REPUBLIC OF ALBANIA
NATIONAL AUTHORITY FOR CYBER SECURITY
DIRECTORATE OF CYBER SECURITY ANALYSIS

Analysis of the posts of the group HaxChiper regarding the alleged cyberattacks against the Republic of Albania

Version: 1.0
Date: 22/01/2026

PËRMBAJTJA

Përmbledhje ....Error! Bookmark not defined.

Informacione Teknike ....Error! Bookmark not defined.

Rekomandime **9**

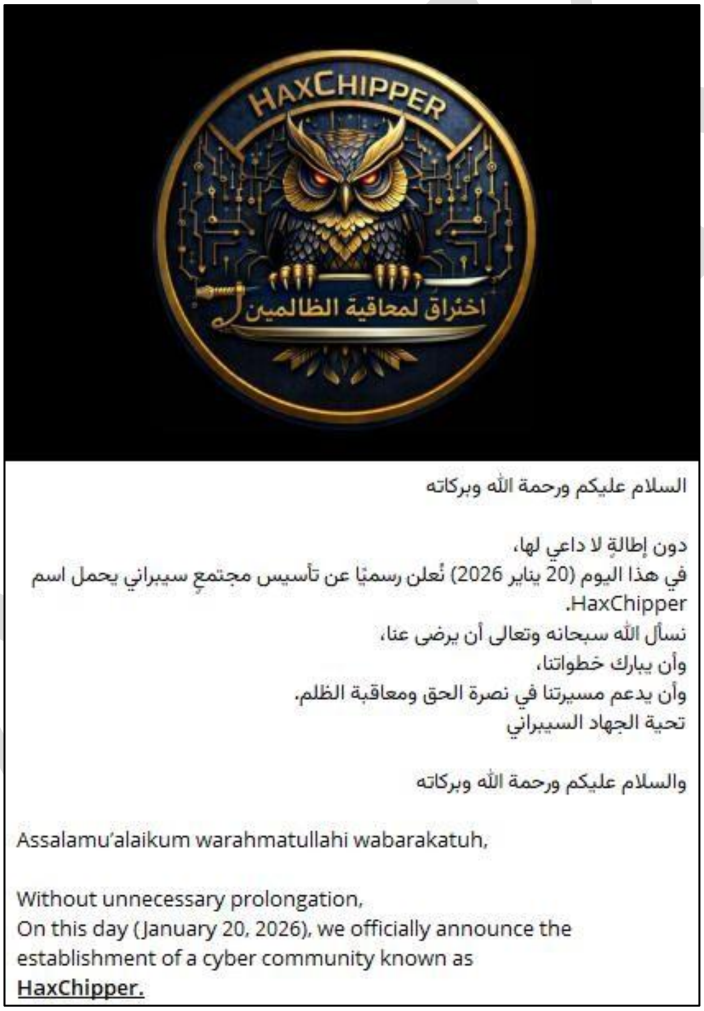
Figura 1 Postimi i parë në këtë kanal.. **Error! Bookmark not defined.**
Figura 2 Foto që tregon se Shqipëria është target.. **Error! Bookmark not defined.**
Figura 3 Sulm Ddos drejt Bashkisë Tiranë.. **Error! Bookmark not defined.**
Figura 4 Sulm drejt institucioneve të Republikës së Shqipërisë.................. **Error! Bookmark not defined.**
Figura 5 Postimi në DarkWeb .... **Error! Bookmark not defined.**
Figura 6 Materialet e publikuara në DarkWeb .... **Error! Bookmark not defined.**
Figura 7 Postimi për sulm DDoS ndaj Qarkut Berat .... **Error! Bookmark not defined.**
Figura 8 pretendimi për sulme te kategorisë DDoS.................................... **Error! Bookmark not defined.**
Figura 9 pretendim i sulm DDoS qarku Dibër .... **Error! Bookmark not defined.**

Summary

On a channel on the social network Telegram, it has been identified that several news items have been published about possible attacks against institutions of the Republic of Albania. However, it has not yet been verified whether these attacks have occurred or not. In these posts, institutions from the governmental and healthcare sectors have been mentioned.

Technical Information

This channel was created on January 19, 2026, and in its first post it is stated that on January 20, 2026, the establishment of the cyber community known as **HaxChipper** will be officially announced.



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

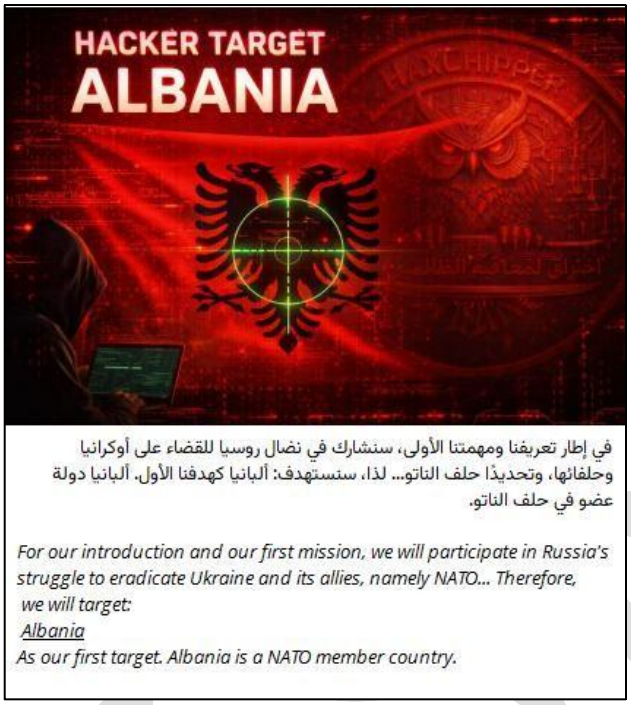
والسلام عليكم ورحمة الله وبركاته

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.**

Figure: 1 First post on this channel

On the same date, the second post was also published, stating that Albania will be a target due to its support for Ukraine.

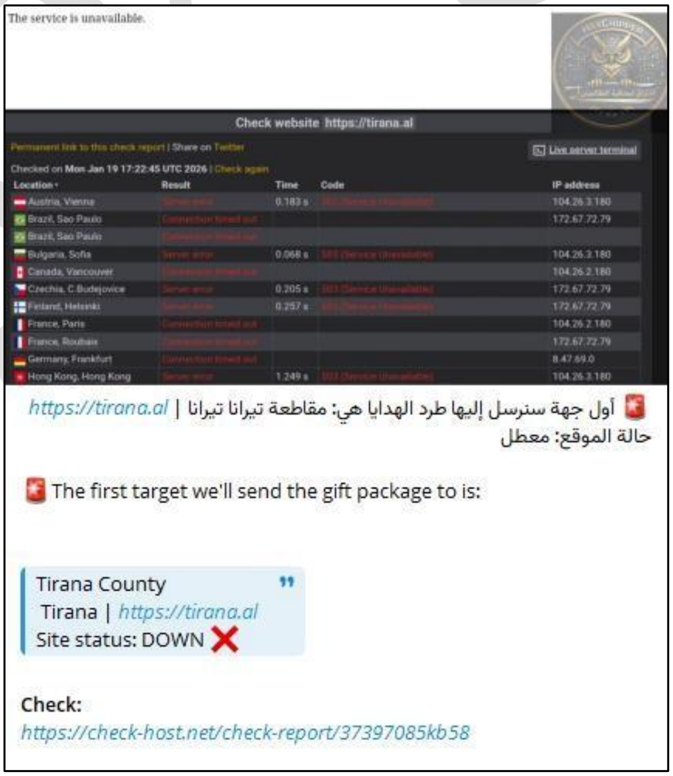


في إطار تعريفنا ومهمتنا الأولى، سنشارك في نضال روسيا للقضاء على أوكرانيا
وحلفائها، وتحديدًا حلف الناتو... لذا، سنستهدف: ألبانيا كهدفنا الأول. ألبانيا دولة
عضو في حلف الناتو.

For our introduction and our first mission, we will participate in Russia's struggle to eradicate Ukraine and its allies, namely NATO... Therefore, we will target:
<u>Albania</u>
As our first target. Albania is a NATO member country.

Figure: 2 Photo showing that Albania is a target

In the third post, there is a photo showing a denial-of-service (DDoS) attack targeting the website of the Municipality of Tirana.



The service is unavailable.

Check website https://tirana.al

Permanent link to this check report | Share on Twitter

Live server terminal

Checked on **Mon Jan 19 17:22:45 UTC 2026** | Check again

Location	Result	Time	Code	IP address
Austria, Vienna	Server error	0.183 s	503 (Service Unavailable)	104.26.3.180
Brazil, Sao Paulo	Connection timed out			172.67.72.79
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Server error	0.068 s	503 (Service Unavailable)	104.26.3.180
Canada, Vancouver	Connection timed out			104.26.2.180
Czechia, C.Budejovice	Server error	0.205 s	503 (Service Unavailable)	172.67.72.79
Finland, Helsinki	Server error	0.257 s	503 (Service Unavailable)	172.67.72.79
France, Paris	Connection timed out			104.26.2.180
France, Roubaix	Connection timed out			172.67.72.79
Germany, Frankfurt	Connection timed out			8.47.69.0
Hong Kong, Hong Kong	Server error	1.249 s	503 (Service Unavailable)	104.26.3.180

🚨 أول جهة سنرسل إليها طرد الهدايا هي: مقاطعة تيرانا تيرانا | https://tirana.al
حالة الموقع: معطل

🚨 The first target we'll send the gift package to is:

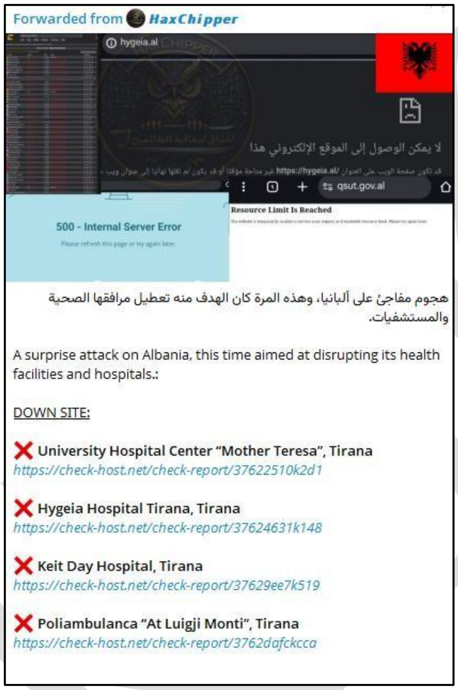
> Tirana County
> Tirana | https://tirana.al
> Site status: DOWN ❌

Check:
https://check-host.net/check-report/37397085kb58

Figure: 3 DDoS attack against the Municipality of Tirana

On January 22, 2026, two photos were posted. Figure 4 shows a **denial-of-service** (**DDoS**) attack targeting:

- **University Hospital Center “Mother Teresa” (qsut.gov.al)**
- **Hygeia Hospital (hygeia.al)**
- **Keit Clinic (keit.al)**
- **Our Lady of Good Counsel Foundation (fzkm.org)**


Forwarded from HaxChipper
hygeia.al
لا يمكن الوصول إلى الموقع الإلكتروني هذا
https://hygeia.al/
qsut.gov.al
Resource Limit Is Reached
500 - Internal Server Error
Please refresh this page or try again later.

هجوم مفاجئ على ألبانيا، وهذه المرة كان الهدف منه تعطيل مرافقها الصحية والمستشفيات.

A surprise attack on Albania, this time aimed at disrupting its health facilities and hospitals.:

DOWN SITE:

❌ University Hospital Center “Mother Teresa”, Tirana
https://check-host.net/check-report/37622510k2d1

❌ Hygeia Hospital Tirana, Tirana
https://check-host.net/check-report/37624631k148

❌ Keit Day Hospital, Tirana
https://check-host.net/check-report/37629ee7k519

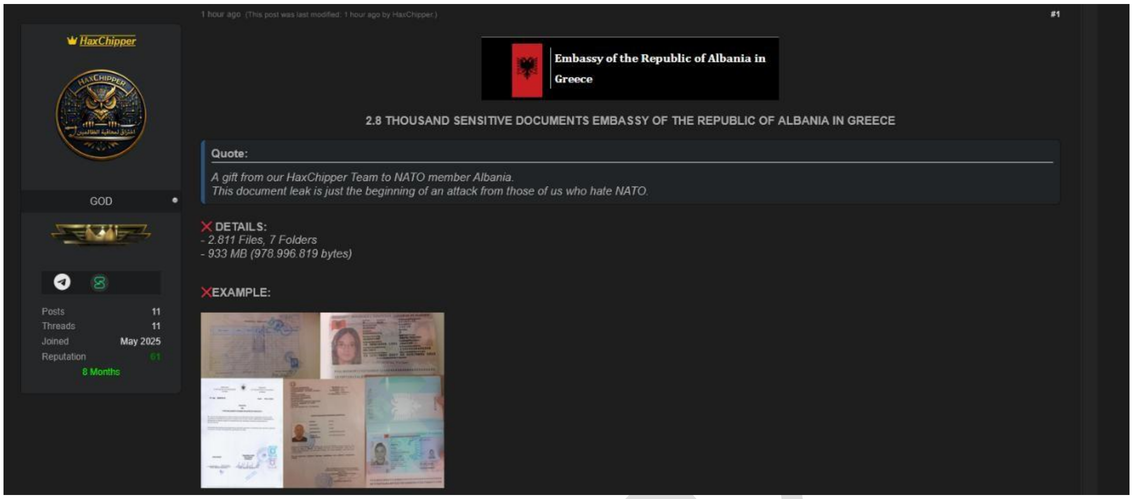
❌ Poliambulanca “At Luigji Monti”, Tirana
https://check-host.net/check-report/3762dafckcca

Figure: 4 Attack against institutions of the Republic of Albania

We emphasize that the websites are accessible, as a result of the blocks applied by anti-DDoS filters implemented by part of the infrastructures.

On January 22, 2026, a post was also published on the dark web by a user with the same name, concerning confidential data of the Embassy of Albania in Athens.

Following verification, this data appears to be old and related to the Homeland Justice attack in 2022. This can also be confirmed by the Homeland Justice logo visible in the published photos.



1 hour ago (This post was last modified: 1 hour ago by HaxChipper.) #1

HaxChipper

GOD

Posts	11
Threads	11
Joined	May 2025
Reputation	61

8 Months

Embassy of the Republic of Albania in Greece

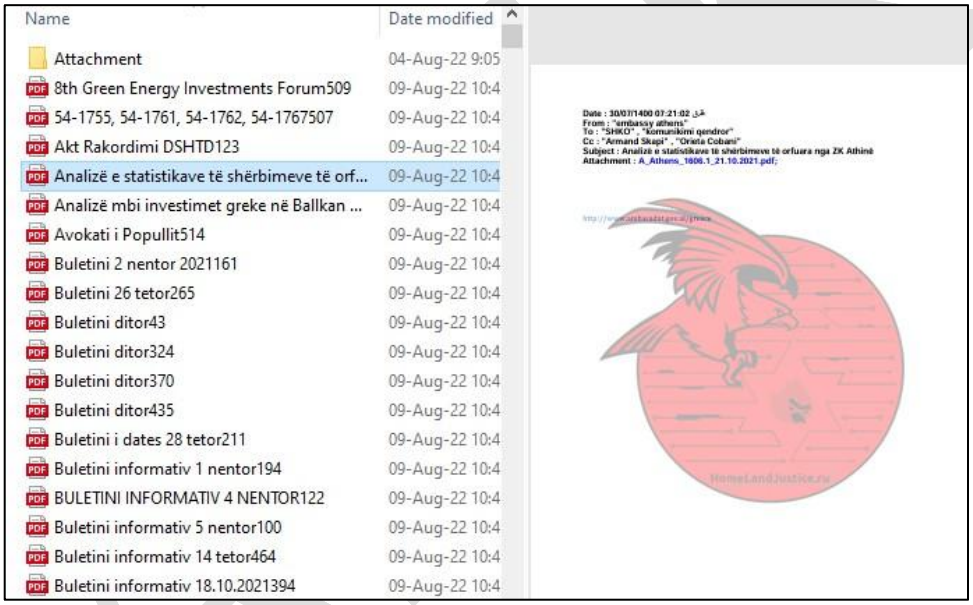
2.8 THOUSAND SENSITIVE DOCUMENTS EMBASSY OF THE REPUBLIC OF ALBANIA IN GREECE

> Quote:
>
> *A gift from our HaxChipper Team to NATO member Albania.*
> *This document leak is just the beginning of an attack from those of us who hate NATO.*

❌ DETAILS:
- *2.811 Files, 7 Folders*
- *933 MB (978.996.819 bytes)*

❌EXAMPLE:

Figure: 5 Post on the Dark Web



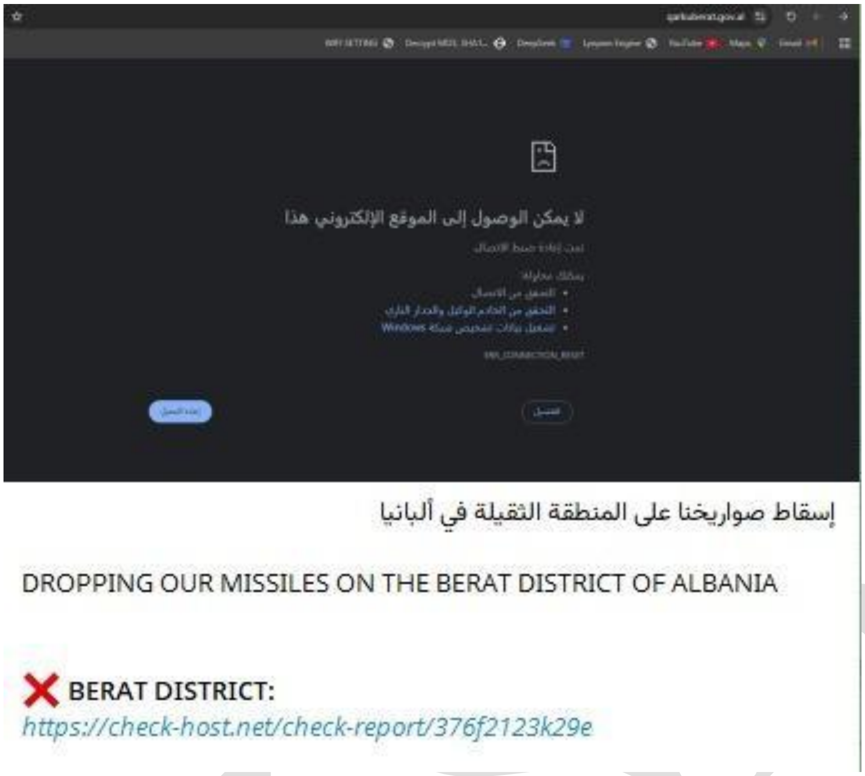
Name	Date modified
Attachment	04-Aug-22 9:05
8th Green Energy Investments Forum509	09-Aug-22 10:4
54-1755, 54-1761, 54-1762, 54-1767507	09-Aug-22 10:4
Akt Rakordimi DSHTD123	09-Aug-22 10:4
Analizë e statistikave të shërbimeve të orf...	09-Aug-22 10:4
Analizë mbi investimet greke në Ballkan ...	09-Aug-22 10:4
Avokati i Popullit514	09-Aug-22 10:4
Buletini 2 nentor 2021161	09-Aug-22 10:4
Buletini 26 tetor265	09-Aug-22 10:4
Buletini ditor43	09-Aug-22 10:4
Buletini ditor324	09-Aug-22 10:4
Buletini ditor370	09-Aug-22 10:4
Buletini ditor435	09-Aug-22 10:4
Buletini i dates 28 tetor211	09-Aug-22 10:4
Buletini informativ 1 nentor194	09-Aug-22 10:4
BULETINI INFORMATIV 4 NENTOR122	09-Aug-22 10:4
Buletini informativ 5 nentor100	09-Aug-22 10:4
Buletini informativ 14 tetor464	09-Aug-22 10:4
Buletini informativ 18.10.2021394	09-Aug-22 10:4

Date : 30/07/1400 07:21:02 ق.ظ
From : "embassy athens"
To : "SHKO" , "Komunikimi qendror"
Cc : "Armand Skapi" , "Orieta Cobani"
Subject : Analizë e statistikave të shërbimeve të orfuara nga ZK Athinë
Attachment : A_Athens_1806.1_21.10.2021.pdf;

http://www.ambasadat.gov.al/greece

Figure: 6 Materials published on the Dark Web

Additionally, on the same date (22.01.2026), several photos were shared in this group in which denial-of-service (DDoS) attacks are suspected against the following infrastructures:



لا يمكن الوصول إلى الموقع الإلكتروني هذا

تمت إعادة ضبط الاتصال.

يمكنك محاولة:

- التحقق من الاتصال
- التحقق من الخادم الوكيل والجدار الناري
- تشغيل بيانات تشخيص شبكة Windows

ERR_CONNECTION_RESET

إسقاط صواريخنا على المنطقة الثقيلة في ألبانيا

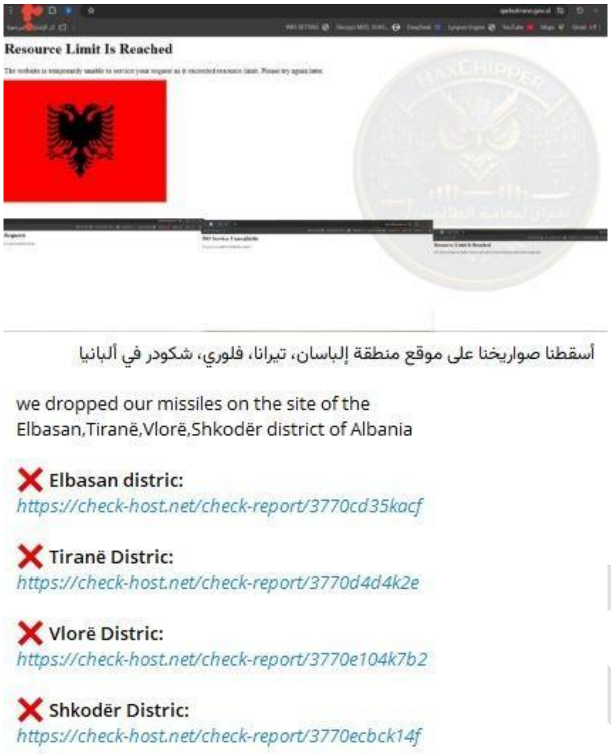
DROPPING OUR MISSILES ON THE BERAT DISTRICT OF ALBANIA

❌ BERAT DISTRICT:
https://check-host.net/check-report/376f2123k29e

Figure: 7Post regarding a DDoS attack against Berat County

On January 22, 2026, photos were also posted. Figure 8 shows a denial-of-service (DDoS) attack targeting:

- **The website of the Elbasan District**
- **The website of the Tirana District**
- **The website of the Vlorë District**
- **The website of the Shkodër District**
- **The website of the Dibër District**



Resource Limit Is Reached

The website is temporarily unable to service your request as it exceeded resource limit. Please try again later.

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

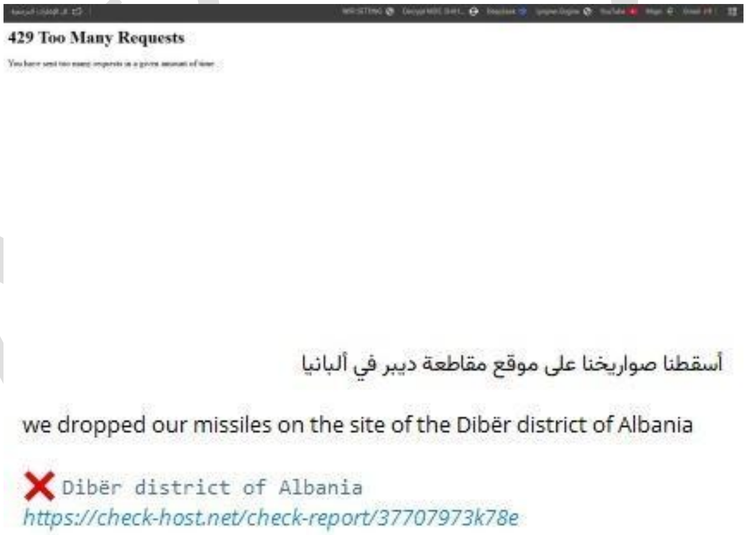
❌ **Elbasan distric:**
https://check-host.net/check-report/3770cd35kacf

❌ **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

Figure: 8 Claim of DDoS category attacks



429 Too Many Requests

You have sent too many requests in a given amount of time.

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

Figure: 9 Claim of a DDoS attack on Dibër District

Recommmends

NSCA Albania recommends:

- **Detection:** If you are observing a high number of incoming requests in the web server logs or saturated bandwidth, this may indicate an attack attempting to disrupt your online service. Understand your critical assets, identify the services exposed to the internet, and assess the vulnerabilities of those services.
- Restrict incoming traffic to Albania only and set limits per second or lower the threshold in the event of a DDoS attack.
- Ensure that users are informed in advance about how to report incidents.
- Implement CAPTCHA systems on public forms without authentication.
- Educate employees and stakeholders about DDoS attacks and risk mitigation strategies.
- Apply proxy servers to redirect traffic.
- Implement Network DDoS Protection, Application DDoS Protection, and Website DDoS Protection filters.
- Continuous monitor logs on critical systems.