email sent to potential victims. Therefore, they will never appear on any security blacklists.
- In most instances, the links included lead to legitimate websites, where the attacker has maliciously inserted a sign in page, and the domain and IP registration will appear legitimate
- Unfortunately, link protection technologies such as "safe links" will not protect the user against these links. Since the link contains a sign in page and does not download any malicious viruses, the user will follow the "safe link" and will still enter the username and password.

Even if an organization has traditional email security technologies enabled, there will be nothing preventing the user from providing their credentials to the cunning cybercriminal. The best hope to stop these attacks is artificial intelligence for real-time spear phishing protection like Barracuda Sentinel in addition to regular training to raise awareness of evolving and new threats.

Barracuda Sentinel saves the day

Barracuda Sentinel's artificial intelligence real-time solution can be taught to automatically detect and quarantine these emails. In this case, Barracuda Sentinel can recognize how a normal email from a popular web service looks based on the signals in the email metadata and body. Here is an example:

- You would expect emails from Facebook to come from messages@facebook.com and include a link to facebook.com.
- It is very unlikely to receive an email from john@facebook.mydomain.com with a link to sdfsdf.co.uk.
- Even if the sdfsdf.co.uk link has a high reputation and does not appear on any blacklists within the context of an email from Facebook, it is extremely unlikely to be legitimate.

Barracuda Sentinel can spot this discrepancy despite the link being reputable and prevent the email from reaching any end users. This is vital as it is guaranteed that someone in your organization will eventually fall for this bait.

Security awareness training is required for all

Organizations must plan for email threats such as these and many others, train all their employees, test them on the latest email threats, and work to ensure everyone is a security advocate. Traditional email security will not catch these threats, and not every employee will delete the email, so incorporating a holistic risk prevention strategy with the latest email security technologies such as Barracuda Sentinel and regular security training such as Barracuda's new Phishline offering will best prepare you for the next threat tactic cybercriminals use to try to steal your information.

US 1.0 • Copyright 2018 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com
Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.