

Forum:[Hack Forums](#)

Thread: [Phishing and anti-phishing techniques: instagram](#)

bob_hacker_543 - February 20, 2023, 8:29 am

Hello good people,

I'm making a research for my studying: "Phishing attacks and countermeasures". I've found that instagram fights with phishing quite good. At least a script-kiddie like me can't phishing it so easily. So I wanted to ask you do you know how they prevent this kind of attacks?

What I have figured out:

1. Evilginx2: their phishlets doesn't work with instagram because all of them outdated. Also, with a little update of the phishlets, we see that handshake to one of their (static.cdninstagram.com) is broken. So, seems like this server is used for downloading js and image files. Also, seems like they use some additional layer of defends because if you just open instagram through proxy (I've built one manually but also some online could be used), you will see "this page doesn't exist" first.
2. You can't build your own html page since API is not available and their internal login functionality that is used in browsers has some dependency on these js files from cdninstagram.com (my observation) and also uses some crypting on passwords. I assume that algorithm/salt is based on this as well.

So my theory is:

when you open instagram.com they send a request to static.cdninstagram.com with some client information. If domain/ip/something else information isn't the same as for instagram.com -> they break connection. Also, static.cdninstagram.com returns js files for loading login form and how to crypt password (so without access to this server you can't use login api).

Do someone knows more about it? Am I right or wrong? is it a good defense or could be easily bypassed?

Thank you in advance.

DramaKing - February 20, 2023, 9:30 am

Obviously, if the victim manually enters instagram.com, they will get Instagram and send credentials over HTTPS to Instagram's servers. If you try to direct the connection to your server, the certificate will be wrong (broken connection as you mention).

bob_hacker_543 - February 20, 2023, 9:58 am

Does that mean I'm right and it's quite good defense that could be hard to bypass?

Since it's a phishing, of course victim will not enter instagram.com manually. Let's say victim has a link (to hacker's website, let's say it's Instagram.com or whatever else) and tries to open/login there with 2FA. The use case is quite simple: by any social engineering technique victim receive a link and trust it. So the victim opens a link and enters credentials, then receive SMS password and login successfully to a service, the hacker receives cookies on their end and could use it to stole user's information.

And if some websites could be hacked by this technique quite easily, instagram seems like spent some time on defending. What's good of course, but would be great to know how they are doing this and how to bypass it (theoretically).

Vishal ram - February 20, 2023, 11:36 am

you need a live panel and scama page so you can get the otp to login live.

bob_hacker_543 - February 20, 2023, 9:33 pm

(Feb 20, 2023 12:36 PM)Vishal ram Wrote: [\[CITE\]](#) you need a live panel and scama page so you can get the otp to login live.

Could you please describe it a bit more? What is "scama page"? Isn't this what I'm referring to - just a phishing "fake" page? it doesn't work like that with instagram or I missed something?