Analiză unei vulnerabilități

Banca Națională a României

Alexandru Angheluș

Identificarea vulnerabilitate

Exploatare continuă

Scenarii de exploatare în atac cibernetic

Măsuri și o mică concluzie.

1. INTRODUCERE

În ultimii ani, importanța securității cibernetice a devenit din ce în ce mai evidentă pentru toți cei care utilizează tehnologia și internetul în activitățile lor. Cu toate acestea, creșterea dependenței noastre de tehnologie ne-a expus la riscuri și amenințări cibernetice fără precedent.

Infractorii cibernetici sunt mereu în căutare de vulnerabilități în infrastructurile critice, cum ar fi sistemele financiare, rețelele de transport sau chiar infrastructura de energie electrică. Odată ce identifică o vulnerabilitate, aceștia pot să acceseze zonele confidențiale ale infrastructurilor și să compromită informațiile sau să cauzeze daune semnificative.

Din fericire, există specialiști în domeniul securității cibernetice care lucrează neobosit pentru a detecta și a remedia vulnerabilitățile în infrastructurile critice. Acești experți fac parte din instituții publice sau sunt parte din echipele structurilor cu competențe în securitate cibernetică. Munca lor este deosebit de importantă pentru a proteja economia și societatea de amenințările cibernetice.

O altă categorie de specialiști este aceea a voluntarilor sau poate nici acest statul nu îl dețin oficial, dar prezența lor subtilă și relativ invizibilă joacă un rol important în securizarea infrastructurilor critice, a instituțiilor publice și uneori a entităților private din România. Aceștia prin activitățile lor identifică atacuri cibernetice, vulnerabilități sau informații sensibile devenite publice și le raportează către Directoratul Național de Securitate Cibernetică al României și/ sau entităților vizate.

Așa cum probabil deja știți sau ați înțeles acum... și eu printre aceștia... de câțiva ani.

Multe informații nu ajung în spațiul public sau ajung într-o formă în care cei care le văd să nu înțeleagă exact unde este vulnerabilitatea(așa cum este și acest articol).. din motive de înțeles, dar în ultimii ani au fost rezolvate foarte multe prin intermediul celor care susțin astfel infrastructura IT și implicit comunitatea de securitate cibernetică din România.

2. SUBIECTUL ARTICOLULUI

Din titlu s-a înțeles care este subiectul, iar detaliile care urmează au ca scop conștientizarea pericolelor din spațiul virtual prin detalierea acțiunilor care pot fi generate de anumite vulnerabilități care sunt aparent fără importanță și în egală măsură spre a înțelege timpul alocat unor astfel de analize și implicațiile care apar pe parcursul acestora.

2.1 Cuvinte cheie

În securitate cibernetică, cu precădere în auditurile de securitate, sunt utilizate diverse cuvinte cheie în căutările manuale sau automate. Acestea sunt adăugate în programe sau platforme de căutare a conținutului indexat de Google și nu numai, rezultatele fiind pe măsura complexității combinațiilor de cuvinte și a relevanței pe care o au legat de ceea ce căutați.

Analiza fiind una generală, dar cu scopul de a identifica vulnerabilități ale infrastructurilor din România, utilizând în căutări domeniile ”.ro” și astfel am ajuns la următorul rezultat:

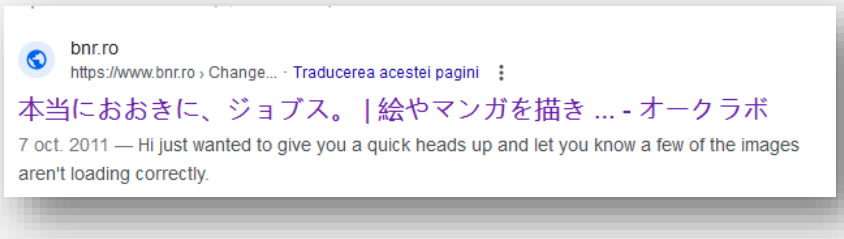


Figura 1. Rezultat Google

Figura 2. Explicația rezultatului (conexiunea este sigură)

Un rezultat destul de convingător, pentru a continua în noua direcție oferită.

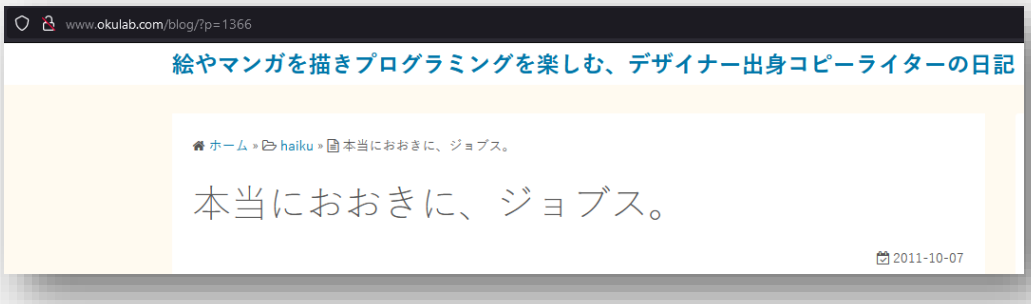


Figura 3. Rezultat redirecționare

Nu voi dezvălui adresa completă a Băncii Naționale a României, dar vă pot spune că în acest moment a fost descoperită o vulnerabilitate prin intermediul căreia un utilizator, chiar și mai experimentat poate fi păcălit prin intermediul adresei oficiale a instituției.

Vulnerabilitatea are denumirea de ”Redirecționare URL către un site nesigur” sau CWE-601: URL Redirection to Untrusted Site ('Open Redirect').

Figura 4. Exemplu redirecționare bnr.ro

Așa cum se poate observa, este folosită adresa oficială, iar dacă adăugăm o altă adresă la final, utilizatorul va ajunge la adresa adăugată… în cazul nostru pe pagina Google.

Parametrii din adresă, partea care nu se vede în imagine, au fost la rândul lor folosiți într-o nouă căutare, pentru a vedea dacă mai sunt și alte pagini web din România care au această vulnerabilitate.. și surpriză:

Figura 5. Exemplu redirecționare bnro.ro

..un al doilea domeniu al Instituției are aceiași vulnerabilitate, cel mai probabil paginile fiind construite pe aceiași structură.

În acest moment vă voi întoarce la *Figura 3* și poate că cei mai atenți la detalii ați observat data afișată în postarea la care am fost direcționați inițial: 2011-10-07, deci vulnerabilitatea exista în 2011 și era exploatată.

2.2 Exploatare continuă

Fiind o vulnerabilitate clară, interesul este să identificăm posibile exploatări ale acesteia. După mai multe variante de cuvinte cheie, am descoperit că există o exploatare continuă a vulnerabilității, adresa vulnerabilă fiind prezentă în rezultatele căutărilor și pe anumite pagini web.

Pagini web compromise:

- Acestor pagini le este modificată structura și vor ajuta la direcționarea vizitatorilor către adresele incluse, având ca scop:
  Vânzarea de bunuri și/ sau servicii, fiind doar o strategie de a aduna vizitatori;
- Inducerea în eroare și utilizarea paginilor false, pentru campanii de fraude financiare
- Utilizare unor domenii puternice, cu trafic mare, pentru a crește vizibilitatea unor alte pagini web.

În cazul nostru, majoritatea domeniilor atașate de adresa BNR duc spre pagini ale unor platforme de jocuri online, de tip online casino(posibil descărcare aplicații) și pagini cu conținut pornografic.

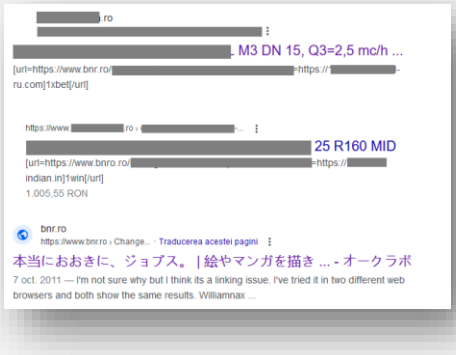


Figura 6. Rezultate căutare cu cuvinte cheie relevante

Figura 7. Adrese adăugate în codul paginilor compromise

Domenii către care direcționează adresele identificate(domeniile sunt modificate parțial):

- Un domeniu .ro – Codul sursă a fost modificat și conține multe astfel de direcționări;
- 1win-___an.in, 1xbet-down___-ru.com, 1-xbet-___-apk.com, xd__o.tech, he___venxxx.ru, q__.ac.ir, k___k.com, t___ultra.com, film__da.ru, mo__us.info, zi___ool.info, i-porn__.com, fre__lim.at etc;
- t.me/filmfilm___ (Canal Telegram RU).

3. VARIANTE ȘI SCENARII DE ATAC CIBERNETIC

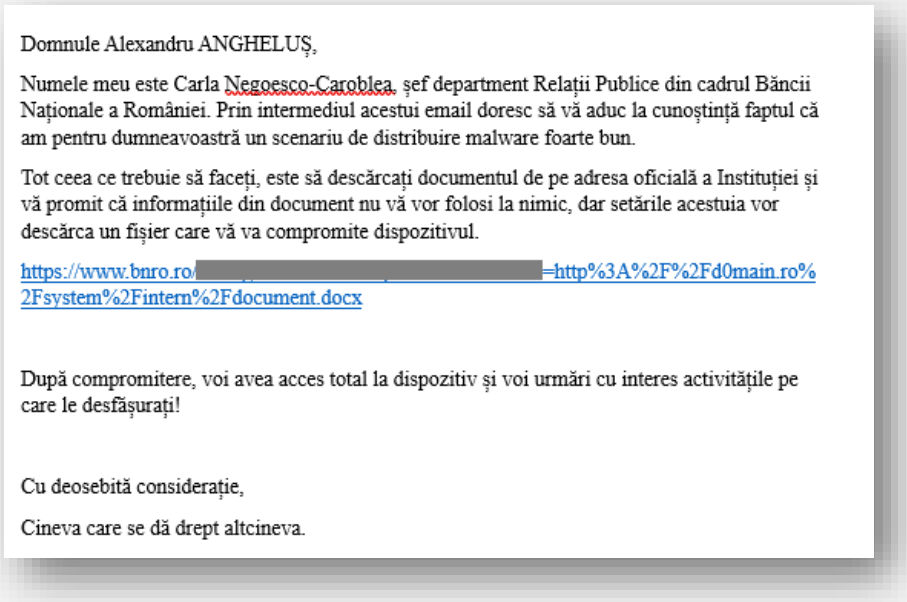
Atacurile cibernetice care implică interacțiunea cu utilizatorii sunt cele mai des folosite și au o rată foarte mare de succes, deoarece o mare parte dintre utilizatorii de tehnologie nu au avut parte de educație cibernetică, folosind dispozitivele fără a conștientiza pericolul generat de tehnologie și internet, fără a fi conștienți de riscurile la care se expun în fiecare zi.

Putem include 3 variante de atac cibernetic care pot fi utilizate în exploatarea acestei vulnerabilități, iar în funcție de capacitatea fiecăruia, putem să ne imaginăm scenariile care pot fi folosite în aceste atacuri cibernetice.

Ceea ce vor avea în comun aceste atacuri este ingineria socială, modalitatea de convingerea utilizatorului să acceseze/ descarce/ instaleze ceea ce își dorește atacatorul.

3.1 **Malware** (documente infectate).

Cum ar fi dacă angajații, colaboratorii, partenerii, clienții sau persoane de interes ar primi un email prin care le este prezentată o povestioară care necesită intervenția acestora și în mesaj este atașată o adresă către un document de pe serverele Instituției?



Domnule Alexandru ANGHELUȘ,

Numele meu este Carla Negoesco-Caroblea, șef department Relații Publice din cadrul Băncii Naționale a României. Prin intermediul acestui email doresc să vă aduc la cunoștință faptul că am pentru dumneavoastră un scenariu de distribuire malware foarte bun.

Tot ceea ce trebuie să faceți, este să descărcați documentul de pe adresa oficială a Instituției și vă promit că informațiile din document nu vă vor folosi la nimic, dar setările acestuia vor descărca un fișier care vă va compromite dispozitivul.

https://www.bnro.ro/[redacted]=http%3A%2F%2Fd0main.ro%2Fsystem%2Fintern%2Fdocument.docx

După compromitere, voi avea acces total la dispozitiv și voi urmări cu interes activitățile pe care le desfășurați!

Cu deosebită considerație,

Cineva care se dă drept altcineva.

Figura 8. Exemplu email cu distribuire de malware(plus puțin umor)

Ceea ce înainte era *https://www.google.com/*

Acum a devenit *http://d0main.ro/system/intern/document.docx,* mai exact un document găzduit pe un oarecare domeniu.

Iar dacă am făcut cursuri de educație cibernetică împreună, vă aduceți aminte de varianta în care nu apăsăm pe adrese sau butoane din email, ci putem copia adresa și o punem în bară, pentru a vedea unde vrea să ne direcționeze. Ei bine, în cazul acesta adresa pare cât de oficială se poate...

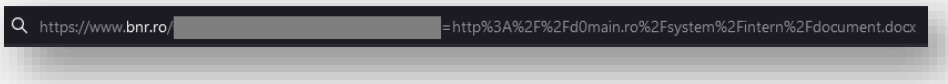
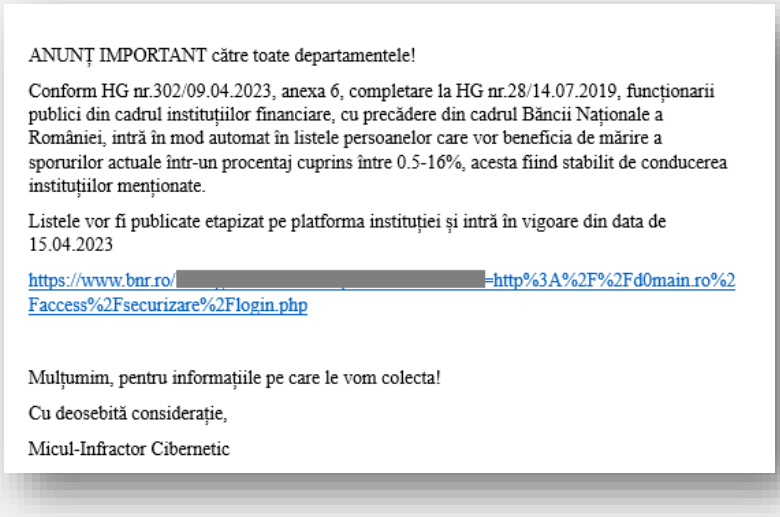


Figura 9. Exemplu de mascare a adresei de redirecționare

3.2 **Phishing**

Ce se poate întâmpla în cazul în care angajații sunt puși în fața unui scenariu relevant, în cadrul unui atac cibernetic de tip Phishing?

Care sunt șansele ca un atac de acest tip să poată induce în eroare angajații sau clienții, având în vedere că phishing-ul bancar este foarte des folosit?



ANUNȚ IMPORTANT către toate departamentele!

Conform HG nr.302/09.04.2023, anexa 6, completare la HG nr.28/14.07.2019, funcționarii publici din cadrul instituțiilor financiare, cu precădere din cadrul Băncii Naționale a României, intră în mod automat în listele persoanelor care vor beneficia de mărire a sporurilor actuale într-un procentaj cuprins între 0.5-16%, acesta fiind stabilit de conducerea instituțiilor menționate.

Listele vor fi publicate etapizat pe platforma instituției și intră în vigoare din data de 15.04.2023

https://www.bnr.ro/[redacted]=http%3A%2F%2Fd0main.ro%2Faccess%2Fsecurizare%2Flogin.php

Mulțumim, pentru informațiile pe care le vom colecta!

Cu deosebită considerație,

Micul-Infractor Cibernetic

Figura 10. Exemplu de email phishing

Utilizatorul care apasă pe adresa oferită de atacator poate fi direcționată către o pagină falsă de conectare la platforma Instituției și prin introducerea datelor acesta oferă infractorului cibernetic informații despre accesul în infrastructură.

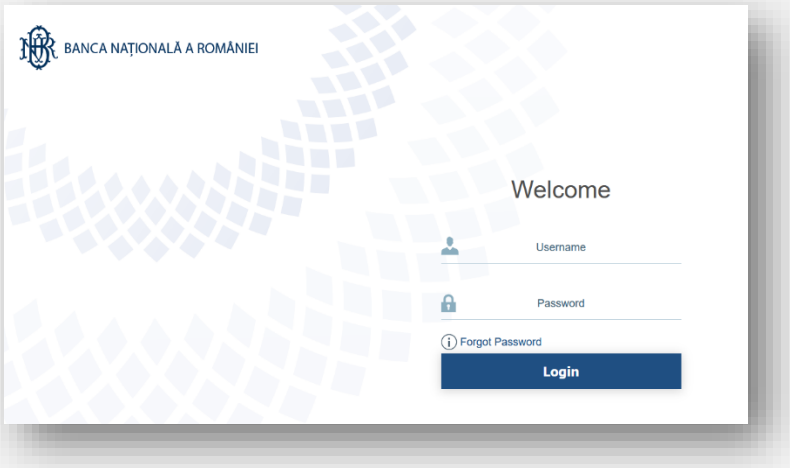


Figura 11. Exemplu pagină falsă utilizată în atac phishing

Aceiași situație. Adresa este cea oficială, doar că a suferit mici schimbări și în loc de acel *https://www.google.com/* avem:

http://d0main.ro/access/securizare/login.php - Pagina falsă utilizată pentru phishing.

3.3 **Știri false**

Prin aceiași metodă, pot fi trimise mesaje către orice adresă de email sau prin SMS, iar cei care apasă pe adresa primită să fie direcționați către o pagină falsă sau un document care conțin informații false despre sistemul bancar.

Sunt convins că vă puteți imagina haosul care ar putea fi generat de o informare financiară ”oficială” din partea băncii naționale!

... mai ales dacă ne amintim de situația cu hârtia igienică, care nu era chiar o problemă de siguranță națională, sau de incidentul cu scumpirile la carburanți.

Figura 12. Sursă: Curs educație cibernetică(Prodefence/ Cyberaid.eu)

4. DERULAREA ATACULUI CIBERNETIC

Toate cele menționate anterior sunt scenarii și posibil să nu funcționeze, dacă luăm în considerare nivelul de educație cibernetică, sistemele de securitate ale infrastructurii, procedurile de comunicare etc, dar 100% este nevoie de acceptarea acestora ca și posibile acțiuni ale infractorilor cibernetici.

Distribuirea acestor scenarii poate fi făcută în foarte multe moduri, dar depinde de cine inițiază atacul, scopul urmărit și resursele care sunt alocate atacului cibernetic.

Așa cum deja am menționat, campaniile de atac cibernetic se folosesc de ingineria socială (social engineering) pentru a convinge utilizatorii, invocând o serie de probleme urgente sau câștiguri miraculoase; Frica, bucuria, rușinea, dezorientarea fiind armele cele mai des folosite de atacatori.

Modalitatea de distribuire a acestor campanii este reprezentată în imaginea următoare și cu această ocazie puteți înțelege că un atac cibernetic poate veni din orice direcție, inclusiv prin utilizarea unor conturi compromise ale familiei sau prietenilor.

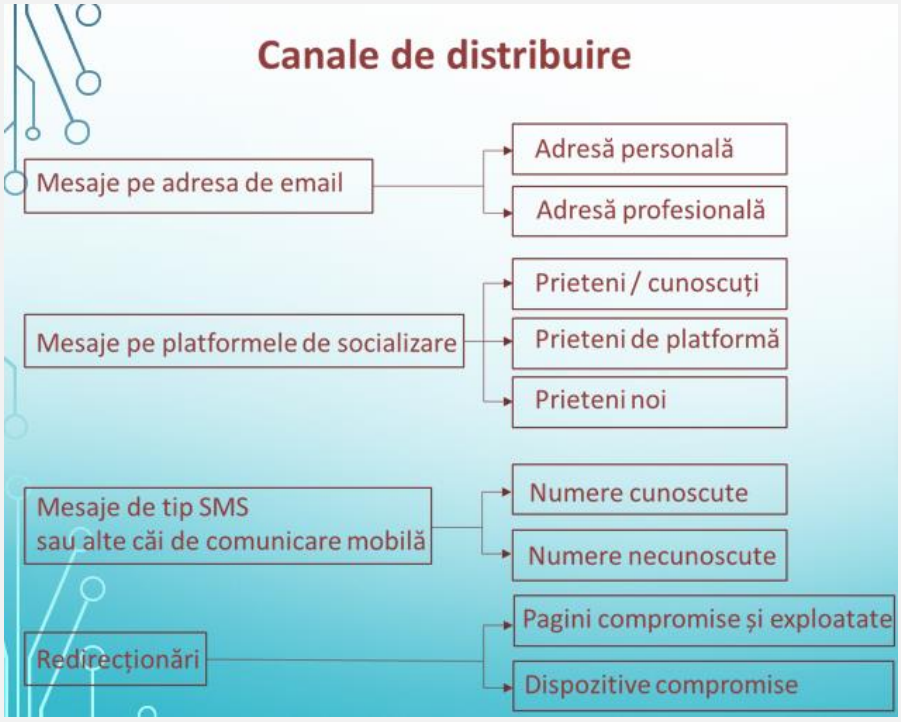


Figura13 . Sursă: Curs educație cibernetică (Prodefence/ CyberAID.eu)

5. Măsuri

La nivel de instituție nu are rost să ofer indicații administratorilor infrastructurii, deoarece sunt convins că vor găsi modalitatea de restricționare a redirecționărilor de pe adresele respective, mai ales că au primit deja avertizarea în legătură cu vulnerabilitatea și cel mai probabil după remediere utilizarea acelor adrese vor direcționa utilizatorul spre o pagină a Instituției inspirată din setările unor alte instituții bancare.

Figura 14. Mesaj utilizare redirecționare restricționată

În ceea ce privește utilizatorii, pe lângă indicațiile clasice de a fi atenți unde își introduc datele sau de unde descarcă anumite aplicații, pot spune că este destul de complicată această variată de atac, așa cum am mai menționat, totul pare sigur... mai puțin pagina unde veți fi direcționați, iar în cazul aplicațiilor sau documentelor descărcate.. uff.. utilizați versiuni bune de antivirus, actualizate și corect configurate.

6. Concluzie

Concluzia este una generală și valabilă pentru toate instituțiile/ companiile.

Uneori suntem predispuși la ignorarea unor vulnerabilități din infrastructură(în cazul în care am fost informați despre ele), deoarece acestea nu au impact direct asupra sistemelor componente și considerăm că este un risc acceptabil.

Acum, după analizarea posibilelor scenarii și a impactului pe care îl poate avea asupra tuturor celor cu care interacționează aceste sisteme, ne putem gândi și la varianta în care personalul și colaboratorii pot fi induși în eroare, la clienții care în mare parte nu au avut parte de educație cibernetică și la impactul pe care îl poate avea asupra imaginii entității pe care o administrăm.

Securitatea cibernetică este o responsabilitate comună!