myNetWatchman

About us
Our mission is to provide the highest fidelity, most timely intelligence aimed at disrupting cyber fraud.

Compromised Email (CompEmail)

Overview

The Compromised Email (CompEmail) APIs are a set of Application Programming Interfaces (APIs) for querying myNetWatchman's data store of compromised email addresses. All of the email boxes in mNW's Compromised Email data set have been successfully accessed (with the correct password) by criminals. Users with compromised email accounts are a higher risk for various types of fraud. User accounts with compromised email addresses are at risk even if the account credentials are secure.

Tactical Uses
- Account Takeover
  - Query customer addresses to identify customers at risk of ATO
  - Discontinue use of email as a secure channel of communication (2FA, password reset, transaction details, etc.)
  - Audit recent account and transaction activity of customers with compromised email accounts
- Elevate risk scores for new and existing customers with compromised email accounts
- Elevate risk scores for accounts at risk for BEC attacks
- Query addresses of high value customers, senior employees, or employees with elevated privileges
- Identify email communications between employees and compromised customers
- Financial Institutions – find compromised accounts linking to P2P payments (e.g. Zelle, Interac)

Operationalizing
- Include as part of periodic customer or internal security audits
- Integrate into your new account signup process

Email mnwsupport@mynetwatchman.com to get started with the CompEmail API in your organization.