REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Analizë e domaineve jolegjitime Smishing

Versioni: 1.0
Datë: 22/07/2025

PËRMBAJTJA

Ky raport ka kufizime dhe duhet interpretuar me kujdes!

Disa nga këto kufizime përfshijnë:

Faza e parë:
Burimet e informacionit: Raporti është bazuar në informacionet të vendosura në dispozicion në momentin e përgatitjes së tij. Ndërkohë, disa aspekte mund të jenë të ndryshme nga zhvillimet aktuale.

Faza e dytë:
Detajet e analizës: Për shkak të kufizimeve burimore, disa aspekte të skedarit keqdashës mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të raportit.

Faza e tretë:
Siguria e informacionit: Për të mbrojtur burimet dhe informacionet konfidenciale, disa detaje mund të jenë të zbutura ose jo të përfshira në raport. Ky vendim është marrë për të mbajtur integritetin dhe sigurinë e të dhënave të përdorura.

Ky raport nuk është një dokument përfundimtar.

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi për përdorimin e gabuar ose pasojat e ndonjë vendimmarrjeje të bazuar në këtë raport.

Informacione Teknike

Në kuadër të monitorimit të vazhdueshëm për fushata phishing kundër shtetasve të Republikës së Shqipërisë, janë identifikuar disa domain-e jolegjitime të krijuara me qëllim mashtrimi (*impersonation*), të cilat imitojnë faqe zyrtare të bankave të nivelit të dytë për të mbledhur të dhëna sensitive nga përdoruesit.

Qëllimi i aktivitetit keqdashës

Këto faqe imitojnë dizajnin dhe strukturën e faqes zyrtare të *Raiffeisen Bank* për të fituar besimin e përdoruesve.
Synimi është marrja e të dhënave personale si:

- Numri i kartës bankare, CVV, PIN
- Kredencialet e hyrjes në e-banking
- Informacione të tjera sensitive si të dhënat e pajisjes dhe të shfletuesit.

Rast studimi *raiffeisen-lidhje[.]com*

IP e lidhur: *15[.]197[.]130[.]221* – është raportuar më parë si pjesë e fushatave të smishing.

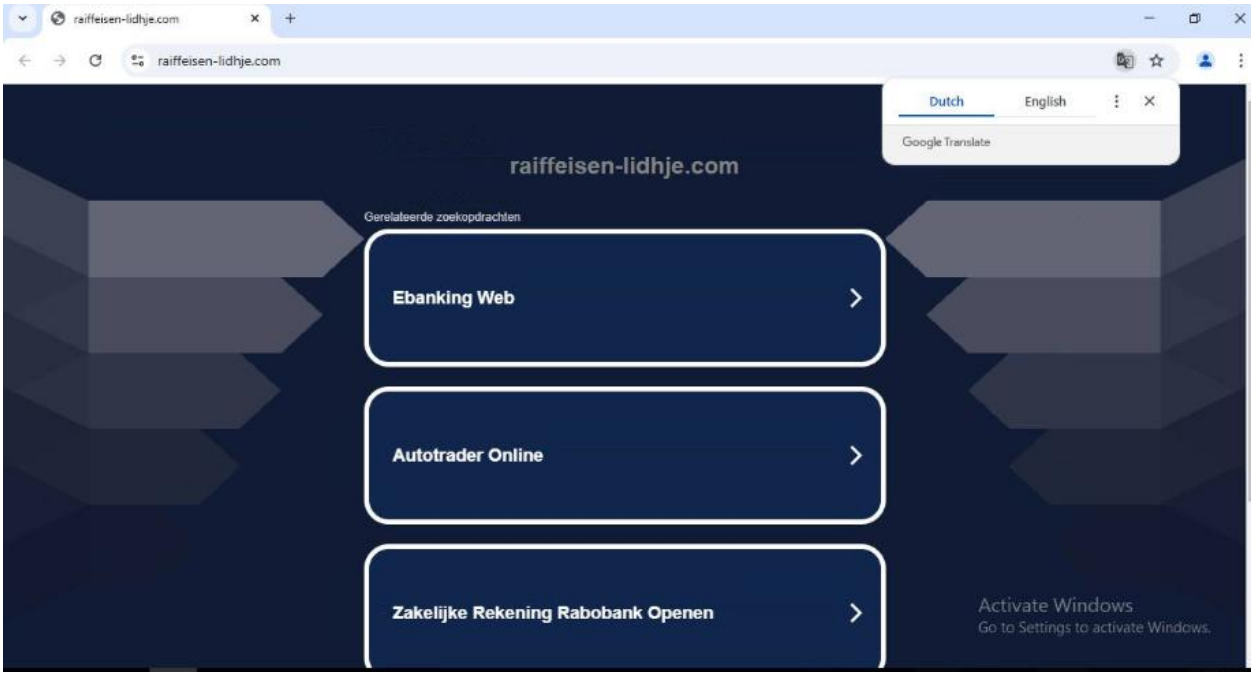

Figura 1Faqja që hapet kur aksesohet url.

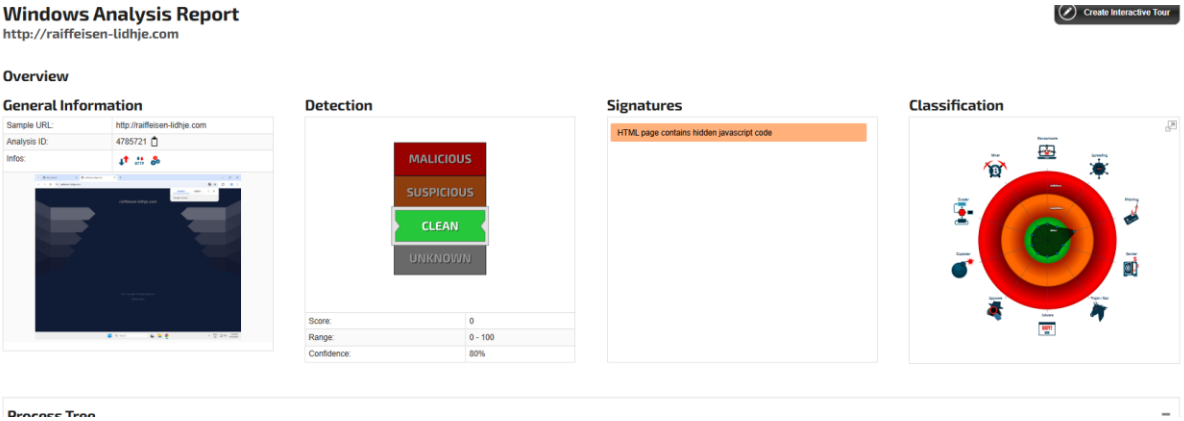

Figura 2 Raporti i Analysis mbi URL raiffeisen-lidhje[.]com

Në analizimin e kryer janë evidentuar elementë të dyshimtë si më poshtë:

IP e lidhur me këtë domain rezulton *IP **15[.]197[.]130[.]221***, IP kjo e cila ka marrë raportime të shumta si IP e përdorur në shumë **fushata smishing**, disa të ngjashme me rastin tonë, sic shfaqet në raportet e mëposhtme, të dy të krijuar ne 2025.

- *https://cofense.com/blog/exploiting-sms-threat-actors-use-social-engineering-to-target-companies*
- *https://www.recordedfuture.com/research/stimmen-aus-moskau-russian-influence-operations-target-german-elections*

JoeSandbox: Ka identifikuar aktivitet të dyshimtë.

urlscan.io: Ka etiketuar URL si “malicious”.

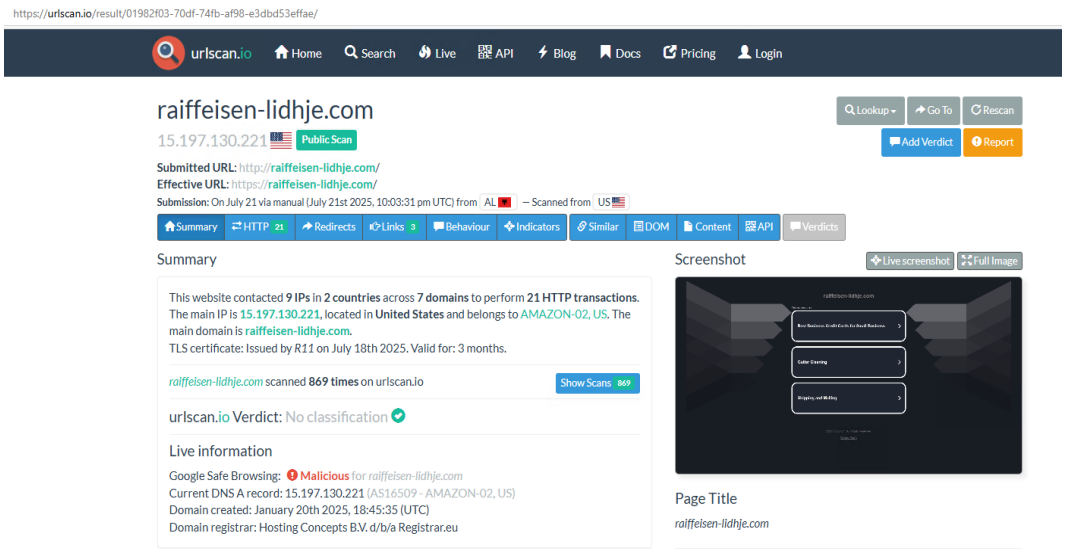

Figura 3 urlscan.io

any.run: Raportuar si "malicious activity".

Figura 4 anyrun sandbox scan

MXToolbox dhe VirusTotal: Domaini figuron në blacklist.

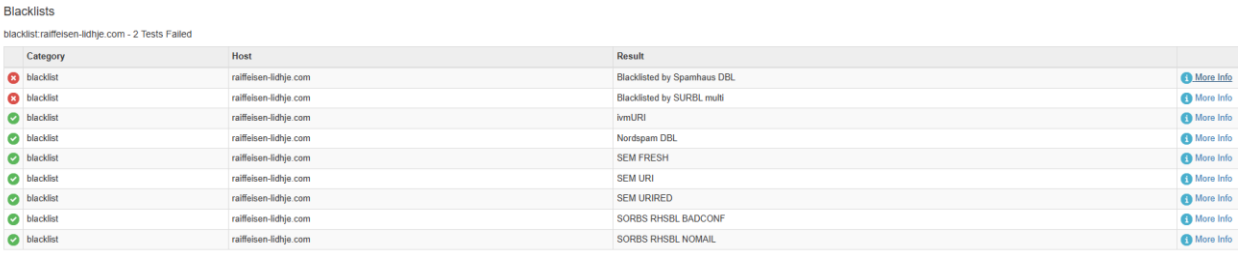

Figura 5 mxtoolbox scanim

Nga një analizim i kryer me *"Inspect element"*, është evidentuar aksesimi i një linku që përmban një script **js** të fshehur (obfuscated):

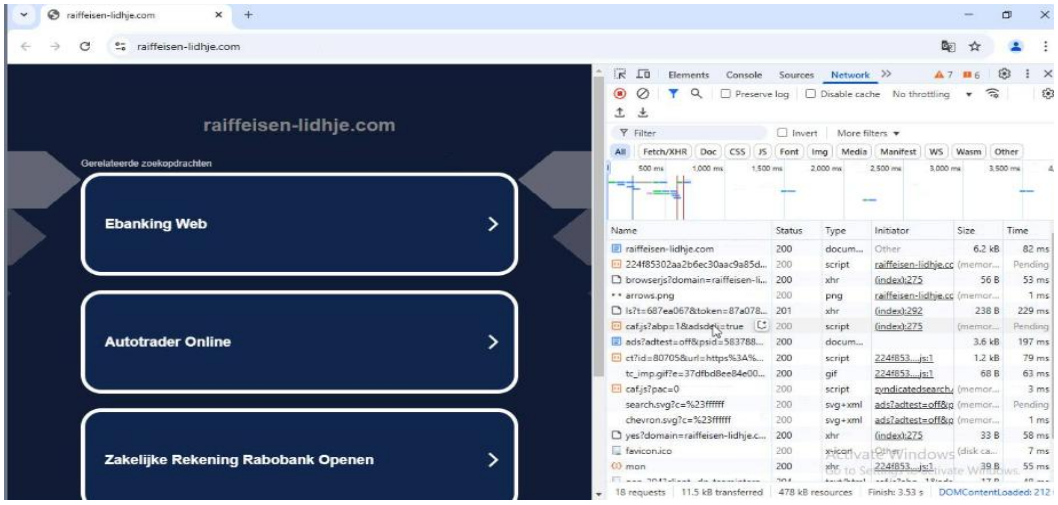

Figura 6 Lidhjet e kryera ne aksesimin e url raiffeisen-lidhje.com

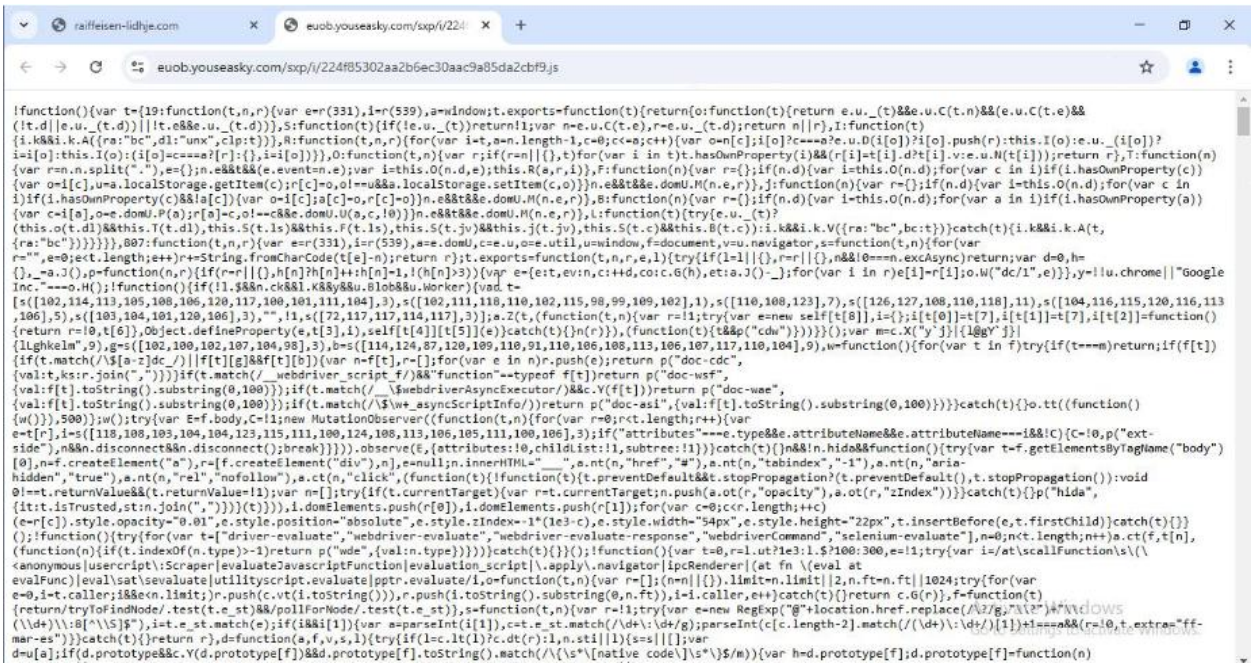

Figura 7 Scripti JS qe behet run me aksesimin e url.

Ky script i fshehur **(obfuscated JavaScript)** në faqen e phishing ka si qëllim:

Mbledhjen e të dhënave nga shfletuesi dhe pajisja e përdoruesit, u cakton vlera objekteve të ndryshëm dhe krijon shtigje ("*paths*") specifike nëse ato nuk ekzistojnë, me qëllim komunikimin me faqen në fjalë.
Gjithashtu, kryen kërkesa për të përcaktuar vendndodhjen (geolocation) dhe mbledh informacion shtesë. Një funksion tjetër i këtij kodi është verifikimi nëse pajisja ka të aktivizuar ndonjë formë autentifikimi *(p.sh. Biometrik, FaceID etj.),* informacion që mund të keqpërdoret në kombinim me të dhëna të tjera si versioni i shfletuesit, rezolucioni i ekranit dhe parametra të ngjashëm, për të krijuar një **"browser fingerprint"** dhe për të ndjekur aktivitetin e përdoruesit.
Ky mekanizëm mund të përdoret gjithashtu për të vjedhur kredencialet e përdoruesit përmes shfrytëzimit të autentifikimit biometrik.

```
PublicKeyCredential.isUserVerifyingPlatformAuthenticatorAvailable()
```

Rast studimi *raiffeisenrinov[.]com*

Gjatë monitorimit proaktiv të fushatave phishing të drejtuara ndaj klientëve të Raiffeisen Bank, është identifikuar një tjetër domen jolegjitim: *raiffeisenrinov[.]com.* Ky domen është krijuar me qëllim të qartë për ***impersonimin e bankës***, duke ndjekur të njëjtat metoda të përdorura më parë në fushatat mashtruese të identifikuara dhe bllokuara.

Qëllimi i këtij domaini është po i njëjtë në marrjen e kredencialeve të e-banking, të dhënave bankare, të dhënave personale dhe të ndjeshme të përdoruesve.

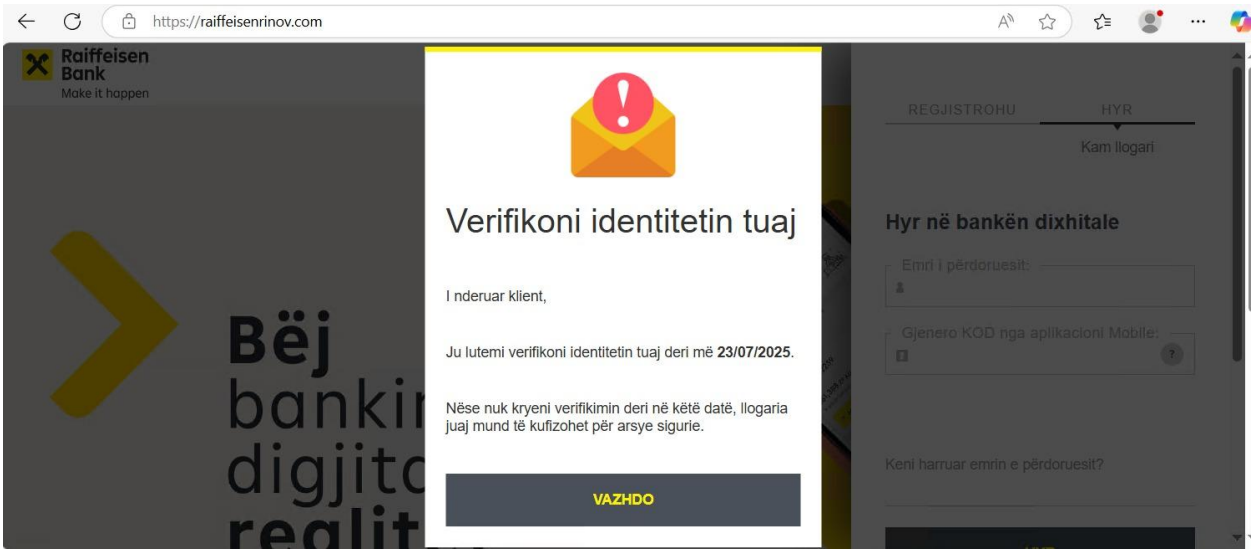

Figura 8 Ndërfaqja e parë

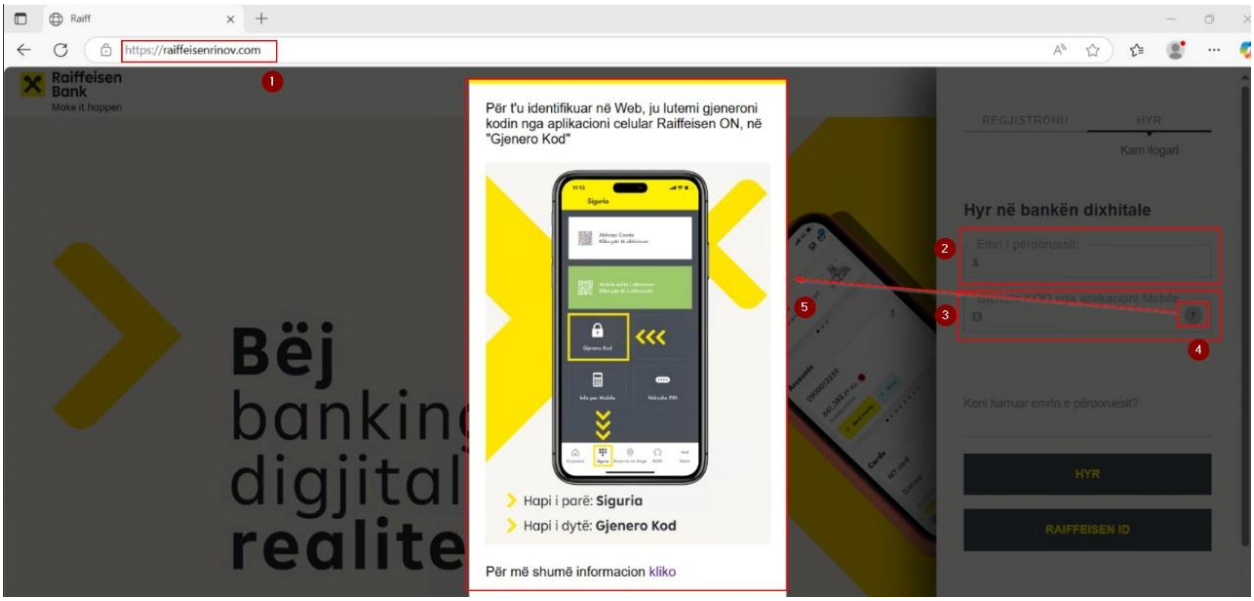

Figura 9 Ndërfaqja e dytë

1- Domaini keqdashës
2- Emri i përdoruesit i cili vendoset nga viktima
3- Token i gjeneruar nga aplikacioni mobile
4- Informacion për manualin
5- Manuali

Pasi klikohet hyr, të dhënat automatikisht kalohen në serverin e sulmuesit.

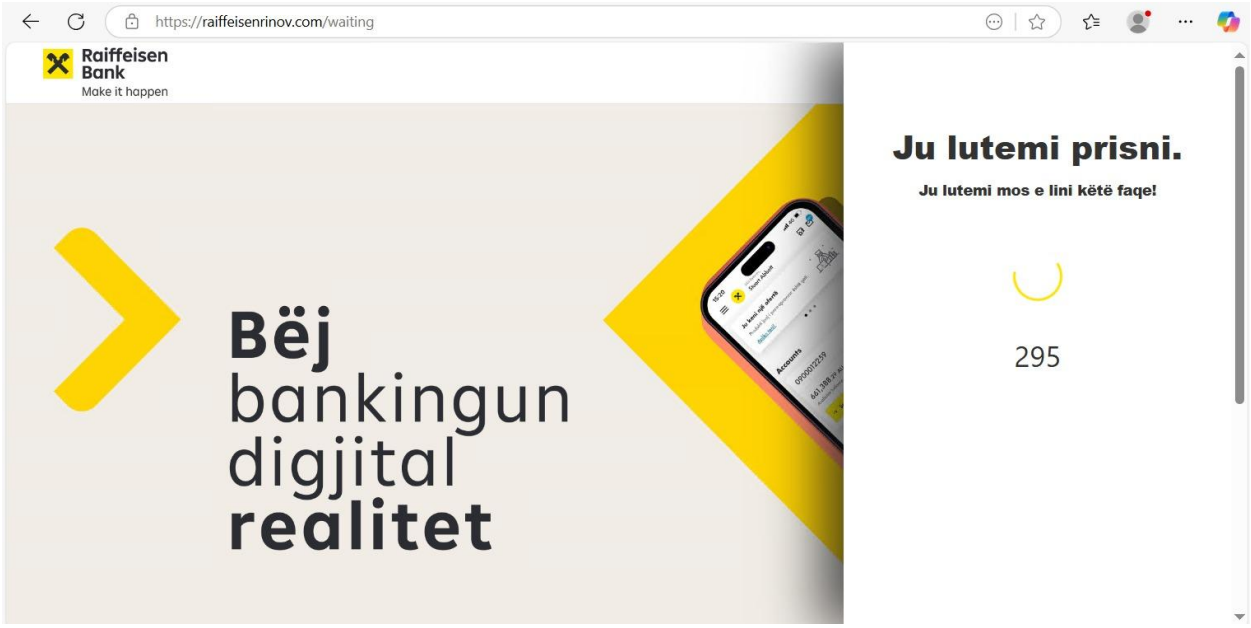

Figura 10 MFA check

Gjatë një analize të kryer më 22 korrik 2025 mbi domainin *raiffeisenrinov.com*, u evidentuan disa tregues që sugjerojnë me shumë gjasa se ky domain është krijuar për qëllime mashtruese, veçanërisht për imitimin e një institucioni bankar të njohur si Raiffeisen Bank. Faqja u analizua pas raportimit të një incidenti me karakter smishing, ku një përdorues kishte marrë këtë link përmes SMS-it.

Domaini u regjistrua po atë ditë në një infrastrukturë të huaj (SHBA) përmes një hosti të panjohur, dhe nuk përmban asnjë përmbajtje reale ose funksionalitet të vlefshëm për përdoruesin final. Në vend të kësaj, faqja gjeneron menjëherë një cookie të tipit PHPSESSID, pa ndërveprim të përdoruesit, çka sugjeron se është ndërtuar mbi një strukturë të thjeshtë ose një kit phishing. Më tej, analiza teknike tregon mungesë të përmbajtjes HTML, një certifikatë SSL e lëshuar nga një autoritet i panjohur ("R11"), dhe direktiva të vendosura në faqe që ndalojnë indeksimin nga motorët e kërkimit (X-Robots-Tag: noindex, nofollow).

Elementët e përfshirë në këtë sjellje janë të përputhshëm me modele të njohura të faqeve mashtruese që përdoren për grumbullim të kredencialeve bankare apo të dhënave sensitive përmes kopjimit vizual të faqeve të besueshme.

Elementë Teknikë të Identifikuar
Kategori Vlera / Përshkrimi
Domain raiffeisenrinov.com
Data e regjistrimit 22.07.2025
IP i hostuar 155.94.155.102 (Charleston, SC, SHBA)
ASN AS214943 (RAILNET Railnet LLC)
Web server nginx
X-Powered-By PHP/8.3.23 në Plesk
Përmbajtje Content-Length: 0, pa HTML të dorëzuar

Certifikatë SSL Lëshuar nga "R11", jo e njohur në CA-të publike
Protokoll sigurie TLS 1.3, cipher AES_128_GCM, ECH jo i aktivizuar
Cookie PHPSESSID = ebalvms3mn269g0rf13l6irobf (session, jo HttpOnly, jo Secure)
X-Robots-Tag noindex, nofollow
Pragma / Cache no-store, no-cache, must-revalidate
Lidhje favicon.ico E kërkuar, por përgjigjja gjithashtu bosh

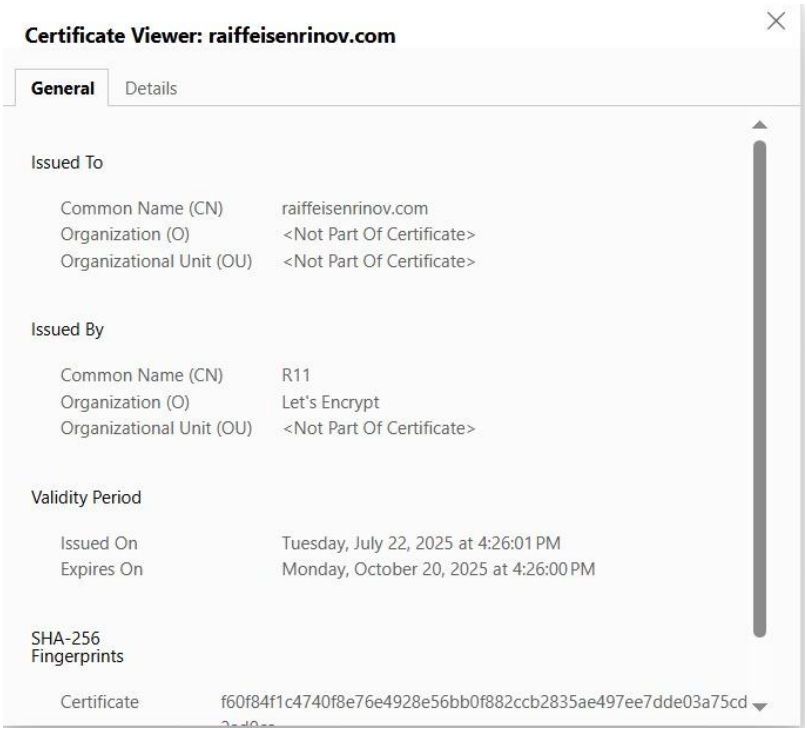

Figura 11 Certifikata e përdorur

Indikatorët e Kompromitimit

Nr	Tipi	Vlera (Domain/IP)	Statusi	Përshkrim
1	Domain	perditesim-raiffeisen[.]com	Bllokuar	Imiton faqe zyrtare, mbledh të dhëna
2	URL	https[:]//shposta-al[.]com	Bllokuar	Faqe phishing në formë njoftimi poste
3	Domain	raiffeisen-rinovoj[.]com	Bllokuar	Mashtrim për rinovim kredencialesh
4	IP Address	192[.]3[.]176[.]117	Bllokuar	IP e përdorur për host phishing
5	Domain	raiffeisen-lidhje[.]com	Bllokuar	Aktivitet phishing, analizuar si malicious
6	Domain	al-raiffeisen[.]com	Bllokuar	Imitim domain kombëtar për Shqipëri
7	Domain	lidhje-raiffeisen[.]com	Bllokuar	Domain mashtrues

Nr	Tipi	Vlera (Domain/IP)	Statusi	Përshkrim
8	Domain	lidhje-al[.]com	Bllokuar	Mashtrim për linqe të rreme
9	Domain	kontakt-raiffeisen[.]com	Bllokuar	Përdorur për vjedhje të dhënash
10	Domain	raiffeisen-lidhje-al[.]com	Bllokuar	Kombinim për të mashtruar përdorues shqiptar
11	Domain	raiffeisen-albania[.]com	Bllokuar	Domain i ngjashëm me atë zyrtar
12	Domain	raiffeisen-lajm[.]com	Bllokuar	Prezantohet si burim lajmesh të bankës
13	Domain	raiffeisen-info[.]com	Bllokuar	Domain me qëllim informimi të rremë
14	IP Address	45[.]139[.]104[.]97	Bllokuar	Host phishing
15	IP Address	45[.]139[.]104[.]34	Bllokuar	Host i lidhur me phishing
16	Domain	raiffeisenrinov[.]com	Dërguar për bllokim	Mashtrim për rinovim llogarie
17	IP Address	155[.]94[.]155[.]102	Dërguar për bllokim	Host phishing

Konkluzione

- Fushata phishing është e organizuar dhe targeton drejtpërdrejt klientët e *Raiffeisen Bank*.
- Domainet janë të krijuara për të mashtruar përdoruesit dhe për të vjedhur të dhëna kritike bankare.
- Në bashkëpunim me AKEP dhe ekipet e sigurisë së bankës, është bërë e mundur bllokimi i shpejtë i shumicës së faqeve të dyshimta.
- Të gjitha domainet e lartpërmendura janë **bllokuar**.
- Janë realizuar **analiza teknike të thelluara** për vlerësimin e rrezikut.
- Vijon komunikimi aktiv me ***Raiffeisen Bank*** **dhe ekspertët** ***Akep*** për të adresuar raste të reja dhe për të ndërmarrë masa proaktive.

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Vendosja e mekanizmave **anti-phishing** në endpoint-e dhe sistemet e email-it të klientëve.
- **Fushata ndërgjegjësimi** për klientët për të rritur kujdesin ndaj mesazheve të dyshimta.
- Bashkëpunim i vazhdueshëm me AKEP, ISP-të dhe platforma ndërkombëtare për **takedown të shpejtë**.
- **Raportim i menjëhershëm në AKSK (Autoriteti Kombëtar për Siguri Kibernetike)** për çdo domain ose aktivitet të dyshuar, në mënyrë që të mundësohet **bllokimi në kohë reale** i linqeve me përmbajtje keqdashëse.