REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Analizë mbi tentativën phishing dhe marrjen e aksesit të llogarisë në “Telegram”

Versioni: 1.0
Datë: 14.08.2025

PËRMBAJTJA

LISTA E FIGURAVE

Përshkrim i tentativës *phishing*

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK) ka identifikuar dhe analizuar një fushatë të re *phishing* që synon kompromet imin e llogarive të aplikacionit **"Telegram".** Kjo fushatë bazohet në teknika të inxhinierisë sociale, duke dërguar mesazhe të rreme me përshkrim për përdoruesin për t' u klikuar ("Ekzistojnë fotografi tuaja në internet"), të cilat përmbajnë një lidhje *(link)* që çon drejt një faqeje të rreme të krijuar nga aktorët keqdashës për të imituar pamjen dhe funksionalitetin e platformës zyrtare.

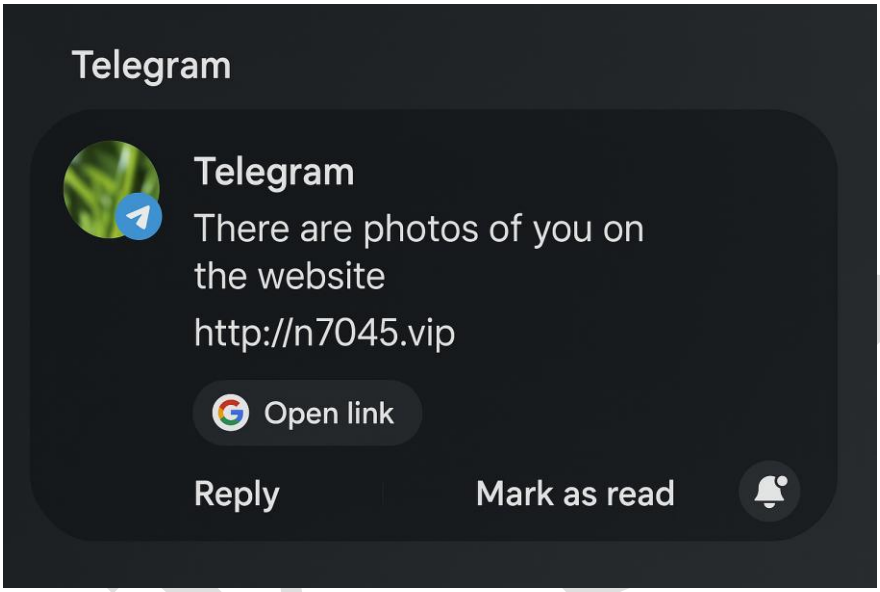


Figura 1- Shembull i mesazhit phishing në Telegram

Procesi i marrjes së aksesit në llogarinë e Telegram përmes një *link*-u jo legjitim

Në fazën e parë, përdoruesi vendos numrin e telefonit në faqen e rreme të krijuar nga aktorët keqdashës me qëllim imitimin e shërbimit legjitim që ofron aplikacioni zyrtar Telegram. Në prapaskenë, aktorët keqdashës e përdorin numrin për të nisur një proces autentikimi real në Telegram-in zyrtar (p.sh., përmes API-së ose aplikacionit web). Si pjesë e procedurës standarde, Telegrami dërgon një kod verifikimi (OTP) në numrin e dhënë, përmes SMS.

Në fazën e dytë kërkohet vendosja e kodit (OTP) për të përfunduar procesin e **MFA** të Telegram. Pasi viktima vendos kodin, sulmuesi kupton që sapo ka marrë akses dhe po përdor llogarinë ne Telegram njesoj dhe në kohë reale me perdoruesin "viktimë".

Ky kompromet im mundëson aktorit keqdashës të lexojë biseda, të shpërndajë mesazhe të tjera *phishing* tek kontaktet e viktimës dhe të kryejnë veprime të tjera keqdashëse me të njëjtin qëllim, duke rritur ndjeshëm rrezikun e përhapjes së sulmit.

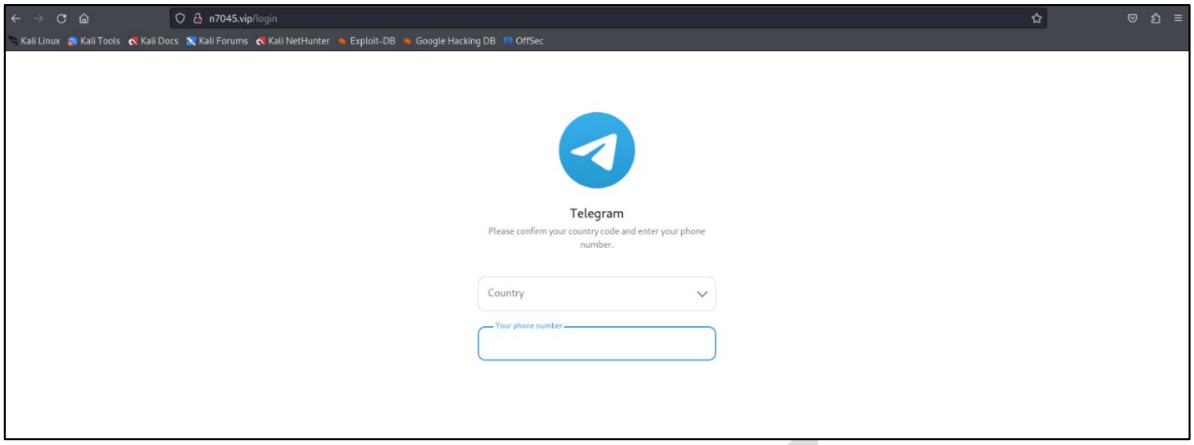


Figura 2- Faqja e imituar e Telegram

Analiza e tentativës së përdorur, ka evidentuar se IP-ja ku është hostuar faqja keqdashëse përmban një sërë domain-esh të ngjashme, çka sugjeron përdorimin e metodave të automatizuara për gjenerimin dhe qarkullimin e tyre. Lista e plotë e indikatorëve të kompromet imit (IOCs) është përfshirë në këtë raport me qëllim identifikimin, bllokimin dhe ndërgjegjësimin e të gjithë përdoruesve të rrjeteve sociale dhe jo vetëm.

Teknikat e inxhinierisë sociale të përdorura në fushatë

Mesazhi shfaqet si i dërguar nga një person i njohur, duke shfrytëzuar besimin ekzistues midis kontakteve. Teksti i tij përdor elementë që krijojnë urgjencë dhe kuriozitet. Dizajni i faqes është realizuar për të imituar në mënyrë të përpiktë rrjetin social Telegram, duke përfshirë në mënyrë identike logon, ngjyrat dhe format e hyrjes, gjë që i bën përdoruesit të ndihen sikur ndodhen në një mjedis të sigurt dhe në platformën zyrtare.

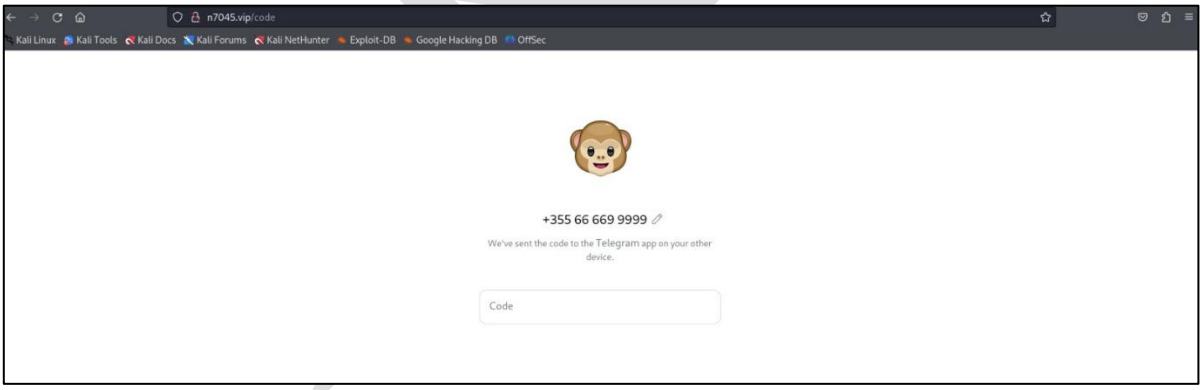


Figura 3- Momenti kur kërkohet kodi autorizimit.

Në rastet kur është autorizuar aksesi, për të marrë masa në mënyrë të menjëhershme sugjerohet të ndiqen hapat e mëposhtëm:

1) Të klikohet “No. It’s not me!”, duke treguar që personi që ka aksesuar telegramin tuaj nuk është i autorizuar
2) Të shihet lista e pajisjeve të lidhura me telegramin tuaj, dhe të ndalohen të gjitha sesionet e paautroizuara

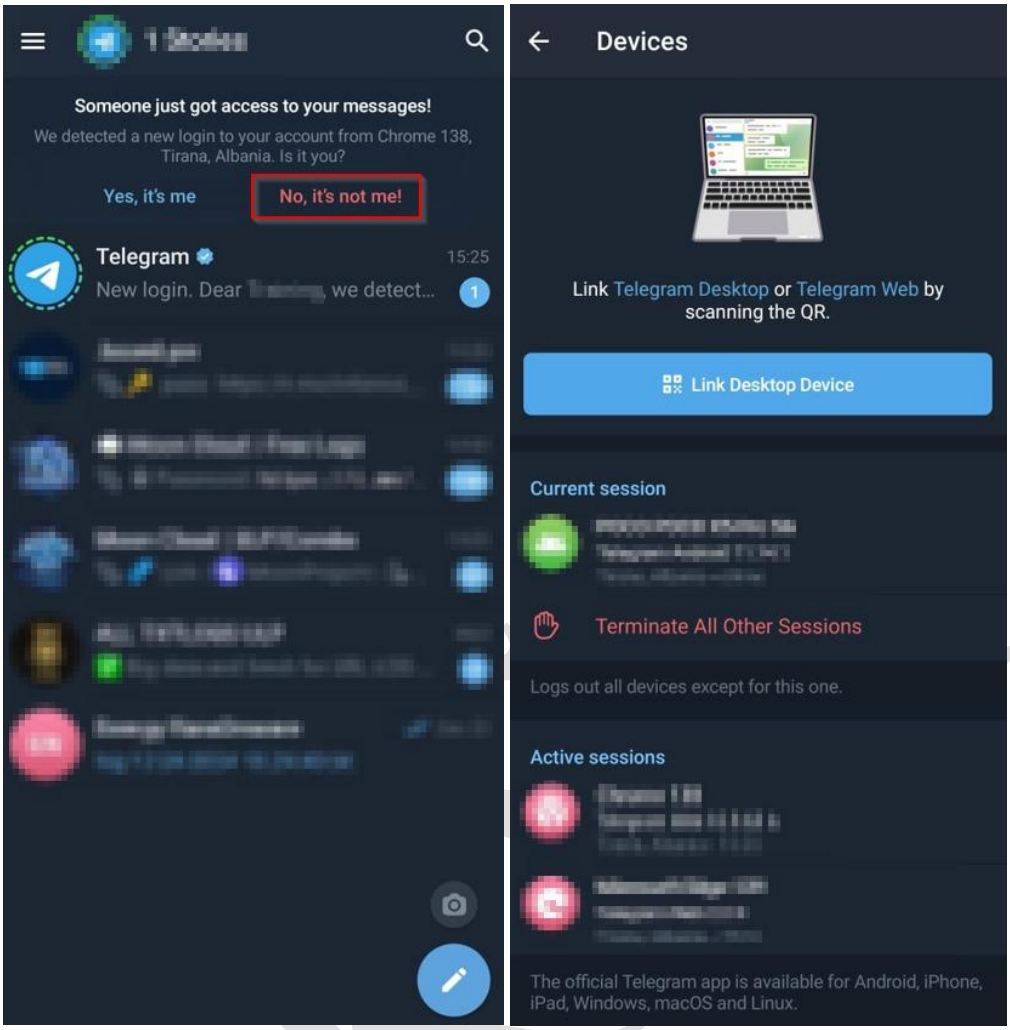
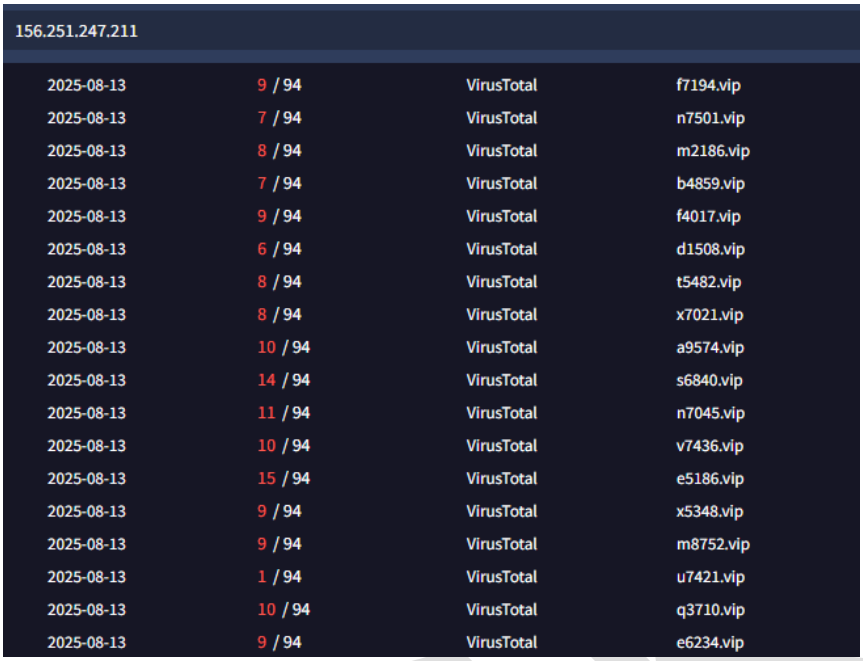


Figura 4- Marrja e masave për të nxjerrë personat e pautorizuar

Informacione Teknike

Nga verifikimi dhe krahasimi me databaza të IOCs të mëparshme, është konstatuar se IP-ja **156[.]251[.]247[.]211** dhe domain-et e lidhura me të ndjekin një model të përsëritur emërtimi *(p.sh., n####.vip, f####.vip),* i cili përputhet me struktura të mëparshme të përdorura në fushata phishing të targetuara ndaj aplikacioneve të mesazheve si *WhatsApp* dhe *Facebook Messenger*.



156.251.247.211			
2025-08-13	9 / 94	VirusTotal	f7194.vip
2025-08-13	7 / 94	VirusTotal	n7501.vip
2025-08-13	8 / 94	VirusTotal	m2186.vip
2025-08-13	7 / 94	VirusTotal	b4859.vip
2025-08-13	9 / 94	VirusTotal	f4017.vip
2025-08-13	6 / 94	VirusTotal	d1508.vip
2025-08-13	8 / 94	VirusTotal	t5482.vip
2025-08-13	8 / 94	VirusTotal	x7021.vip
2025-08-13	10 / 94	VirusTotal	a9574.vip
2025-08-13	14 / 94	VirusTotal	s6840.vip
2025-08-13	11 / 94	VirusTotal	n7045.vip
2025-08-13	10 / 94	VirusTotal	v7436.vip
2025-08-13	15 / 94	VirusTotal	e5186.vip
2025-08-13	9 / 94	VirusTotal	x5348.vip
2025-08-13	9 / 94	VirusTotal	m8752.vip
2025-08-13	1 / 94	VirusTotal	u7421.vip
2025-08-13	10 / 94	VirusTotal	q3710.vip
2025-08-13	9 / 94	VirusTotal	e6234.vip

Figura 5 - Lista e domaineve keqdashëse

Analiza gjithashtu tregon se aktorët keqdashës përdorin TLD **.vip** për shkak të kostos së ulët, kontrolleve të pakta nga registruesit dhe mundësisë për rihapjen e shpejtë të faqeve të reja pas mbylljes së atyre ekzistuese. Bazuar në këto të dhëna, ekziston një probabilitet i lartë që këto elementë të jenë pjesë e një infrastrukture të qëndrueshme dhe të centralizuar, të operuar nga një grup i specializuar në *phishing* ndaj disa platformave, me aftësi për t'u përhapur shpejt dhe për t'u përshtatur me masa të reja sigurie.

Ky lloj sulmi paraqet një rrezik të lartë për individët dhe institucionet nëse ka mungesë ndërgjegjësimi lidhur me klikimin e cdo link-u të ardhur si dhe në rast interaktiviteti me aktorin keqdashës, m kompromet imi i një llogarie Telegram ndikon drejtpërdrejt në konfidencialitetin e komunikimeve dhe integritetin e të dhënave personale. Pasi aktorët keqdashës marrin kontrollin e llogarisë, ata mund të shpërndajnë mesazhe phishing tek të gjithë kontaktet brenda pak minutash, duke shkaktuar një efekt zinxhir përhapjeje. Për institucionet, ekziston rreziku i përdorimit të llogarive të punonjësve për të kryer fushata mashtruese, për të mbledhur informacion të ndjeshëm ose për të ndikuar në reputacionin e tyre. Duke qenë se ky model sulmi mund të përsëritet lehtësisht me domain-e dhe infrastrukturë të re, potenciali për përhapje të shpejtë dhe të gjerë mbetet i lartë.

Indikatorët e Kompromet imit (IOCs)

Indikatorët e Kompromet imit (IOCs) të paraqitur më poshtë janë identifikuar gjatë analizës teknike të fushatës phishing dhe përfaqësojnë elementët kryesorë që mund të përdoren për zbulimin dhe bllokimin e aktivitetit keqdashës. Këto të dhëna janë të rëndësishme për profesionistët e sigurisë kibernetike dhe administratorët e sistemeve, pasi mundësojnë identifikimin proaktiv të trafikut të dyshimtë dhe marrjen e masave parandaluese në kohë:

156[.]251[.]247[.]211
n7045[.]vip
f7194[.]vip
n7501[.]vip
m2186[.]vip
b4859[.]vip
f4017[.]vip
d1508[.]vip
t5482[.]vip
x7021[.]vip
a9574[.]vip
s6840[.]vip
v7436[.]vip
e5186[.]vip
x5348[.]vip
m8752[.]vip
u7421[.]vip
q3710[.]vip
e6234[.]vip

Rekomandime

AKSK rekomandon udhëzime praktike për qytetarët me qëllim parandalimin e kompromentimit të llogarive të tyre dhe mbrojtjen nga fushata të ngjashme phishing. Rekomandimet e mëposhtme bazohen në analizën e rastit dhe përfshijnë hapa të menjëhershëm që duhen ndjekur për të minimizuar rrezikun dhe për të ruajtur sigurinë e informacionit personal:

1) Të mos klikohet mbi link-e të dërguara nga persona ose kanale të panjohura
2) Kontrollimin e URL përpara se të vendosen të dhënat konfidenciale dhe sensitive.
3) Raportimin menjëherë të mesazheve *phishing* brenda platformës dhe njoftimin e përdoruesit viktimë .
4) Nëse keni vendosur kodin që përdoret një herë të dërguar nga platforma, kontrolloni sesionet aktive në Telegram dhe hiqni çdo pajisje të panjohur të lidhur.
5) Kryerja e fushatave të ndërgjegjësimit të brendshëm për punonjësit mbi rreziqet e phishing-ut në aplikacionet e mesazheve.
6) Bllokimi i IP-së dhe domain-eve të listuara në Indikatorët e Kompromentimit (IOCs) në firewall, proxy dhe endpoint security.