THREAT BULLETIN

TAR20230427-002: [Threat Analysis Report] Phishing Campaign Targeting Facebook Session Cookies

TLP
White

PUBLISHED DATE
28 Apr 2023 14:38:07

DESCRIPTION

TLP:CLEAR Disclosure is not limited.

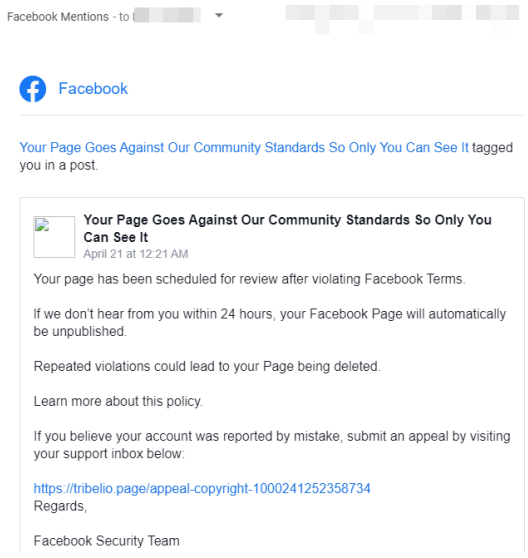
Summary

The MD-ISAC has recently observed a phishing campaign targeting Facebook page administrators, where the page administrators receive a notice that their page has been suspended due to a violation of community standards. Phishing emails often impersonate social media site login pages, hoping to gain access to pages with a large following. Access to a large social media account can allow threat actors to spread false information, compromise other users, or even infect other users with malware.

While this technique is not something new, what is notable about this newly observed campaign is that the actor is not attempting to harvest login credentials. Rather, the goal of this attack is to prompt the user via video instructions to give over session cookie values, thereby allowing the actor to take over the logged in session and bypass MFA.

Technical Details

The MD-ISAC has observed a phishing campaign in which the threat actor created a Facebook account with the display name "Your Page Goes Against Our Community Standards So Only You Can See It." The actor then created a post stating that "Your page has been scheduled for review after violating Facebook Terms. If we don't hear from you within 24 hours, your Facebook Page will automatically be unpublished." The post also provided a link that the page admin can click to "appeal" the decision. In each post, the actor tagged a list of accounts, thus causing the account admins to receive an email from Facebook regarding the mention. This message passes the basic email application and user security checks, because it is from a Facebook email account and matches all other emails that the recipient is used to receiving.


Facebook Mentions - to

Facebook

Your Page Goes Against Our Community Standards So Only You Can See It tagged you in a post.

Your Page Goes Against Our Community Standards So Only You Can See It
April 21 at 12:21 AM

Your page has been scheduled for review after violating Facebook Terms.

If we don't hear from you within 24 hours, your Facebook Page will automatically be unpublished.

Repeated violations could lead to your Page being deleted.

Learn more about this policy.

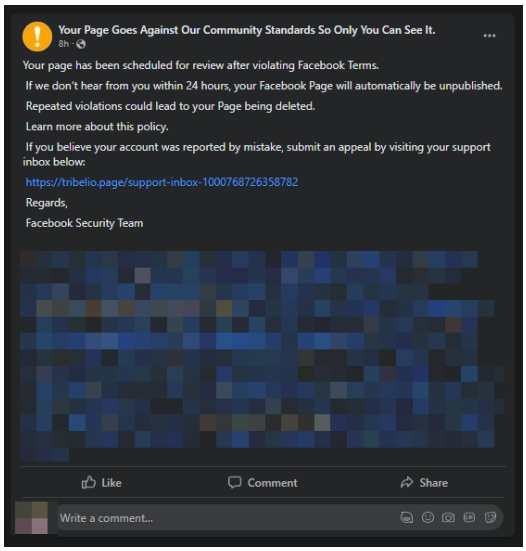
If you believe your account was reported by mistake, submit an appeal by visiting your support inbox below:

https://tribelio.page/appeal-copyright-1000241252358734
Regards,

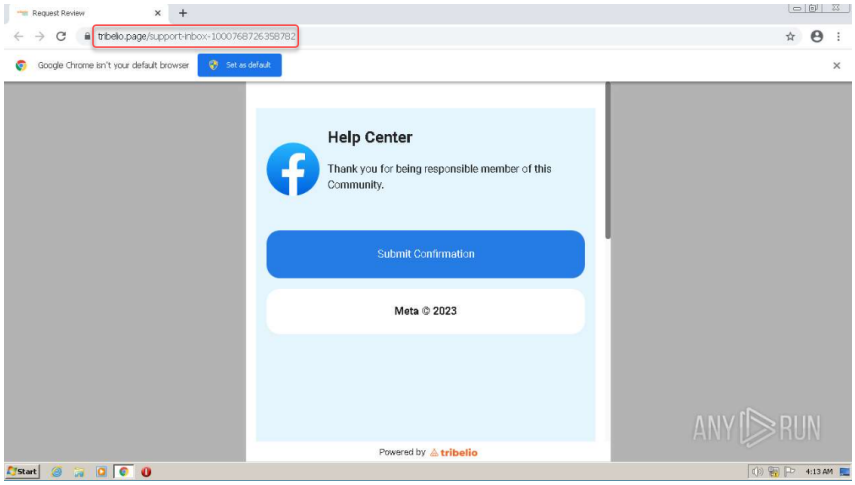
Facebook Security Team

Email Message from Facebook Notifying the user of the account mention

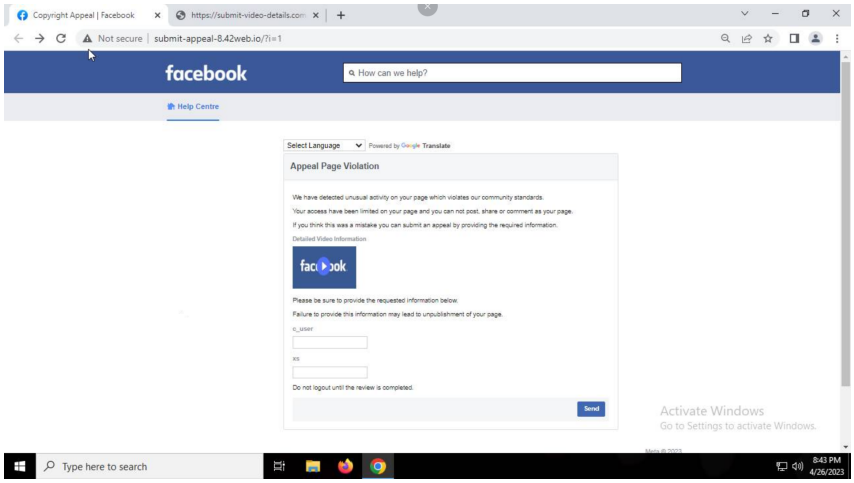
When the user opens the post linked in the page, the user is given a link to "appeal" the decision. The fact that this post is hosted on facebook.com lends a false legitimacy to the claim, even though Facebook does not use posts as a method of communicating with users regarding account matters.



Facebook post containing the account mention

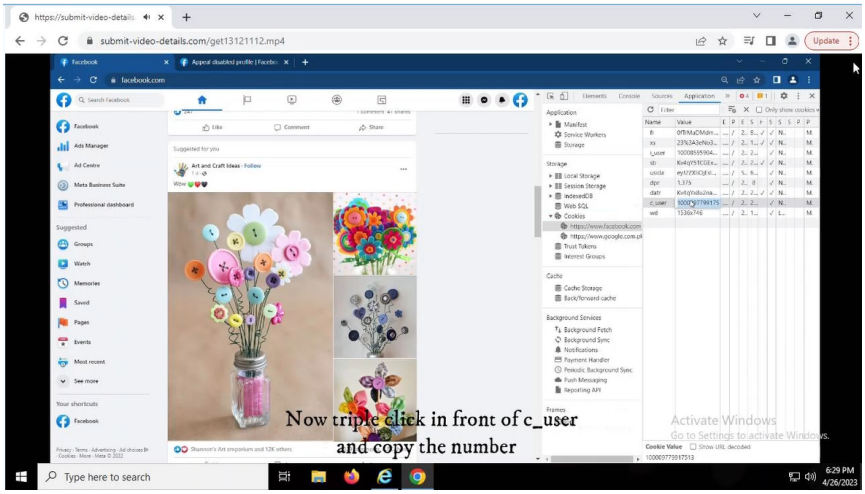


Upon clicking the link contained in the Facebook post, the user is directed to a site (not on the Facebook domain) inviting them to submit a confirmation to the Facebook help center. When navigating to the “help center,” the user is directed to submit a “copyright appeal.”



The user is instructed to watch a video to learn how to submit the appeal. The video instructs the user to login to Facebook using the Chrome browser on a PC. The user is then instructed to open the Chrome developer tools, navigate to the cookies list, and copy out the values in the c_user

and xs cookies. The user is then expected to use those values to submit an appeal, and is advised not to log out until the “review” is completed.



A still shot of the video explaining how a user can access the cookie data. If you would like a copy of the video provided by the actor, please email md-isac@maryland.gov.

These values will likely be used by the actor to take over the user session, thus bypassing the need to use credentials and MFA tokens. The c_user cookie contains the value of the current user’s ID. The xs value contains the session number, the session secret, and an optional secure flag, separated by a %3A.

With this data, the actor can then take over the user session, thus allowing him to change the login and MFA information and take full control of the account.

It is also worth noting that it is possible to buy or sell valid session cookies on the dark web. These are often captured via stealer malware or bogus browser extensions, and new cookies are listed for sale daily.

Indicators of Attack/Compromise

Note that relevant indicators were included in the associated ICARs as well.

Message sender: mentions@facebookmail.com

Message Subject: [REDACTED]: Your Page Goes Against Our Community…

https[://]tribeliop[.]page/support-inbox-1000768726358782

https[://]tribelio[.]page/support-inbox-10007687263677782

http[://]submit-appeal-8[.]42web[.]io/

http[://]submit-video-details[.]com/

Tactics and Techniques

Establish Accounts: T1585
Phishing for Information: T1598
Steal Web Session Cookie: T1539
Valid Accounts: T1078
Account Manipulation: T1098
Compromise Accounts: T1586

Mitigations

User Training: M1017
Software Configuration: M1054
User Account Management: M1018

Detections

Persona: DS0021
User Account: DS0002

References

https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a

https://gbhackers.com/how-hackers-steal-web-session-cookies-from-facebook-in-chrome/

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report incidents to MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).

Reporting and Contact Information

In the case of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5-406(b)(2)) mandate that you report this via the Maryland Incident Reporting System. It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).