AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

ALB-PhishMesh

FUSHATA SMISHING QË SYNON SHQIPËRINË

Threat Landscape | Maj – Korrik 2026

TLP: CLEAR

Versioni: 1.1

Përmbledhje Ekzekutive

Gjatë periudhës **maj–korrik 2026**, u identifikua një valë e vazhdueshme fushatash ***Smishing*** ku përmbajtja ishte në gjuhën shqipe dhe shënjestroheshin qytetarët në Republikën e Shqipërisë. Mesazhet janë shpërndarë kryesisht përmes *SMS*-ve dhe *iMessage* (***produktet e Apple***), duke përdorur identitete që imitojnë Platforma Qeveritare, Institucione Postare, Banka të nivelit të dytë, operatorë të telekomunikacionit dhe shërbime të ndryshme abonimi ku qëllimi kryesor i aktorëve keqdashës është me motiv financiar, duke vjedhur të dhënat e kartave bankare.

Figura 1. Informacione Kryesore të fushatës PhishMesh.

Mesazhet mashtruese krijojnë një ndjenjë urgjence drejt qytetarëve, duke pretenduar se marrësi ka një pako të bllokuar, një gjobë të papaguar, një pagesë të papërfunduar ose një llogari që duhet riaktivizuar. Përmes lidhjeve të përfshira në mesazh, përdoruesi drejtohet drejt një domain ose *URL*-je mashtruese që imiton faqen e institucionit përkatës.

Qëllimi i mundshëm i këtyre faqeve është mbledhja e të dhënave personale, kredencialeve të autentikimit, të dhënave të kartës bankare dhe, në disa raste, kodeve OTP. Komprometimi i këtyre të dhënave mund të mundësojë marrjen e paautorizuar të llogarive, realizimin e transaksioneve jo legjitime, vjedhjen e identitetit ose forma të tjera të mashtrimit financiar.

Analiza fillestare përfshin **119 observime bruto**, të cilat pas filtrimit, rezultuan në **103 indikatorë unikë kompromet imi**. Nga këta, **25** janë adresa **IPv4** dhe **76** janë domain-e ose **URL**. Dy indikatorët e tjerë përfshijnë një adresë email-i të raportuar dhe një vlerë me format të parregullt, e cila kërkonte verifikim manual përpara shpërndarjes finale për bllokim.

Evidenca e analizuar mbështet me **besueshmëri të lartë** ekzistencën e një aktiviteti të përsëritur ***Smishing***, përdorimin dhe imitimit të institucioneve shqiptare si dhe synimin për mbledhjen e të dhënave të ndjeshme.

Megjithatë, evidenca aktuale nuk është e mjaftueshme për të konfirmuar se të gjitha aktivitetet kontrollohen nga një aktor i vetëm, përdoret një platformë e përbashkët Phishing-as-a-Service, se domain-et gjenerohen përmes një ***DGA****-je (Domain Generation Algorithm*) apo se faqet që imitojnë bankat realizojnë ndërmjetësim aktiv *AitM (Adversary-in-the-Middle)* dhe vjedhje të token-it të sesionit.

Këto vlerësime mbeten hipoteza analitike dhe kërkojnë telemetri shtesë, përfshirë *passive DNS* me timestamp, artefakte HTML/JavaScript, certifikata TLS, PCAP, loge proxy dhe telemetri bankare të transaksioneve në rastet kur preket një qytetar në Republikën e Shqipërisë.

Fushata vlerësohet me **nivel të lartë rreziku për qytetarët**, veçanërisht për shkak të përshtatjes në gjuhën shqipe, imitimit të institucioneve me besueshmëri të lartë dhe synimit të mundshëm për vjedhjen e kredencialeve dhe të dhënave financiare.

Pas identifikimit dhe verifikimit, indikatorët me besueshmëri të lartë janë dërguar në kohë reale nga AKSK drejt AKEP, operatorëve ISP dhe shërbimit të telefonisë mobile, institucioneve dhe infrastrukturave kritike dhe të rëndësishme për monitorim apo bllokim, gjithashtu marrjen e masave të tjera parandaluese, mbrojtëse apo hetuese në bashkëpunim me Drejtorinë e Krimit Kibernetik pranë Policisë së Shtetit.

119 OBSERVIME BRUTO	103 INDIKATORË UNIKË	25 IPv4 UNIKE	76 FQDN/URL UNIKE

VLERËSIMI KRYESOR

Fushata **ALB-PhishMesh** tregon që aktorët keqdashës kanë aftësi për të ndryshuar me shpejtësi emrat e domain-eve, pretekstet dhe infrastrukturën e hostimit. Masat mbrojtëse prioritizojnë bllokimin e domain-eve dhe URL-ve të konfirmuara, monitorimin e ridrejtimeve, identifikimin e varianteve të reja dhe zbatimin e një cikli të kontrolluar:

Raportim → Triazh → Validim → Pasurim → Bllokim → Monitorim

Bllokimi i adresave IP zbatohet vetëm pas verifikimit të lidhjes së tyre me përmbajtjen mashtruese dhe analizimit të rrezikut të *Shared Hosting*, **CDN** (*content delivery network*) ose shërbimeve cloud që mund të kenë impakt në rast bllokimi.

Gjykimet kryesore

- **Prania dhe synimi:** evidencë e lartë për fushata smishing të përshtatura në gjuhën shqipe dhe të drejtuara ndaj qytetarëve në Republikën e Shqipërisë.
- **Modeli:** pretekst lokal + link i maskuar + faqe që imiton institucionin + kërkesë për të dhëna sensitive + kërkesë për pagesën finale.
- **Infrastruktura:** IP të shpërndara në disa ASN cloud/hosting; kjo tregon fleksibilitet operacional, por jo identitetin e autorit.
- **Veprimi prioritar:** bllokim i domain-it/URL-së me besim të lartë, njoftim drejt AKEP dhe monitorim i varianteve të reja.
- **Kufizimi:** bllokimi i IP në vendorë cloud pa verifikim, mund të shkaktojë impakt të lartë në operacionalitetin e përdorimit të internetit pasi mund të hostohen website të tjera, CDN apo Load Balancer, proxy etj,ku në këtë rast nuk sugjerohet apo rekomandohet.
- **Atribuimi – besueshmëri e ulët:** Ofruesi i hostimit, ASN-ja ose vendndodhja e adresës IP nuk identifikojnë autorin e aktivitetit.
- **Veprimi prioritar:** Domain-et dhe URL-të me besueshmëri të lartë bllokohen në bashkëpunim me AKEP si dhe në bashkepunim me ofruesit e shërbimit të internetit në Shqipëri.
- **Kufizimi operacional**: Bllokimi i CDN ose i adresave IP të përbashkëta, pa verifikim teknik, mund të ndikojë bllokimin e shërbimeve legjitime dhe nuk rekomandohet.

1. Qëllimi, Fusha dhe Metodologjia

1.1 Qëllimi

Ky raport paraqet një vlerësim të peizazhit të fushatave smishing të drejtuara ndaj qytetarëve në Shqipëri gjatë periudhës **maj–korrik 2026**.

Analiza synon të identifikojë teknikat, taktikat dhe procdedurat e përdorura nga sulmuesit, institucionet dhe sektorët e imituar, kanalet e shpërndarjes, infrastrukturën mbështetëse dhe teknikat e përdorura për të drejtuar qytetarët drejt faqeve mashtruese.

Raporti vlerëson gjithashtu lidhjet kohore, tematike dhe infrastrukturore për rastet e raportuara, me qëllim identifikimin e modeleve të përsëritura, veprimeve operacionale dhe varianteve të reja të fushatës.

Në përfundim, raporti përcakton një model të kontrolluar për vlerësimin përfundimtar dhe shpërndarjen e indikatorëve të kompromet imit drejt AKEP, ISP, operatorëve, institucioneve dhe infrastrukturave për monitorim dhe bllokim në nivel kombëtar si dhe me partnerët ndërkombëtar.

1.2 Fusha e analizës

Analiza është përqendruar në aktivitetet smishing që paraqesin një lidhje të drejtpërdrejtë me Shqipërinë, bazuar në përdorimin e gjuhës shqipe, imitimin e institucioneve vendase, si dhe synimin e shërbimeve të përdorura gjerësisht nga qytetarët shqiptarë.

Fusha e analizës përfshin:

- Mesazhe të shpërndara përmes SMS-ve, iMessage (produkteve Apple) dhe shërbimeve të ngjashme të komunikimit mobile.
- Imitimin e Platformave Qeveritare dhe shërbimeve të tjera publike.
- Imitimin e Shërbimit Postar dhe shërbimeve të tjera të logjistikës apo transportit.
- Imitimin e bankave të nivelit të dytë dhe shërbimeve të pagesave.
- Imitimin e operatorëve të telekomunikacionit dhe shërbimeve të abonimit.
- Domain-et, URL-të dhe adresat IP të lidhura me faqet mashtruese.
- Infrastrukturën e hostimit dhe rrjetet autonome të përdorura.
- Modelet e inxhinierisë sociale dhe teknikat e mbledhjes së të dhënave.
- Procesin e reagimit, shpërndarjes dhe bllokimit të indikatorëve.

Raporti fokusohet në analizën e fushatës dhe ndikimin e saj të mundshëm në Shqipëri. Ai nuk synon identifikimin përfundimtar të individëve ose grupeve që qëndrojnë pas aktivitetit.

1.3 Burimet e evidencës

Analiza është mbështetur në një kombinim të evidencës së drejtpërdrejtë, të dhënave teknike dhe burimeve të inteligjencës së kërcënimeve kibernetike.

Burimet kryesore përfshijnë:

- *Screenshot*-e të mesazheve, SMS-ve dhe iMessage të raportuara nga qytetarët ose institucionet.
- Përmbajtjen teksti të mesazheve dhe lidhjet e përfshira në to.
- Domain-et, URL-të, adresat IPv4 dhe informacionin përkatës të ASN-ve.

- Datat e observimit dhe kronologjinë e shfaqjes së indikatorëve.
- Të dhëna shtesë nga Google Threat Intelligence, VirusTotal apo platforma të tjera.
- Informacion nga passive DNS, certifikatat TLS dhe historiku i zgjedhjes DNS.
- Të dhëna mbi regjistrimin, hostimin dhe ofruesit e infrastrukturës.
- Dokumentacion teknik nga MITRE ATT&CK, FIRST TLP dhe burime të tjera zyrtare.
- Informacion teknik i raportuar nga operatorët, institucionet dhe partnerët e sigurisë kibernetike.

1.4 Metodologjia e analizës

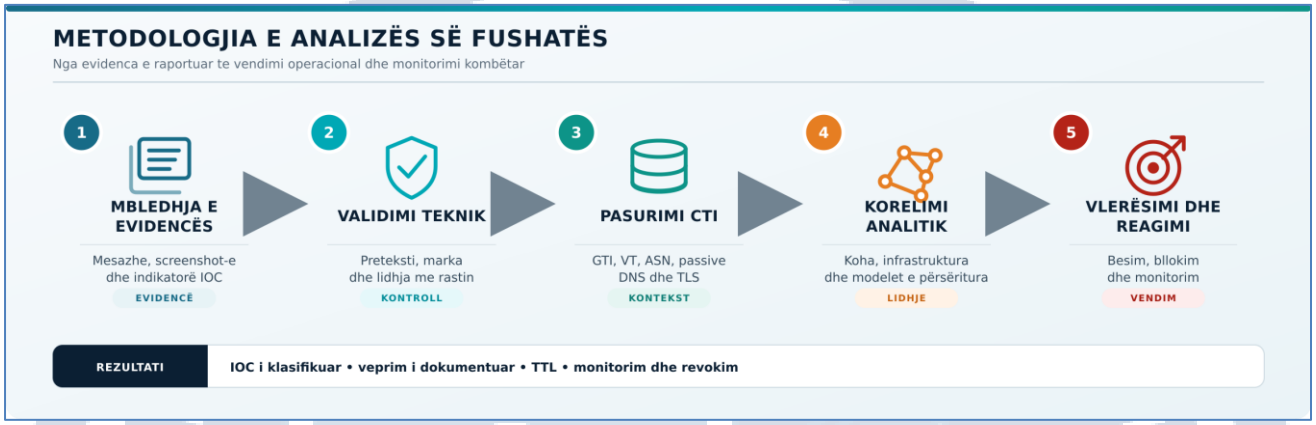

Figura 2. Metodologjia e analizës.

1.4.1 Mbledhja e evidencës

Në fazën fillestare janë mbledhur mesazhet e raportuara, screenshot-et, lidhjet, domain-et, adresat IP dhe informacioni kohor i disponueshëm.

1.4.2 Validimi teknik

Indikatorët janë kontrolluar për të përcaktuar lidhjen e tyre me mesazhin e raportuar, institucionin e imituar, pretekstin e përdorur dhe fushatën përkatëse.

1.4.3 Pasurimi i indikatorëve

Indikatorët janë pasuruar me të dhëna nga GTI (Google Threat Intelligence) / VT (Virus Total), passive DNS, ASN, informacioni i hostimit, certifikatat TLS dhe burime të tjera të inteligjencës së kërcënimeve kibernetike.

1.4.4 Korrelimi analitik

Rastet janë krahasuar sipas:

- periudhës së aktivitetit;
- pretekstit të përdorur;
- institucionit të imituar;
- strukturës së mesazhit;
- modelit të emërtimit të domain-eve;
- adresave IP dhe ASN-ve;
- ofruesve të hostimit;
- certifikatave dhe lidhjeve passive DNS;

- ngjashmërisë së faqeve dhe elementeve teknike.

Korrelacioni është përdorur për të identifikuar veprime operacionale dhe modele të përsëritura, pa i trajtuar automatikisht këto lidhje si provë të një aktori të vetëm.

1.4.5 Vlerësimi dhe reagimi

Në fazën përfundimtare është përcaktuar niveli i besueshmërisë, rreziku potencial dhe veprimi i rekomanduar për secilin indikator.

Indikatorët me evidencë të lartë prioritizohen për bllokim dhe shpërndarje operacionale. Indikatorët me evidencë të pjesshme mbahen në monitorim ose i nënshtrohen vlerësimit të mëtejshëm.

2. Pamja e Përgjithshme e Peizazhit

Ritmi i raportimeve rritet ndjeshëm gjatë qershorit, kur shfaqen paralelisht imitime të platformave qeveritare, postare dhe bankare. Korriku është periudhë e pjesshme deri më 14.07.2026 dhe nuk duhet krahasuar si muaj i plotë.

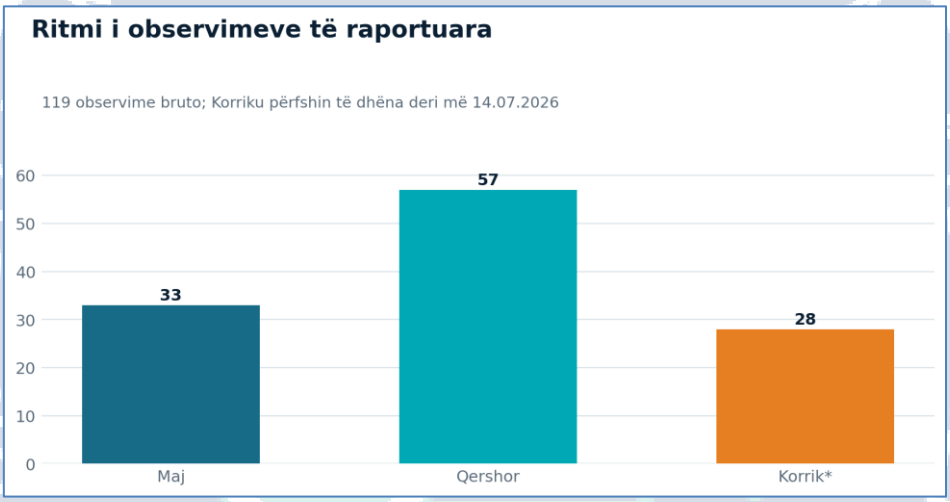

Figura 3. Observimi mujor.

2.1 Tematikat e imitimit

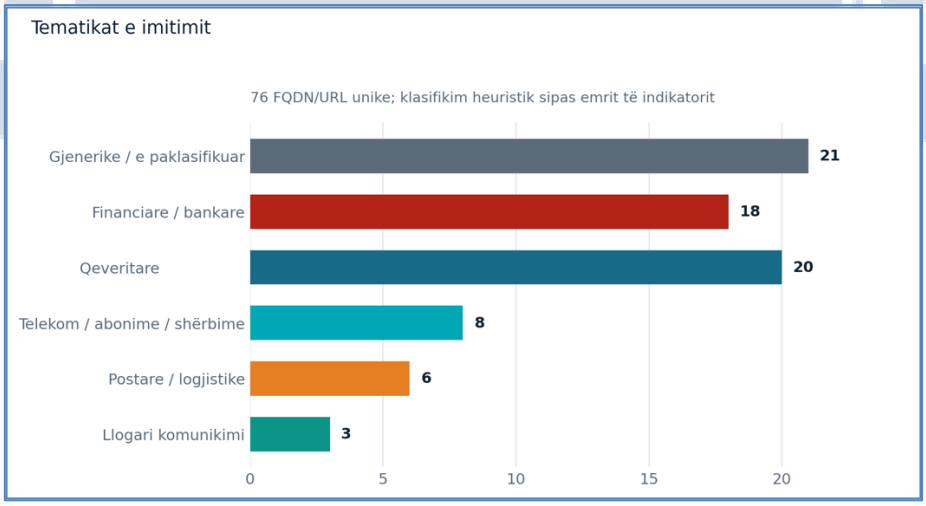

Figura 4. FQDN/URL unike sipas tematikës nga emri i indikatorit.

2.2 Evolucioni

Periudha	Preteksti dominant	Shembuj të vëzhguar	Objektivi i mundshëm
10–31 Maj	Aktivizim, abonim, postë, Banka	ntflx-shqiperia[.]com; aktivpostalb[.]com; bkt[.]kycu-banka[.]one	Të dhëna llogarie/kartë
03–11 Qershor	Qeveritare, tarifa, gjoba, Bankare, ISP	e-albaniagov[.]eu[.]cc; ealbania-tarife[.]cc; vodafoni[.]sbs	Kredenciale/pagesë
26–29 Qershor	Rotacion variantesh platforma qeveritare	e-albaniasu[.]eu[.]cc; albnia-gov[.]xyz	Kredenciale/identitet
03–14 Korrik	Banka/RaiPay, Posta, imitim gjobë	raipayal24[.]com; 537198[.]help; 236321[.]help	Kartë, OTP ose pagesë

2.3 Modele të përsëritura

- Lokalizim sipas institucionit dhe sektorit, ndërsa infrastruktura dhe dërguesi ndryshojnë me shpejtësi.
- Domain-e, typosquatting dhe hoste ***SaaS*** përdoren paralelisht; emri i shkurtër nuk mjafton për ta quajtur DGA.
- Domain-et bankare të korrikut paraqesin kohë të shkurtër ndërmjet ***creation date***, ***first_seen*** dhe raportimit të mesazheve.
- Preteksti postar kërkon zakonisht adresë ose tarifë të vogël; preteksti qeveritar/bankar synon kredenciale, kartë ose OTP.

3. Evidenca Vizuale e Mesazheve

Screenshot-et tregojnë përshtatje shumë të mirë në gjuhën shqipe, përdorim të kërkesës urgjente dhe përpjekje për të krijuar një ndërveprim paraprak ***("Përgjigjuni me 1/Y")*** para hapjes së linkut. Identifikuesi i dërguesit mund të jetë llogari e kompromentuar, i falsifikuar ose i abuzuar; nuk është provë e identitetit të sulmuesit.

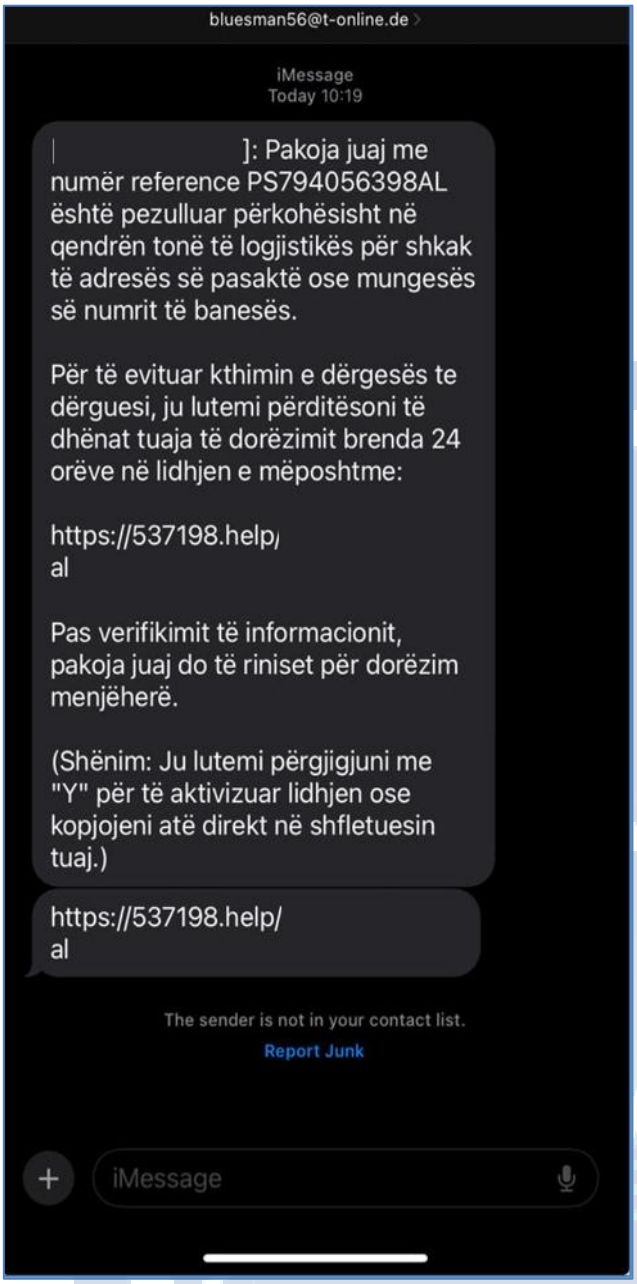

Figura 5. Imitim i Postës me domain 537198[.]help.

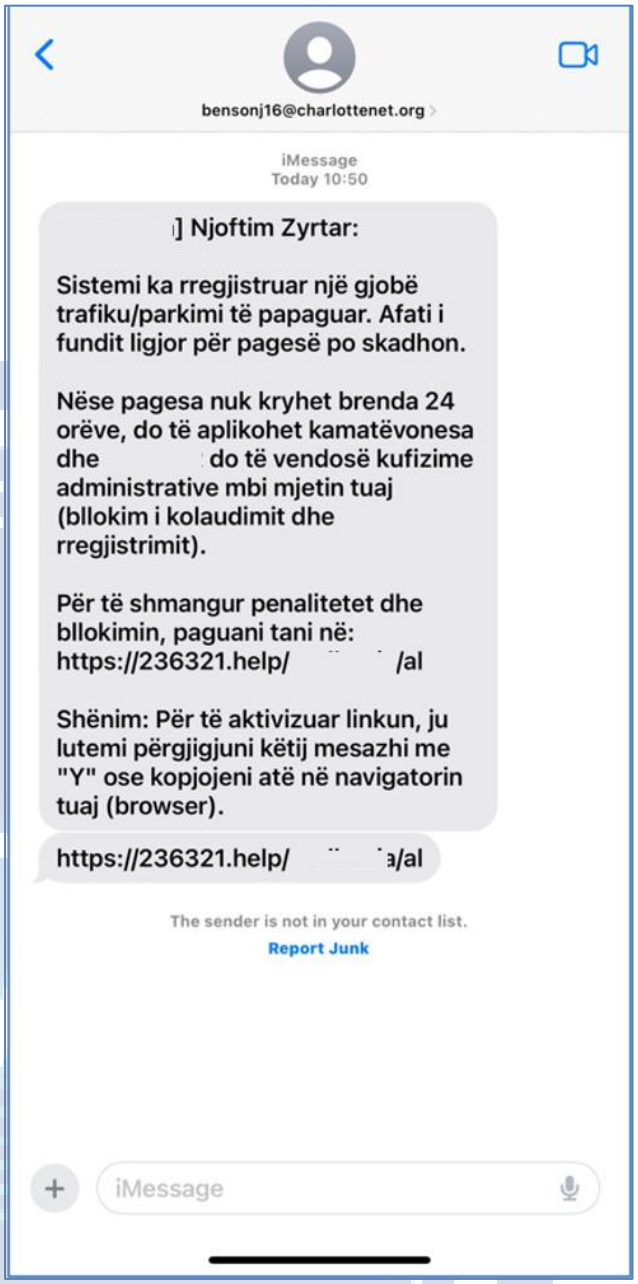

Figura 6. Imitim me domain 236321[.]help.

3.1 Treguesit e inxhinierisë sociale (Social Engineering)

- Urgjencë kohore: "**brenda 24 orëve**", "**afati po skadon**" ose një orar i kërkuar për përditësimin.
- Autoritet i rremë: tituj si "***Gjoba Njoftim Zyrtar***" ose "[***Posta***]".
- Pasojë me impakt: kthim pakoje, penalitete, bllokim kolaudimi/regjistrimi ose humbje shërbimi.
- Veprim nga përdoruesi fundor: kërkesa për t'iu përgjigjur mesazhit me "1" ose "Y" përpara klikimit/kopjimit të linkut.

3.2 Variant i ri: postashqiptare[.]art

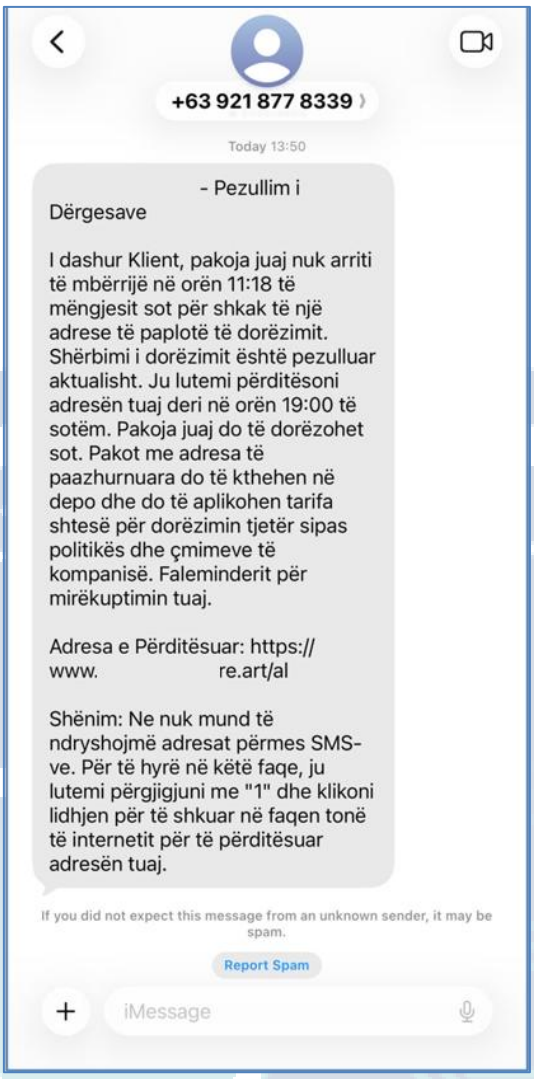

Figura 7. Mesazh i lokalizuar me pretekst dërgese dhe domain postashqiptare[.]art.

Ky variant përdor një numër ndërkombëtar dhe riprodhon të njëjtën logjikë: problem me adresën, afat i shkurtër, link i jashtëm dhe kërkesë për përgjigje. Përsëritja e strukturës së tekstit ndërmjet dërguesve dhe domain-eve të ndryshme është një sinjal i fortë për përdorimin e modeleve të ripërdorshme, por nuk provon vetvetiu një operator të vetëm.

> **RREZIK OPERACIONAL**
> Përgjigjja ndaj mesazhit konfirmon se adresa/numri është aktiv dhe mund të ndryshojë mënyrën si platforma e mesazheve e trajton bisedën. Apple dokumenton se linket nga dërgues të panjohur mund të mos hapen dhe se përdoruesi duhet ta shënojë dërguesin si të njohur; sjellja ndryshon sipas versionit dhe konfigurimit. Prandaj “Reply 1 bypass” nuk duhet përshkruar si dobësi e iOS.

4. Zinxhiri Teknik i Sulmit

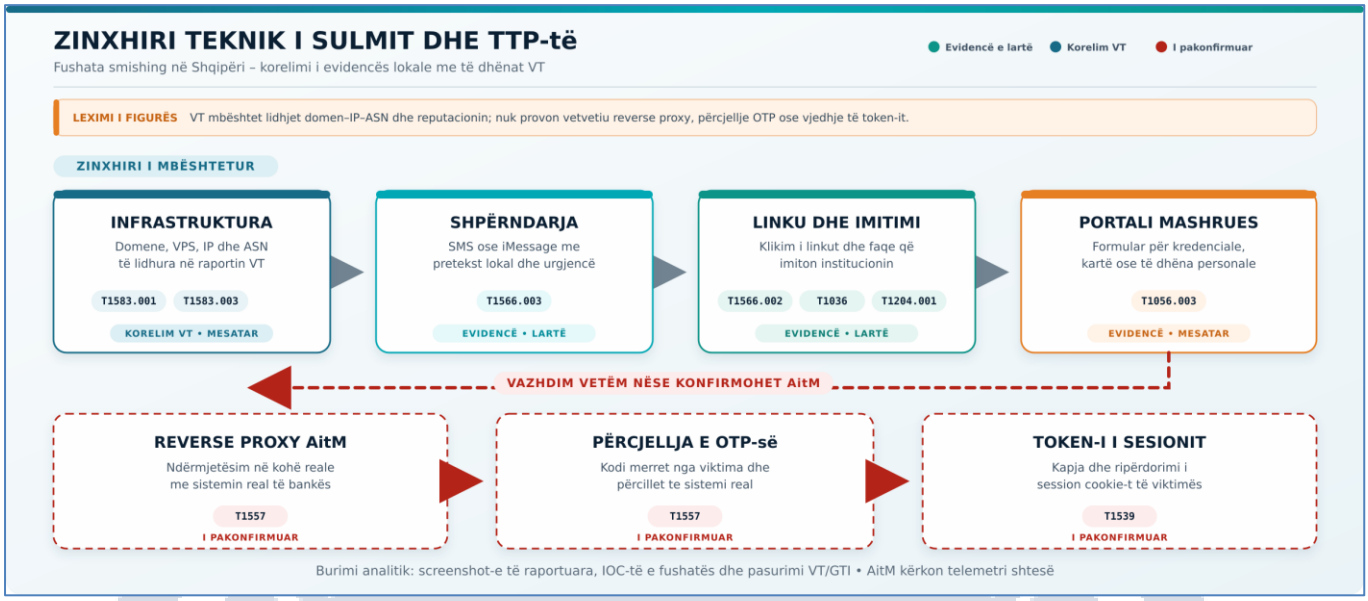

Figura 8. Zinxhiri Teknik i Sulmit.

Analiza e mesazheve të raportuara dhe pasurimi i indikatorëve mbështesin një zinxhir sulmi që fillon me përgatitjen e infrastrukturës, vijon me shpërndarjen e mesazheve smishing dhe përfundon me drejtimin e viktimës te një portal mashtrues.

Të dhënat mbështesin lidhjet ndërmjet domain-eve, adresave IP, ASN-ve dhe ofruesve të hostimit. Megjithatë, këto lidhje nuk provojnë se serverëat kanë funksionuar si reverse proxy AitM ose se kanë kapur OTP dhe token-e sesionesh.

Për këtë arsye, zinxhiri ndahet në dy pjesë:

- **Zinxhiri i mbështetur nga evidenca:** infrastruktura, shpërndarja e mesazhit, linku mashtrues, imitimi i institucionit dhe portali për mbledhjen e të dhënave.
- **Skenari AitM për verifikim:** ndërmjetësimi me sistemin real, përcjellja e OTP-së dhe vjedhja e token-it të sesionit.

4.1 Faza 1 – Përgatitja

Regjistrohen ose abuzohen domain-e që imitojnë institucionin, domain-e numerike me TLD të lira dhe hoste të platformave të ligjshme. Paralelisht përdoren llogari email-i, numra telefoni ose identitete të tjera dërguese që mund të jenë kompromet uar.

4.2 Faza 2 – Shpërndarja dhe preteksti

Mesazhi dërgohet në pajisje mobile dhe përmban një skenar me presion kohor. Përmbajtja është përshtatur me shërbime reale shqiptare që qytetarët përdorin, duke rritur mundësinë e aksesimit.

4.3 Faza 3 – Faqja mashtruese

Linku hap një faqe që mund të imitojë institucionin dhe të kërkojë adresë, të dhëna personale, kredenciale, numër karte, CVV dhe/ose OTP. Kjo përputhet me teknikën **MITRE ATT&CK T1056.003 Web Portal Capture** kur përdoret portal i rremë për kapjen e inputit.

4.4 Faza 4 – Monetizimi

Qëllimi i mundshëm është përdorimi i të dhënave për transaksione të paautorizuara, marrje llogarie ose vjedhje identiteti. Pa log-e bankare ose artefakte të panelit, nuk mund të përcaktohet nëse fushata kryen ***AitM***, vjedh session cookie apo vetëm mbledh input statik.

4.5 Harta e MITRE ATT&CK

Faza	MITRE ATT&CK	Përdorimi në fushatë	Besimi
Përgatitja e domain-eve	T1583.001 – Acquire Infrastructure: Domains	Domain të krijuara ose përdorura për fushatat smishing.	Mesatar
Përdorimi i VPS-ve	T1583.003 – Acquire Infrastructure: VPS	Infrastrukturë VPS e lidhur me domain të raportuara në VT.	Mesatar
Shpërndarja	T1566.003 – Spearphishing via Service	SMS dhe iMessage të përdorura për shpërndarjen e mesazheve.	I lartë
Linku mashtrues	T1566.002 – Spearphishing Link	Mesazhi përmban një link drejt portalit mashtrues.	I lartë
Veprimi i viktimës	T1204.001 – User Execution: Malicious Link	Viktima klikon ose kopjon linkun në shfletues.	I lartë
Imitimi i institucionit	T1036 – Masquerading	Imitohen Platforma Qeveritare, Postare dhe bankat.	I lartë
Mbledhja e të dhënave	T1056.003 – Web Portal Capture	Portal i rremë për kredenciale, kartë ose të dhëna personale.	Mesatar
Reverse proxy AitM	T1557 – Adversary-in-the-Middle	Ndërmjetësim i mundshëm me sistemin real të bankës.	I pakonfirmuar
Kapja e sesionit	T1539 – Steal Web Session Cookie	Kapja dhe ripërdorimi i mundshëm i session cookie-t.	I pakonfirmuar

Shënim: T1583.001 dhe **T1583.003** nënkuptojnë marrjen ose sigurimin e infrastrukturës nga sulmuesi. Të dhënat mund të konfirmojnë përdorimin dhe lidhjen teknike, por jo domosdoshmërisht mënyrën si infrastruktura është ndërtuar.

4.6 Taktikat dhe Teknikat dhe Procedurat e Avancuara (TTP)

- **Anashkalimi i Filtrave të Sigurisë në iOS (iMessage Bypass)**

Për të rritur suksesin e sulmit, sulmuesit shfrytëzojnë inxhinierinë sociale për të manipuluar sistemin e sigurisë së Apple iOS. Kur një dërgues i panjohur dërgon një lidhje (link) në iMessage, iOS e mban lidhjen të paklikueshme për të mbrojtur përdoruesin.

Sulmuesit vendosin shënimin teknik: "Përgjigjuni me '1' për të aktivizuar lidhjen". Sapo viktima dërgon mesazhin "1", iOS e klasifikon këtë si një ndërveprim legjitim nga përdoruesi dhe e kthen linkun në të klikueshëm menjëherë.

- **Arkitektura e Sulmit AitM (Adversary-in-the-Middle)**

Në variantet që synojnë shërbimet bankare online, faqja phishing mund të funksionojë si një ndërmjetës aktiv ndërmjet viktimës dhe sistemit real të bankës. Ky skenar njihet si **Adversary-in-the-Middle – AitM** ose ndërmjetësim i sesionit në kohë reale.

Rrjedha e mundshme e sulmit është:

A. Viktima hap lidhjen e marrë përmes SMS/iMessage dhe vendos emrin e përdoruesit dhe fjalëkalimin në portalin mashtrues.

B. Serveri phishing i përcjell kredencialet në kohë reale te sistemi i vërtetë i bankës.
C. Banka aktivizon procesin e autentikimit dhe i dërgon viktimës një kod OTP ose kërkesë SmartToken.
D. Portali mashtrues i kërkon viktimës të vendosë kodin e sigurisë dhe ia përcjell atë sistemit real.
E. Pas autentikimit, banka krijon një sesion të vlefshëm. Nëse serveri ndërmjetës kap cookie-n ose token-in e sesionit, sulmuesi mund të marrë kontrollin e sesionit të autentikuar.
F. Viktimës mund t'i shfaqet një mesazh gabimi ose "Sistemi po përpunon kërkesën", ndërkohë që sulmuesi tenton të përdorë sesionin e kompromet uar.
G. Në këtë rast, kodi OTP nuk thyhet teknikisht. Ai merret nga viktima dhe përcillet në kohë reale, duke mundësuar tejkalimin e efektit mbrojtës të autentikimit shumëfaktorësh.

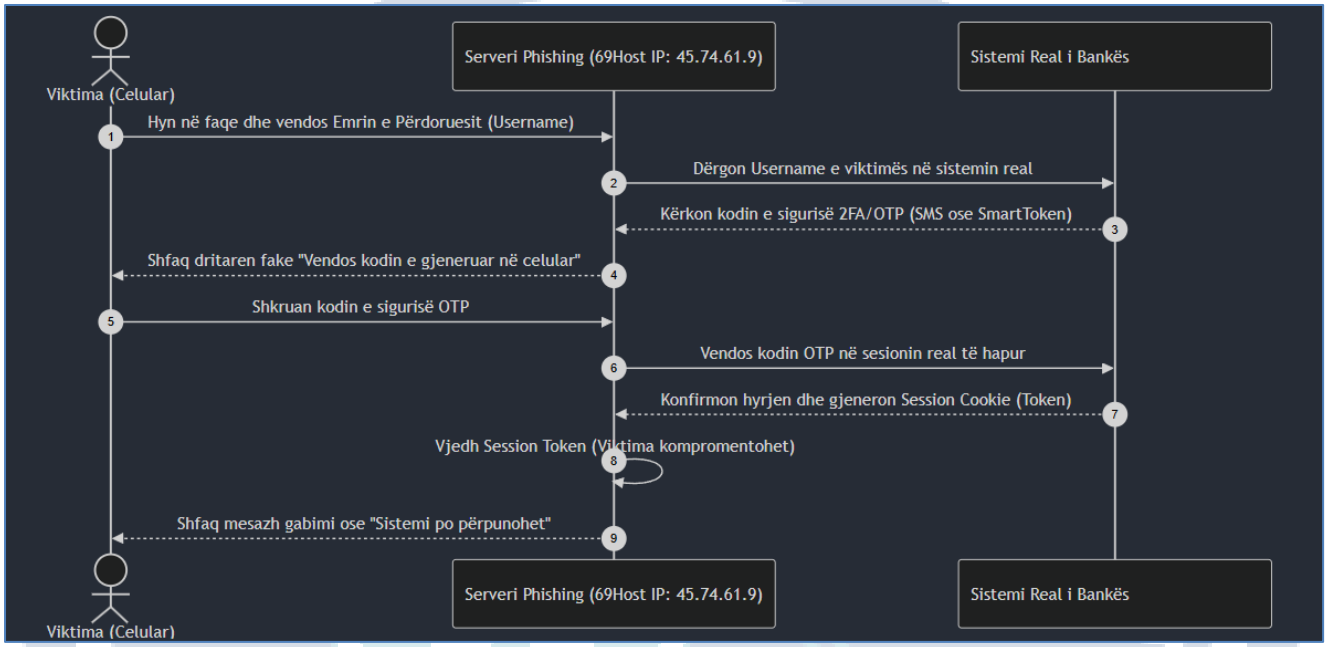

Figura 9. Arkitektura e Sulmit AitM (Adversary-in-the-Middle).

Duke mos patur evidenca të plota si: PCAP files, logs apo informacione teknike të nevojshme, kjo skemë nuk është përfundimtare.

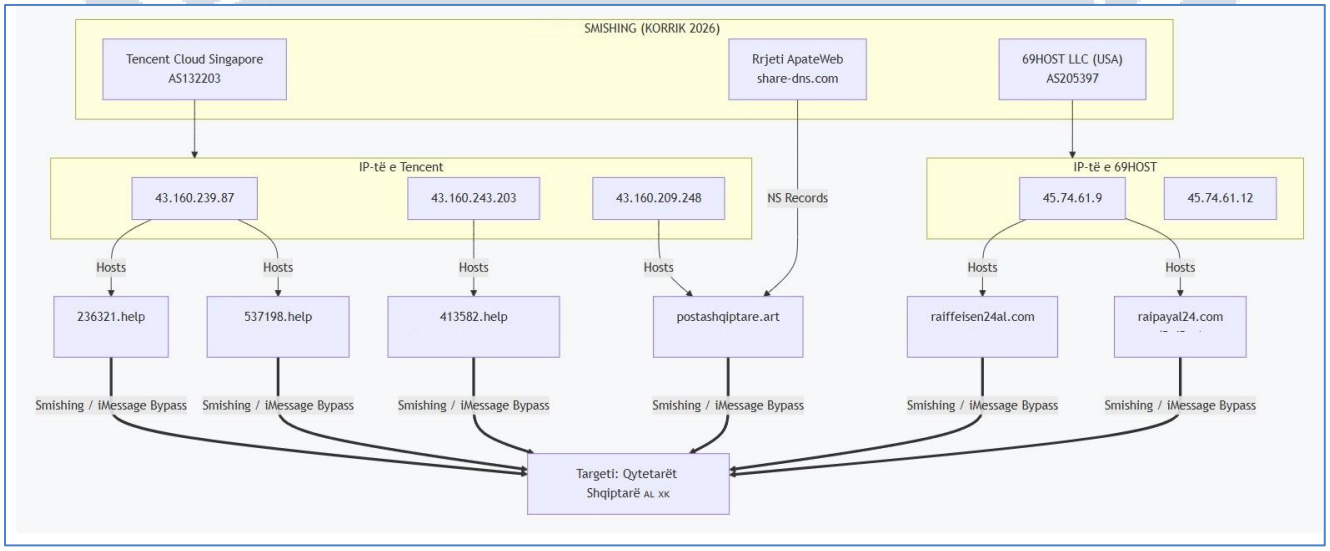

Figura 10. Diagramë e analizuar rreth disa prej sulmeve.

5. Analiza e Infrastrukturës

Lista përmban 25 adresa IPv4 unike në disa rrjete autonome. Përqendrimi më i madh i observimeve është në AS132203 dhe AS202412. Kjo sugjeron përdorim të përsëritur të ofruesve cloud/hosting, por nuk krijon lidhje të mjaftueshme për atribuim ose për bllokim të prefiksit të plotë ASN.

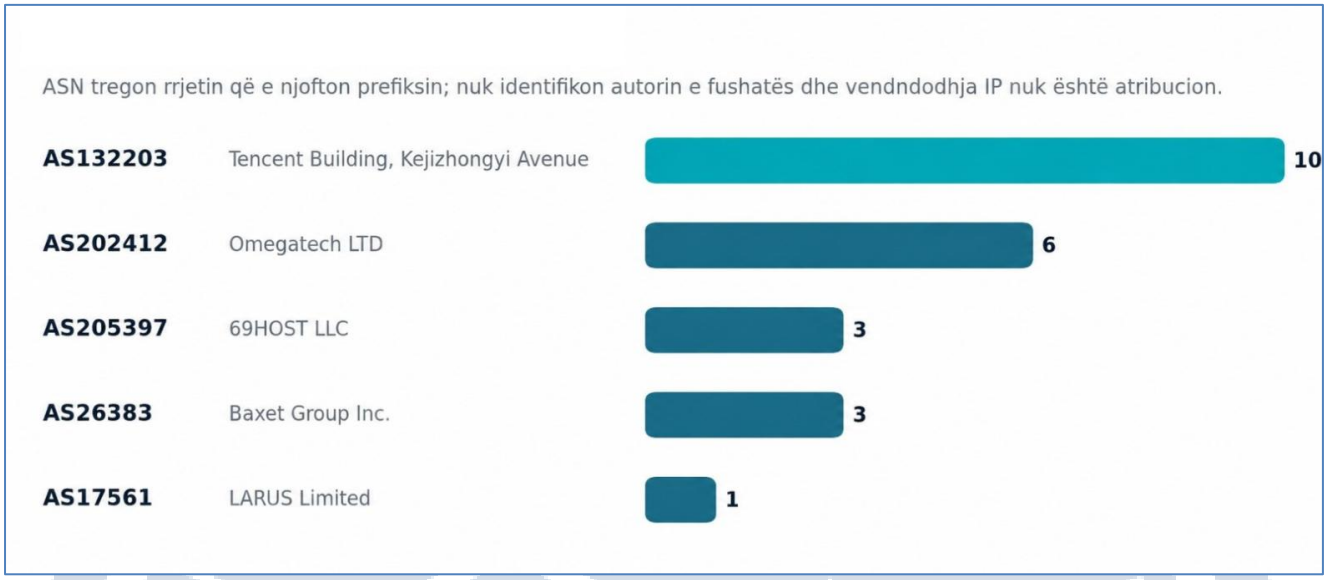

Figura 11. Observime IP sipas ASN; numër raportimesh dhe jo numër aktorësh.

5.1 Grupime analitike

Cluster	ASN / Ofrues	Observime	Vlerësim
C1	AS132203 / Tencent	10	Rotacion i disa IP-ve; kërkohet passive DNS/TLS për lidhje domain–IP
C2	AS202412 / Omegatech LTD	6	Përsëritje e 158.94.208[.]88 dhe 158.94.209[.]88
C3	AS26383 / Baxet Group Inc.	3	Dy IP në 167.17.184.0/24; vendndodhje (Geolocation) kontradiktore
C4	AS205397 / 69HOST LLC	3	IP të raportuara gjatë valës së Phishing bankare të korrikut
C5	ASN të tjera	Observime individuale	Ofrues cloud/VPN/hosting; lidhje më e dobët

Shënim
Emrat e ofruesëve – ***Tencent, Omegatech, Baxet, 69HOST, M247, Alibaba, Weebly*** – përshkruajnë infrastrukturën e përdorur. Nuk nënkuptojnë përfshirje të ofruesit në aktivitetin kriminal.

5.2 GTI/VT

Të dhënat e mëposhtme përfaqësojnë një pamje të inteligjencës kibernetike nga ***GTI/VirusTotal*** dhe pasqyrojnë gjendjen e indikatorëve në momentin e verifikimit.

Rezultatet si *1/94* tregojnë se, në atë moment, 1 nga 94 motorë sigurie e ka klasifikuar indikatorin si keqdashës ose të dyshimtë për kategorinë ***Phishing***. Këto rezultate janë dinamike dhe mund të ndryshojnë me përditësimin e vlerësimeve. Për këtë arsye, rezultati 0/94 nuk duhet të interpretohet automatikisht si provë se indikatori është i padëmshëm, por vetëm se nuk është identifikuar nga motorët e sigurisë në kohën e analizës.

Për domain-et, data e regjistrimit përbën një sinjal të rëndësishëm kur është pranë kohës së identifikimit të parë (***first seen***) ose fillimit të fushatës. Për subdomain-et, kjo datë zakonisht i përket domain kryesor të regjistruar dhe duhet të dallohet nga data e observimit të vetë subdomainit.

Për adresat IP nuk përdoret termi "***creation date***". Në raport duhet të ruhet emërtimi dhe kuptimi i saktë i fushës së GTI-së, si: ***first seen, last seen, last analysis date*** ose data e observimit në passive DNS/TLS. Rezultatet e GTI/VT përdoren si të dhëna pasuruese shtesë dhe vlerësohen së bashku me evidencën e mesazheve, lidhjet infrastrukturore dhe kontekstin e fushatës.

Indikatori	Data	Veprimi	VT	Ofruesi	Vlerësimi analitik
raiffeisen24al[.]com	13/07/2026	Krijim domain-i	6/94	Vercel / Name.com	Korrelacion i fortë kohor/hostimi; AitM nuk është provuar
raipayal24[.]com	14/07/2026	Krijim domain-i	1/94	Vercel / Name.com	Regjistrim just-in-time
raipay24al[.]com	14/07/2026	Krijim domain-i	1/94	Vercel / Name.com	Regjistrim just-in-time
postashq-al[.]com	19/05/2026	Krijim domain-i	1/94	Openprovider	Korrigjon datën e pavlefshme; etiketa DGA nuk është provuar në mënyrë të pavarur
e-albania[.]eu[.]cc	06/06/2026	Observim subdomain-i	2/94	Gname.com / Tencent HK	Lidhje DNS me vlerë; veprimi i regjistrimit ndryshon nga një domain i zotëruar
bkt[.]kycu-banka[.]one	21/05/2026	Metadata prind/subdomain	0/94	Dynadot / Cloudflare	0 detektime nuk do të thotë legjitim; origjina mbetet e maskuar
e-albania[.]biz[.]id	08/06/2026	Observim subdomain-i	1/94	Baxet Group Inc.	Lidhje DNS me vlerë; duhet validuar timestamp-i historik
ntflx-shqiperia[.]com	13/05/2026	Krijim domain-i	2/94	Cloudflare	Korrelacion marke/preteksti; adresa Cloudflare nuk atribuon origjinën
158[.]94[.]208[.]88	19/09/2025	CTI e paspecifikuar	11/94	AS202412 Omegatech LTD	Korrelacion DNS pasive
83[.]217[.]208[.]207	27/03/2025	CTI e paspecifikuar	4/94	AS205775 Neon Core Network	Evidencë me vlerë nëse ruhen SAN/fingerprint/timestamp

Indikatori	Data	Veprimi	VT	Ofruesi	Vlerësimi analitik
45[.]74[.]61[.]9	11/12/2024	CTI e paspecifikuar	0/94	AS205397 69HOST LLC	Web në të njëjtën IP rrit lidhjen; nuk provon reverse proxy/AitM
43[.]166[.]168[.]169	11/12/2024	CTI e paspecifikuar	0/94	AS132203 Tencent Cloud	Lidhja kërkon timestamp-e passive DNS/TLS

5.3 Gjetje nga korrelimi i të dhënave

- **Regjistrim fillestar (*just-in-time registration*):** Tri domain-e që imitojnë shërbime bankare rezultojnë të regjistruara më 13–14 korrik 2026 dhe të lidhura me të njëjtën adresë IP. Afërsia kohore, ngjashmëria e emërtimit dhe infrastruktura e përbashkët mbështesin me besim të lartë përfshirjen e tyre në të njëjtin grupim operacional. Megjithatë, kjo lidhje nuk mjafton për atribuimin përfundimtar ndaj një aktori apo disa aktorës të caktuar.
- **Vonesë në detektim (*detection lag*):** Disa nga domain-et e reja paraqiten me rezultate të ulëta, si **1/94** ose **6/94**.
- **Infrastrukturë e përbashkët ose e ndërmjetësuar:** Përdorimi i shërbimeve si *Cloudflare*, *Vercel* dhe platformave të tjera **SaaS** mund të fshehë ose ndërmjetësojë serverin kryesor. Për këtë arsye, bllokimi në nivel **FQDN/URL** është zakonisht më i saktë dhe zvogëlon rrezikun e bllokimit të shërbimeve legjitime që përdorin të njëjtën infrastrukturë.
- **Lidhje përmes certifikatave dhe passive DNS:** Korrelimet ndërmjet domain-eve dhe adresave IP kanë vlerë analitike vetëm kur shoqërohen me kohën e observimit, burimin e të dhënave dhe, kur është e mundur, me elemente të certifikatës **TLS**, si **SAN**, ***fingerprint***-i dhe periudha e vlefshmërisë. Kjo mundëson dallimin ndërmjet një lidhjeje aktive gjatë fushatës dhe një lidhjeje historike ose të përkohshme.

> **PËRFUNDIM - GTI**
> Korrelacioni i së njëjtës IP, *Registrar*, creation window dhe preteksti është evidencë e fortë për një veprim operacional. Nuk evidenton pronarin e serverit, reverse proxy AitM ose një aktor të vetëm.

5.4 Lidhjet infrastrukturore

- Passive DNS me timestamp që lidh FQDN-in me IP-në gjatë kohës së fushatës.
- Certifikatë TLS, SAN, *fingerprint* ose serial i përbashkët ndërmjet hosteve.
- HTML/JavaScript, *favicon* hash, titull faqeje ose strukturë formulari i njëjtë.
- Name servers, registrar, email registrimi.
- Redirect chain, panel administrimi, API endpoint ose telemetri e përbashkët.

6. Vlerësimi i Besueshmërisë dhe Atribuimi

Gjykimi	Besimi	Baza e evidencës	Çfarë mungon
Fushatë smishing e lokalizuar për Shqipërinë	I lartë	Screenshot-e në shqip, marka lokale, URL të dukshme	Shkalla totale e shpërndarjes
Synim për të mbledhur të dhëna sensitive	I lartë	Pretekst pagese/verifikimi dhe rrjedha e mesazhit	Kapje e plotë e formularit

Gjykimi	Besimi	Baza e evidencës	Çfarë mungon
Përdorim i modeleve të ripërdorshme	Mesatar–i lartë	Strukturë dhe gjuhë e përsëritur	Hash/template source
Infrastrukturë e vetme operacionale	I ulët	Mbivendosje tematike dhe kohore	Lidhje teknike të shumta, të pavarura
AitM për kapjen e OTP/session cookie	I pakonfirmuar	Pretendim në draftin fillestar	PCAP, panel, proxy logs, bank telemetry
DGA	I pakonfirmuar	Domain-e të shkurtra/numerike	Algoritëm, seed, seri e gjeneruar

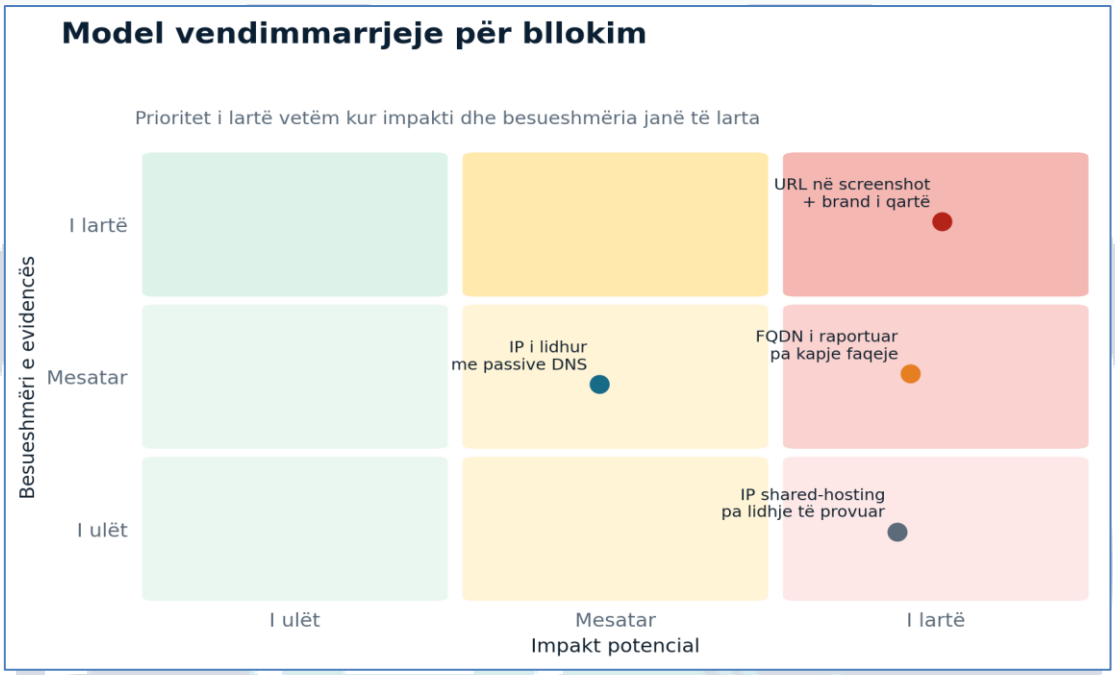

Figura 12. Besueshmëria dhe impakti përcaktojnë urgjencën e bllokimit.

6.1 Emërtimi i fushatës

"ALB-PhishMesh" është emër analitik neutral që përshkruan rrjetin e varianteve smishing të përshtatura dhe lokalizuara për Shqipërinë. Emri nuk identifikon një threat actor dhe nuk duhet trajtuar si atribuim. ***Emërtimet nuk rekomandohen pa prova që lidhin kontrollin operacional të infrastrukturës dhe aktorin.***

7. Reagimi Operacional dhe Bllokimi në Nivel Kombëtar

Reagimi nis me raportimin ose evidentimin e fushatës nga AKSK, i ndjekur nga analiza teknike dhe nxjerrja e indikatorëve të kompromitimit. Pas vlerësimit të besueshmërisë dhe rrezikut, AKSK merr vendimin operacional dhe i përcjell AKEP-it indikatorët e rekomanduar për bllokim. AKEP njofton ofruesit shqiptarë të internetit për zbatimin e masave përkatëse. Në vijim, AKSK monitoron efektivitetin e bllokimit, identifikon variante të reja të fushatës dhe përditëson indikatorët sipas nevojës.

Figura 13. Procesi nga raportimi deri te bllokimi, monitorimi dhe revokimi.

8. Mbledhja e Evidencës, Ndërgjegjësimi dhe Komunikimi Publik

AKSK mbledh raportime për fushatat *smishing* nga inteligjenca kibernetike, monitorimi i ekipeve SOC dhe Analiza, qytetarët, institucionet publike, bankat, operatorët dhe kanale të tjera komunikimi kombëtare apo ndërkombtare. Raportimet, si *screenshot*-et, përmbajtja e mesazhit, adresa e dërguesit, lidhja dhe koha e marrjes, analizohen për identifikimin e shpejtë të fushatës dhe marrjen e masave parandaluese dhe mbrojtëse.

Paralelisht, AKSK zhvillon komunikim të vazhdueshëm publik përmes rrjeteve sociale, mediave, intervistave dhe emisioneve informuese. Njoftimet shpjegojnë mënyrën e mashtrimit, institucionet e imituara, shenjat paralajmëruese dhe mënyrën e sigurt të raportimit.

Figura 14. AKSK - Ndërgjegjësimi dhe Komunikimi Publik.

Bankat, Institucione Postare dhe Institucionet Qeveritare të imituara, mbështesin ndërgjegjësimin duke publikuar paralajmërime në kanalet e tyre zyrtare. Ky bashkëpunim mundëson informimin në kohë të qytetarëve, zgjerimin e evidencës dhe reagimin më të shpejtë ndaj varianteve të reja të fushatës. Para publikimit, të dhënat personale dhe informacionet sensitive anonimizohen.

9. Përfundime

- Fushata **ALB-PhishMesh** përfaqëson një kërcënim aktiv dhe vazhdimisht të përshtatshëm ndaj qytetarëve në Shqipëri. Aktorët keqdashës imitojnë shpesh institucione të besuara, përdorin mesazhe urgjente dhe ndryshojnë me shpejtësi domain-et dhe infrastrukturën e hostimit. Shpërndarja në disa platforma **Cloud** dhe **ASN** tregon elasticitet dhe fleksibilitet operacional të aktorëve keqdashës, por nuk provon se të gjitha aktivitetet drejtohen nga një aktor i vetëm.

- Reagimi duhet të mbështetet në raportimin e shpejtë, analizën e evidencës, bllokimin e kontrolluar të ***FQDN/URL***-ve, shkëmbimin e indikatorëve dhe monitorimin e vazhdueshëm. Paralelisht, njoftimet publike dhe bashkëpunimi me bankat, operatorët, Postën Shqiptare dhe institucionet e imituara mbeten thelbësore për uljen e ekspozimit të qytetarëve dhe identifikimin e varianteve të reja.

10. Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Mos klikimin, aksesimin apo vendosjen e të dhënave që kërkohen nga këto raste smishing.
- Raportimin e menjëhershëm drejt institucioneve përgjegjëse.
- Nëse preken llogari bankare, njoftimin dhe raportimin e menjëhershëm drejt institucionit bankar.

Aneksi A – Regjistri i Adresave IPv4

Adresat IP paraqiten në format ***defang***. Vlerat *first_seen* dhe *last_seen* bazohen vetëm në observimet e raportuara dhe nuk përfaqësojnë domosdoshmërisht periudhën e plotë të aktivitetit. Para bllokimit të një adrese IP, AKSK verifikon nëse ajo përdoret nga infrastrukturë e përbashkët (shared hosting), për të shmangur ndikimin te shërbimet legjitime.

#	First seen	Last seen	IPv4	ASN	Ofruesi	CC	Obs.	Vlerësimi	Veprimi
1	2026-06-09	2026-10-09	102[.]135[.]105[.]119	AS213441	Slayer Group Limited	SC	2	Kërkon verifikim	Validim + TTL
2	2026-06-04	2026-06-04	146[.]70[.]197[.]133	AS9009	M247 Europe SRL	DK	1	Mesatare	Validim + TTL
3	2026-06-04	2026-06-04	155[.]117[.]232[.]4	AS399486	12651980 CANADA INC.	US	1	Mesatare	Validim + TTL
4	2026-06-11	2026-06-11	156[.]232[.]205[.]80	AS17561	LARUS Limited	VE	1	Mesatare	Validim + TTL
5	2026-05-21	2026-07-13	158[.]94[.]208[.]88	AS202412	Omegatech LTD	DE	4	Mesatare	Validim + TTL
6	2026-05-22	2026-05-25	158[.]94[.]209[.]88	AS202412	Omegatech LTD	NL	2	Mesatare	Validim + TTL
7	2026-06-08	2026-06-10	167[.]17[.]184[.]183	AS26383	Baxet Group Inc.	AL, US	2	Mesatare	Validim + TTL
8	2026-07-02	2026-07-02	167[.]17[.]184[.]246	AS26383	Baxet Group Inc.	–	1	Mesatare	Validim + TTL
9	2026-05-31	2026-05-31	193[.]46[.]255[.]244	AS47890	Unmanaged Ltd	RO	1	Mesatare	Validim + TTL
10	2026-06-10	2026-06-10	43[.]131[.]5[.]123	AS132203	Tencent Building, Kejizhongyi Avenue	DE	1	Mesatare	Validim + TTL
11	2026-06-07	2026-06-07	43[.]131[.]63[.]47	AS132203	Tencent Building, Kejizhongyi Avenue	DE	1	Mesatare	Validim + TTL
12	2026-06-07	2026-06-07	43[.]135[.]32[.]162	AS132203	Tencent Building, Kejizhongyi Avenue	HK	1	Mesatare	Validim + TTL
13	2026-05-22	2026-05-22	43[.]157[.]137[.]42	AS132203	Tencent Building, Kejizhongyi Avenue	BR	1	Mesatare	Validim + TTL
14	2026-07-13	2026-07-13	43[.]160[.]209[.]248	AS132203	Tencent Building, Kejizhongyi Avenue	–	1	Mesatare	Validim + TTL
15	2026-07-13	2026-07-13	43[.]160[.]239[.]87	AS132203	Tencent Building, Kejizhongyi Avenue	–	1	Mesatare	Validim + TTL
16	2026-07-03	2026-07-03	43[.]160[.]254[.]237	AS132203	Tencent Building, Kejizhongyi Avenue	SG	1	Mesatare	Validim + TTL
17	2026-06-07	2026-06-26	43[.]166[.]168[.]169	AS132203	Tencent Building, Kejizhongyi Avenue	US	2	Mesatare	Validim + TTL
18	2026-06-26	2026-06-26	43[.]166[.]71[.]216	AS132203	Tencent Building, Kejizhongyi Avenue	BR	1	Mesatare	Validim + TTL
19	2026-07-10	2026-07-10	45[.]74[.]47[.]68	AS205397	69HOST LLC	–	1	Mesatare	Validim + TTL
20	2026-07-10	2026-07-10	45[.]74[.]61[.]12	AS205397	69HOST LLC	–	1	Mesatare	Validim + TTL
21	2026-07-14	2026-07-14	45[.]74[.]61[.]9	AS205397	69HOST LLC	–	1	Mesatare	Validim + TTL
22	2026-06-04	2026-06-04	46[.]232[.]159[.]110	AS29580	A1 Bulgaria EAD	BG	1	Mesatare	Validim + TTL
23	2026-06-04	2026-06-04	74[.]115[.]51[.]6	AS27647	Weebly, Inc.	CA	1	Mesatare	Validim + TTL

#	First seen	Last seen	IPv4	ASN	Ofruesi	CC	Obs.	Vlerësimi	Veprimi
24	2026-06-09	2026-06-09	8[.]218[.]8[.]175	AS45102	Alibaba (US) Technology Co., Ltd.	SG	1	Mesatare	Validim + TTL
25	2026-05-22	2026-05-22	83[.]217[.]208[.]207	AS205775	Neon Core Network LLC	RU	1	Mesatare	Validim + TTL

Aneksi B – Regjistri i FQDN/URL-ve

FQDN-të dhe URL-të klasifikohen bazuar në emërtimin, pretekstin e përdorur dhe kontekstin e fushatës. Indikatorët me emërtime të përgjithshme ose me lidhje të paqarta kërkojnë verifikim shtesë përmes evidencës së përmbajtjes, DNS pasive, certifikatave TLS ose burimeve të tjera të besueshme përpara bllokimit.

#	First seen	Last seen	FQDN	Path i vëzhguar	Tematika	Obs.	Vlerësimi	Veprimi
1	2026-07-13	2026-07-13	236321[.]help	/e-albania/al	Qeveritare	1	E lartë	Blloko FQDN
2	2026-07-10	2026-07-10	24raiffeisenal[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
3	2026-07-10	2026-07-10	24raipay[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
4	2026-07-13	2026-07-13	527199[.]help	/e-albania/al	Qeveritare /	1	Mesatare	Blloko FQDN
5	2026-07-13	2026-07-13	537198[.]help	/postashqiptare/al	Postare / logjistike	1	E lartë	Blloko FQDN
6	2026-05-31	2026-05-31	account-verification-required[.]gt[.]tc	/Signal-Primary-Device	Llogari komunikimi	1	Mesatare	Blloko FQDN
7	2026-05-10	2026-05-10	aktivo2026[.]com	–	Telekom / abonime / shërbime	1	Mesatare	Blloko FQDN
8	2026-05-22	2026-05-26	aktivpostalb[.]com	–	Postare / logjistike	3	Mesatare	Blloko FQDN
9	2026-07-05	2026-07-05	al-raipay[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
10	2026-06-26	2026-06-26	albania-al[.]cfd	–	Qeveritare /	1	Mesatare	Blloko FQDN
11	2026-06-26	2026-06-26	albania-al[.]icu	/al	Qeveritare /	1	Mesatare	Blloko FQDN
12	2026-06-29	2026-06-29	albnia-gov[.]xyz	/CYKdVLeF9g	Qeveritare /	1	Mesatare	Blloko FQDN
13	2026-06-26	2026-06-26	alibania[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
14	2026-06-26	2026-06-26	alibanna[.]work	/al	Qeveritare /	1	Mesatare	Blloko FQDN
15	2026-05-23	2026-05-25	alshqiptare[.]com	–	Postare / logjistike	3	Mesatare	Blloko FQDN
16	2026-06-09	2026-06-09	altuiobc[.]top	/al	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
17	2026-07-08	2026-07-08	asp[.]goveis[.]icu	/als	Qeveritare /	1	Mesatare	Blloko FQDN
18	2026-05-22	2026-05-22	bkt[.]kycu-banka[.]one	/bkt/	Financiare / bankare	1	Mesatare	Blloko FQDN
19	2026-06-03	2026-06-03	bkt[.]log-info[.]one	–	Financiare / bankare	1	Mesatare	Blloko FQDN
20	2026-06-04	2026-06-04	bkt[.]login-sign[.]one	–	Financiare / bankare	1	Mesatare	Blloko FQDN
21	2026-06-04	2026-06-04	bkt[.]sign-kos[.]one	–	Financiare / bankare	1	Mesatare	Blloko FQDN
22	2026-06-09	2026-06-09	czatc[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
23	2026-06-10	2026-06-10	dpshtrr[.]ktlffm[.]com	/al	Qeveritare /	1	Mesatare	Blloko FQDN
24	2026-05-25	2026-05-25	dsfg45678976[.]github[.]io	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko

#	First seen	Last seen	FQDN	Path i vëzhguar	Tematika	Obs.	Vlerësimi	Veprimi
25	2026-06-07	2026-06-07	e-albainia[.]eu[.]cc	/al	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
26	2026-06-07	2026-06-07	e-albania-al[.]cdf	/al	Qeveritare /	1	Mesatare	Blloko FQDN
27	2026-06-08	2026-06-09	e-albania[.]biz[.]id	/HLUNm6gSZh; /LnN3PTzqPE	Qeveritare /	2	Mesatare	Blloko FQDN
28	2026-06-07	2026-06-07	e-albania[.]eu[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
29	2026-06-09	2026-06-09	e-albania[.]it[.]com	/al	Qeveritare /	1	Mesatare	Blloko FQDN
30	2026-06-07	2026-06-07	e-albaniaa[.]eu[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
31	2026-06-07	2026-06-07	e-albaniagov[.]eu[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
32	2026-06-07	2026-06-07	e-albanian[.]eu[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
33	2026-06-26	2026-06-26	e-albaniasu[.]eu[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
34	2026-06-09	2026-06-09	e-albiania[.]eu[.]cc	/al	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
35	2026-06-09	2026-06-09	e-allbania[.]eu[.]cc	/al	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
36	2026-06-09	2026-06-09	ealbania-pagese	/al	Qeveritare /	1	Mesatare	Blloko FQDN
37	2026-06-09	2026-06-09	ealbania-pagese[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
38	2026-06-08	2026-06-08	ealbania-tarife[.]cc	/al	Qeveritare /	1	Mesatare	Blloko FQDN
39	2026-06-11	2026-06-11	gjpdf[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
40	2026-05-18	2026-05-18	gspexit105[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
41	2026-06-09	2026-06-09	hfnjw[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
42	2026-05-22	2026-05-22	iikgeepw[.]top	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
43	2026-06-11	2026-06-11	kyzcw[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
44	2026-05-10	2026-05-10	lidhi[.]com	–	Telekom / abonime / shërbime	1	Mesatare	Blloko FQDN
45	2026-06-09	2026-06-09	llogaria-ime[.]com	/main	Financiare / bankare	2	Mesatare	Blloko FQDN
46	2026-06-04	2026-06-04	login[.]bkt-info[.]one	–	Financiare / bankare	1	Mesatare	Blloko FQDN
47	2026-05-22	2026-05-22	login[.]bkt-xk[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
48	2026-05-20	2026-05-20	netflix-gz[.]com	–	Telekom / abonime / shërbime	1	Mesatare	Blloko FQDN
49	2026-06-04	2026-06-04	notificationaccessaleert[.]weebly[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
50	2026-05-13	2026-05-13	ntflx-shqiperia[.]com	–	Telekom / abonime / shërbime	2	Mesatare	Blloko FQDN
51	2026-05-26	2026-05-26	ntfmembactu[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
52	2026-06-09	2026-06-09	oacyo[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko

#	First seen	Last seen	FQDN	Path i vëzhguar	Tematika	Obs.	Vlerësimi	Veprimi
53	2026-05-19	2026-05-19	postashq-al[.]com	–	Postare / logjistike	1	Mesatare	Blloko FQDN
54	2026-06-05	2026-06-05	postashqalb[.]com	–	Postare / logjistike	1	Mesatare	Blloko FQDN
55	2026-07-13	2026-07-13	postashqiptare[.]art	/al	Postare / logjistike	1	E lartë	Blloko FQDN
56	2026-06-07	2026-06-07	qcwld[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
57	2026-07-05	2026-07-05	raiffeisen-al[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
58	2026-07-14	2026-07-14	raiffeisen24al[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
59	2026-07-05	2026-07-05	raiffeisenal-info[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
60	2026-07-05	2026-07-13	raipay-al[.]com	–	Financiare / bankare	2	Mesatare	Blloko FQDN
61	2026-07-14	2026-07-14	raipay24al[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
62	2026-07-03	2026-07-05	raipayal[.]com	–	Financiare / bankare	2	Mesatare	Blloko FQDN
63	2026-07-14	2026-07-14	raipayal24[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
64	2026-05-10	2026-05-10	riaktivizo2026[.]com	–	Telekom / abonime / shërbime	1	Mesatare	Blloko FQDN
65	2026-05-25	2026-05-25	richardborges[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
66	2026-05-21	2026-05-21	riperteritje-shendetit[.]com	–	Telekom / abonime / shërbime	1	Mesatare	Blloko FQDN
67	2026-06-09	2026-06-09	sbwxc[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
68	2026-06-03	2026-06-03	sign[.]log-info[.]one	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
69	2026-05-31	2026-05-31	signal[.]idmsa[.]name	/2FA	Llogari komunikimi	1	Mesatare	Blloko FQDN
70	2026-05-31	2026-05-31	signal[.]menu	/2FA	Llogari komunikimi	1	Mesatare	Blloko FQDN
71	2026-07-10	2026-07-10	siguri-raipay[.]com	–	Financiare / bankare	1	Mesatare	Blloko FQDN
72	2026-05-11	2026-05-11	survey2026[.]online	–	Telekom / abonime / shërbime	1	Mesatare	Blloko FQDN
73	2026-05-18	2026-05-18	viet69[.]al	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
74	2026-06-03	2026-06-03	vodafoni[.]sbs	–	Telekom / abonime / shërbime	1	Mesatare	Blloko FQDN
75	2026-06-09	2026-06-09	yujght[.]site	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko
76	2026-06-09	2026-06-09	ywxzc[.]com	–	Gjenerike / e paklasifikuar	1	Mesatare	Verifiko

Shënim: *Screenshot*-et paraqesin edhe adresa email-i dhe një numër telefoni si dërgues. Ato ruhen si artefakte prove, por nuk publikohen si indikatorë atribues pa konfirmim se llogaria/numri është nën kontrollin e aktorit keqdashës.

Aneksi C – Snapshot-i GTI/VT i Dorëzuar

Të dhënat në tabelën e mëposhtme paraqesin gjendjen e indikatorëve në GTI/VirusTotal në momentin e analizës. Rezultatet e detektimit janë dinamike dhe mund të ndryshojnë me kalimin e kohës; për këtë arsye, edhe rezultati **0/94** nuk duhet të interpretohet automatikisht si indikator i padëmshëm. Kolona **"Data"** ruan datën e paraqitur në materialin burimor, ndërsa kolona **"Kuptimi"** sqaron nëse ajo i referohet regjistrimit të domain-it, observimit të subdomain-it ose një fushe të paspecifikuar të GTI-së.

#	Indikatori	Tipi	Data	Kuptimi	VT	Ofruesi	Korrelacioni i dorëzuar	Vlerësimi analitik
1	raiffeisen24al[.]com	domain	13/07/2026	domain_creation	6/94	Vercel / Name.com	Raportohet se rezulton në 45.74.61.9; pretekst Raiffeisen	Korrelacion i fortë kohor/hostimi; AitM nuk është provuar
2	raipayal24[.]com	domain	14/07/2026	domain_creation	1/94	Vercel / Name.com	Raportohet se rezulton në 45.74.61.9; pretekst RaiPay	Regjistrim just-in-time;
3	raipay24al[.]com	domain	14/07/2026	domain_creation	1/94	Vercel / Name.com	Raportohet se rezulton në 45.74.61.9; pretekst RaiPay	Regjistrim just-in-time
4	postashq-al[.]com	domain	19/05/2026	domain_creation	1/94	Openprovider	Raportohet se rezulton në 158.94.208.88; pretekst Posta	Korrigjon datën e pavlefshme; etiketa DGA nuk është provuar në mënyrë të pavarur
5	e-albania[.]eu[.]cc	subdomain	06/06/2026	subdomain_observed	2/94	Gname.com / Tencent HK	Raportohet se rezulton në 43.135.32.162	Lidhje DNS me vlerë; veprimi i regjistrimit ndryshon nga një domain i zotëruar
6	bkt[.]kycu-banka[.]one	subdomain	21/05/2026	parent_or_subdomain_metadata	0/94	Dynadot / Cloudflare	Raportohet adresa Cloudflare 104.21.29.175	0 detektime nuk do të thotë legjitim; origjina mbetet e fshehur
7	e-albania[.]biz[.]id	subdomain	08/06/2026	subdomain_observed	1/94	Baxet Group Inc.	Raportohet se rezulton në 167.17.184.183	Lidhje DNS me vlerë; duhet verifikuar timestamp-i historik
8	ntflx-shqiperia[.]com	domain	13/05/2026	domain_creation	2/94	Cloudflare	Phishing me temë Netflix	Korrelacion marke/preteksti; adresa Cloudflare nuk atribuon origjinën
9	158[.]94[.]208[.]88	ipv4	19/09/2025	gti_field_unspecified	11/94	AS202412 Omegatech LTD	Raportohet host për postashq-al.com dhe raipay-al.com	Korrelacion DNS passive me vlerë; duhet qartësuar verifikimi i datës
10	83[.]217[.]208[.]207	ipv4	27/03/2025	gti_field_unspecified	4/94	AS205775 Neon Core Network	Raportohet lidhje certifikate TLS me login.bkt-xk.com	Evidencë me vlerë nëse ruhen SAN/fingerprint/timestamp

#	Indikatori	Tipi	Data	Kuptimi	VT	Ofruesi	Korrelacioni i dorëzuar	Vlerësimi analitik
11	45[.]74[.]61[.]9	ipv4	11/12/2024	gti_field_unspecified	0/94	AS205397 69HOST LLC	Raportohet host për tre domain-e bankare të korrikut	Web në të njëjtën IP rrit lidhjen; nuk provon reverse proxy/AitM
12	43[.]166[.]168[.]169	ipv4	11/12/2024	gti_field_unspecified	0/94	AS132203 Tencent Cloud	Raportohet hosting i fushatës Platforma Qeveritare	Lidhja kërkon timestamp-e DNS/TLS