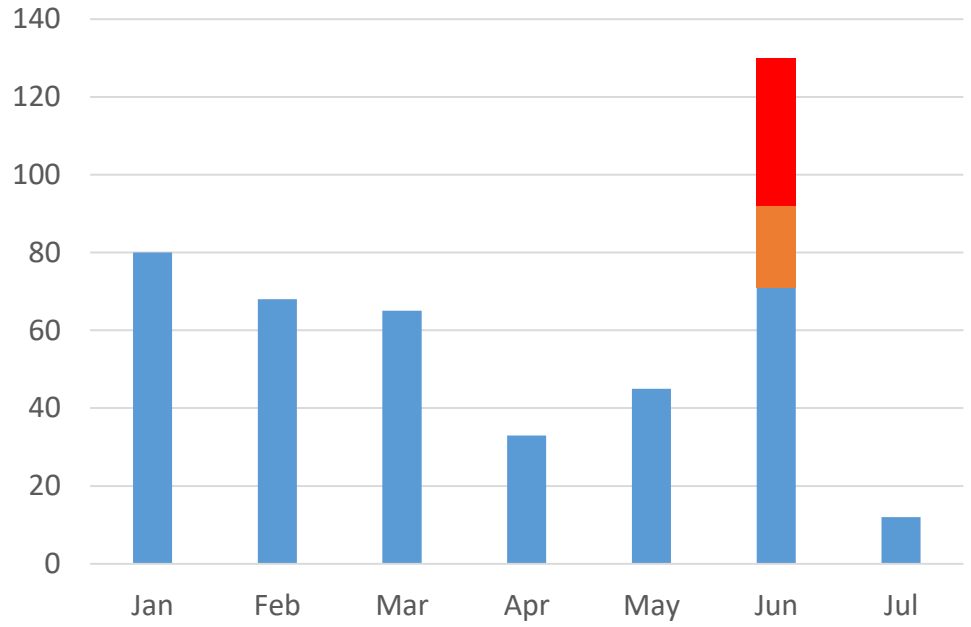
Cause of the June Blacklisting

- Phishing attacks in June caused a large number of account compromises including 38 in a single day
- The amount of mail sent from the large number of compromised accounts in a short period of time caused our servers to be blacklisted



Course of Action

- For years IST has been utilizing several scripts that analyze message tracking logs in Exchange and reports on senders that exceed a threshold of messages
- These accounts are locked, and restricted from sending mail in Connect
- This is an ‘After the fact’ action and a large amount of damage has already been done.
- Most recently we have added subject line(s) to a rule that will quarantine matching messages and prevent further damage, these are actively monitored and released if deemed legitimate.

What we have done to be proactive?

- Message Rate Throttling
- Dailiy Recipient Limits
- Multi Factor Authentication for Outlook Web App
- Office 365 Connector

Future Considerations…

- Outbound Email Sanitization – Currently our inbound message route has two levels of message sanitization:
    - SPAM Assassin and ClamAV on Mxer
    - ProofPoint SPAM and malprotection
  - It has been discussed to place the ProofPoint email protection on the outbound route as well
  - This will assist in protecting our IP address reputation by stopping unwanted messages before they leave campus
- End User Training