UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00194

BRUTE-FORCE ATTACKS SCOURING EMAIL ACCOUNTS

DATE ISSUED: 6th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A "low and slow" attack has been carried out over the past three years scouring popular email platforms attempting to brute-force and compromise email accounts to look for loyalty card, gift cards and rewards that can be stolen and easily resold.

BREAKDOWN

The group is currently attempting to authenticate 5-10 million username/password combinations for email accounts per day with a 0.1% success rate meaning they manage to come away with 50,000-10,000 valid email credentials. The purpose of the attack is to search for what is essentially "cash in your inbox." They will then periodically log in to the victim 's inbox and run scripts to look for digital items of value such as gift cards and loyalty scheme rewards. Attacks of this type is growing as an enterprise as this "cash" or loyalty accounts can be cleaned out, loaded on to a gift card and sold for 80% of its value.

REMEDIATION STEPS

- Use secure password practices to secure your email and all other accounts
  - Non-guessable – no dictionary words, common patterns or phrases easily associated with you
  - Unique – a different password for each account
  - Long – use passphrases rather than words; the longer they are the harder they are to crack.
- Change email passwords if you believe your account has been compromised. Check have I been pwned to check for known compromised accounts https://haveibeenpwned.com/
- Use a password manager to keep track of all your unique passwords.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/attacks-inboxes-gift-card/169187/