**Analiza fenomenului de *spoofing***

I.Introducere

Nu este nimic nou in ceea ce privește spoofing-ul. De fapt, cuvântul "spoof", ca formă de înșelătorie, datează de peste un secol. Potrivit dicționarului online Merriam-Webster, cuvântul "spoof" este atribuit comediantului englez din secolul al XIX-lea Arthur Roberts, cu referire la un joc de pacaleala și înșelăciune creat de Robert. Regulile jocului s-au pierdut în timp. Putem doar să presupunem că jocul nu era foarte amuzant sau ca britanicilor din acea vreme nu le placea sa fie pacaliti. Oricare ar fi cazul, numele a ramas, deși jocul nu.

Abia la începutul secolului al XX-lea, ori de cate ori cineva menționa "spoof" sau "spoofing", se referea la ceva amuzant și pozitiv.

In prezent, spoofing este cel mai des folosit atunci când se vorbește despre criminalitatea informatică. Ori de câte ori un escroc sau o amenințare cibernetica pretinde că este cineva sau ceva ce nu este, este vorba de spoofing.

Spoofing reprezinta un atac cibernetic prin care un atacator se da drept o sursa sigura, primind astfel access la datele din reteaua unei companii. Un atac de tip spoofing este o situație în care o persoană sau un program reușește să se identifice ca fiind altcineva prin falsificarea datelor, pentru a obține un avantaj ilegitim.

Deobicei atacatorii fura informatii esentiale si cer o suma extraordinara pentru recapatarea datelor furate sau raspandesc virusi prin diverse canale. Poate afecta reteaua interna a unei companii si pot infecta mai multe computere. Ei incearca sa iti fure identitatea, datele obtinute putand fi vandute.

Spoofing ul se poate intampla pe diferite canale de comunicatie.

* Prin Email se pot trimite link uri catre diferite siteuri periculoase care sa fure date importante sau sa manipuleze receptorul sa dea informatiile de buna voie.
* Prin IP – se refera la a primi mesaje neautorizate care par ca vin din reteaua interna a companiei
* Prin web – cauti un site si dai de un site similar cu URL ul foarte asemanator, ele fura datele de login si posibil pot cauza un malware computerului din care sunt accesate
* Prin DNS un site alterat te trimite pe un site fals care seamana cu destinatia. Inlocuiesc Ip ul din DNS cu unul pe care il folosesc hackerii
* Prin MAC – Se foloseste tabela ARP prin care hackerii isi trimit IP ul malicios la adresa MAC al tintei. Astfel ei pot sa intercepteze sa modifice sau sa opreaza data trimisa catre Ip ul tintei.
* Prin GPS – se trimit locatii false prin GPS , trimitand tinta in locuri gresite
* Prin sistemul de facial recognition din smartphonuri sau profilele online, atacatorii pot obtine informatii critice despre trasaturile unei persoane

II. IP spoofing

Protocolul de bază pentru trimiterea de date prin rețeaua de Internet și prin multe alte rețele de calculatoare este protocolul Internet (IP). Protocolul specifică faptul că fiecare pachet, mesaj trebuie să aibă un antet care să conțină adresa IP a expeditorului pachetului .

Stratul de legătură de date utilizează ARP (protocolul de rezoluție a adreselor) pentru a traduce adresa IP în adresa MAC. Clientul începe prin a trimite mai întâi un mesaj ARP de difuzare pentru o anumită adresă IP. Stiu IP ul destinatiei, am nevoie si de MAC pentru a trimite un mesaj. Comutatorul difuzează mesajul ARP către toate posturile, cu excepția postului sursă. Atunci când adresa IP de destinație primește mesajul ARP, răspunde scriind adresa MAC și toate celelalte gazde de pe comutator vor renunța.

Adresa IP sursă este în mod normal adresa de la care a fost trimis pachetul, dar adresa expeditorului din antet poate fi modificată, astfel încât destinatarului să i se pară că pachetul provine de la o altă sursă. Adica atacatorul trimite un mesaj care contine IP ul sau, dar il modifica astfel incat sa para ca vine din partea unei surse sigure(ex: coleg de serviciu). Tinta nu va putea sa trimita vreun alt mesaj inapoi catre atacator, caci la baza IP sursei nu coincide cu cel al atacatorului..

IP spoofing are loc la nivelul unei retele, atacatorul trecand de sistemele de aparare folosind un IP intern. Odata trecut de aceste sisteme de aparare, el are acces la datele din interior usor.

IP address spoofing este cel mai frecvent utilizat în atacurile de tip denial-of-service, în care obiectivul este de a inunda ținta cu un volum copleșitor de trafic, iar atacatorului nu îi pasă de primirea de răspunsuri la atac. Pachetele cu adrese IP falsificate sunt mai greu de filtrat, deoarece fiecare pachet falsificat pare să provină de la o adresă diferită și ascunde adevărata sursă a atacului. Atacurile DoS care folosesc spoofing-ul aleg în mod obișnuit adrese aleatorii din întregul spațiu de adrese IP, deși mecanismele de spoofing mai sofisticate pot evita adresele care nu pot fi rutate sau porțiunile neutilizate din spațiul de adrese IP.

IP spoofing-ul poate fi utilizat pentru a obține acces la computere prin mascarea botnet-urilor. Un botnet este o rețea de calculatoare pe care hackerii o controlează dintr-o singură sursă. Fiecare calculator rulează un bot dedicat, care desfășoară activități rău intenționate în numele atacatorului. IP spoofing-ul permite atacatorului să mascheze botnet-ul, deoarece fiecare bot din rețea are o adresă IP falsă, ceea ce face ca actorul rău intenționat să fie dificil de urmărit. Acest lucru poate prelungi durata unui atac pentru a maximiza câștigul.

Unul dintre cele mai frecvent citate exemple de atac de IP spoofing este atacul DDoS al GitHub din 2018. A fost afectată de ceea ce s-a considerat a fi cel mai mare atac DDoS din toate timpurile. Atacatorii au falsificat adresa IP a GitHub în cadrul unui atac coordonat atât de mare încât a pus la pământ serviciul timp de aproape 20 de minute. GitHub a recâștigat controlul prin redirecționarea traficului printr-un partener intermediar și prin spălarea datelor pentru a bloca părțile rău intenționate.

III. MAC spoofing

MAC ul( Media Access Control) este o adresa unica a hardware ului pusa de fabricant, prin care sunt identificate piesele fizice. Adresa MAC este imposibil de schimbat. Dar este posibil sa alterezi modul in care apare ea pe partea de software. Am explicat mai sus cum fuctioneaza trimiterea unui mesaj in retea. Tabela ARP contine adresa IP, adresa MAC si timpul in care este valabil mesajul(300 secunde maxim).

Fiecare adresă MAC include 48 de biți, sau 6 octeți, și este aranjată după următorul model: 00:81:41:41:fe:ad:7e. Primii 24 de biți reprezintă codul producătorului atribuit de Institute of Electrical and Electronics Engineers (IEEE), iar următorii 24 de biți reprezintă numărul dispozitivului definit de producător.

Există instrumente care pot face un sistem de operare să creadă că NIC are adresa MAC aleasă de utilizator. Procesul de mascare a unei adrese MAC este cunoscut sub numele de MAC spoofing. MAC spoofing functioneaza asemanator cu IP spoofing doar ca in loc ca atacatorul sa fie cel care trimite, el se va da drept destinatar.

Teoretic, fiecare dispozitiv de rețea din lume este identificat printr-o adresă MAC. Dar nu toți utilizatorii doresc această transparență pe internet. Un motiv pentru a masca adresa MAC este protecția vieții private - de exemplu, în rețelele WLAN publice. Această utilizare legitimă a mascării MAC este în opoziție cu activitățile ilegale, în care utilizatorii schimbă adresele MAC pentru a eluda restricțiile de acces și măsurile de securitate sau pentru a imita identitatea unui alt dispozitiv de rețea.

Deși falsificarea adreselor MAC nu este ilegală, practica sa a provocat controverse în unele cazuri. În rechizitoriul din 2012 împotriva lui Aaron Swartz, un hacktivist de pe internet acuzat că a accesat ilegal fișiere din biblioteca digitală JSTOR, procurorii au susținut că, deoarece acesta și-a falsificat adresa MAC, acest lucru a demonstrat intenția de a comite acte infracționale

IV.Email Spoofing

E-mail spoofing este atunci când sunt trimise e-mailuri cu adrese de expeditor false cu intenția de a infecta calculatorul cu programe malware, de a cere bani sau de a fura informații. Aceste adrese de expeditor false sunt create astfel încât să pară că provin de la cineva pe care cunoscut, cum ar fi un coleg de serviciu sau un prieten.

Aceste adrese pot fi create fie prin utilizarea unor numere sau litere alternative pentru a arăta ușor diferit de original, fie prin deghizarea câmpului "de la" pentru a fi exact adresa de e-mail a unei persoane din rețeaua dumneavoastră.

Falsificarea e-mailurilor este posibilă datorită modului în care sunt concepute sistemele de e-mail. Aplicația client atribuie o adresă de expeditor mesajelor de ieșire; serverele de e-mail de ieșire nu au cum să stabilească dacă adresa de expeditor este legitimă sau falsă.

Serverele destinatarilor și software-ul antimalware pot ajuta la detectarea și filtrarea mesajelor falsificate. Din nefericire, nu toate serviciile de e-mail dispun de protocoale de securitate. Cu toate acestea, utilizatorii pot examina anteturile de e-mail incluse în fiecare mesaj pentru a determina dacă adresa expeditorului este falsă.

In 2021, cercetarea facuta de Tessian a constatat că angajații primesc în medie 14 e-mailuri malițioase pe an. Unele industrii au fost afectate în mod deosebit, lucrătorii din retail primind în medie 49. Cercetarea ESET din 2021 a constatat o creștere de 7,3% a atacurilor pe bază de e-mail între mai și august 2021, majoritatea făcând parte din campanii de phishing.

V. Web Spoofing

Spoofing-ul de site-uri web constă în a face ca un site web rău intenționat să pară unul legitim. Site-ul falsificat arăta ca o pagină de autentificare pentru un site web pe care tinta il frecventeaza - până la branding, interfața cu utilizatorul și chiar un nume de domeniu falsificat care arată la fel la prima vedere. Infractorii cibernetici folosesc site-uri web falsificate pentru a capta numele de utilizator și parola, dar si datele cardului (aka login spoofing) sau pentru a introduce programe malware pe computerul victimelor (o descărcare drive-by). În general, un site web falsificat va fi utilizat împreună cu un e-mail falsificat, în care e-mailul va conține un link către site-ul web. Ele sunt usor de implementat deoarece un hacker trebuie sa creeze un site copie al unui brand. Partea dificila este sa inregistreze numele de domeniului. Există unele bariere care împiedică crearea unor domenii aproape identice, dar hackerii sunt suficient de isteți pentru a găsi soluții alternative. Dacă reușesc să mascheze identitatea site-ului lor ca fiind altceva, misiunea lor este aproape îndeplinită.

Website spoofing sunt incredibil de greu de identificat. Deoarece înșelătoria are loc în afara perimetrului de securitate al unei organizații, spoofingul de site-uri web este de obicei descoperit doar după ce un număr de utilizatori au căzut deja pradă atacului. Această problemă poate fi combatuta cu soluții de protecție a mărcii care utilizează machine learning și scaneaza internetul pentru a identifica domeniile suspecte și site clonate, blocându-le înainte de a fi lansate sau oprind atacurile în direct.

Multe branduri sunt insa replicate in acest fel. În prezent, Microsoft este marca cea mai falsificată, în creștere cu 15,5% față de anul trecut. Marca lor, cunoscută la nivel mondial, cu multe milioane de oameni care le folosesc software-ul, este irezistibilă pentru hackeri. O altă marcă de profil înalt care se află în prezent pe locul al doilea după Microsoft este PayPal. Compania de comerț electronic de profil înalt și de încredere este o sursă tentantă pentru acest tip de infracțiuni, datorită legăturii sale directe cu finanțele. Facebook ocupă locul al treilea, cu un salt de spoofing de 176% față de anul trecut. O înșelăciune reușită pe Facebook fură liste de contacte care oferă un grup complet nou de prieteni cărora să le fie trimise e-mailuri de phishing. Printre alte site-uri de tip spoofing de profil înalt se numără Netflix, Bank of America și Apple.

VI. DNS spoofing

Sistemul de nume de domeniu (DNS) spoofing este un tip de atac cibernetic care exploatează vulnerabilitățile serverelor DNS pentru a devia traficul de la serverele legitime către servere false.

DNS spoofing și, prin extensie, DNS cache poisoning (otrăvirea cache-ului DNS) se numără printre cele mai înșelătoare amenințări cibernetice. La prima vedere site ul pe care este directionat utilizatorul poate sa arate ca un site web piratat.

Următorul exemplu ilustrează un atac de otrăvire a cache-ului DNS, în care un atacator (IP 192.168.3.300) interceptează un canal de comunicare între un client (IP 192.168.1.100) și un computer server aparținând site-ului www.estores.com (IP 192.168.2.200).

În acest scenariu, un instrument (de exemplu, arpspoof) este utilizat pentru a păcăli clientul să creadă că IP-ul serverului este 192.168.3.300. În același timp, serverul este făcut să creadă că IP-ul clientului este, de asemenea, 192.168.3.300. Atacatorul va folosi arpspoof pentru a modifica adresele MAC din tabelul ARP, facand DNS ul sa creada ca computerul atacatorului este al clientului, pentru a spune computerului clientului sa serverul este al atacatorului. Pachetele IP trimise intre client si server vor fi directionate infractorului. Fișierul host, 192.168.3.300 estores.com este creat pe calculatorul local al atacatorului, care mapează site-ul www.estores.com la IP-ul său local.

Infractorul instalează un server web pe IP-ul computerului local și creează un site web fals care seamănă cu [www.estores.com](http://www.estores.com). In final, toate cererile DNS vor fi directionate catre fisierul gazda al infractorului.

În consecință, site-ul web fals este afișat utilizatorilor și, numai prin interacțiunea cu site-ul, se instalează programe malware pe calculatoarele acestora.

Atacul cibernetic Dyn din 2016 a fost un eveniment semnificativ care a indicat un risc serios pentru DNS. Dyn, care este un furnizor popular de DNS, a fost atacat de două atacuri de negare a serviciului distribuit (DDoS) mari și complexe împotriva infrastructurii DNS. În cele din urmă, mai multe servicii importante de internet și sisteme bancare au fost paralizate. Un aspect interesant al acestui atac este că o mare parte din SUA a fost afectată prin atacarea centrelor de date din doar anumite părți ale SUA. Altfel spus, atacul a vizat în mod direct doar un DNS distribuit la nivel local cu un Botnet local. În plus, Raportul privind securitatea cibernetică, publicat în 2018, descrie DNS ca fiind cea mai mare (82%) țintă a serviciilor de internet a atacurilor de tip application-layer. În ciuda eforturilor de îmbunătățire a problemelor de securitate ale DNS, DNS este în continuare o țintă populară pentru atacurile cibernetice din cauza rolului său esențial pe internet și a vulnerabilității sale.

VII.Trends

Trecerea la munca la distanță a prezentat multe provocări pentru întreprinderi - iar gama, frecvența și probabilitatea crescute a incidentelor de securitate se numără printre cele mai grave. Noile obiceiuri de lucru au contribuit la recenta creștere a numărului de phishing, deoarece echipele IT au mai puțină supraveghere asupra modului în care colegii își folosesc dispozitivele și pot întâmpina dificultăți în a oferi asistență atunci când lucrurile merg prost.

Potrivit raportului Microsoft New Future of Work Report: 80% dintre profesioniștii din domeniul securității intervievați au declarat că s-au confruntat cu o creștere a amenințărilor la adresa securității de când a început trecerea la munca la distanță. Dintre aceștia, 62% au declarat că campaniile de phishing au crescut mai mult decât orice alt tip de amenințare. Angajații au declarat că au crezut că departamentele IT ar fi fost în măsură să atenueze aceste atacuri de phishing dacă ar fi lucrat la birou. Mai mult, un sondaj din august 2021 realizat de Palo Alto Networks a constatat că: "În ceea ce privește mediul de lucru la distanță, în august 2021, Palo Alto Networks a constatat că: 35% dintre companii au raportat că angajații lor fie au ocolit, fie au dezactivat măsurile de securitate la distanță. Lucrătorii din organizațiile care nu aveau instrumente eficiente de colaborare la distanță au fost de peste opt ori mai predispuși să raporteze niveluri ridicate de eludare a securității. 83% dintre companiile cu o utilizare relaxată a BYOD (Bring-your-own-device) au dus la creșterea problemelor de securitate

VIII.Concluzii. Cum ne protejam?

Pentru a determina legitimitatea, fiți atenți la: ortografie necorespunzătoare,Gramatică incorectă/inconsecventă,Structură neobișnuită a frazei sau schimbări de frază.

Aceste erori sunt adesea indicii că comunicările nu provin de la cine pretind a fi.

Alte lucruri la care trebuie să fiți atenți includ: Adresa expeditorului de e-mail: uneori, adresele vor fi falsificate prin schimbarea a una sau două litere fie în partea locală (înainte de simbolul @), fie în numele de domeniu. URL-ul unei pagini web: la fel ca în cazul adreselor de e-mail, ortografia poate fi ușor schimbată pentru a păcăli un vizitator care nu se uită atent. Nu faceți clic pe linkuri necunoscute și nu descărcați atașamente necunoscute/neașteptate. Dacă primiți acest lucru în e-mail, trimiteți un răspuns pentru a cere confirmare. Dacă o adresă de e-mail este falsificată exact, răspunsul va merge la persoana reală cu adresa de e-mail - nu la persoana care a falsificat-o. Nu luați apelurile telefonice ca atare; fiți atenți la informațiile pe care vi le solicită apelantul. Căutați pe Google numărul de telefon prezentat pe ID-ul apelantului pentru a vedea dacă este asociat cu escrocherii. Chiar dacă numărul pare legitim, închideți și sunați dumneavoastră, deoarece numerele de identificare a apelantului pot fi falsificate.

Spoofing-ul poate fi uneori ușor de depistat, dar nu întotdeauna - din ce în ce mai mulți actori rău intenționați desfășoară atacuri sofisticate de spoofing care necesită vigilență din partea utilizatorului. Cunoașterea diferitelor metode de spoofing și a semnelor acestora vă poate ajuta să evitați să fiți o victimă.

Bibliografie

* <https://www.kaspersky.com/resource-center/definitions/spoofing>
* <https://www.forcepoint.com/cyber-edu/spoofing>
* <https://en.wikipedia.org/wiki/Spoofing_attack>
* <https://www.kaspersky.com/resource-center/threats/ip-spoofing>
* <https://www.kaspersky.com/resource-center/definitions/dns>
* <https://www.malwarebytes.com/spoofing>
* <https://en.wikipedia.org/wiki/IP_address_spoofing>
* <https://www.ionos.com/digitalguide/server/know-how/what-is-mac-spoofing/>
* <https://en.wikipedia.org/wiki/MAC_spoofing>
* <https://www.proofpoint.com/us/threat-reference/email-spoofing>
* <https://www.tessian.com/blog/phishing-statistics-2020/>
* <https://www.sosdailynews.com/news.jspx?articleid=%2052FE7D76C2C33CE89DC73D57EDC9C827>
* <https://www.imperva.com/learn/application-security/dns-spoofing/>
* <https://jsssjournal.com/article/view/3660>