



Good Network Hygiene



Is this URL malicious?

# storage.googleapis.com

2607:f8b0:4006:807::2010 

Submitted URL: <https://bit.ly/3SqXfG2>

Effective URL: <https://storage.googleapis.com/dumeredlfava118/dumeredlfava118>

Submission: On November 24 via manual (November 24th 2022, 8:22:58 am UTC) from [CA !\[\]\(e78f798d4ea5c530c9db49e7d26e6b95\_img.jpg\)](#) – Scanned from [CA !\[\]\(034433b90593e82e5460e34e3ed48e9b\_img.jpg\)](#)

[Summary](#)[HTTP !\[\]\(c694a3ff3b077d76910920a6a1593ab4\_img.jpg\)](#)[Redirects](#)[Behaviour](#)[Indicators](#)[Similar](#)[DOM](#)[Content](#)

## Summary

This website contacted **2 IPs** in **1 countries** across **3 domains** to perform **3 HTTP transactions**. The main IP is **2607:f8b0:4006:807::2010**, located in **Hudson Falls, United States** and belongs to **GOOGLE, US**. The main domain is **storage.googleapis.com**. The Cisco Umbrella rank of the primary domain is **469**.

TLS certificate: Issued by **GTS CA 1C3** on November 2nd 2022. Valid for: **3 months**.

[bit.ly](#) scanned **10000+** times on urlscan.io

[Show Scans](#) **10000+**

[storage.googleapis.com](#) scanned **10000+** times on urlscan.io

[Show Scans](#) **10000+**

[urlscan.io](#) Verdict: **No classification** 

## Live information

Google Safe Browsing:  No classification for [storage.googleapis.com](#)


Current DNS A record: **142.250.184.208** (AS15169 - GOOGLE, US)

Submitted URL: <https://bit.ly/35qX0G2>Effective URL: <https://storage.googleapis.com/dumeredifava118/dumeredifava118>Submission: On November 24 via manual [November 24th 2022, 8:22:58 am UTC] from  — Scanned from [Summary](#) [HTTP](#) [Redirects](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

## 3 HTTP transactions

-1 data transactions

[Everything](#) [HTML](#) [Script](#) [AJAX](#) [CSS](#) [Image](#) [Expand all](#)

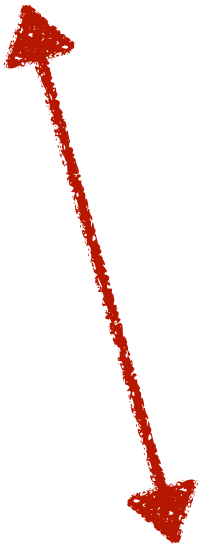
Method	Protocol	Status	Resource	Path	Size	Time	Type	IP
					x-fer	Latency	MIME-Type	Location
GET	H2	200	<b>Primary Request</b> <a href="#">dumeredifava118</a>		6 KB	149ms	Document	<a href="#">2607:f8b0:4006:807::2010</a>
			<a href="https://storage.googleapis.com/dumeredifava118/">storage.googleapis.com/dumeredifava118/</a>		6 KB	103ms	text/html	 GOOGLE
			<b>Redirect Chain</b>					
			- <a href="https://bit.ly/35qX0G2">https://bit.ly/35qX0G2</a> →					
			- <a href="https://storage.googleapis.com/dumeredifava118/dumeredifava118">https://storage.googleapis.com/dumeredifava118/dumeredifava118</a>					
GET			/		0	0		
			<a href="http://carriersupp0r1moduel00.com/">carriersupp0r1moduel00.com/</a>					

## Failed requests

These URLs were requested, but there was no response received. You will also see them in the list above.

Domain [carriersupp0r1moduel00.com](#)  
URL <http://carriersupp0r1moduel00.com/>











YES!

# Good Network Hygiene

➔ Is this URL malicious?

storage.googleapis.com  
2607:f8b0:4006:807::2010 🇺🇸

Submitted URL: <https://bit.ly/3SqXfG2>  
Effective URL: <https://storage.googleapis.com/dumeredifava118/dumeredifava118>  
Submission: On November 24 via manual (November 24th 2022, 8:22:58 am UTC) from CA 🇨🇦 — Scanned from CA 🇨🇦

Summary HTTP Redirections Behaviour Indicators Similar DOM Content

### Summary

This website contacted **2 IPs** in **1 countries** across **3 domains** to perform **3 HTTP transactions**. The main IP is **2607:f8b0:4006:807::2010**, located in **Hudson Falls, United States** and belongs to **GOOGLE, US**. The main domain is **storage.googleapis.com**. The Cisco Umbrella rank of the primary domain is **469**.  
TLS certificate: Issued by GTS CA 1C3 on November 2nd 2022. Valid for: 3 months.

[bit.ly](#) scanned **10000+** times on urlscan.io [Show Scans](#) 10000+

[storage.googleapis.com](#) scanned **10000+** times on urlscan.io [Show Scans](#) 10000+

urlscan.io Verdict: No classification 🟢

### Live information

Google Safe Browsing: 🟢 No classification for storage.googleapis.com  
Current DNS A record: 142.250.184.208 (AS15169 - GOOGLE, US)

storage.googleapis.com  
2607:f8b0:4006:807::2010 🇺🇸

Submitted URL: <https://bit.ly/3SqXfG2>  
Effective URL: <https://storage.googleapis.com/dumeredifava118/dumeredifava118>  
Submission: On November 24 via manual (November 24th 2022, 8:22:58 am UTC) from CA 🇨🇦 — Scanned from CA 🇨🇦

Summary HTTP Redirections Behaviour Indicators Similar DOM Content API Verdicts

### 3 HTTP transactions

~1 data transactions

Method	Protocol	Status	Resource Path	Size x-fer	Time Latency	Type MIME-Type	IP Location
GET	H2	200	<a href="#">Primary Request</a> dumeredifava118 storage.googleapis.com/dumeredifava118/ <a href="#">Redirect Chain</a> <a href="https://bit.ly/3SqXfG2">https://bit.ly/3SqXfG2</a> <a href="https://storage.googleapis.com/dumeredifava118/dumeredifava118">https://storage.googleapis.com/dumeredifava118/dumeredifava118</a>	6 KB 6 KB	149ms 103ms	Document text/html	2607:f8b0:4006:807::2010 🇺🇸 GOOGLE
GET			/carriersupp0r1module00.com/	0 0			

### Failed requests

These URLs were requested, but there was no response received. You will also find them in the list above.

Domain	carriersupp0r1module00.com
URL	http://carriersupp0r1module00.com/

➔ YES!

# Good Network Hygiene



## ➔ HTTPS Everywhere and Cert verification mitigates

- Credential theft due to plain text transport
- Site impersonation. Don't naively trust it because it's GREEN! Both the certified domain and issuer must be trusted. **“If it looks like a duck but isn't certified as a duck, it is not a duck”**