

Arti i phishing

Exclamation Arti i "Phishing" - Kush eshte viktima e rradhes?

Eshte e pabesueshme qe edhe sot e kesaj dite, kohe ne te cilet njerezit jane bere me te ndergjegjshem per sigurine e te dhenave personale ne internet, fenomeni i phishing eshte kaq i perhapur dhe funksionon me sukses. Ne forume te ndryshme gjen username dhe passwords per HI5, MySpace, Windows Live, Yahoo, Steam, Rapidshare etj., pa llogaritur kartat e kreditit te vjedhura ne menyra nga me banalet.

Phishing jo vetem qe nuk po zhduket, por po lulezon... duket sikur perdoruesit sa vijne e behen me naive per te mos thene idiote ne raportet me menyren se si e menaxhojne informacionin personal. Te jete ky faji i shoqerive te ndryshme qe pretendojne se kane rritur sigurine e sherbimeve qe ofrojne apo i vete perdoruesve? Kete nuk di ta them... por ka shume mundesi qe te jete njeri nga ju viktima e ardhshme e nje phishing te sukseshem.

Keshtu qe ta kuptoni sa e thjeshte eshte te ndertosh faqe te tilla dhe te biesh per nje cast viktime e tyre, ndiqni me poshte demostrimet perkatese.

NUK ESHTË QELLIMI I KETIJ TEKSTI TE INSTRUKTOJE TE TJERET SI TE NDERTOJNE FAQE PHISHING, POR TE DEMOSTROJE SA E E THJESHTE ESHTË TE NDERTOHEJ NJE E TILLE DHE RENIA VIKTIME. DUKE E DITUR SI FUNKSIONOJNE GJERAT ESHTË GJITMONE ME E THJESHTE TE MBROHESH. NE FUND TE FUNDIT, SECILI KA TE DREJTEN E AKSESIT TE INFORMACIONIT. MENYRA SE SI PERDORET KY I FUNDIT ESHTË AJO QE BEN DIFERENCEN. JUVE JU DUHET TE DINI QE "PHISHING" ESHTË MASHTRIM, DHE SI PASOJE I DENUESHEM ME LIGJ.

(Njohuri minimale ne HTML do te ishin avantazh per pjesen qe vijon)

Termi phishing eshte analogji per fishing. Eshte shkruajtuar ne ate menyre me shume mundesi duke marre shkas nga "phreaking" ngaqeshte shpjeguar si teknike dhe perdorur fillimisht ne fund te viteve '80 - fillim i '90 ne revistat elektronike Phrack, 2600 etj. AOL dhe disa banka mendohet te kene qene viktimat e para te phishing.

Per me shume histori mbi kete mund te lexoni ne :
<http://en.wikipedia.org/wiki/Phishing>

Phishing eshte favorizuar ne vite nga "bugs" ne shfletues interneti si IExplorer qe kane lejuar kodimin dhe fshehjen e url-ve te vertete, injoranca apo neglizhenca e perdoruesve, ka qene dhe mbetet nje menyre efektive per ti mashtruar perdoruesit ne futjen e te dhenave personale, perfshire ketu, emra perdoruesish, fjalekalime, te dhena personale, karta kredie etj.

Me poshte po demostroj sa e lehte eshte te krijohet nje faqe e tille. Do te marrim 2 shembuj klasike phishing duke perdorur si ekzemplar eksperimenti faqen e hyrjes se Yahoo e cila nuk ka besoj nevojte per prezantim. Perpara se te fillojme ne linkun qe vijon mund te gjeni nje grup me klone faqesh te famshme te cilat perdoren masivisht per phishing... Kujdes! Keta skedare kane si qellim vetem te demostrojne se sa "e vertete" mund te duket nje faqe e tille. Shumica e faqeve kerkojne qe te jeni te lidhur me internetin ne momentin qe i shikoni sepse perdorin imazhe apo elemente te tjere grafike te ruajtur ne serverat reale, online.

Kodi:

http://rapidshare.com/files/61769025/Phishing_Pages_F-I.rar.htmlMos i perdorni keto faqe per qellime te tjera pervec atyre studimore te fenomenit ne fjale. Phishing eshte i jashteligjshem.

Le te shikojme me poshte 2 skenare te mundshem te yahoo phishing :

1.Geocities Phishing - Shiko me shume foto nga une

Ky shembull ka te beje me nje metode e cila ben leve mbi deshiren e viktimes per te ditur me shume, apo per te pare me shume mbi dicka qe i intereson. Sic shume nga ju mund ta dine ne Yahoo Geocities perdoruesit mund te ndertojne faqe personale falas. Nje skenar i mundshem eshte ai qe i shtyn vizitoret ne nje faqe personale te klikojne per te hapur me shume foto nga nje vajze fjala vjen. Linku i shtyn ne faqen qe ka saktesisht kodin html qe vijon :

(Shikoni Dokumentin e Bashkelidhur txt)

Pasi vizitoret klikojne mbi kete link i hapet faqja e yahoo pictures LOGIN. Ne momentin qe vizitori per nje cast i tunduar nga deshira per te pare me shume foto, ben login me username dhe fjalekalimin e tij, keto te dhena i dergohen keqberesit automatikisht me email ne adresen e vendosur ne kete pjese te kodit : <INPUT TYPE="hidden"

NAME="Mail_To" VALUE="force.intruder@gmail.com">.

Me email (ky email mund te kategorizohet si spam nga disa sherbime email) pervec username dhe password me email do te dergohen edhe te dhena te tjera si IP, lloji i browsertit etj.

Sic mund ta shikonit momenti i renies viktime ishte shume i shpejte dhe pamja e faqes eshte per t'u admiruar. Asgje nuk e dallon nga e verteta.

2. Phishing nepermjet promocionit me email etj.

Sot ekzistojne shume sherbime hosting falas te cilat ofrojne edhe suport php, sql etj.

Per nje sulm te suksesshem mjafton nje host qe suporton php edhe kloni i faqes qe do te simulohet. Hoste falas te cilat perdoren shpesh per kete qellim jane :

www.phpnet.us
www.byethost.com
www.t35.com
www.awardspace.com
www.ifastnet.com
www.freehostia.com
www.funpic.be
www.funpic.com
www.funpic.org
www.freehostingnow.com
www.freeweb7.com
www.ripway.com
www.4444mb.com
www.110mb.com
www.my10gb.com/
www.007ihost.com/

Ne linkun me faqe phishing qe dhashe do te shikoni se per yahoo ekzistojne 3 skedare, nje yahoo.html qe eshte skedari qe vikimat do te vizitojne, nje login.php i cili hap dhe shkruan te dhenat ne skedarin e trete: log.txt qe eshte edhe skedari i logeve ku ruhen te dhenat e vikativave. Pasi te tre skedaret ngarkohen ne serverin perkates (nje nga lista e mesiperme), skedari php dhe txt eshte e nevojshme ti nderrohen chmod ne 777 (chmod 777 = Lejo kedo te lexoje, te shkruaje dhe te ekzekutoje skedarin). Nje rezultat eksperimental mund ta shikoni ne kete link

<http://forumishqiptar.t35.com/yahoo.html>

Nderkohe logu mund te kontrollohet thjesht duke vizituar <http://forumishqiptar.t35.com/log.txt>.

Kjo metode perdoret shpesh nepermjet emaileve, duke i derguar viktimave url te maskuara si kjo me lart. Nqs do ti kisha shtuar dicka si :

<http://forumishqiptar.t35.com/forumdisplay.php/Informatike> dhe Internet dhe do te kisha bere nje faqe login fallco te njejte me ate te forumit shqiptar, ka shume mundesi qe mjaft anetare te forumit te binin viktime.

Morali final : Sa here qe beheni gati te fusni username apo password, karte kredie apo te dhena te tjera te rendesishme personale, ndaluni nje cast dhe sigurohuni qe informacioni po shkon ne vendin e duhur. Per te mesuar me shume mbi volumin e phishing mund te vizitoni : <http://www.antiphishing.org/>

Kodi:

HTML.TXT

<http://www.speedyshare.com/919579127.html>