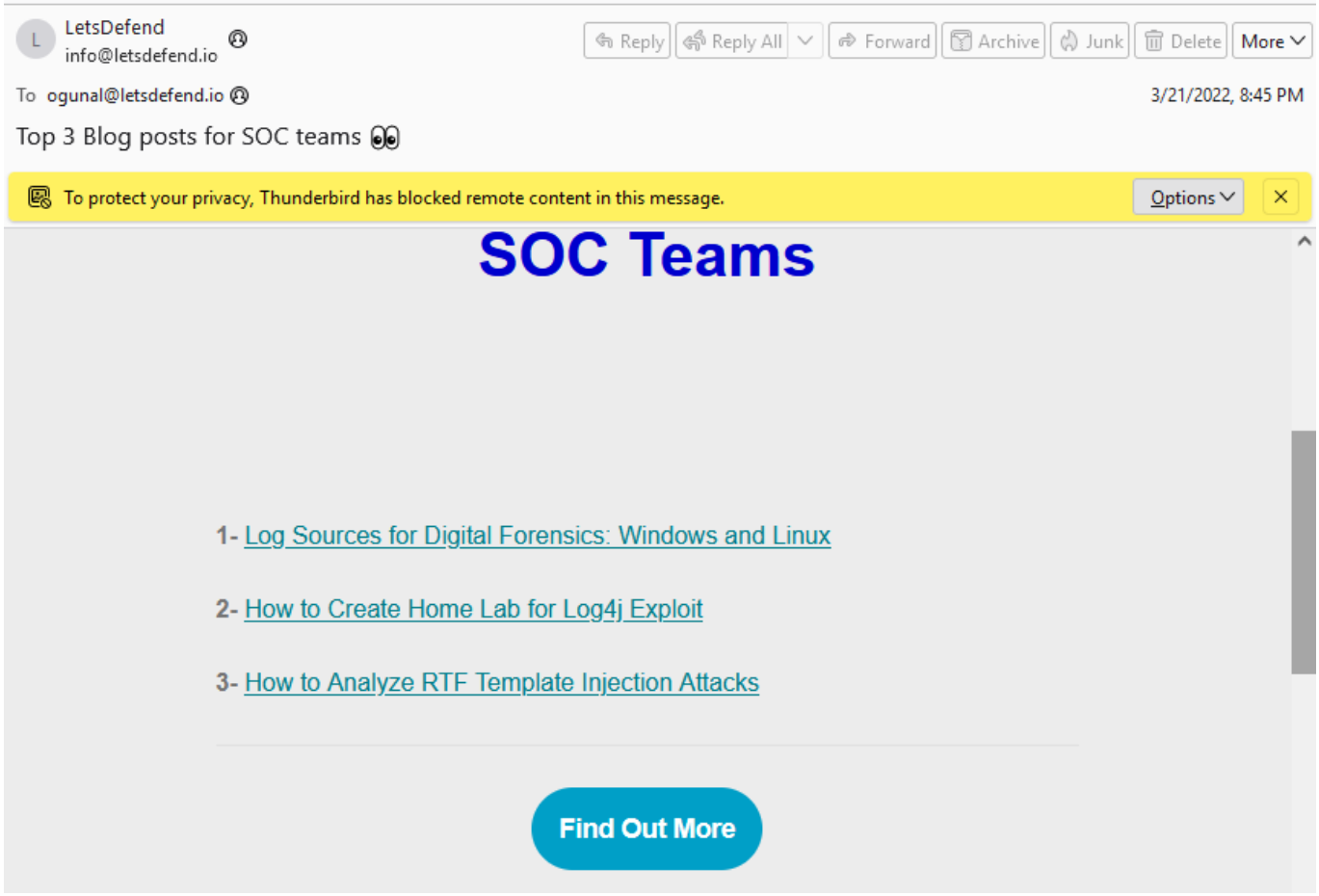
Phishing Email Analysis Report

Cybersecurity Internship

Prepared by: Thumma Kiranmai

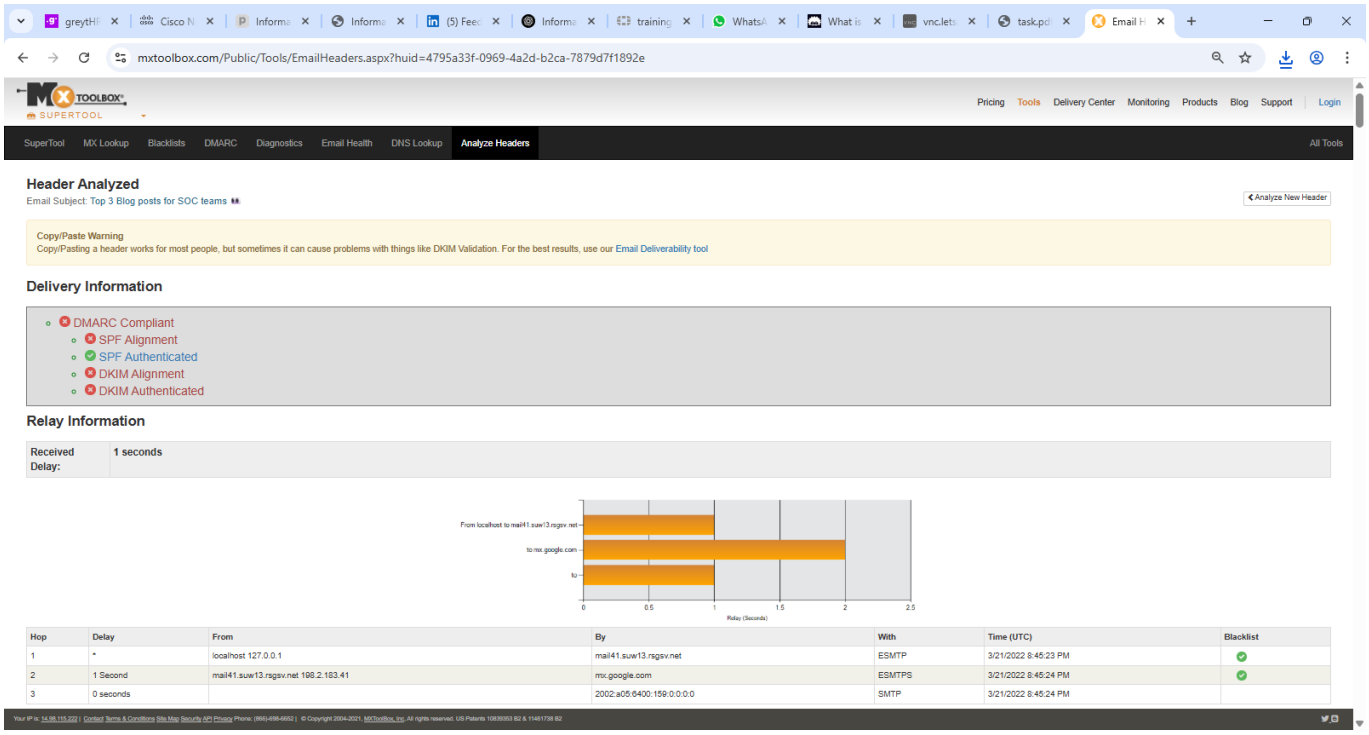
Date: May 27, 2025

Received Email Analysis



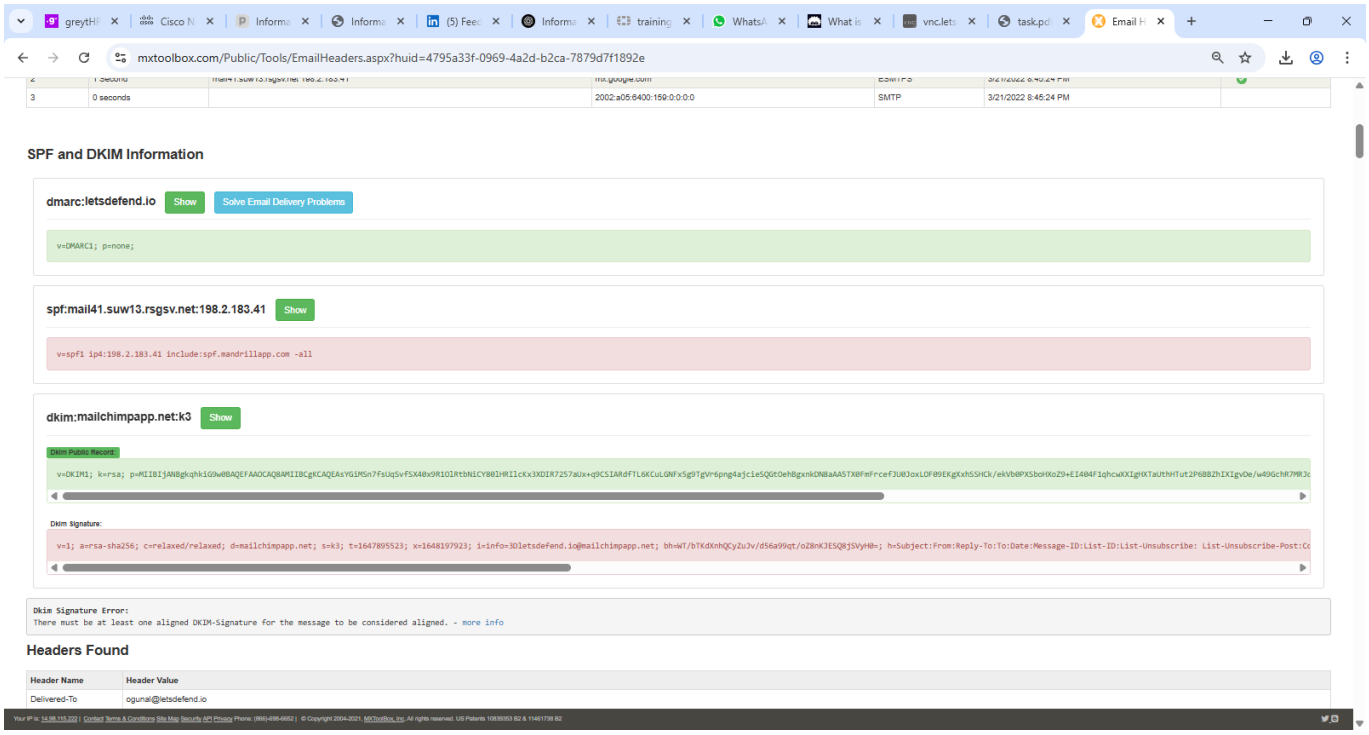
This section displays an email designed to appear as a legitimate message from LetsDefend. The email offers cybersecurity blog content targeting SOC professionals. The sender address is shown as info@letsdefend.io. Despite appearing credible, the email client flags the message and blocks remote content to protect the user from potential trackers or embedded threats. The visual layout includes a call-to-action button and brief descriptions of blog topics. There's no visible malicious link, but a lack of personalization can be noted. The layout and format resemble promotional content. However, the legitimacy of such messages must be verified via backend metadata. The presence of tracking elements or third-party analytics scripts can't be ruled out. Overall, it appears to be a promotional email. This entry sets the context for technical analysis to follow. The visual format mimics typical newsletters used in targeted phishing.

Email Header Analysis



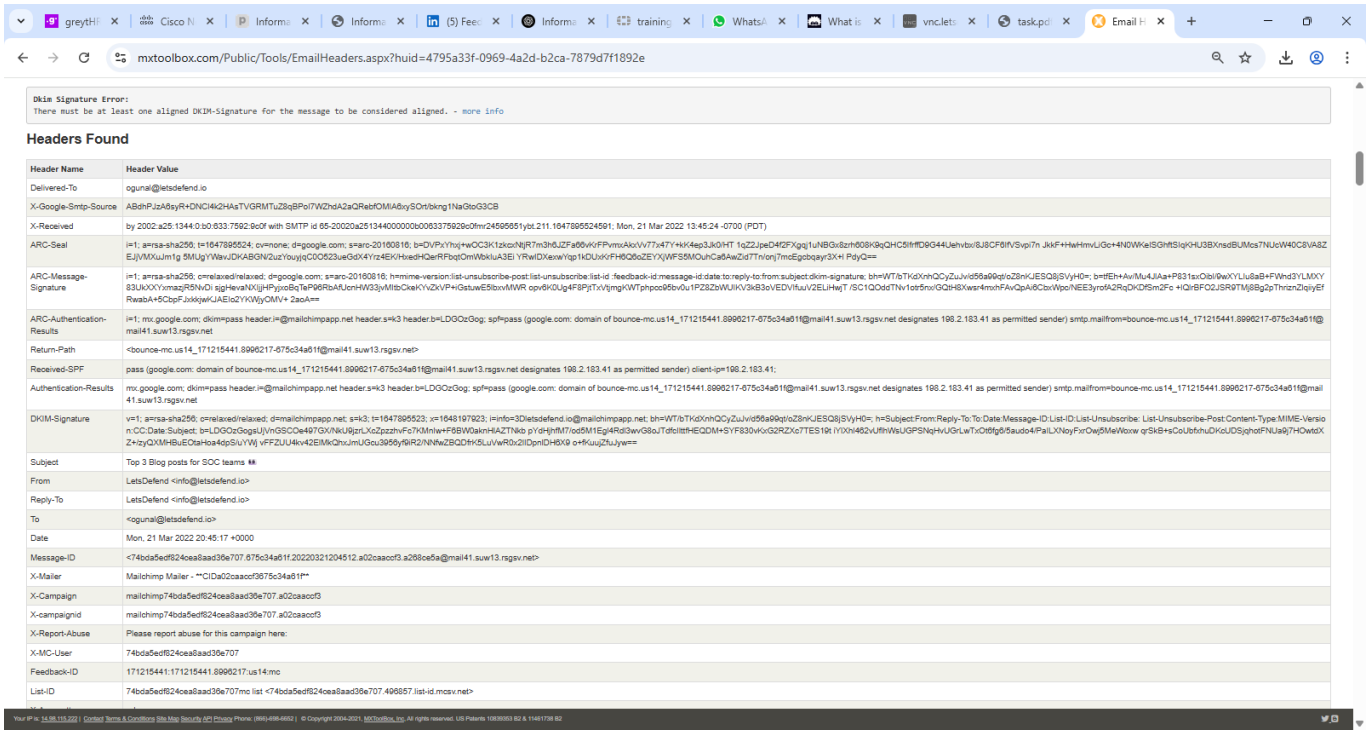
This analysis focuses on the technical metadata of the email. It reveals that while SPF and DKIM passed authentication checks, both failed domain alignment. Consequently, DMARC evaluation failed. This misalignment often occurs when third-party services like Mailchimp send emails on behalf of an organization without full domain integration. The delivery path and DKIM signature point to mailchimpapp.net, not letsdefend.io. Email clients and servers use this information to assess trust. The fail result under DMARC suggests the message could be forged or misconfigured. This makes the message more likely to be flagged or rejected in enterprise filters. Email administrators must configure SPF and DKIM to align precisely. Domain alignment failures are a common vector for spoofing. The result indicates that even legitimate services can produce untrusted messages if setup is incorrect.

SPF/DKIM Record Details



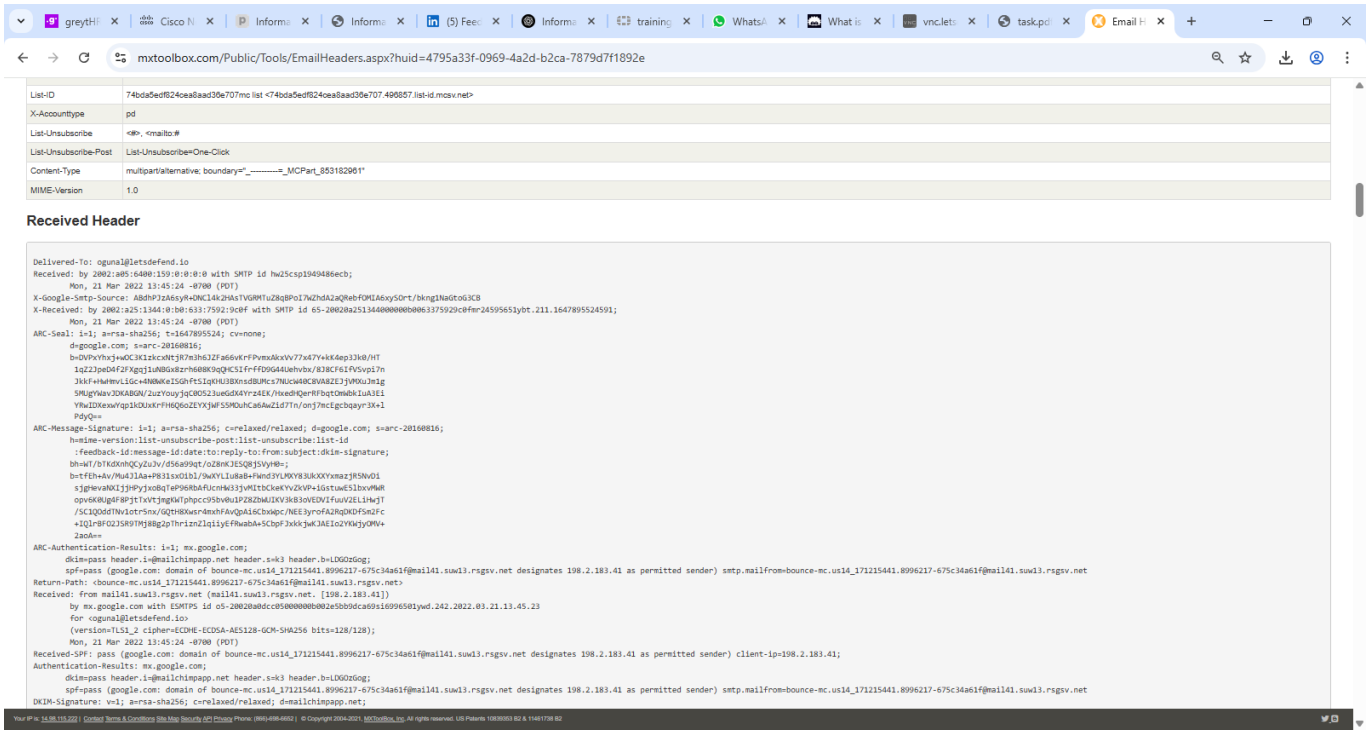
This section isolates the authentication records within the header. It highlights SPF passing through permitted IPs but failing alignment due to the sender domain mismatch. DKIM was signed by mailchimpapp.net, indicating use of an external service. The key takeaway is that DKIM signatures must match the "From" domain to ensure trust. Failure to align SPF or DKIM leads to DMARC failure, weakening sender reputation. This configuration error is exploited in domain spoofing attacks. Even properly signed emails are untrusted if the domain isn't aligned. The key focus here is on DNS-level security protocols. Correct SPF, DKIM, and DMARC policies must align to pass all authentication layers. Organizations using third-party mailers must configure subdomains properly. This ensures alignment and prevents unintentional DMARC failures.

ARC, Return Path, and Delivery Chain



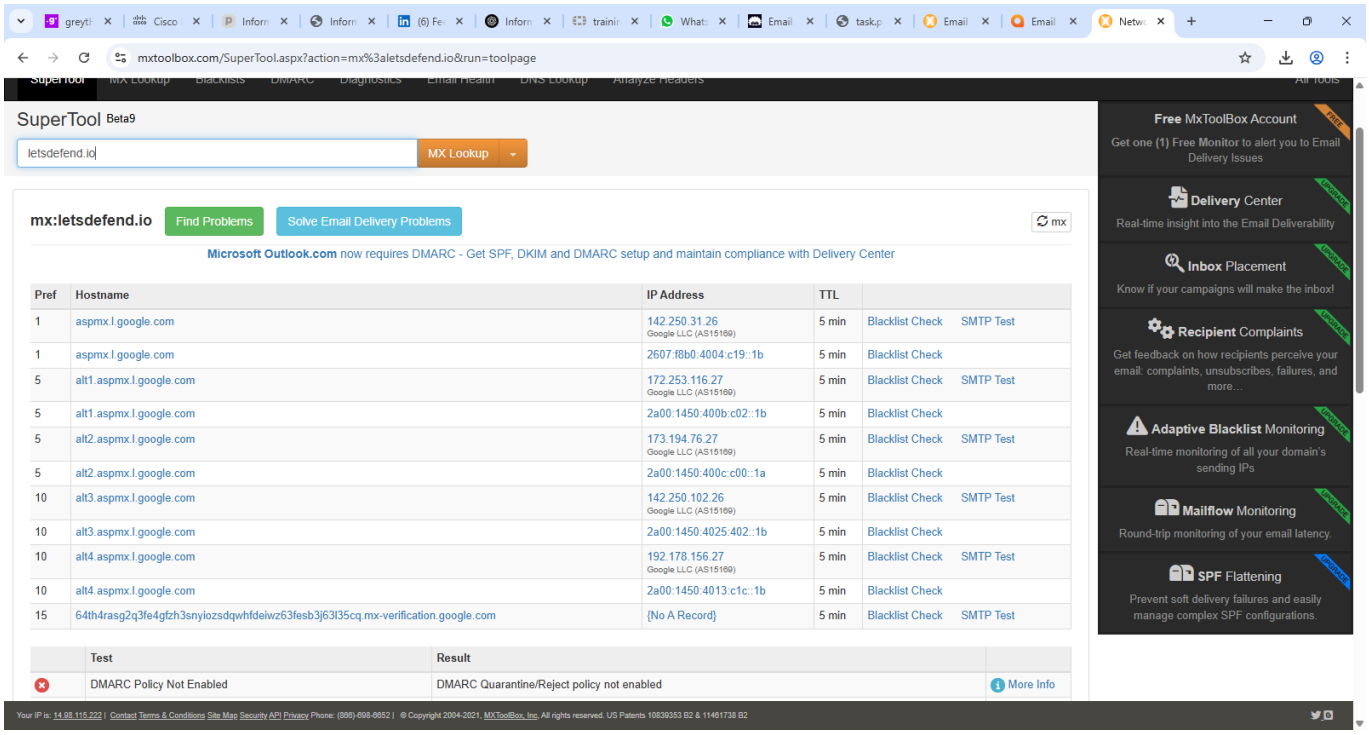
This page shows deep metadata, including ARC-Authentication-Results, Return-Path, and other relaying indicators. It confirms the email's path through relay servers not affiliated with LetsDefend directly. The Return-Path doesn't align with the From address, another sign of spoofing or misconfiguration. ARC fields show that the message passed intermediary validation but may still fail the receiving server's policy checks. This highlights the complexity of email delivery and authentication. Security teams must inspect both visible fields and transport metadata. ARC is particularly useful in forwarding scenarios. It ensures message authentication survives multiple hops. However, misconfigured Return-Path or non-aligned mail servers reduce credibility. Messages must originate from approved and properly configured servers to pass verification. Otherwise, users and security systems cannot fully trust the source.

Received Field Chain



Here we see the complete relay path - the chain of servers the message passed through. It's listed in reverse chronological order. The last server listed is the original sender. The topmost entry shows the final mail server delivering to the inbox. This section proves the message originated from an unexpected domain, not LetsDefend. Relay hops through domains like mailchimpapp.net raise red flags. This field is critical for tracing spoofed or forged emails. It allows analysts to map the true origin of the email. Received chains should always include expected servers. If unknown mail relays appear, the message may have been hijacked or relayed via spoofing. Security systems use these headers to build trust scores. Unexpected IPs reduce message trust and increase the chance of being marked as spam or phishing.

MX Server Details



This section reveals the mail exchange (MX) configuration of the letsdefend.io domain. The domain uses Google's mail infrastructure (aspmx.l.google.com) to send and receive legitimate messages. If a message claims to be from letsdefend.io but comes from any other server (e.g., emkei.cz or an unknown IP like 101.99.94.116), it is clearly forged. This comparison allows analysts to confirm whether an email was truly sent by the organization it claims to represent. If there's no match between the originating IP and the official MX record, spoofing is likely. MX verification is a vital part of email threat hunting. Organizations should regularly monitor and secure their MX settings. Third-party spoofing attempts often bypass DMARC by using unregistered servers. Validating against MX records is a fast way to detect these cases.

Remediation Recommendations

- Enforce strict DMARC policies ('reject' or 'quarantine') for all corporate domains.
- Regularly audit and align SPF and DKIM records with all approved mail services.
- Avoid using third-party mailing tools unless properly authenticated and authorized.
- Implement security awareness training to help users spot spoofed or suspicious emails.
- Utilize secure email gateways to pre-filter suspicious emails using AI and signature-based detection.
- Enable logging and analysis of mail headers in SOC workflows for regular anomaly checks.
- Monitor domain DNS settings via tools like MXToolbox and update them when needed.