

Name : Amr Khaled Elgendy  
Group : AMIT - Cyber Security Online 87  
Task : Real Siem Alerts

---

## Alert 1 – SOC Investigation Report

Event ID : 59

Sender: hahaha@ihackedyourcomputer.com

Recipient: mark@letsdefend.io

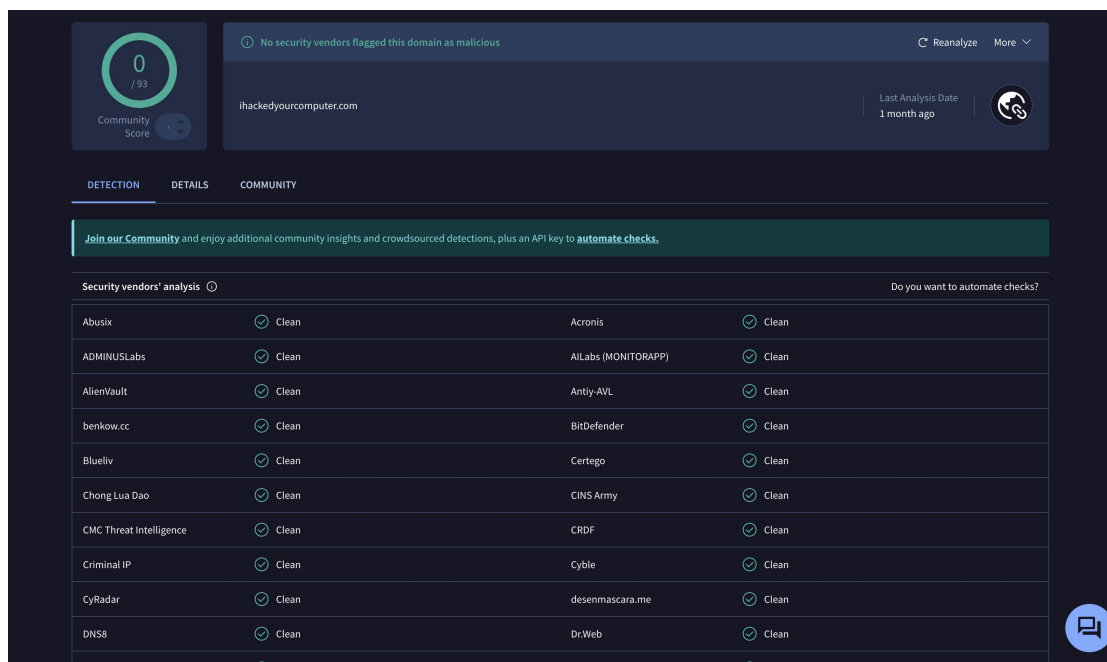
Subject: I hacked your computer

Date : Feb, 14, 2021, 03:00 AM

---

A SOC101 – Phishing Mail Detected alert was generated by the Exchange email security system, indicating a suspicious email attempt.

Initial reputation checks showed that the sender domain was not flagged as malicious by security vendors. However, further analysis of the email content revealed a classic sextortion scam pattern that relies on fear-based social engineering rather than technical compromise.



The screenshot displays the VirusShare domain analysis interface for the domain **ihackedyourcomputer.com**. At the top, a green circle indicates a "Community Score" of 0/93. A message states: "No security vendors flagged this domain as malicious." The "Last Analysis Date" is "1 month ago". Below this, a table titled "Security vendors' analysis" shows results from 20 different vendors, all of which are "Clean".

Security vendors' analysis	
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
benkow.cc	Clean
Blueliv	Clean
Chong Lua Dao	Clean
CMC Threat Intelligence	Clean
Criminal IP	Clean
CyRadar	Clean
DNS8	Clean
Acronis	Clean
AILabs (MONITORAPP)	Clean
Antiy-AVL	Clean
BitDefender	Clean
Certego	Clean
CINS Army	Clean
CRDF	Clean
Cyble	Clean
desenmascara.me	Clean
Dr.Web	Clean

The message contained no URLs, attachments, or malware indicators, and no evidence of system compromise was found. The email targeted a single user only, with no signs of wider distribution.

The email was blocked automatically by the email security gateway, and no user interaction occurred.

The incident was confirmed as a **true positive scam email**, successfully contained, and closed with **no impact** to the user or organization.

---

## Alert 2 – SOC Investigation Report

Event ID: 34

Sender: admin@netflix-payments.com

Recipient: emily@letsdefend.io

Subject: Netflix Deals!

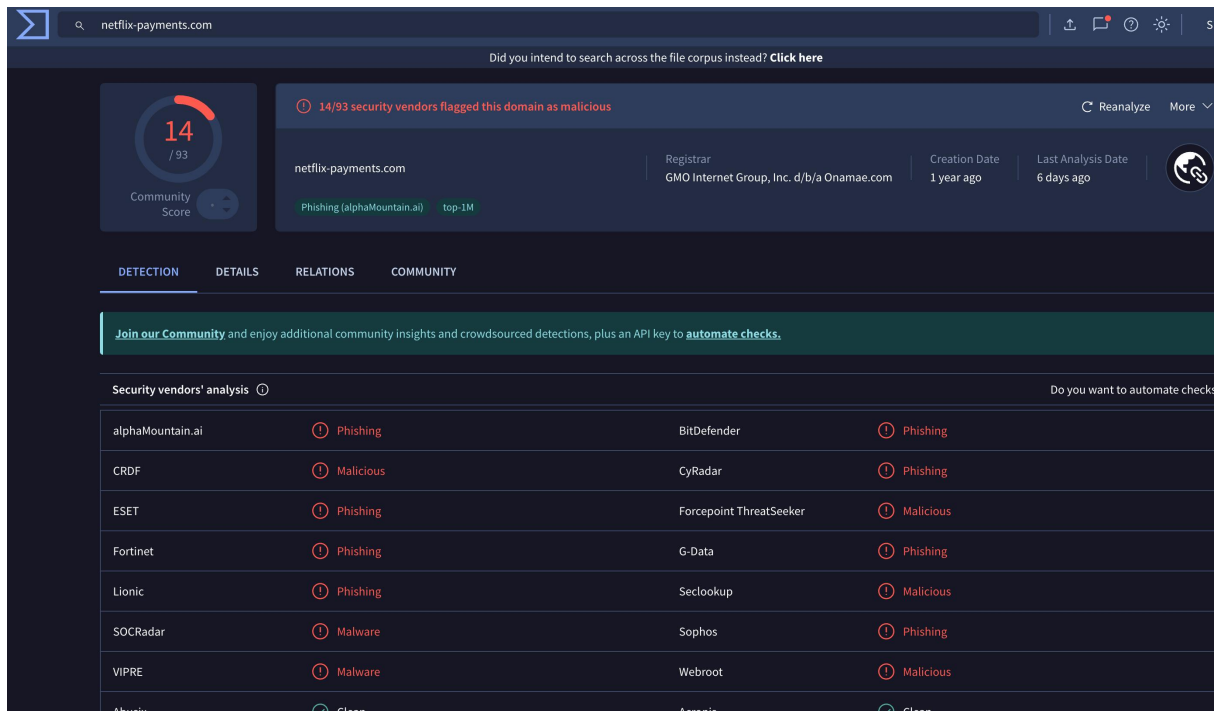
Date: Dec 05, 2020 – 10:33 PM

---

A phishing alert (SOC101 – Phishing Mail Detected) was generated by the Exchange email security system after a suspicious email was delivered to the user.

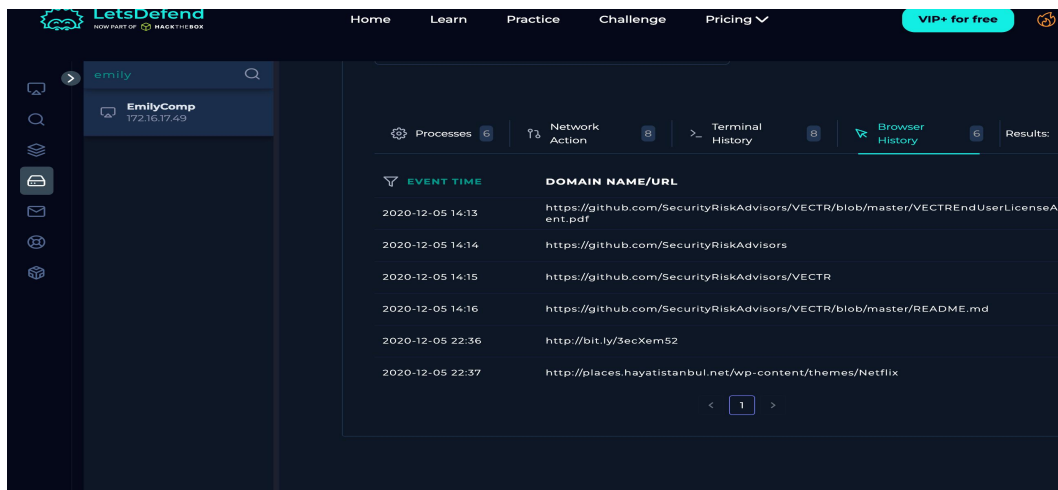
The email originated from an external sender using IP address **112.85.42.180**, and the sender domain was identified as impersonating the legitimate Netflix brand.

Content analysis revealed the use of brand impersonation and promotional wording commonly observed in phishing campaigns, including a malicious URL designed to redirect the user to a fake Netflix login page.



Scope analysis confirmed the email was delivered to a single user only, with no evidence of additional recipients or internal spread.

User activity review confirmed interaction with the email at 10:36 PM, indicating potential credential exposure.



The incident was confirmed as a **true positive**. The sender domain, SMTP source IP, and all associated malicious URLs were blocked. The affected user's credentials were reset as a precautionary measure, user awareness was advised, monitoring was enhanced, and the alert was closed with potential exposure noted.

## Alert 3 – SOC Investigation Report

Event ID: 27

Sender: ndt@zol.co.zw

Recipient: susie@letsdefend.io

Subject: UPS Your Packages Status Has Changed

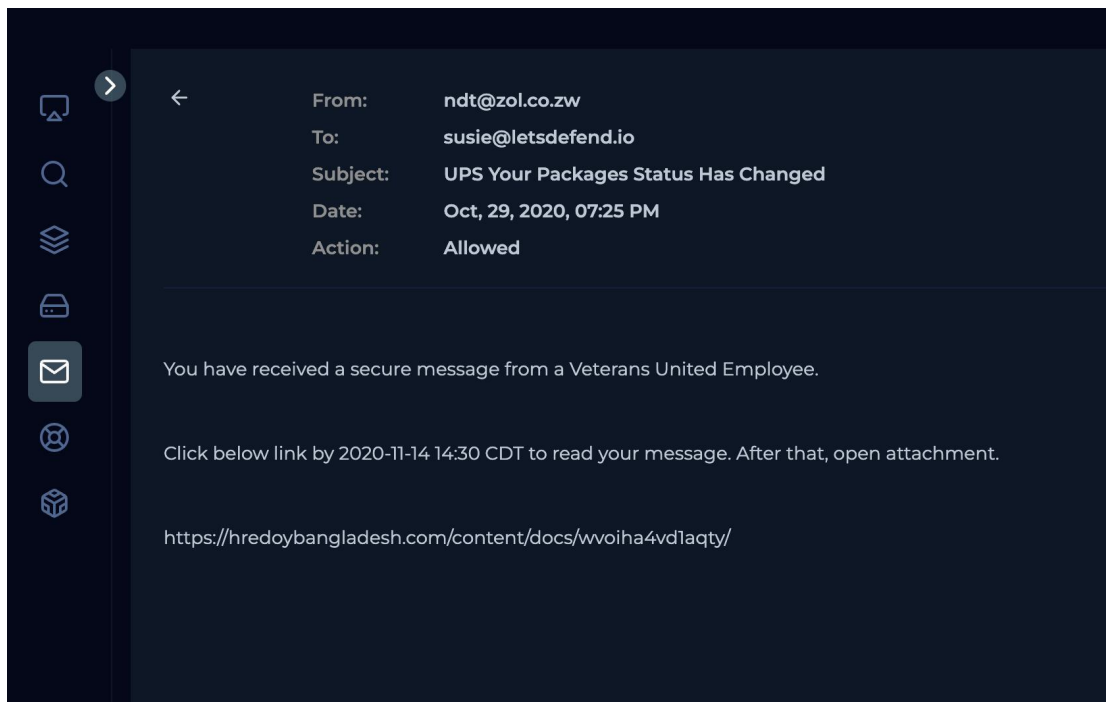
Date: Oct 29, 2020 – 07:25 PM

---

A phishing alert (SOC101 – Phishing Mail Detected) was generated by the Exchange email security system, indicating a phishing attempt. The email was automatically blocked by the security control.

The email originated from an external sender using IP address **146.56.209.252**. The sender domain does not belong to UPS and was identified as suspicious based on impersonation behavior.

Content analysis showed the subject line impersonates a well-known shipping company (UPS), which is a common phishing technique used to lure users into interacting with malicious content.



https://hredoybangladesh.com/content/docs/wvoih4vd1aqty/

10/94 security vendors flagged this URL as malicious

Community Score: 10 / 94

10/94 security vendors flagged this URL as malicious

https://hredoybangladesh.com/content/docs/wvoih4vd1aqty/

hredoybangladesh.com

Last Analysis Date: 5 days ago

DETECTION DETAILS COMMUNITY 6

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

Categories

alphaMountain.ai	Malicious (alphaMountain.ai)
BitDefender	porn
Dr.Web	known infection source
Sophos	spyware and malware
Webroot	Dead Sites
Forcepoint ThreatSeeker	malicious web sites

History

First Submission	2020-10-16 00:14:11 UTC
Last Submission	2026-02-01 17:24:12 UTC
Last Analysis	2026-02-01 17:24:12 UTC

HTTP Response

Final URL

https://hredoybangladesh.com/content/docs/wvoih4vd1aqty/

urlscan.io

hredoybangladesh.com

23.29.122.203

URL: https://hredoybangladesh.com/content/docs/wvoih4vd1aqty/

Submission: On November 05 via manual (November 5th 2020, 3:51:58 pm) from US

Summary HTTP Behaviour Indicators Similar DOM Content API

Summary

This website contacted 1 IPs in 1 countries across 1 domains to perform 1 HTTP transactions. The main IP is 23.29.122.203, located in Tampa, United States and belongs to HVC-AS, US. The main domain is hredoybangladesh.com. TLS certificate: Issued by cPanel, Inc. Certification Authority on October 5th 2020. Valid for: 3 months.

hredoybangladesh.com scanned 13 times on urlscan.io

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: Malicious for hredoybangladesh.com

Current DNS A record: 23.29.122.203 (AS29802 - HVC-AS, US)

Domain created: October 2nd 2020, 08:00:42 (UTC)

Domain registrar: PDR Ltd. d/b/a PublicDomainRegistry.com

Domain & IP information

IP/ASNs	IP Detail	SubDomains	Domain Tree	Links	Certificates
1	IP Address	AS Autonomous System			
1	23.29.122.203	29802 (HVC-AS)			

Screenshot

No Screenshot

Detected technologies

LiteSpeed (Web Server)

Stats

1	0	0	100%	0%
Requests	Ad-blocked	Malicious	HTTPS	IPv6
1	1	1	1	0
Domains	Subdomains	IPs	Countries	Transfer

Scope assessment confirmed that the email targeted a single user only, with no evidence of wider distribution across the organization.

User interaction review confirmed that the email was blocked before delivery and no user interaction occurred.

The incident was confirmed as a **true positive**, successfully contained, and closed with no impact on users or systems.

## Alert 4 – SOC Investigationx Report

Event ID: 8

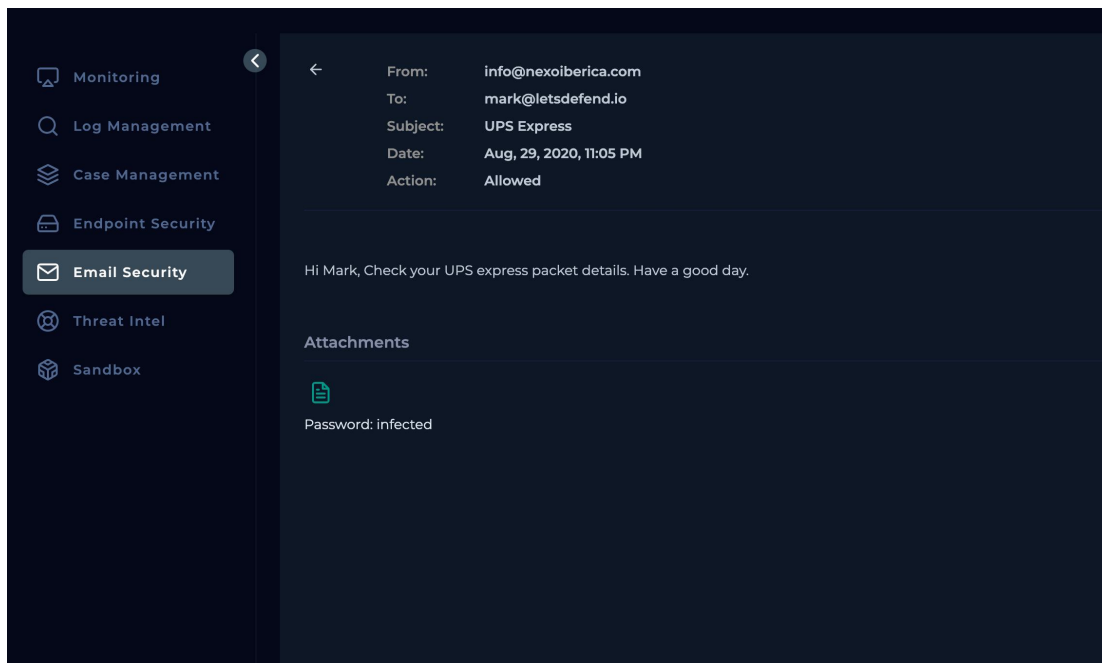
Sender: info@nexoiberica.com

Recipient: mark@letsdefend.io

Subject: UPS Express

Date: Aug 29, 2020 – 11:05 PM

A phishing alert (SOC101 – Phishing Mail Detected) was triggered by the Exchange email security system, indicating a potential phishing email. The email was allowed and delivered to the user.



The email originated from an external sender using IP address **63.35.133.186**. The sender domain is not associated with UPS and was identified as suspicious due to brand impersonation.

Email content analysis showed the subject line impersonates a legitimate shipping service (UPS), a common technique used in phishing campaigns to gain user trust.

Scope assessment confirmed the email targeted a single user only, with no indication of wider distribution within the organization.

User interaction review showed that the email was delivered successfully. No confirmed interaction was observed; however, potential user exposure cannot be ruled out.

The incident was confirmed as a **true positive phishing attempt**. User awareness was recommended, monitoring was advised, and the alert was closed.

