Serghei MAFTEA,
doctor în matematică, lector universitar al Catedrei „Activitatea specială de investigaţii"
a Academiei „Ştefan cel Mare" a MAI

PHISHING-UL CA METODĂ DE FRAUDĂ ON-LINE

Rezumat

Deşi phishing-ul este dintre cele mai vechi escrocherii on-line, aceasta este o problemă care va creşte şi va evolua în viitorul apropiat, deoarece infractorii vor continua să folosească escrocherii ca un mijloc eficient de a genera profit semnificativ. Atacurile se adaptează în mod constant la tehnologie, devin tot mai sofisticate în încercarea de a depăşi contramăsurile folosite pentru detectare. Atacurile de phishing nu numai că au majorat în mod substanţial costurile asociate funcţionării unei afaceri, dar, de asemenea, au afectat securitatea şi increderea clienţilor în mod negativ.

Summary

Although phishing is one of the oldest online scams, phishing is a problem that will grow and evolve over the foreseeable future, as criminals will continue to use the scams as an effective means of generating significant profit. The attacks constantly adapt to technology, becoming more sophisticated in an attempt to outpace countermeasures for detection. Phishing attacks not only have increased substantially the costs associated with running a business, but also have affected security and customer confidence negatively.

Keywords: phishing, HTML, PHP, CCS, link, URL, ID, SSL/TLS, CVC2 / CVV2, PIN, browser, https, spam, e-mail, software maliţios.

Introducere. Beneficiile rezultate ca urmare a dezvoltării şi implementării tehnologiei informaţiei în viaţa cotidiană a oamenilor sunt de necontestat. Totodată, unele persoane aplică tehnologia informaţiei în scopuri ilegale, ce afectează încrederea societăţii în noile tehnologii. Aceast pericol se conturează semnificativ în special în domeniul e-comerţului, deoarece factoricheie, cum ar fi parole şi numere de cont identifică în mod unic consumatorii. Phishing-ul este o metodă on-line pe care hoţii de identitate o pot folosi pentru a obţine în special date personale sensibile, necesare pentru a comite alte infracţiuni.

De aceea la această nouă etapă a dezvolzării tehnologiei informaţiei şi comunicaţiei sunt necesare şi activităţi de prevenire şi combatere a diferitor forme de atacuri cibernetice. Articolul în cauză are ca scop principal punerea în evidenţă a pericolului generat de atacurile de tip phishing şi elucidarea metodelor şi mijloacelor de care fac uz infractorii pentru a realiza un astfel de atac.

Materiale şi metode aplicate. Lucrarea este bazată pe materialele disponibile la momentul studiului, aplicându-se mai multe metode de cercetare, dintre care pot fi evidenţiate metoda analizei, metoda statistică, metoda comparativă, metoda logică.

Statistici. Phishing-ul a devenit un flagel mondial foarte serios, ce pune probleme importante atît utilizatorilor, cît şi companiilor de securitate an de an. Această situaţie este confirmată de multe studii, în care se încearcă să se analizeze multilateral această ameninţare. Atacurile de tip phishing sunt persistente, victime devin persoane fizice şi organizaţii pe scară globală. Astfel, conform sondajelor phishing executate de AntiPhishing Working Group (APWG):

– în trimestrul 2 al anului 2014 au fost observate 128 378 site-uri de phishing, acest număr fiind mai mare doar în primul trimestru al anului 2012 cînd au fost observate 164 032 site-uri de phishing;

– cea mai mare parte din atacurie de tip phising în al doilea trimestru al anului 2014 au avut ca ţintă sistemele de plată, cota acestora constituind 39,80 %;

– în prima jumătate a anului 2014, numărul unic de site-uri de phishing a crescut cu 58 % faţă de aceeaşi perioadă a anului 2013;

– topul ţărilor care sunt gazdă a unor astfel de site-uri în al doilea trimestru al anului 2014 este alcătuit din China, Federaţia Rusă, Ucraina, Germania, Hong Kong, Turcia, Marea Britanie, Canada, Franţa, Polonia, Japonia şi este condus detaşat de SUA, unde se hosteză peste 35 % de astfel de site-uri.

Aceste site-uri web folosite pentru phishing, ce afectează atît branduri bine cunoscute, cît şi companii mai puţin cunoscute, suplimen-

tate cu metode dezvoltate în permanenţă de hackeri au dus şi vor continua să ducă la pierderi financiare importante. Astfel, în studiul publicat în iulie 2013 de British House of Commons, Home Affairs Committee s-a încercat estimarea costurilor atacurilor de tip phishing. Acesta susţine că costul total al criminalităţii cibernetice în Marea Britanie pentru anul 2012 a fost de circa 27 de miliarde de £, dintre care mai mult de 600 de milioane £ pot fi atribuite direct la atacuri de tip phishing.

De asemenea, transformarea unui serviciu de reţea (canal de comunicare considerat sigur) cu rată mare de folosire, precum este email-ul, într-o posibilă sursă de ameninţare (capcană) scade credibilitatea şi încrederea comunităţii virtuale în această soluţie de comunicare.

Termenul „phishing" este folosit în mediul digital pentru a evidenţia o formă elaborată de sustragere de date confidenţiale şi are la origini cuvintele din limba engleză *phone* (telefon) şi *fishing* (pescuit). Pentru acest tip de ameninţare este folosită, de asemenea, şi combinaţia „brand spoofing" (imitarea imaginii). Păcălirea prin phishing presupune trimiterea unui mesaj folosind serviciul e-mail, aparent din partea unei companii sau organizaţii legitime, de încredere, încercînd astfel să se sustragă informaţii personale, pe baza cărora se accesează ilegal conturi bancare sau se creează alte probleme pe baza identităţii furate. În calitate de ţinte ale acestor genuri de scheme criminale servesc mai ales clienţi şi reprezentanţi ai instituţiilor financiare, sistemelor de plată, de exemplu, PayPal, magazinelor on-line gen eBay, companiilor ISP, agenţiilor private şi guvernamentale etc.

Orice persoană poate fi expusă riscului de a deveni victimă a phishing-ului atunci cînd:

– adresa de e-mail devine publică pe Internet;
– completatează online formulare;
– vizitează site-uri web;
– accesează newsgroup-uri.

Aceste situaţii sunt comune practic oricărui utilizator, ca urmare fiecare poate deveni ţintă a unui astfel de atac, în procesul derulării căruia de regulă sînt obţinute informaţii confidenţiale (user-ID, parole, numărul cardului bancar, numărul asociat contului bancar, codul PIN folosit la ATM-uri şi POS-uri, codul numeric personal, contul de asigurare, conturi şi parole ale resurselor de reţea, alte date personale şi financiare). Odată introduse, aceste informaţii îşi pierd atributul de confidenţialitate şi sunt imediat folosite de către infractori. În general este foarte greu ca sursele financiare pierdute să fie recuperate, deoarece paginile folosite pentru phishing sunt dispoibile numai pentru un timp foarte limitat (cîteva zile, ore).

Tehnici de phishing. Autorii schemelor de phishing pentru a inspira încredere creează pagini web contrafăcute (folosind HTML, PHP, CSS, Javascript), ce imită pagini web ale unor companii, corporaţii furnizoare de servicii bine cunoscute, bănci etc.

Un alt pas în activitatea infracţională îl reprezintă colectarea sau generarea de adrese de email, care este urmat, în această formă a pescuitului, de „lansarea momelii". Această activitate, se realizează prin expedierea unui mesaj, folosind serviciul de e-mail sau aplicaţii de mesagerie instantă, cu un subiect credibil, prin care se provoacă receptorul (potenţiala victimă) să introducă informaţii confidenţiale. În acest sens, de regulă, se „propune" fie:

– folosirea de link-uri inserate în mesaj, (care pot fi de orice tip: „click aici"; URL; imagine; text) întru accesarea unei pagini web de phishing;

– completarea unui formular direct în textul mesajului recepţionat;

– pagina de phishing este încorporată direct în scrisoare.

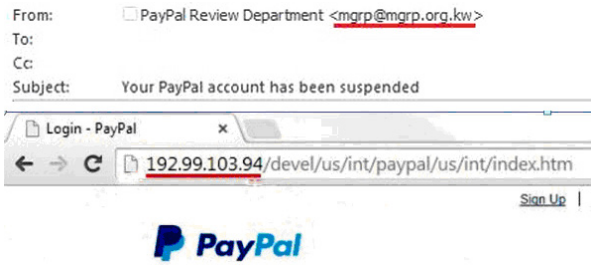
Mesajele de acest tip par să aibă motive plauzibile şi încearcă să vină cu argumente convingătoare, pentru a determina ţinta atacului să acţioneze imediat. Printre cele mai populare trucuri folosite sunt mesaje prin care se atenţionează că are loc depăşirea dimensiunii admisibile a cutiei poştale, upgrade-ul sistemului, blocarea cutiei poştale. Aceste e-mailuri de phishing imită deseori notificări de la servicii de e-mail cunoscute, dar marea majoritate constituie cereri generale, de a confirma datele de autentificare (login şi parola) de la un anumit serviciu. Cel mai probabil, acest lucru se datorează faptului că escrocii trimit notificări false spre toate adresele de care dispun şi nu direcţionat pentru un anumit serviciu poştal.

Segmentul persoanelor de la care se aşteaptă anumite reacţii emoţionale ce îi determină la acţiuni nerezonabile, în special, la transferul de informaţii sensibile, este substanţial majorat de utilizatorii sistemelor de plăţi. Aceştia din urmă primesc scrisori, presupuse a fi expediate de către un anumit reprezentant al unei instituţii financiare, ce conţin ameninţări de suspendare sau de blocare a conturilor, motivul fiind că nu a fost folosit de ceva timp sau este necesar un upgrade. În scopul de a păstra contul, se cere conectarea la cont. Iar pentru aceasta, în mesaj, întru a susţine beneficiarul se propune un link. Urmînd link-ul, se ajunge la o pagină care arată ca site-ul corespunzător sistemului de plăţi, după care se cere şi autentificarea. În ciuda asemanarii sale cu originalul, site-ul este un fals. În acest sens se observă că:

– paginile nu sunt protejate, deoarece lipseşte HTTPS în bara de adrese, ce ar presupune folosirea protocolului SSL/TLS care este necesar în astfel de situaţii;

– în URL-uri este prezent simbolul "@";

– domenul nu aparţine companiei de la care se pretinde că a fost trimis mesajul (adresa IP nu aparţine PayPal).



Pericolelor similare, sunt supuşi şi utilizatorii unor site-uri commerciale utilizate pe larg. Înspre aceştia sunt trimise e-mail-uri în care se anunţă că site-ul a fost atacat şi este necesar ca utilizatorul sa-şi acceseze contul pentru a verifica informaţia. Potenţialele victimele fac un clic pe URL-ul propus, iar brouser-ul afişează site-ul clonă (copia exactă a site-ului legitim). Utilizatorul se autentifică pe sistemul propus de infractori, astfel aceştia obţin aceste date, iar victima este redirectionata spre site-ul legal. În consecinţă, phisherii pot accesa contul victimei şi folosi informaţia personală.

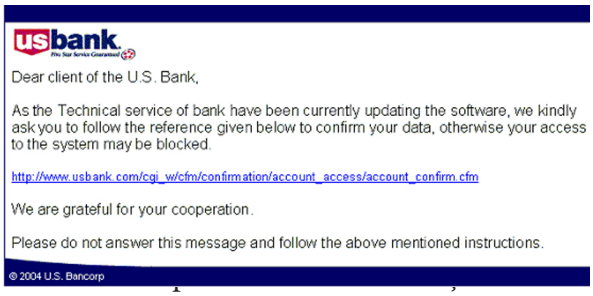
Original Message-----

From:[mailto:identdepmnt_op9679843@usbank.com]

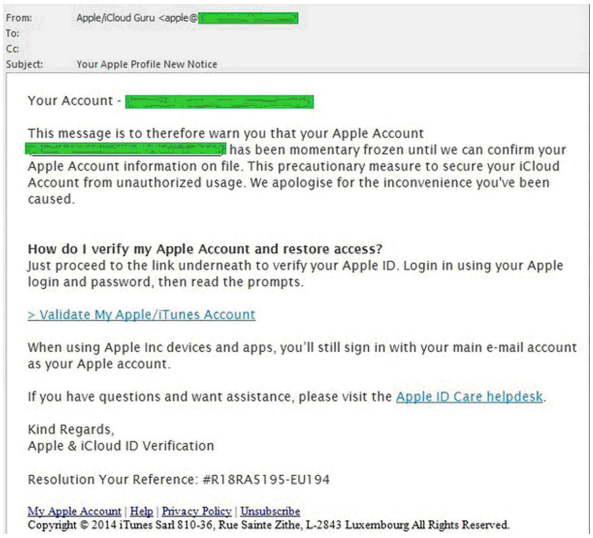
Sent: Sunday, August 29, 2004 11:16 PM

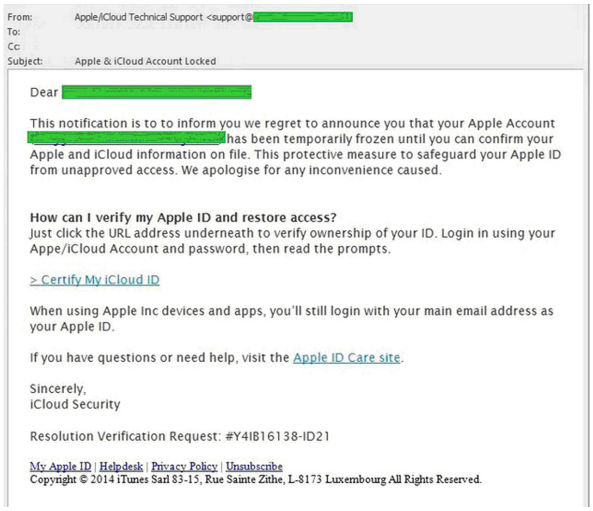
To:

Subject: Urgent Notice From BiIIing Department



de Internet foarte populare. Astfel, de exemplu, infractorii trimit notificări false în numele reprezentanţilor serviciilor iTunes şi iCloud prestate de gigantul IT Apple.



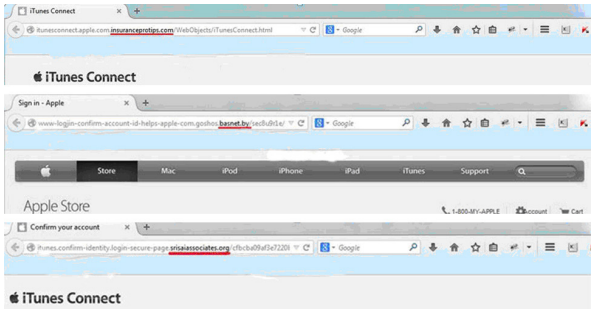


Ca rezultat, se propun ferestre-clonă ale acestor servicii, în care se observă că:

– lipseşte HTTPS;

– domenul nu aparţine Apple;

– în plus faţă de informaţiile necesare pentru a controla ID-ul Apple, se solicită informaţii despre cardul de credit sub pretextul legării sale în cont.



Astfel, phishing-ul, folosind imagini de pe site-ul legal, link-uri ce duc spre site-ul legal, devine tot mai sofisticat fiind mai dificil de a-l deosebi de un site legal şi în consecinţă de a-l depista şi stopa.

După cum s-a menţionat, una dintre principalele metode utilizate de infractorii din spaţiul virtual este folosirea unui mesaj de e-mail credibil, care va direcţiona intenţionat victima spre o pagină web falsă. Unele dintre aceste mesaje pot conţine un formular de înscriere direct în textul conţinut. În acest sens utilizatorii trebuie să conştientizeze faptul că organizaţiile oficiale nu trimit mesaje prin care solicită informaţii personale şi trebuie să inspecteze aceste pagini web pe care au fost direcţionaţi, în vederea verificării corectitudinii adresei URL afişate.

Din păcate, în arsenalul infractorilor cibernetici exista tehnici şi metode ce permit falsificarea URL-ului. Printre acestea se evidenţiază cele ce ţin de specularea neatenţiei utilizatorului, de vulnerabilităţi ale browserelor, de vulnerabilităţi ale sistemelor de operare, ale aplicaţiilor software.

În primul caz URL-ul afişat este foarte asemănător cu cel real, fapt ce poate să nu fie detectat la prima vedere. De exemplu, adresa http://www.rosksbank.com poate fi inlocuita cu http://www.rossksbank.com, adresa http://www.sitibank.com poate fi înlocuită cu http://www.sytibank.com, http://www.mlbank.com poate fi înlocuită cu http://www.mIbank.com, adresa acaunt@tr.com poate fi înlocuită cu acaunt@tr.info. În primul exemplu, inducerea în eroare se bazează pe faptul că adresa este suplimentată cu încă o literă „s", în cel de al doilea exemplu are loc înlocuirea literei „i" cu „y", în cel de al treilea exemplu litera mică „l" este înlocuită cu majuscula literei „i", iar în ultimul exemplu „com" este înlocuit cu „info".

Tot pe neatenţie şi pe faptul că mulţi utilizatori nu examinează bara de adrese se bazează şi cazurile când paginile false nu au ca parte componentă bara de adrese.

Tehnica prezentată este centrată în jurul unui link de manipulare, pe care phisherii îl folosesc, ca atunci cînd utilizatorul face clic pe acesta (link-ul înşelătoar), să se deschidă site-ul fals în loc de site-ul menţionat în link. Una dintre metodele ce pot desconspira escrocheria cu acest link de manipulare este de a plasa mouse-ul peste link, ceea ce permite de a vizualiza adresa reală.

O altă tehnică de phishing pe care infractorii cibernetici o folosesc are ca suport binecunoscutele popup-uri. În acest caz, momeala pentru victimă nu se transmite prin e-mail, dar se foloseşte publicitatea pop-up. Atunci cînd utilizatorul vizitează anumite site-uri, inclusiv de încredere, dar care folosesc popup-uri pentru publicitate, automat într-un browser este deschisă o pagină cu o ofertă de a primi un premiu în bani. Pentru a spori încrederea victimelor, escrocii folosesc în aceste ferestre logo-uri de bănci şi sisteme de plată bine cunoscute. Ferestrele conţin avize precum că vizitatorul a devenit cîştigător şi proprietarul acţiunilor de premii în bani ca urmare a unei campanii lansate de aceste bănci. Activînd butonul pe care este scris „ridică premiul", utilizatorului i se prezintă o pagină unde este solicitat să introducă informaţii asociate cardului de debit/credit. În mod special, se cere să se introducă data valabilităţii şi numărul de card. Următorul pas al acestei escrocherii urmează după folosirea butonului pe care este scris „obţine bani". Clicul pe acest gen de buton prelungeşte aşa-numita procedură de „identificare a proprietarului" prin aceea că se cere de a indica valoarea soldului de pe contul folosit. Aceasta fiind necesar „pentru siguranţa transferului". Este de remarcat faptul că pe

resursele frauduloase de foarte multe ori există avize de prudenţă şi de prevenire a ameninţărilor. De asemenea, se remarcă şi faptul că la indicarea unei sume mici este afişat un mesaj prin care se anunţă că cardul nu este potrivit pentru astfel de operaţiuni. Şi, desigur, pentru finalizarea aşa-numitei „identificări" este necesară indicarea şi a codului de autentificare (CVC2 / CVV2) utilizat la efectuarea unor tranzacţii fără prezenţa fizică a cardului. În final, în locul banilor se emite un mesaj de genul „cardul nu este potrivit pentru astfel de operaţiuni". Criteriul prin care utilizatorul poate pretinde că aceasta este o înşelăciune se bazează pe faptul că în aceste ferestre de pop-up lipseşte bara de adrese.

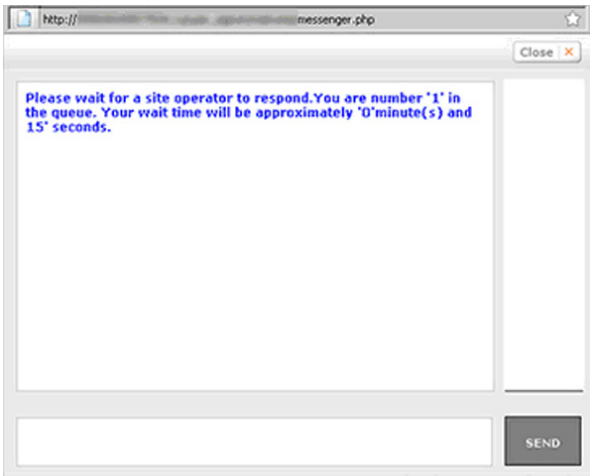
De asemenea, pe promiterea de bani ce aşteaptă să fie ridicaţi se concentrează şi alte scheme de phishing. Bineinteles că de-a lungul timpului s-au folosit promisiuni ca: premii, vacanţe, bunuri electronice sau bani pentru a convinge utilizatorii să viziteze anumite website-uri sau să se înregistreze în diferite programe. Dar următoarea schemă a evoluat atingînd un nivel ridicat. Astfel, noua schemă de fraudă debutează cu un e-mail primit de la o bancă inexistentă, în care se pretinde că o sumă foarte mare de bani a fost plasată într-un cont deschis pe numele respectivului utilizator. Mesajul include un link către banca falsă, un număr de cont şi un cod PIN.

În continuare, mesajul explică modul în care utilizatorul poate transfera banii, accesînd acest cont. Însă pentru ca tranzacţia să poată fi efectuată, utilizatorii trebuie să îşi înregistreze informaţiile personale şi contul real, moment în care acestea sunt furate.

Acest tip de fraudă se aseamănă foarte mult cu faimoasele scrisori nigeriene, prin care utilizatorii sunt invitaţi să îşi trimită detaliile personale şi datele despre contul bancar pentru a ajuta diverse personaje să transfere sume enorme de bani, urmînd să primească cota-parte pentru acest serviciu.

E-mail-ul de acest tip începe, de exemplu, astfel: „Am fost rugaţi de către Mega Magic Foundation of France să vă înştiinţăm că suma de un milion de euro a fost depozitată în banca noastră, DBS Bank, pe numele dvs, această sumă putînd fi transferată imediat în contul dvs. curent". Mesajul se incheie: „Odată logat în contul deschis la banca noastră, puteţi transfera suma dorită direct către contul dvs curent printr-un simplu click pe link-ul „click here to transfer". Evident că utilizatorii creduli vor afla ulterior că de fapt nu existau nici un fel de sume fabuloase şi au fost victimele unei metode de phishing.

O altă tehnică de phishing este realizată prin intermediul telefonului şi a live chat-urilor de asistenţă fictivă pentru clienţii băncilor. Îndrăzneala şi ingeniozitatea phisherilor în acest caz este deosebită. Informaţii confidenţiale sunt obţinute direct de la persoană prin intermediul convorbirilor telefonice, folosind un ID apelant fals. Atacatorii practic obţin pe viu datele necesare de la victimele lor. În acest sens hackerii creează o resursă, care este foarte asemănătoare siteului oficial al băncii. În cazul live chat-urilor de asistenţă fictivă, atunci cînd o persoană încearcă să introducă un nume de utilizator şi o parolă (sau, atunci cînd faci orice altă acţiune în cadrul paginii) într-o fereastră de browser, apare o ofertă de a discuta cu departamentul de combatere a fraudei, în scopul de a valida datele din contul utilizatorului. Mai mult, prin telefon sau chiar pe monitorul victimei apare o fereastră de chat prin care atacatorii încep să convingă victima pentru a oferi e-mail, numărul de telefon şi alte informaţii, care pot fi cumva folosite pentru profit. Experţi RSA au detectat că suportul pentru comunicare prin chat a fost implementat pe baza protocolului deschis Jabber, iar site-ul este hostat pe servere, care stochează şi alte astfel de resurse, precum viruşi şi alte programe malware.



Dear Customer,

We've noticed that you experienced trouble logging into Online Banking.

After three unsuccessful attempts to access your account, your Online Profile has been locked. This has been done to secure your accounts and to protect your private information. is committed to make sure that your online transactions are secure.

To verify your account and identity please call our Account Maintenance Department at **(706) 247-7801** 24 hours / 7 days a week.

Sincerely,

Online Customer Service

Este cunoscut şi phishingul prin intermediul motoarelor de căutare, care este o escrocherie în urma căreia utilizatorul este direcţionat către site-uri care oferă produse sau servicii la costuri reduse. În momentul cînd utilizatorul încearcă să achite pentru produs sau serviciu prin introducerea detaliilor instrumentului de plată (cardul de debit/credit), acestea din urmă sunt colectate de către siteul de phishing. Există şi site-uri bancare false care oferă cărţi de credit sau credite utilizatorilor la o rată scăzută, dar acestea sunt de fapt site-uri phishing.

Etape ale phishing-ului. Generalizînd tehnicile şi schemele de phishing prezentate se pot evidenţia mai multe etape infracţionale pe care le folosesc elementele criminale. Unele din ele nu implică existenţa unui echipament puternic şi costisitor. Nu este nevoie de suportul hackerilor, iar cunoaşterea de PHP, CSS, Javascript şi HTML este necesară la nivel minim. Phisherii care folosesc unele dintre aceste scheme sunt foarte rar programatori sau designeri buni, dar au cunoştinţe foarte bune despe psihologia oamenilor, altfel spus, au abilităţi de inginerie socială. La fiecare din etape pot fi utilizate atît tehnici complexe, cît şi tehnici simple, dar eficiente. În continuare se vor detalia etape caracteristice phishingului bancar.

Etapa de bază poate fi intitulată „Obţinerea adreselor de e-mail".

Demararea schemei necesită o listă de adrese de e-mail ale clienţilor băncii atacate. Extracţia de aceste adrese reprezintă o activitate separată în lumea interlopă. În scopul de a obţine o bază de date cu e-mail-uri se recurge la recrutarea unui angajat al băncii, cu acces la lista de e-mail a clienţilor. Procesul de recrutare se realizează atît în reţea, cît şi offline, în locaţii de agrement, pe stradă, recurgînd la diferite scheme ingenioase cum ar fi cunoştinţe cu domnişoare atrăgătoare urmate de şantaj. Angajaţii băncilor on-line sunt uşor de găsit cu ajutorul tehnologiei de business intelligence. Un angajat al băncii, de obicei, se vinde pentru un salariu lunar de bază. În discuţiile pe forumurile foloste de infractori se vehiculează că fischerii pentru a achiziţiona baze cu adrese e-mailuri ale unei bănci mijlocii. Au nevoie de cîteva mii de dolari. Informaţii despre clienţii băncilor mari, bine cunoscute sunt cu valoare mult mai mare, dar, de regulă, valoarea lor nu ar trebui să depăşească zece mii de dolari.

Etapa 2 poate fi intitulată „Site-clonă şi o scrisoare din partea băncii".

Phishing-ul bancar este organizat prin trimiterea de e-mail-uri în masă în numele administraţiei băncii. Scrisoarea conţine adesea un link (legătură directă) spre un site, care atît după formă, cît şi după conţinut este foarte greu de distins de cel real. Dacă se accesează acest site şi se introduc date ce permit accesul la un anumit cont bancar, utilizatorul poate deveni victimă a unei fraude.

După ce a primit adresa de bază, phisher-ul trebuie:

– Să creeze o pagină care simulează pagina de conectare de Internet banking a băncii atacate.

– În acest sens este necesar să înregistreze un nume de domeniu similar cu cel al băncii. Pentru aceasta se folosesc diferite trucuri:

– domeniu de înregistrare într-o altă zonă de domeniu;

– înlocuirea a uneia sau a două litere din adresă;

– adăugare unui cuvînt la numele băncii.

Principalul scop al acestor manipulări este ca la o privire sumară la bara de adrese a browser-ului victima să creadă că el este exact pe site-ul băncii sale.

Crearea de pagini-capcană nu necesită o expertiză specială. Şablonul este salvat cu opţiuni corespunzătoare comune browsere-lor.

Pentru a captura date de plată personale se foloseste un simplu PHP-cod. Întru realizarea acestei etape, elementele criminale genera-

toare ale acestui atac de tip phishing apelează la ajutor din exteriorul grupării, remunerînd fiecare pagină generată cu 50-70 de dolari. Pentru pagini se cere să aibă următoarea funcționalitate: după ce victima a introdus datele, script-ul să-l direcționeze pe utilizator la pagina de conectare reală a băncii. Raționamentul infractorilor îndreptîndu-se pe presupunerea că utilizatorul va crede că a introdus incorect date sau că conexiunea a eşuat. Această tehnică permite de a frauda chiar şi utilizatorul ce are grijă de a studia site-ul, deoarece acesta nu va detecta nimic suspect – pentru că acum el este pe site-ul real al băncii.

Etapa a 2-a. Să arunce momeala.

Pentru aceasta spre un client se trimite un mesaj-capcană, care poate lua forma unei scrisori cu logo-ul băncii. Textul scrisorii conține o trimitere către un text cu adresa site-ului băncii. Dar dacă se analizează cu atenție proprietățile link-ului respectiv, se poate observa că aceasta este o pagină-capcană, situată pe un domeniu similar. Fisher-ii mizează pe faptul că printre sutele de clienți ai băncii nu toți vor fi atenți şi precauți.

Etapa 3 poate fi intitulată „Încasari"

Odată ce datele privitoare la cardurile bancare sunt disponibile fischer-ului, acesta trebuie să execute mai multe activități ce au drept scop scoaterea banilor folosind conturi bancare false şi sisteme de plată. În cazul în care escrocul este inteligent şi nu este lacom, el nu goleşte complet conturile victimelor, dar foloseşte numai o cantitate relativ mică din bani. În acest sens, fischer-ul pune accentul pe amînarea cît mai mult posibilă a momentului în care serviciul de securitate al băncii va ridica alarma în baza plîngerii unuia dintre clienții fraudați.

Concluzie. Urmare a studiului efectuat, subliniem importanța problematicii generate de atcurile de tip phishing. Analiza tehnicilor şi schemelor folosite în acest gen de activitate infracțională prezintă interes sporit ca urmare a dificultăților privind interpretarea acestor tipuri de fapte din punctul de vedere al angajaților instituțiilor cu sarcini de ocrotire a normelor de drept. Consumatorii on-line trebuie să învețe cum să prevină şi să facă față activităților frauduloase pe Internet cu scopul de a obține date personale în beneficiul financiar al phisherilor. Angajații subdiviziunilor care au ca sarcină prevenirea şi combaterea infracțiunilor ar trebui să poată să recunoască semnele unui posibil atac de phishing şi să ştie cum să reacționeze la un mesaj e-mail de phishing. Prin luarea în considerare a diferitor aspecte evidențiate în acest articol, precum şi prin aplicarea şi a altor măsuri de precauție, consumatorul de Internet va reduce în mod semnificativ pericolul generat de atacurile de tip phishing.

În pofida tuturor măsurilor de precauție, phisherii au tendința să-şi încheie cariera lor nu aşa cum se aşteaptă. Mulți pur şi simplu dispar cu prietenii şi familia pentru totdeauna, dintr-o dată şi fără voie. Persoanele care apelează la structuri criminale pentru a organiza atacuri de tip phishing, de regulă, nu mai au posibilitatea de a ieşi din „afaceri". Despre phisheri norocoşi, care au fost capabili să „se pensioneze" şi să se bucure de roadele activităților lor, nu s-a auzit, de regulă, aceştia sunt plasați în instituții supravegheate.

Bibliografie

1. Charles Arthur, „Police crack down on computer support phone scam". Disponibil la: http://www.guardian.co.uk/technology/2010/jul/19/police-crackdown-phone-scam-computer
2. Shathabheesha, „Reconnaisance with images", June 28 2012. Disponibil la: http://resources.infosecinstitute.com/reconnaissance-with-images/Wikipedia, 'Email spoofing'. Disponibil la: http://en.wikipedia.org/wiki/Email_spoofing
3. Ravi Miranda, „Playing mindgames", July 17 2012. Disponibil la: http://ravimiranda.wordpress.com/tag/colonel-effect/
4. Khadeeja Safdar, „Obama Utility Bill Scam Falsely Claims Federal Aid Program Will Help Pay Bills", 07/09/2012. Disponibil la: http://www.huffingtonpost.com/2012/07/09/obama-utility-bill-scam-federal-aid_n_1659787.html
5. https://www.emc.com/collateral/white-papers/h11933-wp-phishing-vishing-smishing.pdf

6. http://see.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf
7. http://www.cnet.com/news/new-scam-adds-live-chat-to-phishing-attack/
8. https://www.rsa.com/en-us
9. http://www.ic3.gov/
10. Wikipedia, „Phishing". Disponibil la: https://en.wikipedia.org/wiki/Phishing
11. Wikipedia, 'Voice phishing'. Disponibil la: http://en.wikipedia.org/wiki/Voice_phishing
12. Wikipedia, „Phone fraud". Disponibil la: http://en.wikipedia.org/wiki/Phone_fraud
13. https://ro.wikipedia.org/wiki/Business_intelligence
14. http://www.wikihow.com/Forge-Email
15. http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf