The Threat of Unintended URLs

Motivation

• Accounts with high follower counts have posted unintended URLs: @kanyewest (30.6M), @RudyGiuliani (714.2K), @urbandictionary (300.1K).
• Retweeting mechanism combined with existing followers leads to a substantial audience for tweets.
• None of the tested platforms have methods in place to detect unintended URLs.

Threat Model

Bob follows Alice on Twitter. Alice posts an unintended URL. Mallory registers this URL and points it to a malicious server. Bob clicks on this link and gets exposed to malicious content.

Methodology

Automatically Detecting Unintended URLs on Twitter

• We developed a machine learning model to predict unintended URLs. We used a Support Vector Machine classifier with linear kernel and the model accuracy is 93.3%.
• We set up a pipeline that collects daily tweets and makes unintended domain predictions.
• We registered these domains if possible, to record the requests.
• We implemented a crawler that clusters these domains to determine any malicious activity.

Mitigation

We developed a Chrome extension that uses our unintended URL classifier to predict unintended URLs and warn users when they try to post a tweet.

Evaluation

We ran our automated detection framework for 7 months and collected 26,596 unintended URLs.

• 72% of unintended URLs are non-existent.
• 42.3% of the webpages in our dataset (40% being parking domains previously shown to host malicious content) could expose users to potentially dangerous and unwanted content.

Bob follows Alice on Twitter. Alice posts an unintended URL. Mallory registers this URL and points it to a malicious server. Bob clicks on this link and gets exposed to malicious content.

URL | Author | Followers
--- | --- | ---
thing.it | Oprah | 42M
SEE.YOU | Harry_Styles | 34M
Kobe.Osaka | Harry_Styles | 34M

Scan QR code for Chrome extension.