Vulnerability analysis of the Facebook authorization mechanism
Contents

Introduction .............................................................................................................................................. 3
Impact ...................................................................................................................................................... 4
Vulnerability highlights .......................................................................................................................... 4
Attack Vector .......................................................................................................................................... 4
Detail Technical Analysis ...................................................................................................................... 5
  Click and redirections .......................................................................................................................... 5
  Validation of the geographic position ............................................................................................... 6
  Generate, reflect and collect access tokens for Facebook API access ............................................. 7
  Accumulating victim information ...................................................................................................... 9
  Uploading picture and comment ....................................................................................................... 11
  Tagging friends ................................................................................................................................ 12
Malicious servers .................................................................................................................................. 12
Possible defense mechanism against this scam & similar threats ....................................................... 13
Conclusion ............................................................................................................................................... 14
Introduction

With the increasing popularity and number of users on Facebook, cyber criminals now know where to hunt for their victims. As per the recent reports till March 2013 Facebook hosts 1.11 billion user profiles. Now that’s a huge number, and cyber criminals very well realize this. Reports state that scams targeting the social network have doubled. The fact that Facebook is now becoming a huge platform for spammers/scammers/cyber criminals to reach out to more users, easily, is no new news. A post getting viral plays a huge role in spreading them, taking scam propagation to next levels.

In such scenarios, it is important to find out what happened, how an account got compromised and more importantly to remove all traces of the spam links. This research paper is an attempt to dissect a Facebook oriented scam namely ‘lady with razor-sharp axe’, which goes beyond the traditional intentions of a scam on Facebook.
Impact
Victims find themselves involved with numerous Internet scams such as clickjacking attacks, spammy reward offers or survey scams, without their knowledge and permissions. The threat gets dangerous with identity fraud and/or scam attacks getting involved also. Apart from this the scam also stores stolen Facebook access tokens onto command servers for further attacks or exploits, clearly indicating that this attack is not limited to tagging or uploading of photos. Upon clicking the link, Facebook users are unwittingly handing over complete access to their Facebook account, which remains available to attackers even after an affected user logs out from Facebook account.

Vulnerability highlights
CTRL’s investigation on Facebook’s access token authorization mechanism brought into light some key highlights which include:

- When someone connects with an app using Facebook login, the app is able to obtain access token that provides temporary secure access to Facebook APIs. Normally, an app gains rights to a Facebook user’s access token only after the user authorizes that request.
- Facebook’s access token authorization mechanism has a security vulnerability that allows cyber attackers to bypass Facebook’s Access Token Authorization mechanism. This entitles cyber attackers to generate unauthorized yet valid access tokens.
- Such unauthorized yet valid Access Tokens have permissions to perform a range of activities such as uploading photos and videos, posting comments, pay with Facebook, publish content, and send SMS, read mailbox, tag friends’ photos and more. With this, an attacker is able to perform nearly every task which a Facebook user can do and hence can wield various malicious actions.
- The ongoing Facebook spam - ‘lady with razor-sharp axe’ tends to store such stolen Facebook Access Tokens on their servers for further attacks or exploits. This attack is not limited only to tagging or uploading of photos. Facebook users are unwittingly handing over complete access to their Facebook account, which remains available to attackers even after an affected user logs out from Facebook account.

Attack Vector
The attack vector is definitely Facebook-a social networking platform, which is widely used by billions of users and the attack can be categorized as a Web attack.
Detail Technical Analysis

The threat appears as a casual tagged photograph on FB asking users to click on a link in the description. Once the user clicks on the link the following phases occur:

1) Click and redirections
2) Validation of the geographic position and human check
3) Generate and reflect access tokens for Facebook API access
4) Accumulating victim information
5) Uploading picture and comment
6) Tagging friends

Click and redirections

The tagged picture as shown in the image below had a description asking to check what happened next by clicking on the link http://tinyurl.com/xxxxxxx/?cid=51b014466dd6

As soon as the user clicks the link, he/she will be redirected to http://ni-azamoo.xxx.xx.cm/?cid=51b014466dd6

A closer look into this normal looking process, disclosed a number of hidden malicious activities happening, in the backend.
The malicious activity started by accessing 'ringa.php'; hosted on the domain 'xxxxxx.info'. On further investigation it was found that the domain owner's information for 'xxxxxx.info' was protected (or hidden) using 'WhoisGuard' services.

**Validation of the geographic position**

Next an access to http://xxxxxx.info/ringa.php turned out as HTTP 302 redirection to http://nu-zamoo.eu01.xxx.xx.cm/?cid=51b0144660dd6 which has following HTML page,
http://j.maxmind.com/app/geoip.js was used to get city information. The strange fact is that if the victim's city is one of the following then the user was redirected to http://youtube.com
1) Torrance
2) Menlo Park
3) Palo Alto
4) Montara

Although the reason for such an action is unknown, it indicates that the cities are from Silicon Valley and the attackers didn't desire to mess with them.

But in our case the city was Ahmedabad, India and hence we were redirected to http://0xXXXXXXXX/~silali/watch/jack.php which finally looks like below,

Generate, reflect and collect access tokens for Facebook API access
An investigation of the backend activity happening during this process CTRL found the scam generating and reflecting access token by accessing below backend URL to his malicious webpage.

http://0x404f4ce2/~silali/watch/blank3.php?u=view-source%3Ahttps://facebook.com%3Fapi_key%3D139682082719810%26skip_api_login%3D1%26display%3Dpopup%26cancel_url%3Dhttp%3A%2F%2Fwww.facebook.com%3Fapi_key%3D139682082719810%26skip_api_login%3D1%26display%3Dpopup%26error_reason%3Duser_denied%26error%3Daccess_denied%26error_description%3DThe+user+denied+your+request..%26fbconnect%3D1%26next%3Dhttps%3A%2F%2Fwww.facebook.com%2Fdialog%2Fpermissions.request%3F_path%3Dpermissions.request%26app_i d%253D00000000000000000000000000000000%26client_id%253D00000000000000000000000000000000%26redirect_uri%253Dhttps%3A%2F%2Fwww.facebook.com%2Fconnect%2Flogin_success.html%3Fdisplay%3Dpopup%26type%3Duser_agent%26perms%3Doffline_access%26fbconnect%3D1%26from_login%3D1%26rcount%3D1%26rcount%3D2&framed=1

NOTE: 0xXXXXXXX is nothing but HEX conversion of IP address 64.79.76.XXX. Yes, it is one of the evasion technique used against security products uses only IP and FQDN for filtering.
What surprised us is the fact that we found an access token in the URL. In our hunt for an answer for the same, we found the below definition from Facebook.

“When someone connects with an app using Facebook Login, the app will be able to obtain an access token which provides temporary, secure access to Facebook APIs.”

Once victim clicks on the play button (seen in the previous screen, shown above), it asked the user to follow some steps- resembling a human check.

The above key combinations looked suspicious and on further investigation it was revealed that it was used for nothing but copying the above generated access token from the location bar.

A closer look into the process indicated the fact that the user himself was copying and then pasting the generated access token embedded in the URL to the command server for further exploits/usages.

*https://developers.facebook.com/docs/facebook-login/access-tokens/*
As soon as the user enters CTRL+V, the second phase of the malicious activity begins by accessing number of backend URLs explained below. During this duration the scam shows a fancy progress bar to keep the victim waiting for few seconds.

Accumulating victim information
Having obtained access tokens, next the scam tries to accumulate information. Once the scam got the access token, it now has temporary and secure access to Facebook APIs.

It was also found that Facebook's Graph API was been used to check what permissions are available for access token using below backend URL,

https://graph.facebook.com/me/permissions?access_token=CAABZCCktscCEIABKZADaUVmyKMWvi1bXVbd04qghUDNBOH000000000000XX00ZASEPDJuZAuSGH3uOZC21JH2c0X8VjmWdAF6yX12C867ukK3c615SHYOZHAK8gKNYLY4ZAS5eEChJ3uBtR4KHLpNpYuYyZD5=_1371452559417

```
{
    "data": {
        "installed": 1,
        "read_stream": 1,
        "manage_videos": 1,
        "manage_friends_lists": 1,
        "pay_with_facebook": 1,
        "read_wall_posts": 1,
        "read_post_wallboxes": 1,
        "publish_checkins": 1,
        "status_update": 1,
        "photos_upload": 1,
        "video_upload": 1,
        "sts": 1,
        "create_event": 1,
        "rsvp_event": 1,
        "offline_access": 1,
        "email": 1,
        "app_login": 1,
        "create_note": 1,
        "share_photo": 1,
        "publish_stream": 1,
        "publish_likes": 1,
        "uds_management": 1,
        "access_private_data": 1,
        "read_insights": 1,
        "read_requests": 1,
        "manage_notifications": 1,
        "read_friend_lists": 1,
        "manage_pages": 1,
        "physical_login": 1,
        "manage_groups": 1,
        "publish_actions": 1,
        "read_decks": 1,
        "app_notifications": 1,
        "whitelisted_offline_access": 1
    }
}
```
As shown in the above image, the malicious process got all the necessary permissions to propagate itself.

As per the definition by Facebook,

“The Graph API is the primary way that data is retrieved or posted to Facebook. The Graph API Getting Started Guide contains an overview of the basics of the API and walks you through using the Graph API Explorer. It also shows you how names work, how permissions work and what connections are.’

Later, the scam fetched friends list using below backend URL,

https://graph.facebook.com/me/friends?limit=3000&access_token=CAABZCCKsCEIBAKZADalUmyKMWi1bXVbd8O4ghUDN0000000000X0XX0dZASEPDJuZAuSGH3uJ/OZC1JH2c0XBlvjmWdAF6yX1ZCB7uK3c61SQHYOCHHZAKgKINYL4ZASEiECH3U3bRlK4HlpNpvYgZD&_=1371452559959

The response seen was evident of the same,

Yet another backend URL, fetches user’s detail,

https://graph.facebook.com/me?access_token=CAABZCCKsCEIBAKZADalUmyKMWi1bXVbd8O4ghUDN0000000000X0XX0dZASEPDJuZAuSGH3uJ/OZC1JH2c0XBlvjmWdAF6yX1ZCB7uK3c61SQHYOCHHZAKgKINYL4ZASEiECH3U3bRlK4HlpNpvYgZD&_=1371452560235

Yet another backend URL, fetches user's detail,

https://developers.facebook.com/docs/reference/api/
Here is the evidence for that,

Apart from these, the scam was also found posting the hacked victim details to its command centre for offline usage by an attacker;


Uploading picture and comment

After accumulating enough detail, next the scam began with propagation by uploading a photo to victim's Facebook without his information using below POST request using Graph API and access token,
If you can see, the same tiny URL has been shared with uploaded picture for continue the propagation.

Also, added comment to uploaded pic,

If you can see, the same tiny URL has been shared with uploaded picture for continue the propagation.

Also, added comment to uploaded pic,

Tagging friends

In order to assure maximum propagation, the scam tags all friends collected from friends list to the uploaded picture to ensure the obvious reflection the post on their wall or timeline.
After completing all the above mentioned backend activities in a mere time span of 2-3 mins, victim is shown a page like the one shown in the below figure indicating the completion of the process.

And finally redirects to image content making victim believe that the process was genuine.

![Image of verification page](image1.png)

![Image of redirected page](image2.png)

**Malicious servers**

The servers used for the threat include:
1) XXX.XX.cm --- Primary Content Server hosted on Amazon cloud
2) XXXXX.info --- Used for redirection
3) 64.79.76.XXX --- Reflecting server

**Possible defense mechanism against this scam & similar threats**

1) As a Facebook user, do not get tempted to visit or click this video / link
2) Any Facebook user who has already visited this link should immediately change his / her Facebook account password, for this would lead to expiry of old Access Tokens
3) Turn-off “Apps you use” from App Settings in Facebook account so that no app is able to gain access token to Facebook account

**Cyberoam Threat Protection against the ‘lady with razor-sharp axe’ Facebook Scam**

As far as Cyberoam users are concerned with regard to the ‘lady with razor-sharp axe’ scam, they can stay safe by filtering LAN-to-WAN traffic using web filter keeping “Spyware” category as denied. Cyberoam users can also detect/drop access to Facebook Graph API using application filter.
Conclusion

These findings clearly indicate a security vulnerability that allows cyber attackers to bypass Facebook’s Access Token Authorization mechanism, which entitles cyber criminals to generate unauthorized yet valid access tokens. Some of the noteworthy facts of this attack like protecting domain owner information, converting IP addresses into HEX conversation, avoiding attacks on specific cities and so on, indicates the quantum of efforts attackers/criminals are taking to ensuring their identity isn’t revealed.

CTRL has already reported this vulnerability to Facebook and extensive investigation from CTRL would be revealed upon suitable reciprocation or release of security patch from Facebook. In the wake of such growing threat incidents, Cyberoam believes that users of Social Media need to be provided with adequate awareness to promote safe social networking.

As far as Cyberoam users are concerned with regard to the ‘lady with razor-sharp axe’ scam, they can filter LAN-to-WAN traffic using web filter keeping “Spyware” category as deny. Cyberoam users can also detect/drop access to Facebook Graph API using application filter.