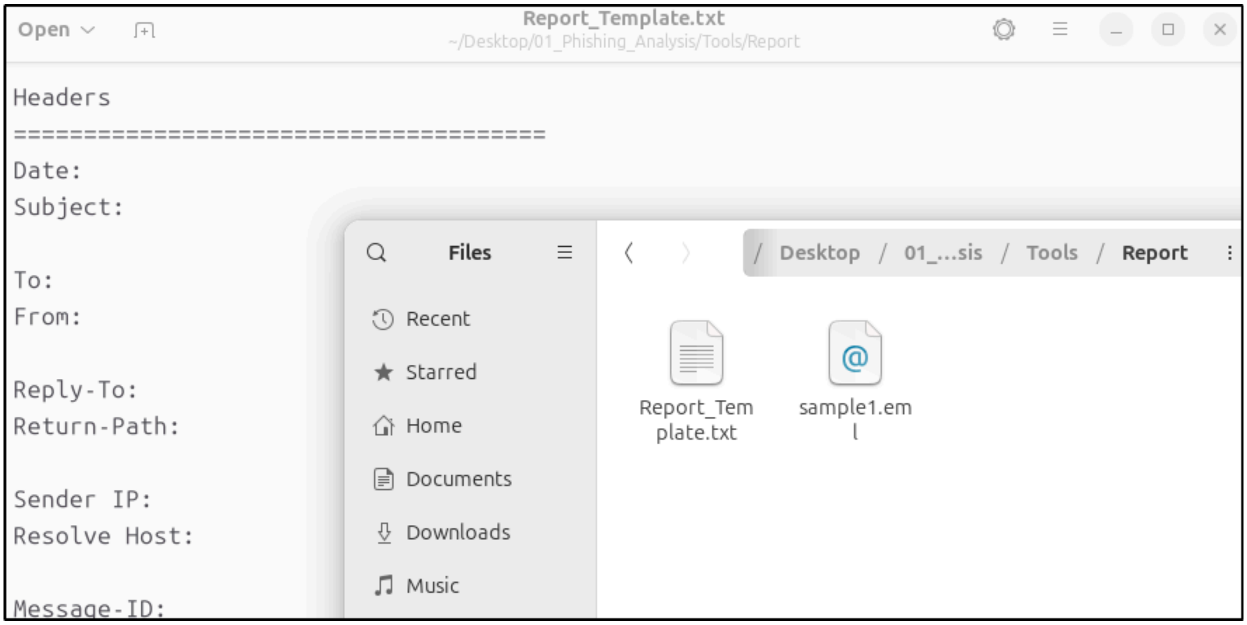
Documentation and Reporting

Accurate and thorough documentation is the most important part in investigating and responding to phishing emails. Documentation makes sure all actions should be tracked, and it justifies any response actions taken. It also provides a reference for future incidents and it helps in the continuous improvement of the SOC processes. However, we also want to make sure notes are kept clear, relevant and concise. Organizations often have templates and automated functions to assist in writing concise and consistent documentation in tickets. The exact method for documentation is something that depends on the organization, but this section explains some general information on what is important to include.

Collect artifacts in the form of IoCs. IoCs in this case are any artifacts that can be attributed and linked to an attack, in this case for a phishing email. Then we'll want to analyze these artifacts so we can get evidence that supports our verdict and conclusion. Once a verdict has been reached, defensive actions taken or recommended need to be documented as well.

The course provides a report template with sections for Headers, URLs, Attachments, Description, Artifact Analysis, Verdict and Defence Actions. There is also a sample eml file that we can use to write a report about.



```
Headers
======================================
Date:
Subject:

To:
From:

Reply-To:
Return-Path:

Sender IP:
Resolve Host:

Message-ID:
```

Use screenshots to document tool output and findings from analyses. This is considered best practice.

Sample Report

Headers

==
Date: Fri, 16 Sep 2022 19:20:13
Subject: Re: Reminder: [Activity Report] Your account is sign in on a new device. Friday, September 16, 2022 #[636274168]

To: asmith@hotmail.com
From: cafepress@mail.cafepress.com

Return-Path: msprvs1=XjGVrJidPKaSN=bounces-098020-32419@tbh51blx.imdreampores.ovh

Sender IP: 209.85.221.104
Resolve Host: mail-wr1-f104.google.com

Message-ID:
<Ti6MiLxTCWMiAH1sP7JxbGrEJIqKsD3Nv4CKIa8Mwrs@mail-pf1-f420.googlegroups.com>

URLs
==
hxxps[://]cabinetlekagni[.]com/

Description
==
The email claims to be from Amazon support, and is asking to verify the account due to a suspicious login.

There are several indications of urgency: It claims to have put the Amazon account on hold, cancelled pending orders, and that the account will be permanently suspended if no action is taken by the next day.

Artifact Analysis
==
Sender Analysis:
Although the email body claims to be from Amazon Prime, the From address in the header is unrelated to Amazon.

Additionally, the Return-Path and Received headers indicate that this email originated from a google.com mail server, and also uses OHV Cloud hosting technology, neither of which are affiliated with amazon.

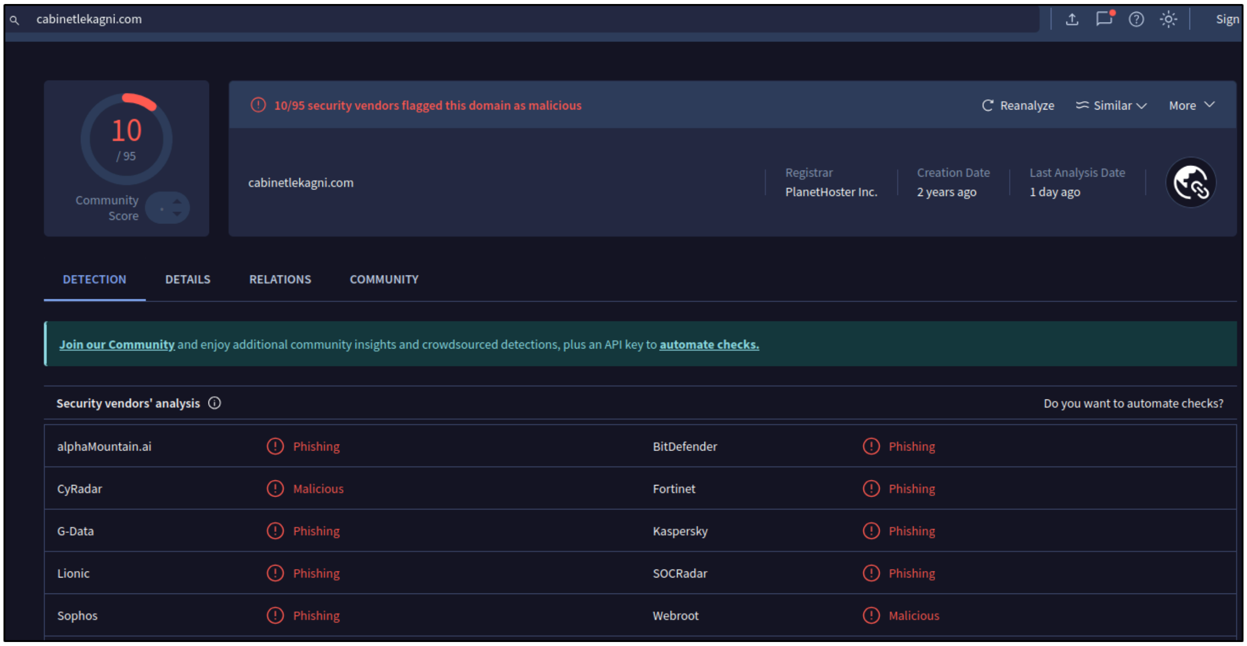
URL Analysis:

After performing a URL reputation check on VirusTotal, the URL embedded into the call to action button of this email was found to be malicious, as it redirects to a phishing website.

Attachment Analysis:
No files were attached to this email.

Verdict
==
Due to the sender being unaffiliated with Amazon, this email is a clear impersonation and spoofing attempt.

Additionally, after analyzing the URL contained in the email's call to action, it was flagged on VirusTotal to be malicious.



10/95 security vendors flagged this domain as malicious

cabinetlekagni.com

Registrar: PlanetHoster Inc.
Creation Date: 2 years ago
Last Analysis Date: 1 day ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	BitDefender	Phishing
CyRadar	Malicious	Fortinet	Phishing
G-Data	Phishing	Kaspersky	Phishing
Lionic	Phishing	SOCRadar	Phishing
Sophos	Phishing	Webroot	Malicious

As a result of the analysis, this email has been determined to be malicious.

Defense Actions
==
After performing a message trace, no other users within the organization received an email from this sender or with a similar subject line.

To prevent the malicious sender from sending any other email to the organization, I have blocked the "cafepress@mail.cafepress.com" email address on the email gateway.

Due to the malicious nature of the domain, I have blocked any incoming emails that contain “cabinetlekagni[.]com” on the email gateway.

To ensure users are unable to access this malicious URL or domain, I have blocked “cabinetlekagni[.]com” on the EDR and on the Web Proxy.

Additional Phishing Practice

Phishing Pot by Corvo is a collection of real phishing samples that were collected with honeypot email accounts. This is a great resource for research, to practice analysing real-world phishing emails, and to practice writing reports.

PhishTank is a collection and database of live suspected phishing ULRs.

MalwareBazaar is a database of malware provided by the threat intelligence community.

Summary

Professional phishing incident documentation requires systematic collection and analysis of indicators of compromise (IoCs), supported by clear evidence and structured reporting. The documentation process follows a standard template covering headers, URLs, attachments, artifact analysis, verdict determination, and defensive actions taken. Best practices include using screenshots for evidence preservation, defanging malicious URLs for safe handling, and providing specific implementation details for recommended controls. Effective reports translate technical findings into business-relevant conclusions while maintaining detailed audit trails for compliance and continuous improvement purposes. The combination of thorough analysis with clear communication ensures that technical expertise translates into organizational security enhancement.