### **Target of Scan**

The scan was run on: [afifjukka@gmail.com](mailto:afifjukka@gmail.com)

**Log Overview**

**Total entries: 4,994**

**Loaded modules: Similar to the previous scan, includes sfp\_abuseipdb, sfp\_abstractapi, and many more.**

### **Suspicious Activity Detected**

There are a series of errors indicating failed connections to strange hostnames, like:

* http://koinqhyhgwkbizeant...
* http://vlogme2kjnsanxhsfh...
* http://ussajm3cffn6xsy5rd...
* http://aniozgjggq2pzxznog...

These appear to be:

* Auto-generated or obfuscated domains
* Possibly tied to malware C2 servers, phishing, or dark web infra

**we found — 404 suspicious .onion domains linked (directly or indirectly) to** [**afifjukka@gmail.com**](mailto:afifjukka@gmail.com)

These are some of the hidden services SpiderFoot tried (and failed) to reach:

1. koinqhyhgwkbizeantw757pu3cridwyhckruq3gn62ri2tdo3wjxygid.onion
2. vlogme2kjnsanxhsfhjthlyjy2j3n7vzyf5rkvpurpttm7rcf227fkad.onion
3. ussajm3cffn6xsy5rdtqjwune2mf2w7qrxx2wklv2mz66oyosempe5yd.onion
4. aniozgjggq2pzxznogrlpoioks7iu3emj6bwebz3yptl4pkoukzd6kid.onion
5. pasteelo23czesvydfsgeiotb3xvuyo32bcorajd4l6fl6y33aic5tqd.onion

**these types of domains are typical of:**

* **Pastebins**
* **Dark web forums or marketplaces**
* **Malware drop zones**
* **C2 servers**

### **What This Could Mean**

The presence of .onion domains in the scan results could indicate:

* The email has been mentioned or linked on dark web forums
* It's been associated with leaked data, pastes, or threat actor discussions
* An attempt was made to probe dark web resources for matches

### **Emails Linked (21 total)**

Here are some of the emails that appeared in connection with the scan:

* WSXPpK8fiSrqQhNCpWQpHTAA@mail.gmail.com
* mlevedahl@gmail.com (appears multiple times in MIME-style message IDs)
* jltobler@gmail.com (similarly present in multiple forms)
* afifjukka@gmail.com (your original target)
* Other potentially random or alias-based Gmail addresses

### 

### **Domains Identified (380 total)**

Mix of suspicious, Tor-based, and known domains. Examples:

* www.adultism.com — may suggest ties to adult content (could be benign or reputationally risky)
* .onion addresses like:  
  + koinqhyhgwkbizeant...onion
  + vlogme2kjnsanxhsfh...onion
  + ussajm3cffn6xsy5rd...onion
* Others like urllib3.connection.HTTPConnection indicate technical error messages or failed HTTP attempts.

### **Usernames Detected**

* vv887ex1ty
* afifjukka

The first one (vv887ex1ty) looks like a handle/alias — might be worth investigating on social media, paste sites, or forums.

#### 

#### **Noteworthy Points:**

* The presence of **multiple .onion domains** indicates that this email may be mentioned in **dark web pastebins, markets, or threat forums**.
* Some domains are broken, suggesting past use or takedowns.
* Multiple emails tied to structured message headers (like mlevedahl@gmail.com, jltobler@gmail.com) could hint at past communications or leaks.