

PAGINA 2

I. Amenințările informatice

CE ESTE MALWARE? Malware (prescurtarea de la "malicious software" în limba engleză) este un termen generic și se referă la orice software rău-intenționat (malițios) care a fost creat cu scopul de a rula în mod neautorizat și ascuns față de utilizatorul computerului.

CE ESTE UN TROIAN? Un troian este un program malițios (malware) care este adesea prezentat utilizatorului ca un program legitim. Utilizatorul fiind păcălit, adesea prin inginerie socială, să descarce și execute aplicația malițioasă pe computerul său. Odată activat troianul permite atacatorului să controleze și să monitorizeze calculatorul victimei sau să acceseze informații sensibile (parole, poze, etc) stocate pe acesta.

CE ESTE UN "KEYLOGGER"? Înregistratoarele de taste, keyloggers în limba engleză, sunt programe destinate înregistrării tastelor apăsate de către utilizator și folosite, de pildă în troieni, pentru a obține informații sensibile ca parole, coduri PIN, numere de carduri, etc. Aceste programe rulează în background și sunt invizibile pentru un utilizator obișnuit. Ele pot fi instalate pe un calculator în urma unui atac de tip "drive-by-download" sau pot fi instalate împreună cu programele piratate.

CE ESTE UN ADWARE? Adware-ul este o formă de malware care descarcă sau afișează anunțuri nedorite când utilizatorul navighează online, de asemenea, acesta colectează date de marketing sau alte informații fără știrea utilizatorului și redirecționează căutările utilizatorului către diferite website-uri ce afișează anunțuri publicitare. Aplicațiile adware se instalează automat cu unele programe gratuite pe care dvs. le instalați de pe Internet sau cel mai adesea "vin la pachet cu" programele piratate.

PAGINA 3

CE ESTE UN ATAC DE TIP "DRIVE-BY DOWNLOAD"? Un atac de tip "drive-by-download" se referă la descărcarea ne-intentionată (fără știința utilizatorului) și fără ca acesta să observe, pe un computer sau terminalul mobil, a unor programe malițioase. De obicei un astfel de atac reușește datorită lipsei actualizărilor de securitate (ex. actualizări ale browserului sau ale sistemului de operare).

CE ESTE UN ATAC DE TIP "MAN-IN-THE-MIDDLE"? Un atac de tip "man-in-the-middle" (omul de la mijloc), este un atac sofisticat în care atacatorul se interpune ca "stație de transit" în comunicația dintre două sisteme, utilizatorul legitim "având impresia" că cele două sisteme discută direct, când de fapt, în realitate, atacatorul controlează toată conversația, fiind capabil să intercepteze și modifice mesajele schimbate de cele două părți. Folosind un astfel de atac atacatorul ar putea modifica date ale unor tranzacții financiare.

CE ESTE UN ATAC DE TIP "MAN-IN-THE-BROWSER"? Un atac de tip "man-in-the-browser" este un tip de atac "man-in-the-middle" prin care un troian de tip proxy infectează un browser web folosindu-se de vulnerabilitățile de securitate ale browser-ului. Troianul modifică pagini web, elemente ale unei tranzacții sau chiar întreaga tranzacție, toate aceste acțiuni având loc "în background", fără ca utilizatorul să observe. Un astfel de atac ar putea fi contracarat prin utilizarea unei metode de verificare a tranzacției care să folosească un "canal" (un alt mediu de transmisie, ex. SMS) diferit de cel care a fost utilizat pentru inițierea tranzacției. (ex. web).

PAGINA 4-5

II. Amenințări de tip inginerie socială

Ingineria socială, social engineering în limba engleză, este arta de a manipula, minți, sau influența pe ceilalți ca să realizeze/nu realizeze anumite acțiuni ori să divulge informații confidențiale. Este oarecum similar cu un truc de câștigarea încrederii sau cu o simplă fraudă. Acest termen se aplică de obicei celor care utilizează șiretlicuri pentru a culege informații sau pentru a accesa sistemele informatice, în unele cazuri atacatorul nu vine niciodată față-în-față cu victima.

În continuare prezentăm cele mai cunoscute tipuri de inginerie socială.

CE ÎNSEAMNĂ "PHISHING"/ "SMSishing"? În domeniul informatic, phishing (eng) reprezintă o formă de activitate criminală care constă în obținerea datelor confidențiale, cum ar fi credențialele de acces (username, parola, PIN, OTP) pentru aplicații financiare sau informații referitoare la cardul de credit, folosind tehnici de manipulare a identității unei persoane sau a unei instituții. Un atac de tip phishing constă, în mod normal, în trimiterea de către atacator a unui mesaj electronic, folosind programe de mesagerie instantă (e-mail) – PHISHING, sau telefon (SMS) - SMSishing, în care utilizatorul este sfătuit să introducă credențialele de acces (nume utilizator, parola), numere de card, coduri PIN, etc.

Un exemplu de phishing: primiți un email în care ați fost informat că ați câștigat o excursie în străinătate iar tot ce trebuie să faceți pentru a primi voucherul de călătorie este să introduceți (pe un site asemenator cu cel al băncii) următoarele informații pentru a confirma identitatea: numele, adresa și datele cardului dvs.

Un exemplu de smsihing: primiți un mesaj SMS de la un număr necunoscut care pretinde a fi banca dvs. și care va invită să descărcați o nouă versiune a aplicației de mobile banking. ATENȚIE! Cel mai probabil în acest caz veți descărca și rula un malware care va da atacatorului posibilitatea să controleze și să monitorizeze telefonul dvs. mobil, inclusiv să poată captura credențialele de acces pentru aplicația legitimă de online banking.

DE UNDE AU ADRESA MEA DE E-MAIL SAU NUMĂRUL MEU DE TELEFON? De cele mai multe ori aceste informații sunt culese din surse publice (ex. site-uri de anunțuri) dar și din bazele de date făcute publice în urma unor breșe de securitate ale diferitelor servicii online unde ați furnizat datele respective de contact. Aceste informații sunt schimbate sau re-vandute în mod frecvent de atacatori pentru a fi folosite în atacuri de tip “phishing”.

DE UNDE ȘTIU EI CU CE BANCĂ LUCREZ? Atactorii nu știu acest lucru, dar dacă trimit multe mesaje cu siguranță nimeresc și persoane care lucrează cu banca prezentată în mesajul de phishing, dacă persoanele nu sunt atente acestea furnizează atacatorilor informațiile pe care aceștia le caută.

CE FAC DACĂ PRIMESC UN E-MAIL SAU UN SMS "SUSPICIOS"? Cel mai bine este să ștergeți direct mesajul respectiv, mai ales dacă conține link-uri sau atașamente. De asemenea, ori de câte ori aveți suspiciuni cu privire la originea unui mesaj (email sau sms) este bine să contactați banca pe unul din canale de suport oficiale (ex. telefonul sau email-ul menționat pe websiteul public).


PAGINA 6-9

CE ESTE VISHING? Vishing este un termen care provine din termenii voice și phishing și reprezintă o formă de înșelătorie prin care utilizatorul este păcălit să furnizeze informații sensibile, credențialele de acces, numere de card, sau coduri de acces, cu scopul de a impersona utilizatorul de drept sau a fi folosite de atacator în alte atacuri de inginerie socială.

Un exemplu de vishing: primiți un telefon de la o persoană care pretinde a fi un angajat al băncii care dorește să verifice numărul cardului, codul PIN sau codul de securitate al cardului deoarece a fost inițiată o alertă de securitate.

CE ESTE “CEO FRAUD”? Un alt tip atac încadrat în categoria Inginerie Socială este “CEO Fraud” sau “Business Email Compromise (BEC)”. În ce constă acesta înșelătorie, atacatorul reușește să compromită serverul de email al unei companii sau să creeze o casuță de email asemănătoare cu cea oficială a companiei vizate. Eventual schimbând o literă, cifra zero (0) în loc litera O.

Atacatorul folosește aceasta identitate falsă pentru a informa prin email partenerii de afaceri ai companiei cu privire la schimbarea conturilor de plată a facturilor. De obicei persoana care este impersonată este directorul companiei sau directorul financiar. În email-ul trimis directorul financiar precizează că începând de acum înainte plățile către companie să fie efectuate într-un cont nou, cont care se află la dispoziția atacatorului. Partenerul de afaceri fără să suspecteze fraudă și fără să facă verificări suplimentare efectuează plata în contul indicat, astfel banii ajung în posesia atacatorului.

Pentru a preveni astfel de situații, vă recomandăm să:  evitați, pe cât posibil, să folosiți corespondența electronică neprotejată pentru vehicularea informațiilor cu caracter comercial

sensibil sau cu caracter confidențial (coduri IBAN, parole, detalii de plată, etc); Ț folosiți întotdeauna softuri antivirus pentru protecția calculatoarelor dvs; Ț NU efectuați plăți către conturi noi pe care nu le-ați mai utilizat, pe baza unor instrucțiuni primite prin email și fără să verificați mai întâi validitatea acestor conturi cu partenerii dvs, prin intermediul altor canale de comunicație care nu au legătură cu poșta electronică. Pe lipsa acestei verificări mizează infractorii, deci dacă o veți face, veți contracara cu succes tentativa de fraudă. Verificarea nu o faceți în niciun caz prin e-mail sau prin mijloace de contact sugerate prin intermediul poștei electronice – vă sfătuim să luați legătura în mod direct cu partenerii dvs, prin mijloace sigure și cunoscute (numere de telefon/fax pe care le-ați mai folosit în trecut); Ț în situația în care ați efectuat o plată către un cont eronat, contactați urgent banca dvs. pentru a putea afla dacă mai sunt posibile demersuri de blocare/returnare a sumelor implicate; De asemenea, vă încurajăm ca în situația în care considerați că ați fost victima unei astfel de tentative de fraudă să înștiințați cât mai rapid organele de poliție locale.

FRAUDE LA VÂNZAREA ONLINE A BUNURILOR Pot exista situații în care persoanele care doresc să vândă anumite bunuri sau produse apelează la diferite platforme on-line aparținând unor companii care se ocupă cu intermedierea schimburilor pe internet (pagini de vânzări/cumpărări online, market-uri online, etc). În urma unei tranzacții încheiate pe o astfel de platformă vânzătorul primește un mesaj e-mail de la cumpărător. În acest mesaj cumpărătorul îi cere vânzătorului să expedieze obiectul vândut prin poștă, de obicei către destinații din zona continentului african (dar nu numai).

Pentru a determina vânzătorul să expedieze produsul înaintea primirii prețului de achiziționare potențialul cumpărător include în mesajul e-mail o confirmare de plată (falsă). Din aceasta reiese, în mod eronat, faptul că sa efectuat plata prin transfer bancar și că vânzătorul poate să intre în posesia banilor doar după ce va face dovada faptului că a expediat produsul către adresa indicată de falsul cumpărător. În realitate vânzătorul a fost înșelat și nici o sumă de bani nu a fost transferată de cumpărător. Astfel de mesaje frauduloase de confirmare a tranzacțiilor pot include logo-ul sau denumirea unor bănci cunoscute sau chiar numele unor angajați ai băncilor respective.

O altă variantă a acestui tip de înșelăciune este aceea în care potențialul cumpărător încearcă să convingă vânzătorul să trimită împreună cu produsul vândut și o sumă de bani, reprezentând contravaloarea unei taxe fictive pe care ar fi trebuit s-o plătescă pentru tranzacție, urmând să-și recupereze banii la finalizarea tranzacției ce ar avea loc după dovedirea expedierii coletului și a sumei de bani cerute. În realitate vânzătorul este înșelat și nici o sumă de bani nu mai ajunge la acesta.

Pentru a preveni astfel de situații, vă recomandăm să: Ț nu efectuați tranzacții decât pe platformele cunoscute de intermediieri online Ț verificați cu atenție reputația cumpărătorului și ce tranzacții a efectuat în trecut (atunci când este posibil) Ț comunicați cu partenerul de afaceri și pe alte canale nu doar pe email (ex. telefon, video-call) Ț verificați cu atenție termenii și condițiile platformei care intermediază vânzarea Ț vă informați cu privire la riscurile care pot apărea în urma unei astfel de

tranzacții De asemenea, vă încurajăm ca în situația în care considerați că ați fost victima unei astfel de tentative de înșelătorie să înștiințați cât mai rapid organele de poliție locale.

PAGINILE 10-11

IV. Amenințări privind utilizarea serviciilor de plată pe internet

Nu este recomandat să accesați site-ul de Internet Banking al băncii dintr-un link primit pe email sau SMS. Întotdeauna navigați (scriind adresa în browser) pe siteul oficial și folosiți linkurile de acolo. Linkurile primite pe email vă pot redirecționa către un site fals controlat de atacator. Acesta vă poate păcăli să introduceți credențialele de acces pe acest site fals controlat de atacatori.

Activați opțiunea de blocare a ferestrelor pop-up. Nu dați click pe "Agree" sau "OK" pentru a închide o fereastră. În schimb, faceți click pe "X" în colțul ferestrei sau apăsați Alt+F4 pe tastatură.

Verificați cu atenție dacă atunci când desfășurați operațiuni financiare (transferuri sau plăți cu cardul) conexiunea utilizată este una securizată (https://). Băncile folosesc certificate de securitate cu validare extinsă și adresa siteului vizitat apare cu verde și poate fi văzută imaginea unui lăcășel închis în bară de adresa URL (). Dacă browserul vă avertizează că există o problemă cu certificatul siteului este recomandat să nu continuați și să contactați banca.

Dezactivați salvarea parolelor (în special salvarea automată a acestora) în browser. Această metodă nu reprezintă o opțiune pentru păstrarea în siguranță a acestora. Dacă doriți să păstrați securizat aceste date folosiți întotdeauna un manager de parole (ex. KeePass, 1Password, LastPass, RoboForm, etc).

Credențialele de acces (utilizator, parola, cod acces, etc) sunt informații personale și nu trebuie comunicate altor persoane. NU notați pe foi hârtie sau în fișiere text nesecurizate aceste informații sensibile.

Încercați pe cât posibil să folosiți parole complexe de minim 8 caractere, aceste parole trebuie să conțină cel puțin 4 caractere de formă: 1. O literă mare (A... Z) 2. O literă mică (a... z) 3. O cifră (0... 9) 4. Un semn special (!, @, #, \$, %, ?, ^, etc)

O parolă complexă este de formă: lFmMlflo8!

Dacă nu doriți să folosiți un manager de parole pentru a păstra parolele complexe folosiți ca parolă o frază pe care o puteți ține minte ușor. De exemplu fraza "În fiecare Miercuri merg la film la ora 8!" ar

putea fi transformată într-o parolă ușor de ținut minte de formă: lFmMlflo8! (utilizând prima literă a fiecărui cuvânt)

Pentru că există posibilitatea că parola dvs. să fie aflată odată cu trecerea timpului este recomandat că parola să fie schimbată periodic. De asemenea este foarte important să NU FOLOSIȚI ACEEAȘI PAROLĂ pentru mai multe servicii (ex. cont email, cont internet banking, cont rețea socializare, etc). Dacă aveți cel mai mic dubiu că o parolă a fost aflată (compromisă) schimbați-o imediat!

Aveți grijă ca nimeni să nu vă privească atunci când introduceți o parolă sau un cod PIN. Evitați să introduceți parole pe terminale (computere din internet cafe-uri, tablete, telefoane, etc) pe care nu le dețineți sau cunoașteți, aceste terminale pot avea instalate programe de tip keylogger care vă pot căpăta credentiale de acces. Întotdeauna alegeți opțiunea de deconectare (Log Off sau Sign Out) atunci când nu mai folosiți un anumit serviciu.

Pentru orice nelămuriri sau probleme legate de serviciile de plată pe internet se recomanda utilizarea canalelor de suport puse la dispoziție de către bancă (ex. email, telefon, etc). În astfel de situații nu folosiți decât datele de contact publicate pe site-ul oficial al băncii. Bancile NU apelează (telefonic, email sau SMS) la clienții săi pentru a cere informații precum: CNP, număr card, PIN, ID logare, parola, cod token sau orice alte informații personale. O astfel de cerere reprezintă o posibilă tentativă de fraudă și pentru siguranța dvs. este recomandat să informați banca folosind canalele oficiale.

PAGINA 12

V. Amenințări privind plățile cu cardul

Păstrați cardul bancar cu aceeași grijă cu care păstrați și actul de identitate. Memorați numărul Personal de Identificare (PIN) – niciodată să nu îl scrieți. Nu păstrați acest număr alături de card, scris în telefon sau altundeva unde poate fi citit de o altă persoană. Nu comunicați acest număr nimănui, nici celor din familie.

Dacă alegeți să păstrați documentul de la bancă, prin care vi s-a comunicat PIN-ul, în nici o situație să nu păstrați acest document în același loc unde este cardul - nu se recomandă păstrarea documentului.

În cazul în care alegeți să vă creați un nou PIN sau să îl schimbați pe cel ce v-a fost dat, evitați alegerile evidente cum ar fi data nașterii personală sau a membrilor familiei.

Se recomandă să utilizați un PIN diferit pentru fiecare card pe care îl dețineți. Se recomandă de asemenea să semnați imediat pe banda de semnătură de pe spatele cardului, după ce îl primiți de la bancă.

Se recomandă să păstrați securizat o listă cu numerele cardurilor pe care le dețineți, împreună cu numerele de contact unde trebuie să anunțați în cazul în care acestea au fost pierdute sau furate. Un număr de card poate fi stocat securizat sub următoarea formă 4256 03XX XXXX 1234.

La efectuarea unei tranzacții pe internet sunt necesare următoarele date: ☐ Tipul cardului: Visa, MasterCard, etc. ☐ Nume (așa cum apare pe card) ☐ Numărul cardului (cele 4 grupuri a câte 4 cifre aflate pe card) ☐ Data expirării cardului (se găsește sub numărul cardului și este de forma II/aa) ☐ CVV2 (Card Verification Value – nume utilizat de Visa) sau CVC2 (Card Verification Code – nume utilizat de MasterCard), acesta este un cod de siguranță format din 3 cifre și este tipărit pe verso-ul cardului. Mai poate fi întâlnit pe Internet și sub denumiri cum ar fi Card Security Code/Verification Code etc. ☐ parola sau codul OTP pentru tranzacții prin sistemul “3D Secure” (Verified by Visa, sau Mastercard Securecode), în cazul în care cardul este înrolat într-un astfel de sistem.

Toate aceste informații, mai puțin parola 3D Secure, se află înscrise pe card, de aceea trebuie să păstrați cardul în siguranță și să nu dați ocazia să fie obținute aceste informații de către alte persoane. Parola 3D-Secure sau codul unic OTP sunt elemente de siguranță, de antifraudă, dezvoltate de VISA și MasterCard. Folosirea acestui sistem permite creșterea securității tranzacțiilor online, deoarece parola sau codul unic OTP (ori ambele) sunt solicitate la fiecare comandă online prin sistemul 3D Secure.

Dacă aveți unul sau mai multe carduri emise sub sigla Visa sau MasterCard aveți opțiunea de a le înrola în acest sistem. Primul pas este să contactați banca emitentă a cardului dumneavoastră și să solicitați înrolarea în acest sistem, apoi să urmați pași indicați de către bancă. Avantajele 3D Secure sunt: ☐ Reducerea riscului de fraudă datorită faptului că doar persoana care cunoaște parola 3D Secure, sau care cunoaște codul OTP creat unic pentru acea tranzacție 3D Secure (și primit prin SMS, token sau alte canale), poate tranzacționa online pe site-uri care folosesc acest sistem antifraudă; ☐ Dacă datele cardului dumneavoastră înrolat în 3D Secure sunt folosite fraudulos de către o terță parte pentru a comanda pe site-ul unui comerciant care nu folosește acest sistem de protecție, veți avea câștig de cauză la disputarea sumei aferente tranzacției.

Nu răspundeți e-mailurilor care par a fi trimise de banca emitentă, în care vă sunt solicitate datele sensibile ale cardului (număr card, data expirării, codul CVV2/CVC2, parola 3D Secure sau codul PIN) sub pretextul unor verificări, modificări, premii, culegerii de informații pentru respectarea unor modificări legislative etc.

Atunci când efectuați cumpărături online încercați să achiziționați de la comercianți cunoscuți, care se bucura de o bună reputație.

Se recomanda folosirea pentru plățile pe Internet a unui card dedicat, acest card se poate atașa unui cont în care să aveți doar sumele pe care doriți să le utilizați în acest scop. Evitați folosirea cardurilor atașate conturilor de salarii sau cele cu descoperire de cont (overdraft).

Majoritatea cardurilor nu sunt activate implicit pentru plățile pe Internet. Activați această opțiune doar dacă intenționați să faceți plăți pe Internet cu acel card. Activarea se poate face cu ajutorul băncii sau direct în aplicația băncii, depinde de fiecare bancă în parte. Nu păstrați această opțiune activă în situația în care considerați că nu veți mai folosi acel card la plăți pe Internet.

PAGINA 13-16

VI. Amenințări privind utilizarea rețelelor wireless (WiFi)

Evitați conectarea laptopului sau a smartphone-ului la o rețea wireless nesecurizată. Rețele Wi-Fi gratuite (restaurant, cafenele, aeroporturi) sunt cele mai vulnerabile dacă nu sunt securizate corespunzător. Atunci când vă conectați la o rețea nesecurizată orice persoană aflată în raza de acțiune a rețelei ar putea intercepta traficul dvs. și “vedea” anumite informații ce au fost transmise nesecurizat. Dacă totuși sunteți nevoit să vă conectați la o astfel de rețea evitați să introduceți parole de acces sau să folosiți servicii financiare online.

Nu lăsați router-ul de acasă nesecurizat și nu folosiți protocolul de securizare WEP. Acest protocol nu este sigur și un atacator poate obține accesul la rețeaua wireless și intercepta traficul din această rețea.

Se recomandă să folosiți protocolul WPA2, să configurați o parolă cât mai lungă și să schimbați numele implicit (SSID-ul) al rețelei wireless.

Schimbați parola preconfigurată din fabrică pentru interfața de administrare și configurare a router-ului, folosind o altă parolă puternică, deoarece parolele inițiale se pot găsi ușor pe internet și pot fi folosite de persoane rău voitoare care au acces în rețeaua dumneavoastră pentru a modifica în mod malițios anumite setări precum DNSul (putând fi astfel amenințați de un atac de tip “DNS Pharming” – unde chiar dacă introduceți manual și corect adresa web a băncii tale sau a instituției financiare direct în browser, sau o accesezi prin cele mai recente bookmark-uri folosite anterior, vei deschide de fapt un site malițios de tip clona fără să vă puteți da seama că nu sunteți pe site-ul real al băncii – acest tip de atac fiind mult mai periculos chiar decât atacul de tip Phishing pentru că nu exista modalități de identificare a site-ului malițios).