👎 Recommendation: Add Native Microsoft Graph API Support for Email Ingestion

To: Ike Owuraku Amponsah - Shadowserver Email Automation

From: National KE-CIRT/CC (cirt@ke-cirt.go.ke)

Date: 1st August 2025

🎯 Objective

Organizations using Microsoft 365 (Office 365) often restrict or completely disable IMAP access for enhanced security and compliance. As a result, critical feeds such as Shadowserver daily reports cannot be ingested using the current IMAP-only design of this tool.

This recommendation proposes integrating Microsoft Graph API as an alternative email ingestion method to improve compatibility and support broader adoption of the tool.

🔎 Justification

1. IMAP Deprecation Trends in Office 365

- - Disabled IMAP/Basic Authentication by default on M365 tenants.
  - Enforced OAuth2 and Graph API as the primary secure communication mechanism for accessing email.
  Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online

2. Shadowserver Dependency on Email-Based Delivery

- The daily Shadowserver feeds are delivered via email with CSV/ZIP/ attachments. These must be accessed reliably regardless of the underlying mail system.

3. Industry Compatibility

- Adding Microsoft Graph enables usage in:
  - CERTs and SOCs with hardened M365 tenants
  - Enterprises with conditional access policies (IMAP blocked)
  - Cloud-based automation pipelines

💮 Recommended Integration

🔐 Microsoft Graph OAuth2 Support

Add optional Graph-based authentication using client_id, tenant_id, and client_secret.

📥 Microsoft Graph Email Fetch Logic

Replace IMAP logic with Microsoft Graph endpoints like:

> ***GET /users/{email}/mailFolders/inbox/messages?$top=50***
> ***GET /messages/{id}/$value***

📦 MIME Parsing

Use email.message_from_bytes() after fetching MIME via Graph API.

🔄 Recommended Code Refactor

1. Modular Email Ingestion Layer

- Auto-selects method based on .env config or CLI arg

2. .env Support

- Extend .env with:
  email_provider=graph
  client_id=xxxx
  tenant_id=xxxx
  client_secret=xxxx

3. Failover

- If Graph fails, log error and optionally fall back to IMAP.

4. Add support for shadowserver emails that lacks attachments because they contain files that are of larger size than what can be sent on email. E.g. Accessible HTTP Reports that contain over 26,000 events


[*Suspicious Email*] [Kenya] Shadowserver Kenya (CSV) Accessible HTTP Report: 2025-07-31

A

Kenya <kenya-bounces@mail.shadowserver.org> on behalf of autoreports@shadowserver.org
To kenya@shadowserver.org

You forwarded this message on 01/08/2025 06:42.

The report content can be obtained from the following link:
https://dl.shadowserver.org/QYKjwiM0RSdyTsaRElZk5mWG_1s?KKE6M7jR7bfxyg_dPIfoPg
The report is 6.4M bytes and contains 26,014 events.
For more information on this report go to: https://www.shadowserver.org/what-we-do/network-reporting/accessible-http-report/

Kenya mailing list
Kenya@mail.shadowserver.org

📌 Benefits Summary

Benefit	Description
🔐 Secure by Design	Uses modern OAuth2 (no plaintext creds)
☁️ Cloud-first Support	Compatible with M365, Azure AD
🧠 Smart Integration	Seamless fallback with existing logic
📈 Wider Adoption	Enables orgs with IMAP-restricted setups

🧪 Conclusion

Adding Microsoft Graph as a supported email backend enhances the usability, compliance, and future-readiness of the Shadowserver automation pipeline.

We’re happy to collaborate or contribute patches if needed. Let us know how we can support this enhancement.