Zachary Ducker
University of Maryland University College

A Historical Based Approach to Email Threat Prevention

Learn from the past to prevent the future attack.

Problem Statement and Goals

A commonly used external threat vector that is widely successful in exploiting users is email. Phishing, a form of social engineering that usually relies on the communication power of email, is used as a means to place malicious code on a user's endpoint. Two of the most pervasive tactics are either persuading the email recipient to click on a hyperlink that leads to an exploit laced web page, or convincing the user to open an attached file that performs malicious actions. Many compromised systems can have their primary source of attack traced back to a single inbound email message.

The goal of using historical information is to limit the amount of malign emails that reach the inboxes of end users. The purpose of presenting context based graphical information to the user is to easily and quickly aid them in formulating a decision regarding the nature of any unfamiliar email messages and accompanying attachments.

Approach

The modern approach to email security involves the use of reputational databases for mail exchangers and the scanning of embedded hyperlinks and attachments. While these remain relevant methods; the likelihood of detecting and preventing email-borne threats increases by incorporating the use of historical data gleaned from previous email and web activity. Information stemming from emails previously sent from within an organization to an external address as well as web browsing activity related to the domain of incoming email messages is analyzed to determine the significance of their correlation value. For email without historical data, graphical information is displayed before delivering the uncertain email. These graphics (logos, brands, images from the associated domain) assist the user in deciding whether or not the email may be a threat. If the user deems it not to be a threat they choose if they want the email delivered to their inbox. Static images are prepared from any attachments; this generates a preview for the user to review. This visual representation is not capable of running code on the endpoint since it is formatted correctly and created with the organization's security tools.

Results and Future Work

A preliminary review of malicious inbound emails to a commercial enterprise showed that no internally initiated contact had taken place. A query was performed to list the senders of one hundred known malicious emails. This list of senders was transformed into a list of recipients, and a search was conducted for any outbound email to them within a thirty day period. The results showed that the malicious emails were sent from email addresses which were not listed in past email transactions in the last thirty days. To guard against the threat of account takeover where an adversary controls a trusted sender's account; attachments and links are at first opened in a monitored, virtual machine space accessible by the user. If no malicious activity occurs, the links and attachments can be opened directly from the user's endpoint. Future research calls for the testing of users' choices after showing them related graphics for unknown email.

RSAConference Security Scholar

A Historical Approach to Email Threats

Learn from the past to prevent the future attack

Zachary Ducker
University of Maryland University College

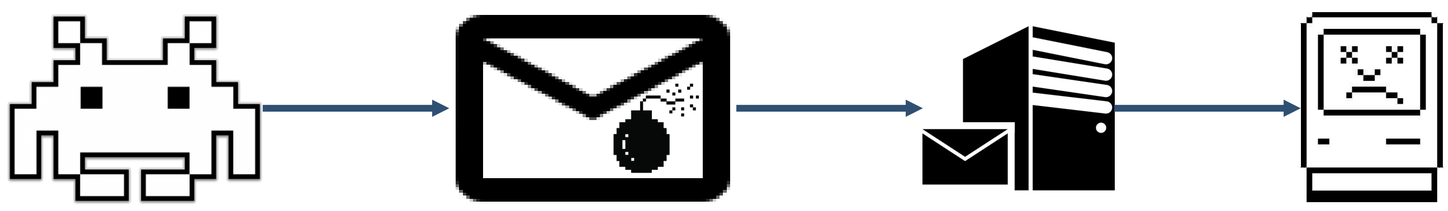
Problem Statement and Goals

External threats often find their way in via email by manipulating users' trust and curiosity.

Emails with exploit-laden attachments and malicious hyperlinks can lead to compromise.

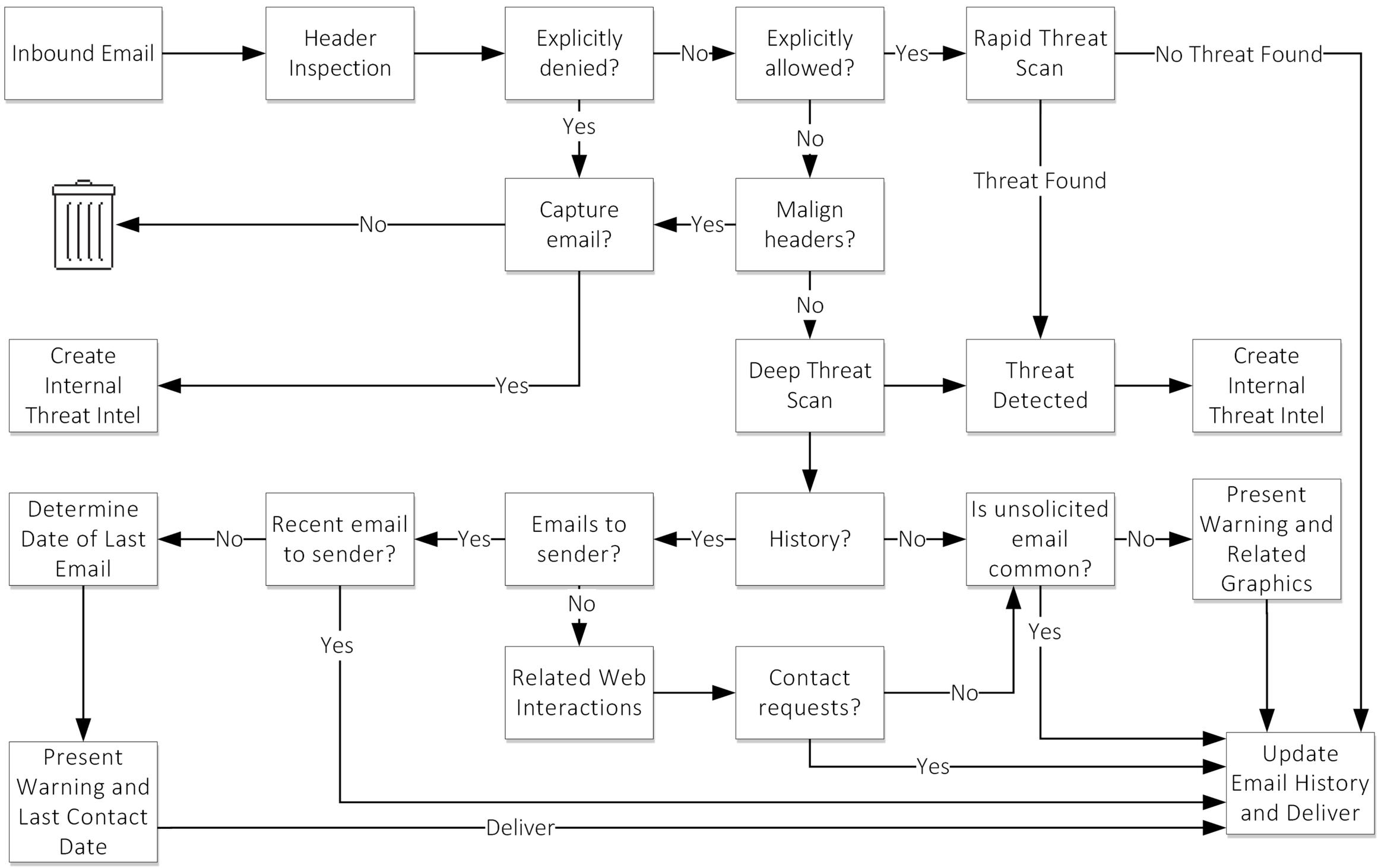
Sensitive data can become inadvertently exposed by responding to nefarious requests found within emails.

The goal is to drastically reduce the amount of risky emails reaching the end users.



Approach

Past email transactions and web browsing history of users within an organization can be used to ascertain the legitimacy of the email. For email without historical data; graphics related to it and its domain will aid the user in deciding its validity.



Going Forward

Plans include fine-tuning the historical information pulled from available sources. A future possibility is the sharing of aggregated and anonymized data across organizations via a central data repository that tracks email senders and domains across specific business sectors. This information would help determine the relevance and risk score of emails.