ODDVAR MOE'S BLOG

Notes from My adventures with Windows security

OFFICE 365 SAFE LINKS BYPASS

Posted on 3 Jan 2018

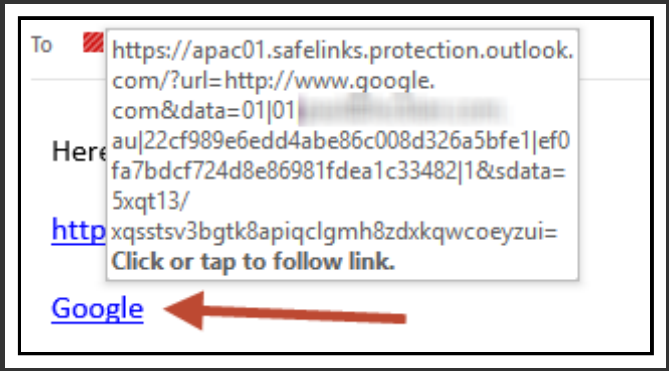
Time for a break from the AppLocker case study to blog about this issue, since I found it very interesting.
This issue was actually discovered by me and a customer of mine by coincidence.
The issue has been run through Microsoft Security Response Center (MSRC) and they concluded that this can be fixed with a Group Policy setting. This blogpost will show the bypass and the setting you need to apply to prevent this Safe link bypass, but first I need to give a brief explanation of the safe link feature for those that are not familiar with it.

Safe links in Office 365 is a part of the Office 365 Advanced Threat Protection. If you have Office 365 Enterprise E5 or Education E5 you have this included. Office 365 Advanced Threat Protection is an add-on to Exchange online. After you buy this add-on you will get the following features:

Feature	ATP standalone	Exchange Online Protection
Safe Links	Yes	No
Safe Attachments	Yes	No
Spoof intelligence	Yes	No
Quarantine	Yes	Yes
Advanced anti-phishing capabilities	Yes	No

More information on the different licenses can be found here:
https://technet.microsoft.com/en-us/library/exchange-online-advanced-threat-protection-service-description.aspx

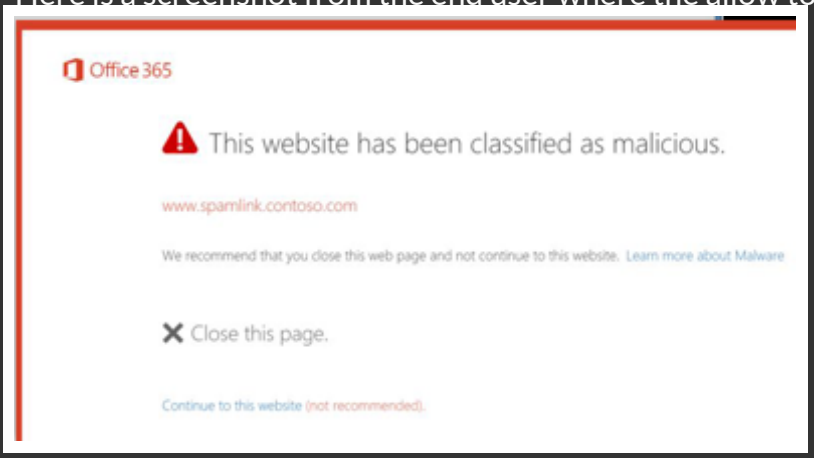
Safe links put simple is basically a service that changes every incoming link to point to safelinks.protection.outlook.com before the mail is delivered to the users inbox. A link to google.com would look like this when it is delivered to the end user:



On the server side you can configure rules for things that should happen if a user clicks on a link that is malicious. You can read more about the different configuration options here:
https://support.office.com/en-us/article/Set-up-Office-365-ATP-safe-links-policies-bdd5372d-775e-4442-9c1b-609627b94b5d

Put simple, you choose if the safe link feature is on/off, and if the user should be allowed to visit sites that are flagged as malicious or not. You can also choose if it is supposed to be enabled for all domains or just certain users.

Here is a screenshot from the end user where the allow to visit the malicious site is enabled:



THE BYPASS

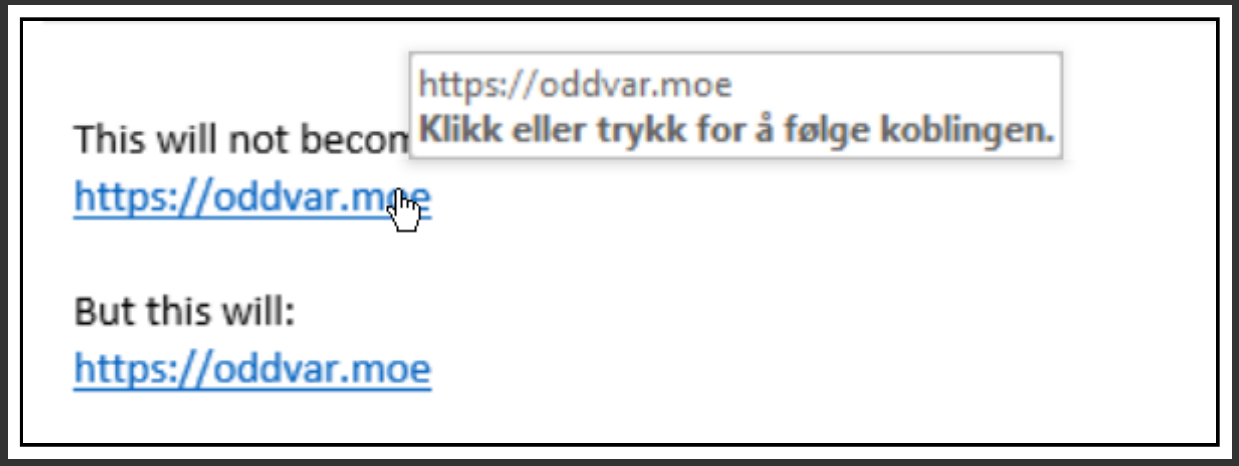
The bypass is really simple and I was surprised that this worked at all. This bypass only works if the receiver is using Outlook (AFAIK). What you do to bypass Safe link is simply to send an email to someone containing an evil link without the link. In the following screenshot you will see two different links within an email message that is about to be sent, the first will be bypassed and the second will be picked up by safe links.

Mail sent:

This will not become a safe link:
https://oddvar.moe

But this will:
https://oddvar.moe

Mail received:

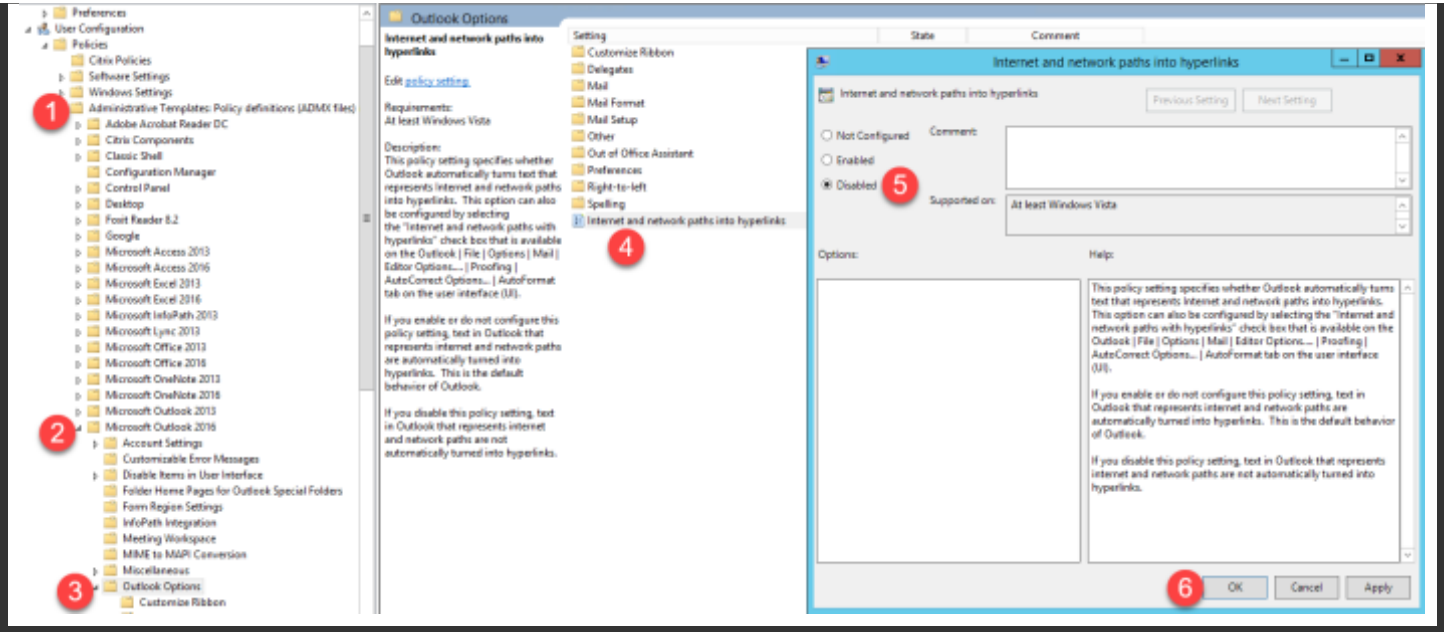


A typical example where you would use this technique is during a phishing attack.

HOW TO PROTECT

The easy way around this is of course to only allow plain-text mail.
The problem with that is that the users will probably complain when they have to copy every link manually instead of clicking it.

Instead I would recommend to turn of automatic conversion of text to hyperlinks in Outlook using Group Policy. The setting is named "Internet and network paths into hyperlinks" and is located directly under "User Configuration –> Administrative templates –> Microsoft Outlook 2016 –> Outlook Options". The setting needs to be set to disabled.



After you have rolled this setting out Outlook will no turn plaintext urls into hyperlinks.

If my blogpost triggered your interest in bypassing safe links I would also recommend to check out these blogposts:

https://emtunc.org/blog/03/2017/bypassing-safe-links-exchange-online-advanced-threat-protection/

https://www.trustedsec.com/2017/02/office-365-advanced-threat-protection-features-shortfalls/

https://halon.io/blog/fooled-microsofts-safe-link-technology/

Cheers!

TIMELINE

- 11/11/2017 – First reported
- 13/11/2017 – MSRC created case
- 16/11/2017 – I requested an update
- 17/11/2017 – I requested an update
- 18/11/2017 – MSRC says a duplicate case exists
- 29/12/2017 – Case closed with this explaination:
  "The engineering team has determined that the behavior described in that and this case is by-design – there's not much that Safelinks can do currently against a client-side setting to autoformat plaintext into clickable hyperlinks. We are, however, evaluating the potential of adding a new feature to integrate with the Safelinks API in Outlook to address issues like this. Customers who are concerned about this issue today can push a GPO update to set the autoformat hyperlinks option as disabled."
- 03/01/2018 – Published this blogpost

RELATED

Windows Defender Attack Surface Reduction Rules bypass
In "Security"

AppLocker – Case study – How insecure is it really? – Part 1
In "Security"

Research on CMSTP.exe
In "Security"

PREVIOUS POST
Harden Windows with AppLocker – based on Case study part 2

NEXT POST
Putting data in Alternate data streams and how to execute it

2 THOUGHTS ON "OFFICE 365 SAFE LINKS BYPASS"

Havard Overas says:
3 Jan 2018 at 3:58 pm
I got this answer from an ATP Program Manager regarding the same thing:

Thanks for sending your email and the details of the issue. The Outlook client has a setting which makes text that looks like URLs clickable ON by default. While this is great for productivity, we believe it's not ideal for implementing the highest level of security. For admins, they can create a GPO to change the setting and turn this setting OFF. If they're not using Outlook, then we recommend them to switch to using Outlook for the best experience. In the future, we'll have even tighter integrations with Outlook to cover this type of scenario even when the setting is ON. I hope that clarifies the concern.

★ Like

Reply

Oddvar Moe [MVP] says:

3 Jan 2018 at 3:35 pm

Okay. Thanks for the feedback. 😊

★ Like

Reply

LEAVE A REPLY

Enter your comment here...

Search …

SEARCH

POWERED BY WORDPRESS.COM.