

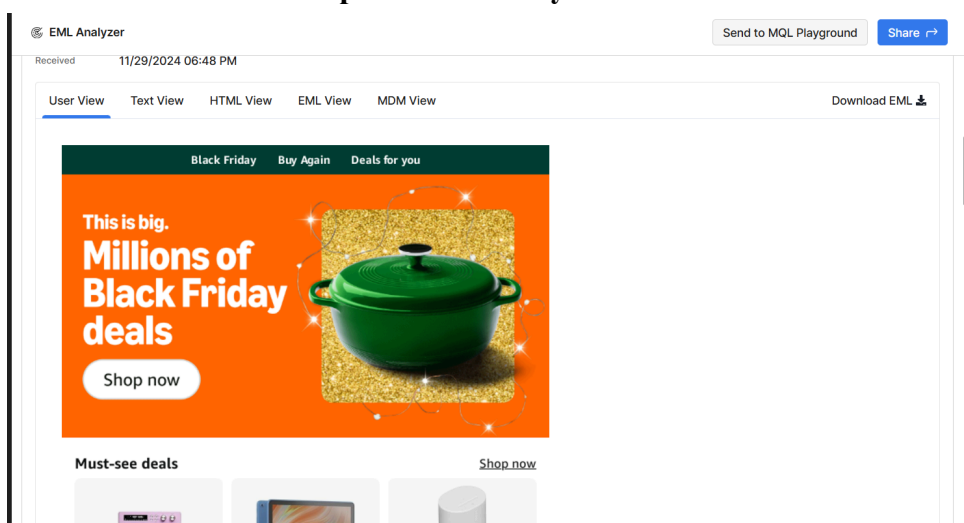
Project: Phishing Analysis

Clay Jones

Objective:

Pull down a github repo containing live phishing email samples in a ubuntu environment and use tools such as URL scan and Sublime Security to decide whether or not it is a phishing attempt or not. Afterward a report will be made on the findings.

Email 1: A Simple Black Friday Email from Amazon



Investigation:

Attack Score Learn more ⓘ Note: Attack Score is most accurate in the Sublime product since it uses organization context and history

Attack Score Verdict

Likely Benign Currently in BETA

Message Details

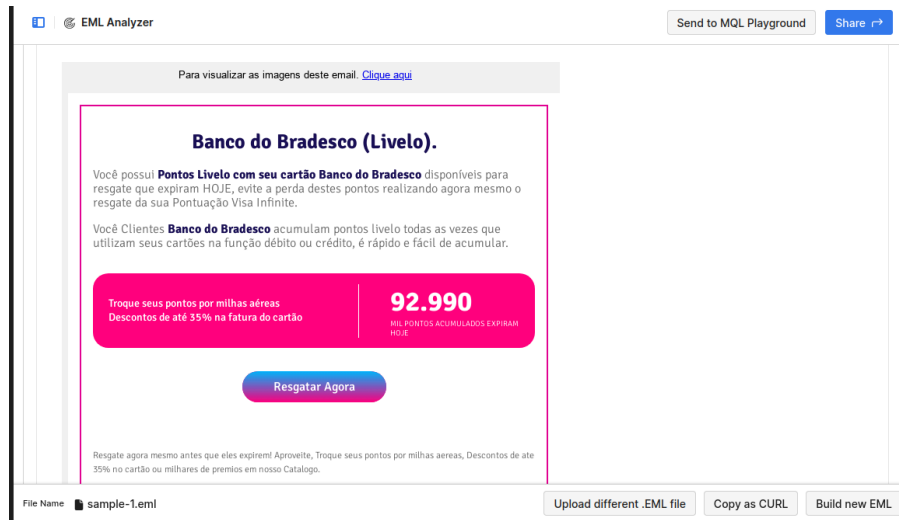
Message Insights (10)

Mismatched Sender (From) and Return-Path: 202411292129368ce5a...	Domains in body (2): www.amazon.com amazon.com
Domains in headers (3): e252-41.smtp-out.amazonses.com	High trust sender domain: store-news@amazon.com
Links in body (60): https://www.amazon.com/gp/r.html?C=3L28BW37...	Message-ID: <0100019379d44fc2-baf4144c-393b-48bc-83d0-6a...
Return-Path: 202411292129368ce5aba3867848ee9ab8b3d46610p...	Sender domain registrar: MarkMonitor Inc.
Sender Prevalence: new	UTC offset of sender: 0

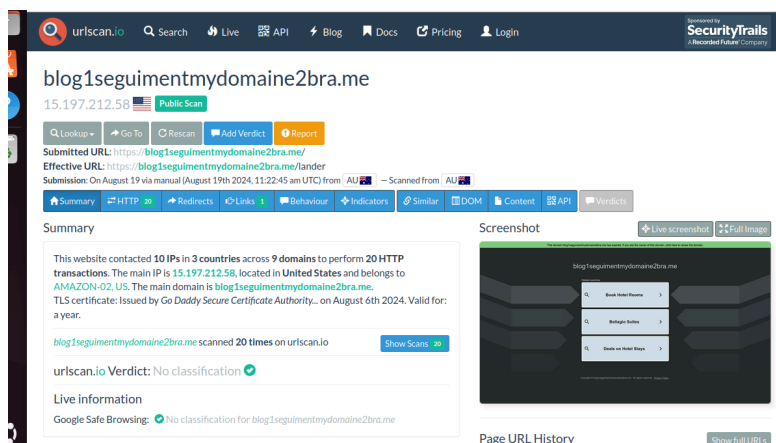
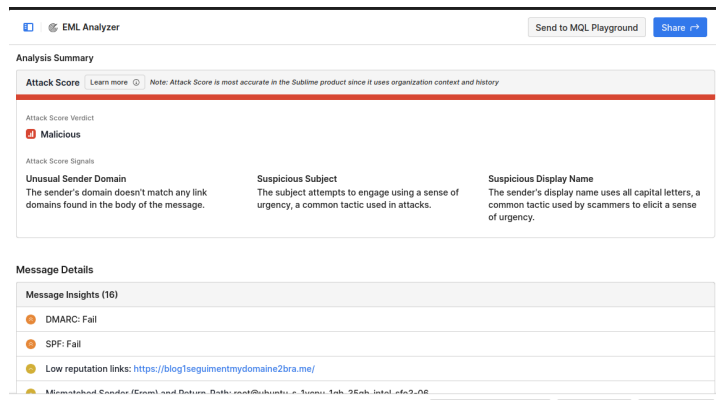
Conclusion:

This email is harmless because amazon.com is a registered, known, and safe domain. This email was sent to my own mailbox. It was included because I wanted to test if the tools worked.

Email 2: A email from a Brazilian banking service



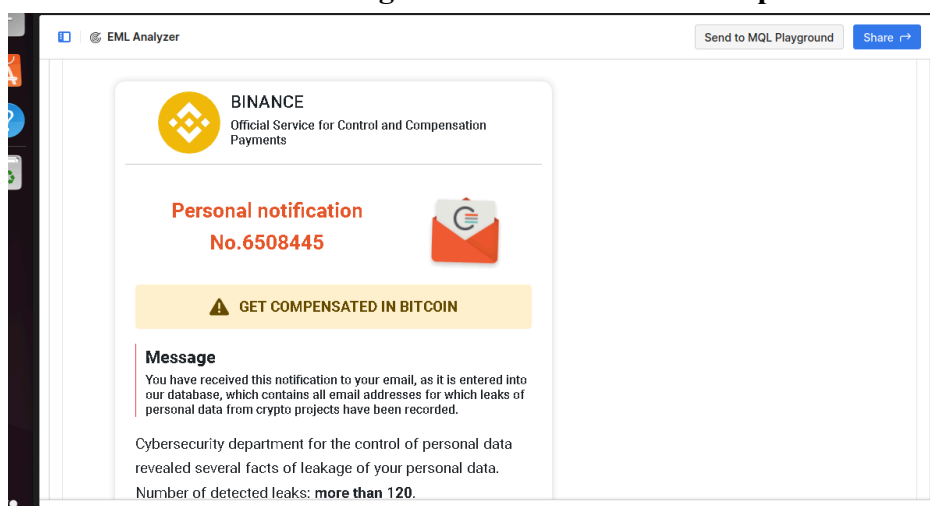
Investigation:



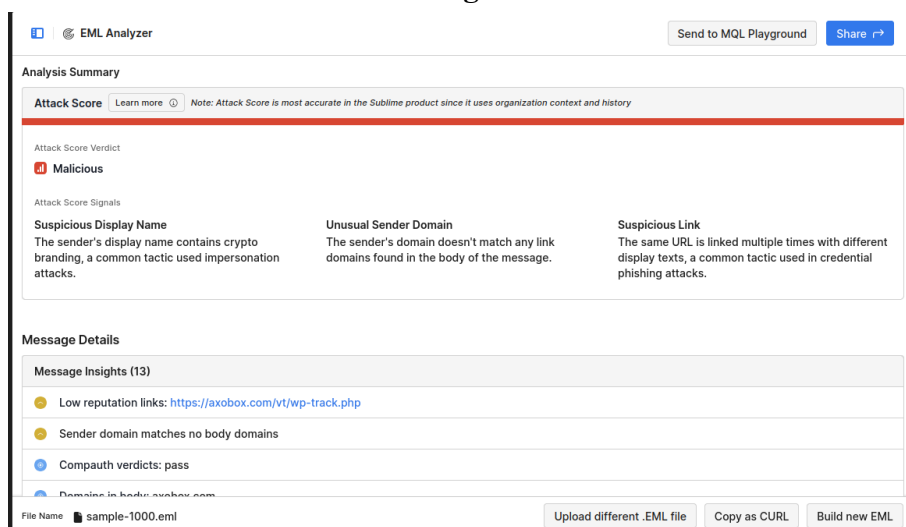
Conclusion:

Conclusion is that this email is a phishing attempt. This email is impersonating a Brazilian banking service. This is proven because of the unusual sender domain, suspicious subject, and the low link reputation.

Email 3: Email claiming information has been compromised



Investigation:



Conclusion:

Conclusion is that this is likely a phishing attempt. The social engineer is using a hoax to get the recipient to act. This is likely phishing because of the suspicious display name, unusual domain, suspicious link, and having the same url linked multiple times.