

## Phishing Analysis Report

---

### Headers

---

Date: Fri, 16 Sep 2022 19:20:13 +0000

Subject: 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

Reply-To:

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

Sender IP: 209.85.221.104

Resolve Host: mail-wr1-f104.google.com

Message-ID: <Ti6MiLxTCWMiAH1sP7JxbGrEJlqKsD3Nv4CKla8Mwrs@mail-pf1-f420.googlegroups.com>

### URLs

---

hxps[://]cabinetlekagni[.]com/

## **Description**

---

---

This email is claiming to be from amazon prime and it's asking the receipts to verify their account.

It claims that account has been placed on Hold due to suspicious login.

There are several indications of urgency within the content of this email. As it claims the account will be suspended by “September 17, 2022” if the account is not verified by then

## **Artifact Analysis**

---

---

Sender Analysis:

Although claiming to be from amazon prime, the from address clearly indicates a mailbox originating from an unrelated domain.

Additionally, the return-path and received headers indicate that this email originated from google.com mail server and also utilized OVH cloud hosting technology, neither of which are affiliated with Amazon.

URL Analysis:

After performing URL reputation check using URLs can and Virus Total, the URL within the call-to-action button of this email was found to be malicious, as it redirects to a phishing website.

It appears to be hosting a credential capture page, that when submitted, will log and steal the credentials of any victims

## Verdict

---

Due to the original 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 of action, it was flagged on URL scan and Virus total to be malicious.

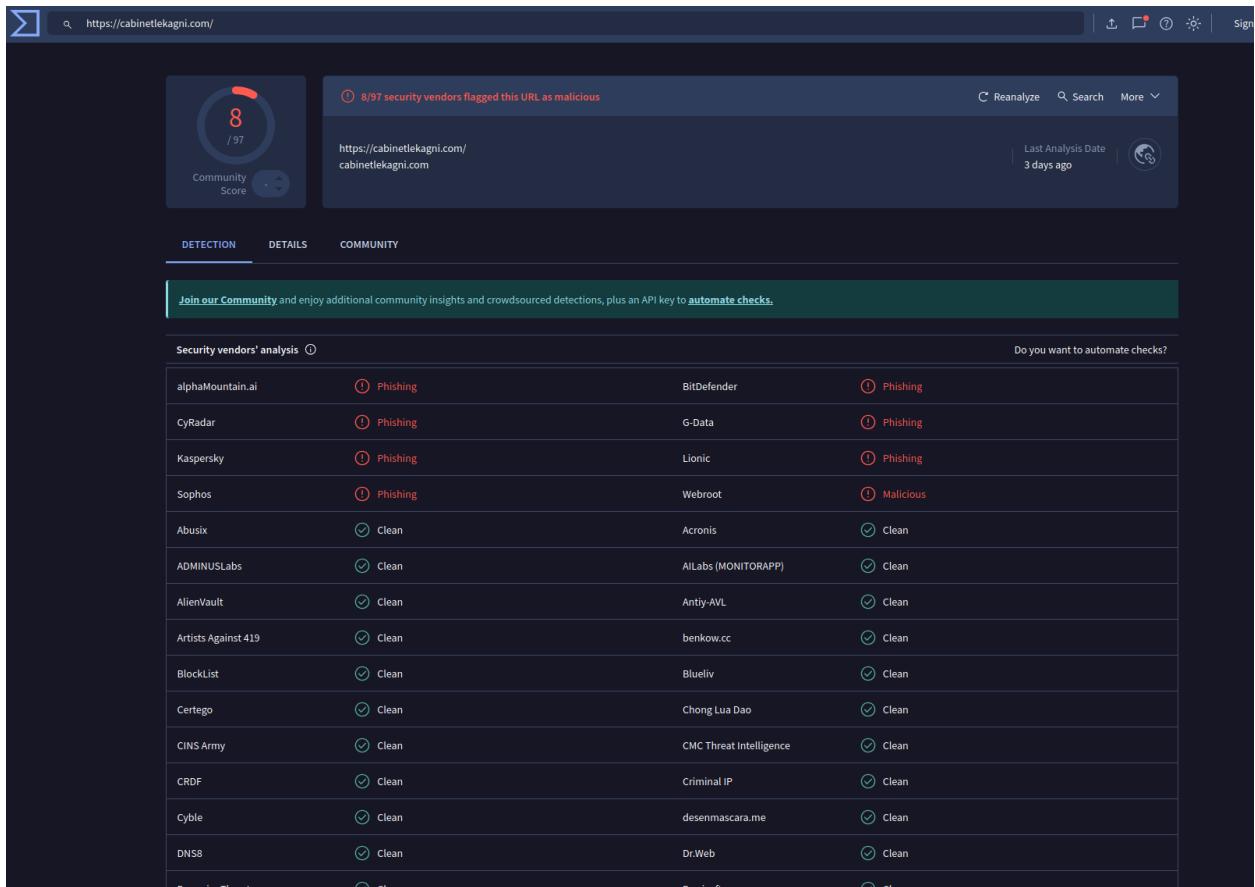


Figure 1 Virus total analysis

sbffidbserv.sviluppo.host

149.62.187.89 | Malicious Activity! [Private Scan](#)

Submitted URL: <https://cabinetlekagni.com/>  
 Effective URL: <https://sbffidbserv.sviluppo.host/s/Dose/signin.php>  
 Submission: On May 17 via manual (May 17th 2024, 6:52:14 pm UTC) from CA - Scanned from FR

[Summary](#) [HTTP 9](#) [Redirects](#) [Behaviour 0](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

This website contacted 3 IPs in 4 countries across 4 domains to perform 9 HTTP transactions. The main IP is 149.62.187.89, located in Italy and belongs to COLTENGINE COLTENGINE Network, IT. The main domain is sbffidbserv.sviluppo.host.

TLS certificate: Issued by R3 on May 16th 2024. Valid for: 3 months.

This is the only time sbffidbserv.sviluppo.host was scanned on urlscan.io!

urlscan.io Verdict: Potentially Malicious [?](#)

Targeting these brands: [Schweizerische Bundesbahnen \(Transportation\)](#)

Screenshot

Live information

Figure 2 URLScan.io verdict

## Defense Actions

---

After performing a message trace, no other user within the organization received an email from this sender or with this subject line.

To prevent the malicious sender from sending any other email to the organization, I have blocked the [cafepress@mail.cafepress.com](mailto: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 the URL on the EDR and on the Web Proxy