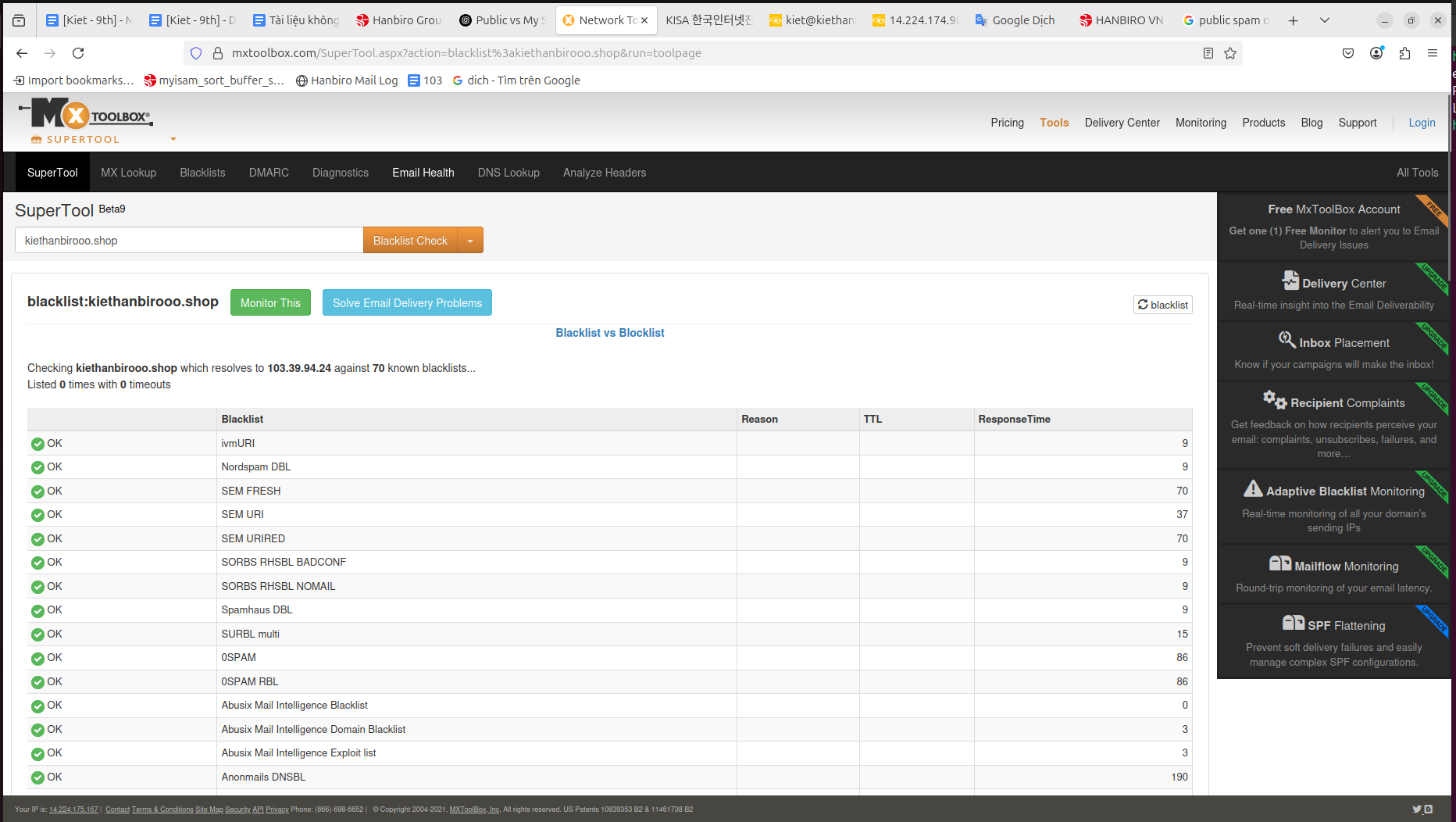
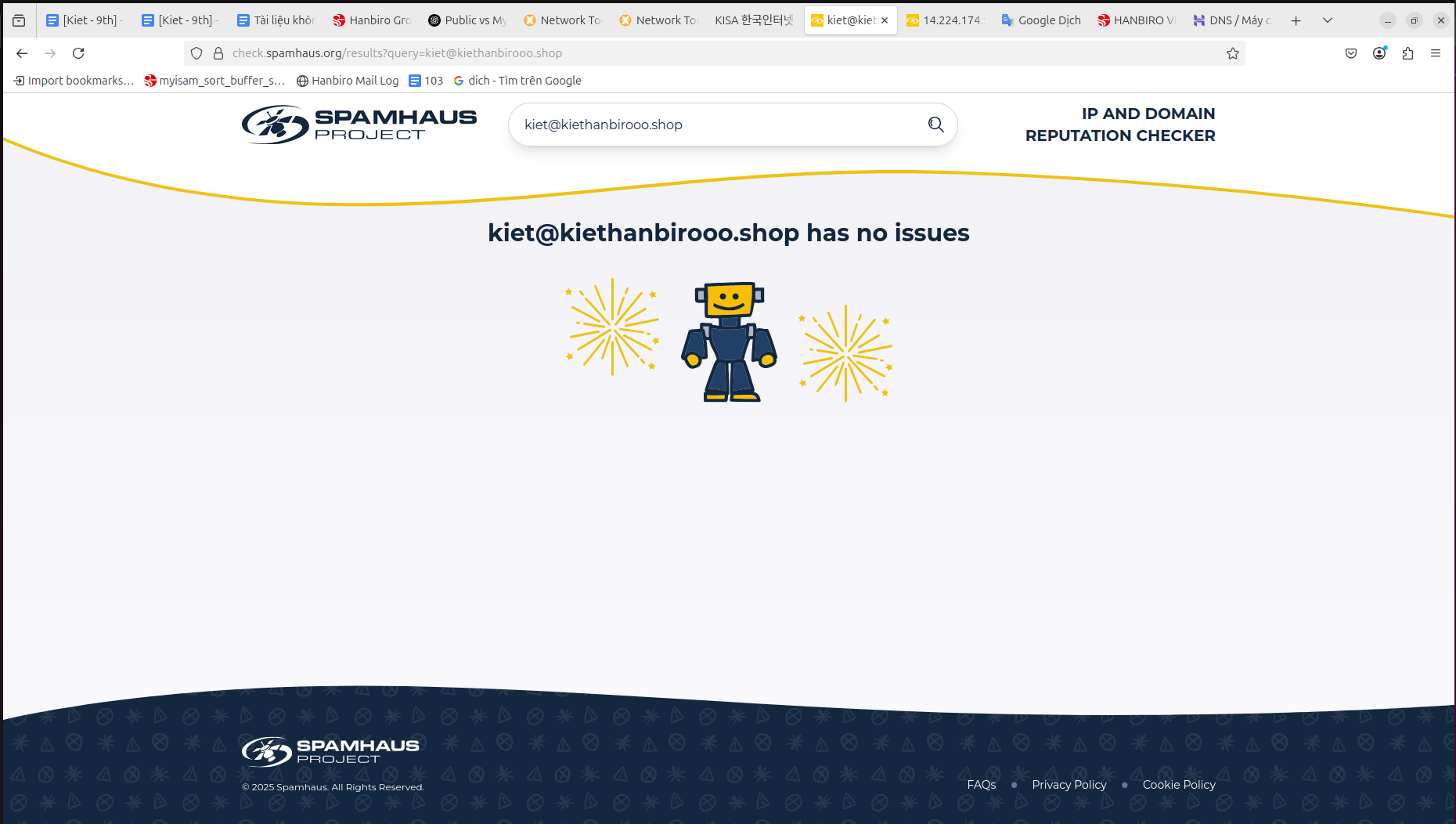
***Question:* Technical background or links to how RBLs like Spamhaus or KISA operate and how often IPs get updated. How to delist IP if it was listed in some popular RBLs (Spamhaus, ...)**

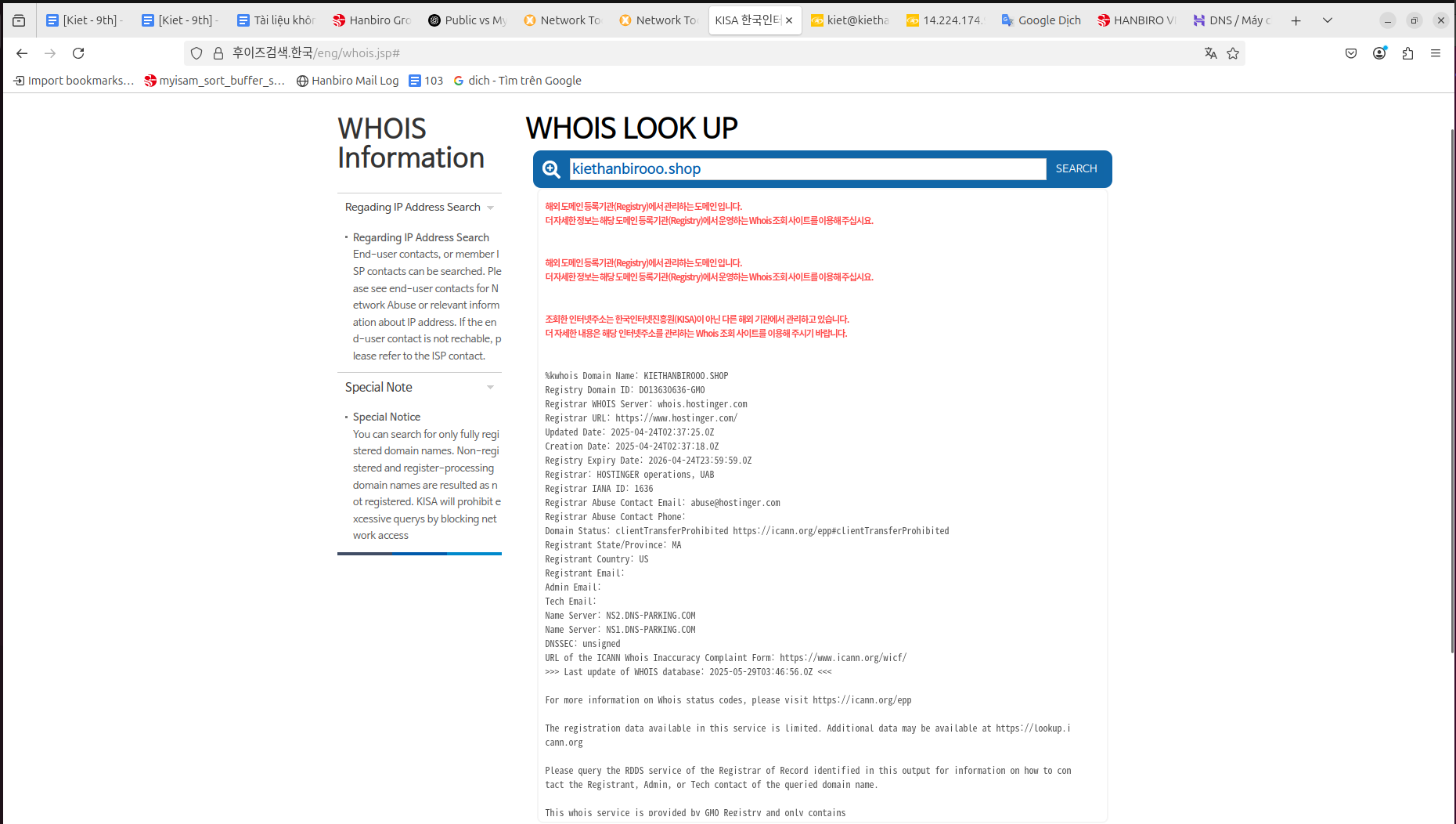
* check blacklist domain **kiethanbirooo.shop** in MxToolBox:



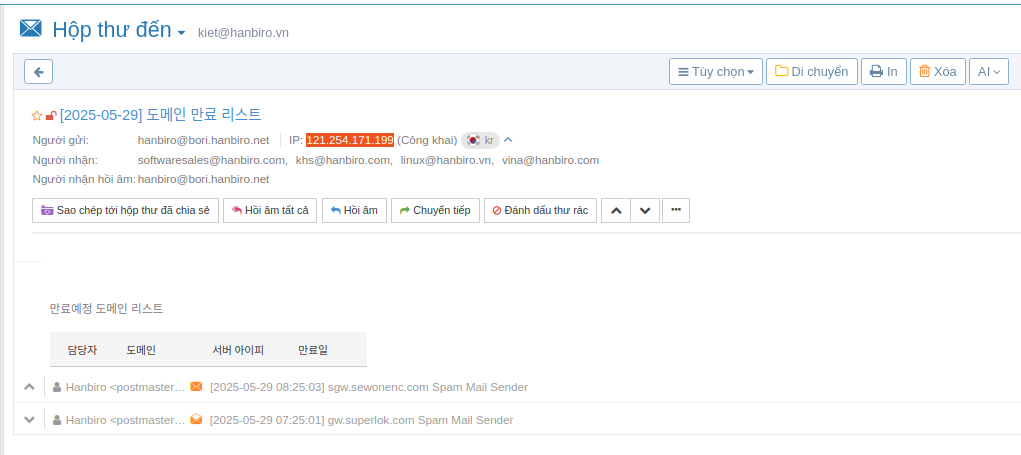
* check on Spamhaus:

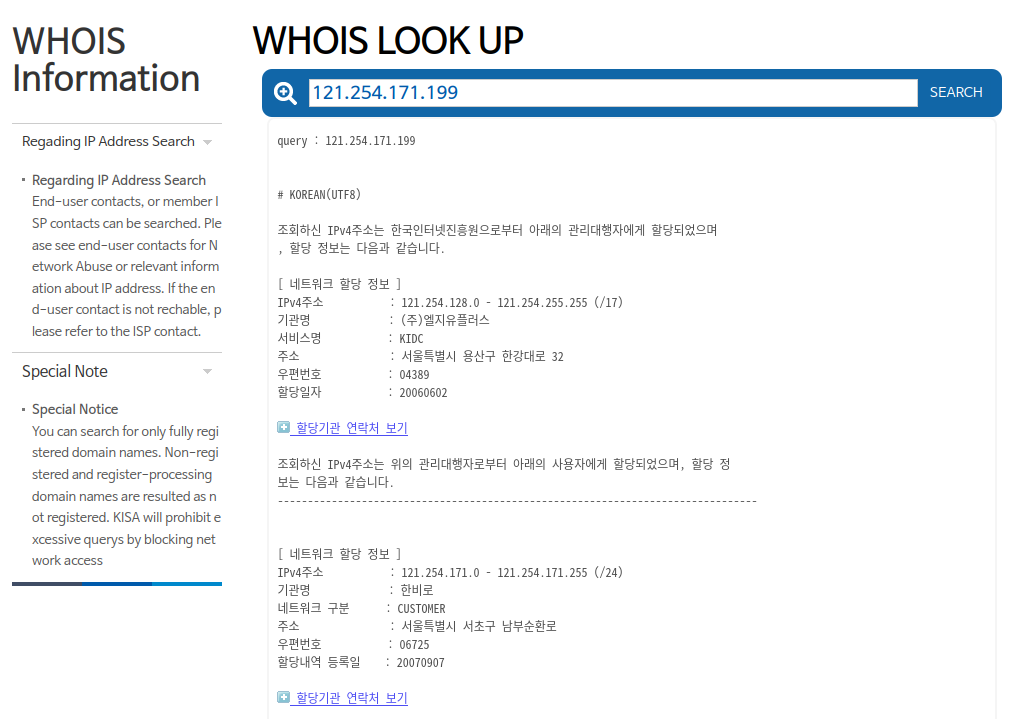


* check on KISA:



* check IP Korea:







**RBL (Real-time Blackhole Lists)**

* is a real-time list of IP addresses (or domains) that have been identified as spamming, spreading malware, phishing, or displaying suspicious activity
* used by email filtering systems to automatically reject or flag emails from “bad” sources

**Spamhaus RBL**:

* SBL (Spamhaus Block List): Spam IPs, open relay servers, professional spammers
* XBL (Exploits Block List): IPs infected with malware or botnets
* PBL (Policy Block List): IPs that should not send direct emails (like residential IPs)
* Spamhaus uses:
* Honeypot email traps (fake or inactive email addresses used to identify and block spammers)
* Reports from users and service providers (ISPs)
* Analysis of unauthorized email sending behavior
* Update Frequency:
* Realtime (updated continuously, sometimes within minutes)
* IPs can be removed automatically if no longer active, depending on the list

LINK check: <https://check.spamhaus.org>

**KISA Spam DB (Korea Internet & Security Agency):** Korean government database used to track:

-> IP, phone number, spam domain

-> Malicious SMS/email content in Korea

* How it works - Combination of:

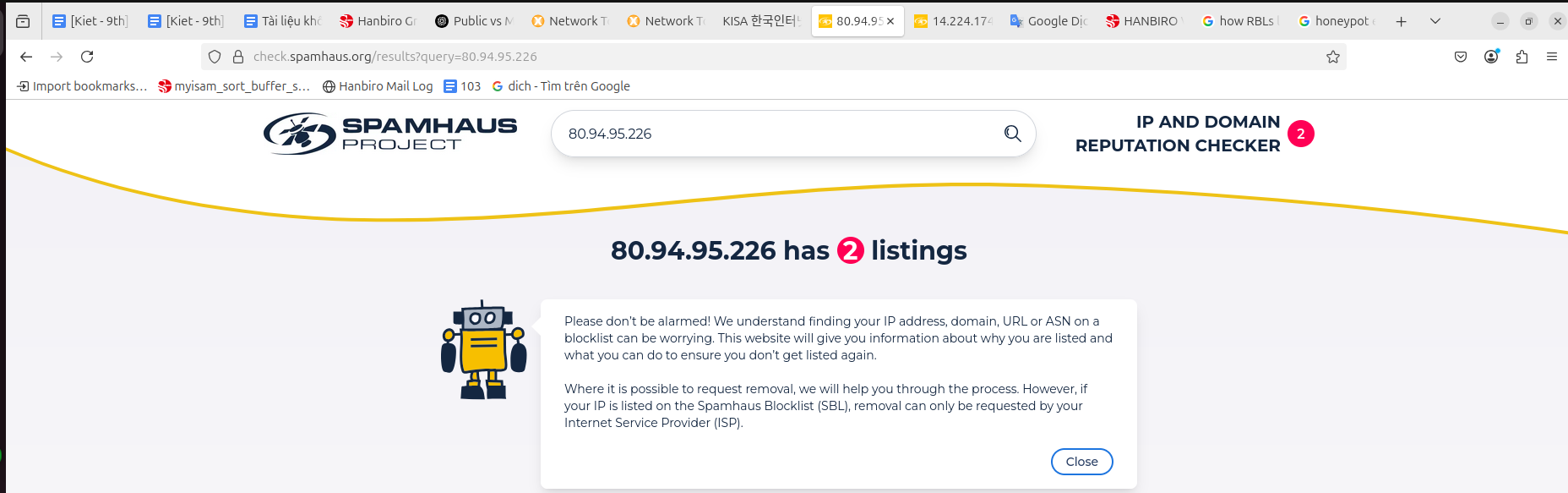
-> User reports

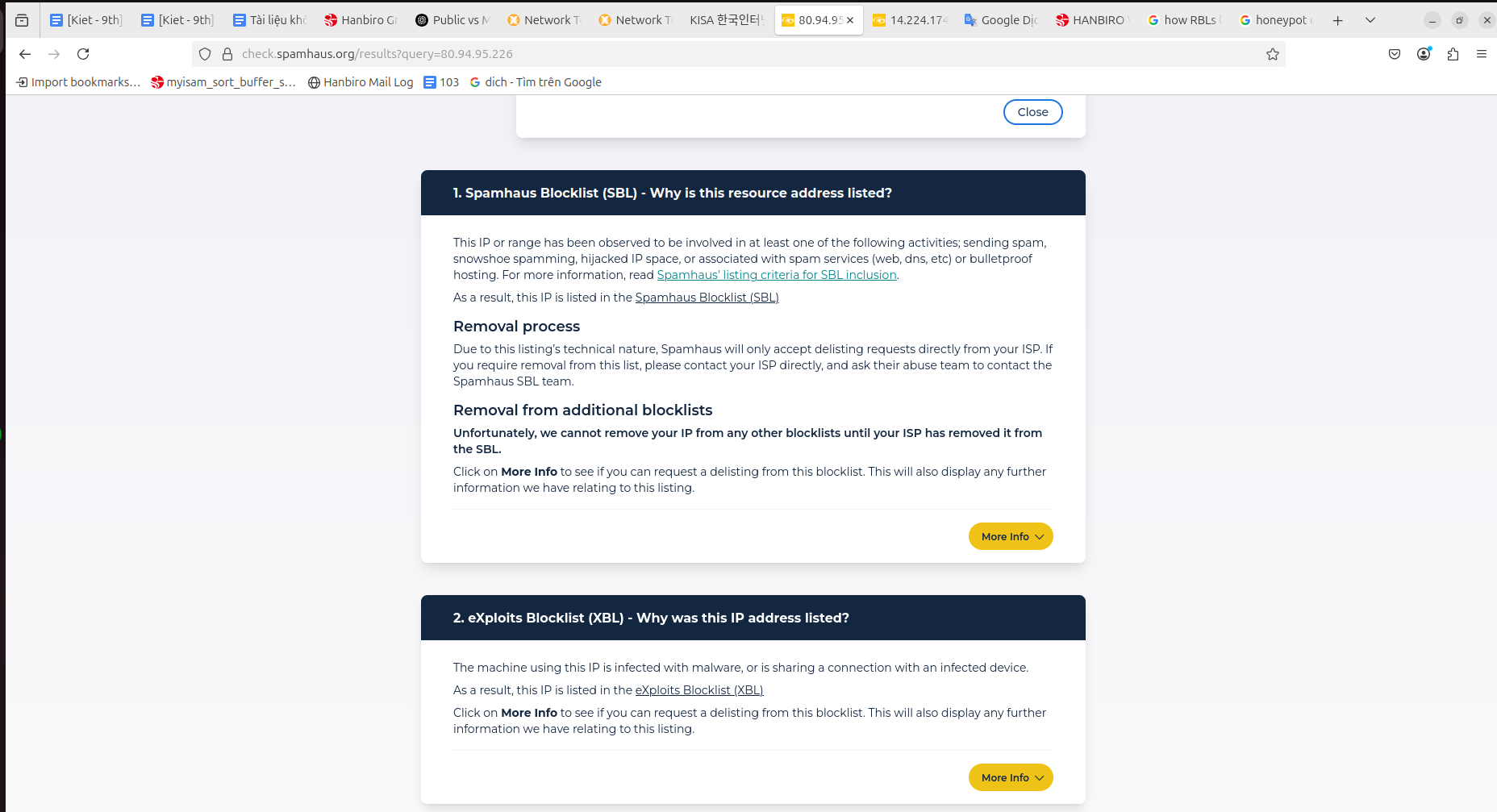
-> Email system analysis in Korea

-> Email & SMS content monitoring

* Update frequency: Depending on the number of reports and verifications -> batch or daily
* check: <https://www.spamcop.or.kr>

**# Check IP 80.94.95.226 in Spamhaus**





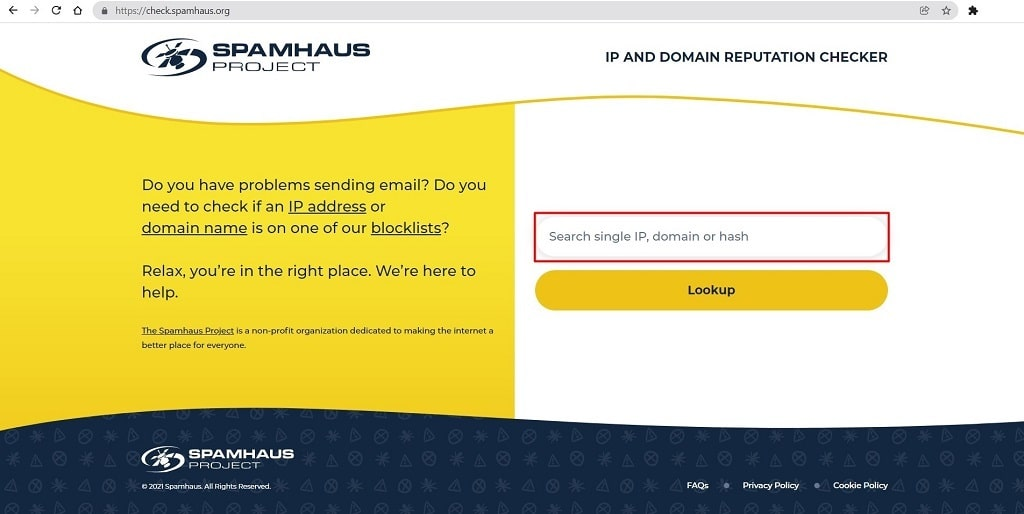
**# Before requesting delisting:**

* No spam/malware is being sent from your server
* Your mail server is properly configured (SPF, DKIM, DMARC)
* Reverse DNS (PTR record) is set correctly
* Your server is not an open relay
* Devices behind NAT are secure (for XBL/malware lists)

**# How to Remove Your IP from Spamhaus Blocklists:**

1. Check if Your IP is Listed

* Use the official Spamhaus lookup tool: <https://check.spamhaus.org>
* Enter your IP address to see if it appears on any Spamhaus blocklists (SBL, XBL, PBL, DROP, …)
* The tool will show the reason why your IP was listed



2. Identify the Reason for Listing

* Different Spamhaus lists have different purposes:
* SBL (Spamhaus Block List): IP involved in sending spam or malicious activities
* XBL (Exploits Block List): IP infected with malware or exploited in botnets
* PBL (Policy Block List): IPs that should not send email directly (usually dynamic residential IPs)
* DROP (Don't Route Or Peer): IPs or subnets involved in severe abuse or cybercrime
* Check your mail server logs or system thoroughly to find the exact cause

3. Fix the Underlying Problem

* Do not request removal before fixing the root cause
* Clean malware, fix server misconfigurations, patch vulnerabilities
* Ensure proper email authentication (SPF, DKIM, DMARC) and stop sending spam

4. Request Delisting

* For SBL and DROP, your ISP usually must request removal because they manage those IPs
* For PBL, if you own a single IP, you can submit a removal request via the PBL form
* Listings in CSS and XBL expire automatically if no new spam or exploits are detected, but you can request removal sooner if fixed
* Submit your request on the Spamhaus website with your contact information
* Removal may take from a few minutes up to 24 hours

5. Prevent Future Listings

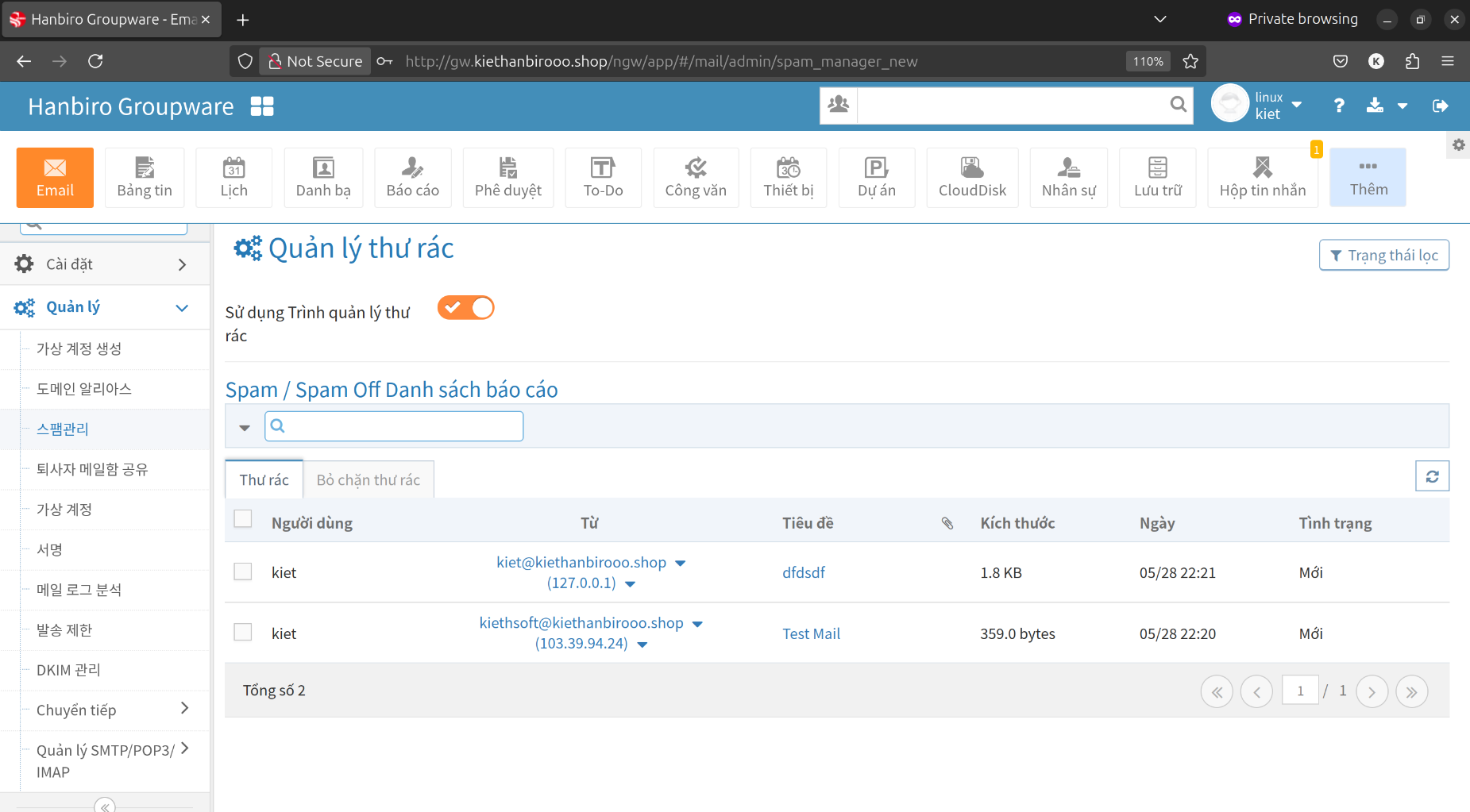
* Keep your systems secure and updated
* Use proper email authentication and monitor outbound mail
* Avoid sending unsolicited emails

***Referenced articles:*** <https://www.ipxo.com/blog/remove-ip-from-spamhaus-blocklist/>

***Referenced video:*** <https://www.youtube.com/watch?v=uLS9tl3_wdw>

***Question:* Test more case with Spam Manager, explain how different between Public Spam DB, My Spam DB**

* Test Case with Spam Manager:



**Public Spam DB** are publicly maintained databases of known spam senders, IPs, domains, or message patterns

* Characteristics:
* Maintained by third parties like Spamhaus, Barracuda, SpamCop, …
* Wide coverage: Includes data collected from across the internet
* Frequently updated by a large community or organization
* Free or subscription-based access
* Used by many email servers or spam filters to block common/global spam
* Examples:

*Spamhaus Block List (SBL)*

* A list of IP addresses that are known to be sources of spam or malware
* Maintained by Spamhaus, one of the world's most respected anti-spam organizations

*Barracuda Reputation Block List (BRBL)*

* A list of IP addresses that send emails with a bad reputation, often marked as spam
* Developed by Barracuda Networks, specializing in email and network security

*SURBL (Spam URI Realtime Blocklists)*

* A list of domains or URLs that are often included in spam emails
* Helps detect emails that contain links to phishing sites, viruses or spam ads
* Limitations:
* Might block legitimate senders if they're mistakenly listed
* Not tailored to your specific spam patterns or users
* Dependent on external update frequency and accuracy

**My Spam DB** is a private, custom spam database maintained by you or your organization

* Characteristics:
* Built from your own email traffic or application data
* Can include custom rules, blocked IPs/domains, or message fingerprints
* Reflects specific spam threats seen in your environment
* You have full control over entries and can whitelist/blacklist as needed
* Examples:
* An internal list of repeat spammers hitting your contact forms.
* A set of message hashes or phrases marked as spam by your users.
* Logs or reports of phishing attempts targeting your users specifically.
* Limitations:
* Requires manual effort or automation to maintain
* May not catch new global spam campaigns unless updated or combined with a public DB
* Smaller scope - only reflects your environment

**Summary Table**

| **Feature** | **Public Spam DB** | **My Spam DB** |
| --- | --- | --- |
| Source | external | internal (in system) |
| Coverage | global | local |
| Control | low | full |
| Customization | limited | high |
| Maintenance | automatic (3rd party) | manual or automated |
| Accuracy (local) | moderate | high |
| Risk of false positives | moderate | low (if well-tuned) |