Computer Emergency Response Team of Mauritius

CERT-MU Security Alert

Date of Issue: 20 June 2025

Data Leaks: 16 billion credentials compiled since the beginning of 2025, exposed for Apple, Google, Telegram and Facebook

Description

A massive data leak, potentially the largest in history, has exposed 16 billion records across numerous platforms, including Apple, Google, Telegram and Facebook. Researchers discovered 30 datasets containing billions of login credentials, URLs, and passwords, labeling it a "blueprint for mass exploitation." Experts recommend users enhance their security by switching to passkeys to mitigate risks from phishing and account takeovers.

As per security researchers, these credentials were exposed through data breaches through ”infostealer malware” and “Credential-Stuffing attacks” since early 2025:

The data was likely collected over time and repackaged by a threat actor or researcher before being briefly exposed online.

What Are Infostealers?

Infostealers are a type of malware that infects computers and harvests credentials, browser-stored passwords, crypto wallets, and sensitive data. The stolen information is stored in what’s called an infostealer log — typically in the format:

URL:username:password

These logs are often sold on dark web forums or distributed freely to build credibility within cybercrime communities.

What You Should do to check whether you are impacted:

1. Check if Your Credentials Were Leaked:

   - Use trusted tools like Have I Been Pwned to see if your email or password appears in known data breaches.

2. Look for Unusual Logins or Alerts:

   - Review your recent login activity on key services like Google, Microsoft, Facebook, and banking apps.
   - Check for any “unrecognized device” or “suspicious activity” alerts.

3. Run a Full Malware/Virus Scan:

   - Use a reputable antivirus or anti-malware solution to scan your device.
   - If malware is detected (especially an infostealer), remove it before taking further actions.

4. Change Your Passwords (After Scanning):

   - Change your password to protect your accounts.

5. Enable Two-Factor Authentication (2FA):

   - Turn on 2FA on accounts that support it.
   - Prefer app-based 2FA (e.g., Google Authenticator, Authy) over SMS-based codes.

6. Stay Informed:

   - Follow cybersecurity updates from trusted sources.
   - Be cautious of phishing emails claiming to help you with this breach.

7. Report Concerns to Your IT or Security Team:

   - If you're part of an organization, report any suspicious findings or issues immediately for further investigation.

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org