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

Analizë e postimeve të grupit HaxChiper mbi sulmet kibernetike të pretenduara drejt Republikës së Shqipërisë

Versioni: 1.0
Datë: 22/01/2026

PËRMBAJTJA

Përmbledhje

Në një kanal në rrjetin social Telegram është evidentuar, se janë publikuar disa lajme për sulme të mundshme drejt institucioneve të Republikës e Shqipërisë. Megjithatë nuk është vërtetuar akoma nëse këto sulme kanë ndodhur apo jo. Në këto postime janë përmendur institucionet e sektorit qeveritar dhe shëndetësor.

Informacione Teknike

Ky kanal është krijuar në datën 19 Janar 2026 dhe në postimin e tij të parë thuhet se në datën 20 Janar 2026 do të shpallet zyrtarisht themelimi i komunitetit kibernetik të njohur si **HaxChipper**.

السلام عليكم ورحمة الله وبركاته

دون إطالةٍ لا داعي لها،
في هذا اليوم (20 يناير 2026) نُعلن رسميًا عن تأسيس مجتمعٍ سيبراني يحمل اسم HaxChipper.
نسأل الله سبحانه وتعالى أن يرضى عنا،
وأن يبارك خطواتنا،
وأن يدعم مسيرتنا في نصرة الحق ومعاقبة الظلم.
تحية الجهاد السيبراني

والسلام عليكم ورحمة الله وبركاته

Assalamu'alaikum warahmatullahi wabarakatuh,

Without unnecessary prolongation,
On this day (January 20, 2026), we officially announce the establishment of a cyber community known as HaxChipper.

Figura 1 Postimi i parë në këtë kanal

Po në këtë datë është postuar dhe lajmi i dytë ku thuhet se Shqipëria do të jetë target për shkak të mbështetjes së saj për Ukrainën.

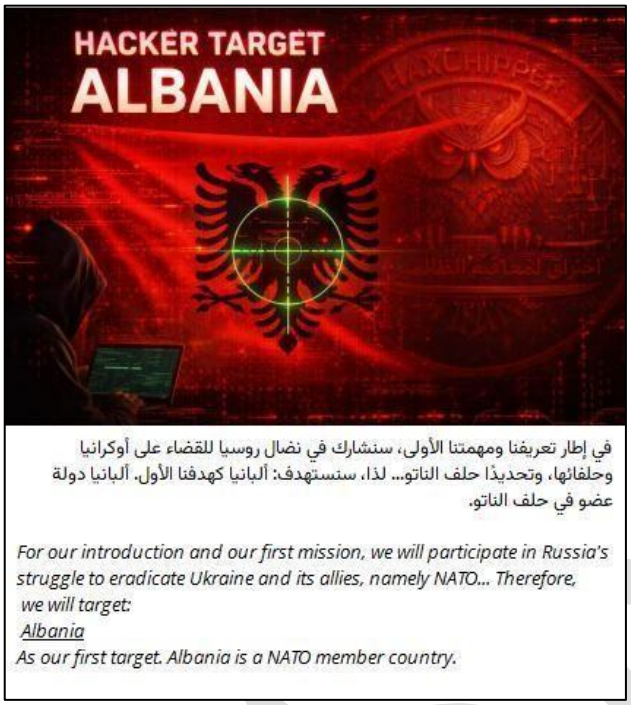

Figura 2 Foto që tregon se Shqipëria është target

Në postimin e tretë është një foto që tregon sulm të kategorisë së mohimit të shërbimeve (**DDoS**) drejt faqes së Bashkisë së Tiranës.

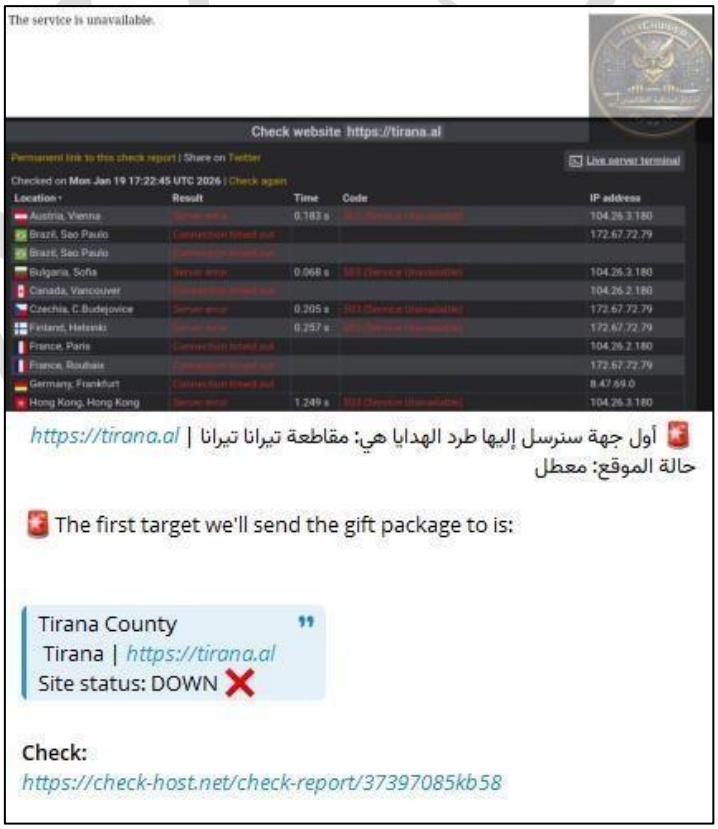

Figura 3 Sulm Ddos drejt Bashkisë Tiranë

Në datën 22 Janar 2026 u postuan 2 foto. Figura 4 tregon për sulm të kategorisë së mohimit të shërbimeve (**DDoS**) drejt:

- **Qendra Spitalore Universitare "Nënë Tereza" (qsut.gov.al)**
- **Spitali Hygeia (hygeia.al)**
- **Klinika Keit (keit.al)**
- **Fondacioni Zoja e Këshillit të Mirë (fzkm.org)**

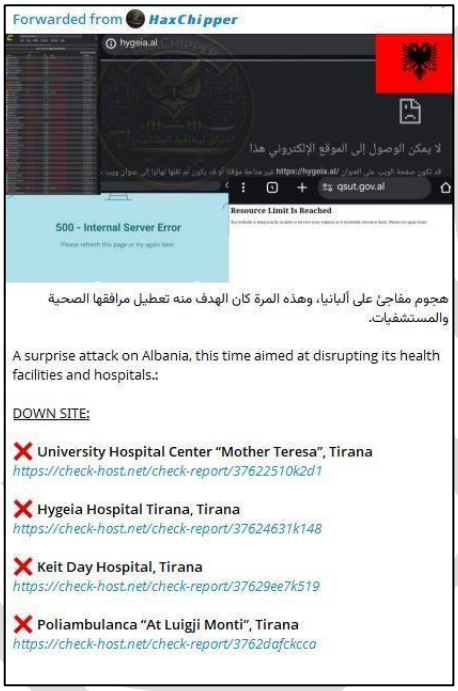

Figura 4 Sulm drejt institucioneve të Republikës së Shqipërisë

Theksojmë se faqet web arrihen të aksesohen si pasojë e bllokimeve nga filtrat e vendosura anti-DDoS nga një pjesë e infrastrukturave

Më 22 Janar 2026 është publikuar edhe një postim në dark web nga përdorues me të njëjtin emër për të dhëna konfidenciale të Ambasadës së Shqipërisë në Athinë.

Pas verifikimeve, këto të dhëna rezultojnë të vjetra, dhe i përkasin sulmit të Homeland Justice në vitin 2022. Kjo mund të vërtetohet edhe nga logo e Homeland Justice në fotot e publikuara.

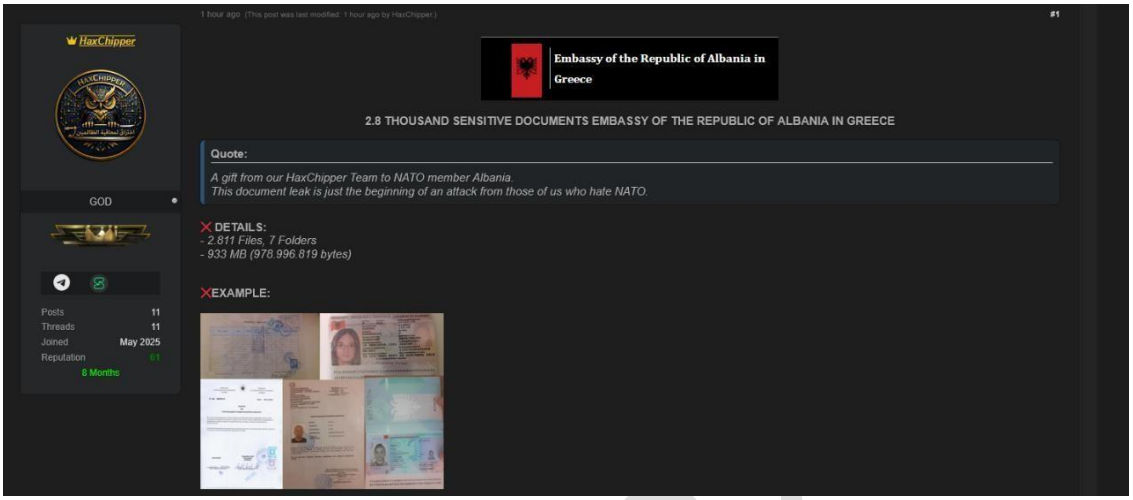

Figura 5 Postimi në DarkWeb

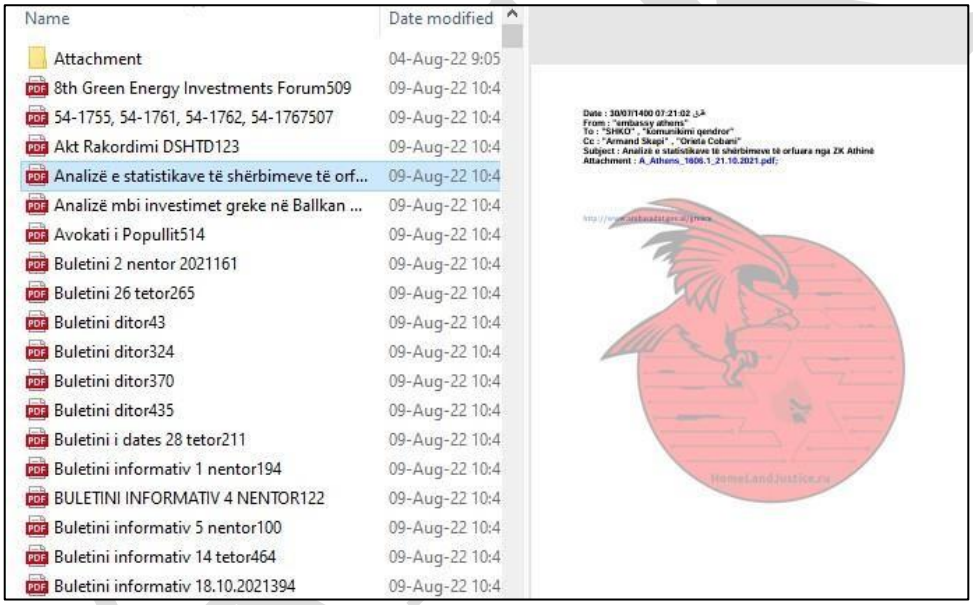

Figura 6 Materialet e publikuara në DarkWeb

Gjithashtu po në këtë grup janë shpërndarë datë 22.01.2026 disa foto ku dyshohet për sulme të mohimit të shërbimeve DDoS drejt infrastrukturave si më poshtë vijon:

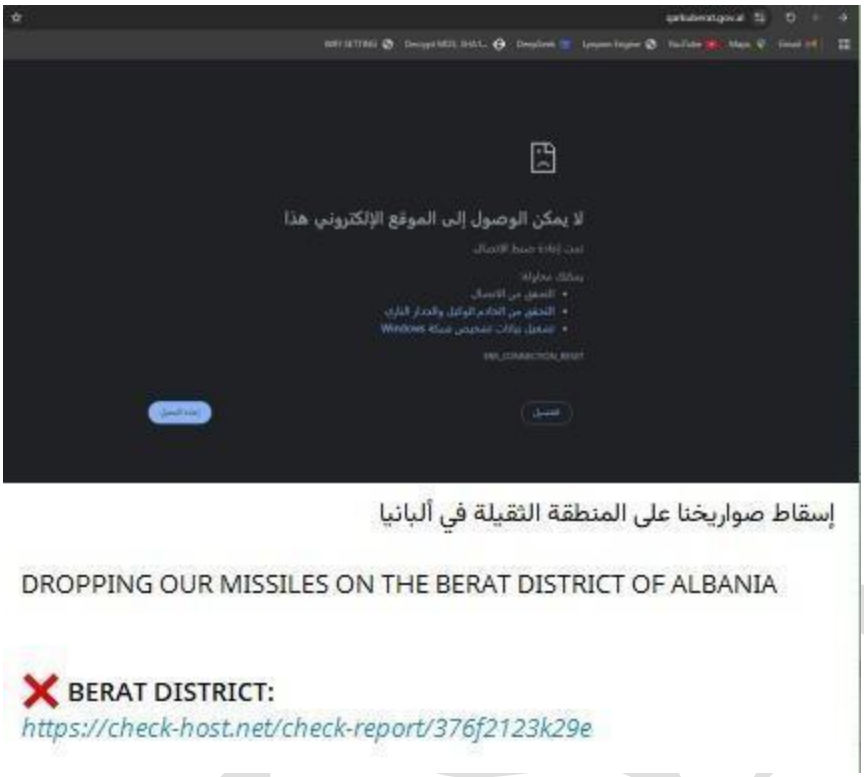

Figura 7 Postimi për sulm DDoS ndaj Qarkut Berat

Në datën 22 Janar 2026 u postuan gjithashtu foto. Figura 8 tregon për sulm të kategorisë së mohimit të shërbimeve (**DDoS**) drejt:

- **Webfaqe e qarkut Elbasan**
- **Webfare e qarkut Tiranë**
- **Webfaqe e qarkut Vlorë**
- **Webfaqe e qarkut Shkodër**
- **Webfaqe e qarkut Dibër**

أسقطنا صواريخنا على موقع منطقة إلباسان، تيرانا، فلوري، شكودر في ألبانيا

we dropped our missiles on the site of the
Elbasan,Tiranë,Vlorë,Shkodër district of Albania

❌ **Elbasan distric:**
https://check-host.net/check-report/3770cd35kacf

❌ **Tiranë Distric:**
https://check-host.net/check-report/3770d4d4k2e

❌ **Vlorë Distric:**
https://check-host.net/check-report/3770e104k7b2

❌ **Shkodër Distric:**
https://check-host.net/check-report/3770ecbck14f

Figura 8 pretendimi për sulme te kategorisë DDoS

أسقطنا صواريخنا على موقع مقاطعة ديبر في ألبانيا

we dropped our missiles on the site of the Dibër district of Albania

❌ Dibër district of Albania
https://check-host.net/check-report/37707973k78e

Figura 9 pretendim i sulm DDoS qarku Dibër

Rekomandime

AKSK rekomandon:

- Detektimi: Nëse po evidentoni shumë kërkesa hyrëse në webserver logs, ose bandwidth të mbushur, kjo mund të tregojë një sulm i cili po përpiqet të bllokojë shërbimin tuaj në internet. Kuptoni asetet tuaja kritike, identifikoni shërbimet ndaj të cilave jeni ekspozuar në internet dhe dobësitë e këtyre shërbimeve.
- Izolim i trafikut hyrës vetëm për shtetin Shqiptar, vendosni limite/sekond ose "lower the threshold" në rast Sulmi DDoS.
- Sigurohuni që perdoruesit të dinë paraprakisht se si mund të raportojnë incidente.
- Zbatoni sistemet captcha në forma publike pa autentifikim.
- Edukimi i punonjësve dhe palëve të interesuara mbi sulmet DDOS dhe strategjitë e zvogëlimit të rrezikut.
- Aplikimin e proxy servers për të ridrejtuar trafikun.
- Implementoni filtra Network DDoS Protection, Application DDoS Protection, Website DDoS Protection.
- Monitorim i vazhdueshëm i logeve në sistemet tuaja kritike.