

Name : Amr Khaled Elgendi  
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 shows a detailed security analysis report for the domain `ihackedyourcomputer.com`. At the top, it states "No security vendors flagged this domain as malicious". Below this, the domain name is listed. On the right, there are buttons for "Reanalyze" and "More". A timestamp indicates the "Last Analysis Date" was "1 month ago".

The main section is titled "Security vendors' analysis" and lists 21 vendors, each showing a "Clean" status with a green checkmark icon. The vendors include Abusix, ADMINUSLabs, AlienVault, benkow.cc, Blueliv, Chong Lua Dao, CMC Threat Intelligence, Criminal IP, CyRadar, DNS8, Esenmascara, F-Secure, Fortinet, G DATA, Google Safe Browsing, Hesecu, Kaspersky, McAfee, Microsoft, Norton, Oracle, Qihoo 360, Symantec, Trend Micro, and Webroot. There is also a "Community Score" card on the left with a score of 0/93.

At the bottom, there is a button labeled "Do you want to automate checks?" and a blue circular icon with a white play symbol.

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.

The screenshot shows a security analysis interface for the domain `netflix-payments.com`. At the top, a circular "Community Score" icon displays a red "14" out of 93. A message indicates that 14/93 security vendors flagged the domain as malicious. Below this, the domain name is listed along with its registrar (GMO Internet Group, Inc. d/b/a Onamae.com), creation date (1 year ago), and last analysis date (6 days ago). Navigation tabs include DETECTION, DETAILS, RELATIONS, and COMMUNITY. A green banner encourages joining the community for additional insights. The main content area is titled "Security vendors' analysis" and lists findings from various vendors:

Vendor	Category	Result
alphaMountain.ai	Phishing	Phishing
CRDF	Malicious	Phishing
ESET	Phishing	Malicious
Fortinet	Phishing	Phishing
Lionic	Phishing	Malicious
SOCRadar	Malware	Phishing
VIPRE	Malware	Malicious
Abusix	Clean	Clean
BitDefender	Phishing	Phishing
CyRadar	Phishing	Phishing
Forcepoint ThreatSeeker	Malicious	Malicious
G-Data	Phishing	Phishing
Seclookup	Malicious	Malicious
Sophos	Phishing	Phishing
Webroot	Malicious	Malicious
Acronis	Clean	Clean

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 screenshot shows a network monitoring interface for a user session named "EmilyComp" (IP 172.16.17.49). The left sidebar includes icons for Home, Learn, Practice, Challenge, Pricing, and VIP+ for free. The main panel displays event history and browser history. The browser history section shows the following timeline:

Event Time	Domain Name/URL
2020-12-05 14:13	https://github.com/SecurityRiskAdvisors/VECTR/blob/master/VECTREndUserLicenseAgreement.pdf
2020-12-05 14:14	https://github.com/SecurityRiskAdvisors
2020-12-05 14:15	https://github.com/SecurityRiskAdvisors/VECTR
2020-12-05 14:16	https://github.com/SecurityRiskAdvisors/VECTR/blob/master/README.md
2020-12-05 22:36	http://bit.ly/3ecXemS2
2020-12-05 22:37	http://places.hayatistanbul.net/wp-content/themes/Netflix

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

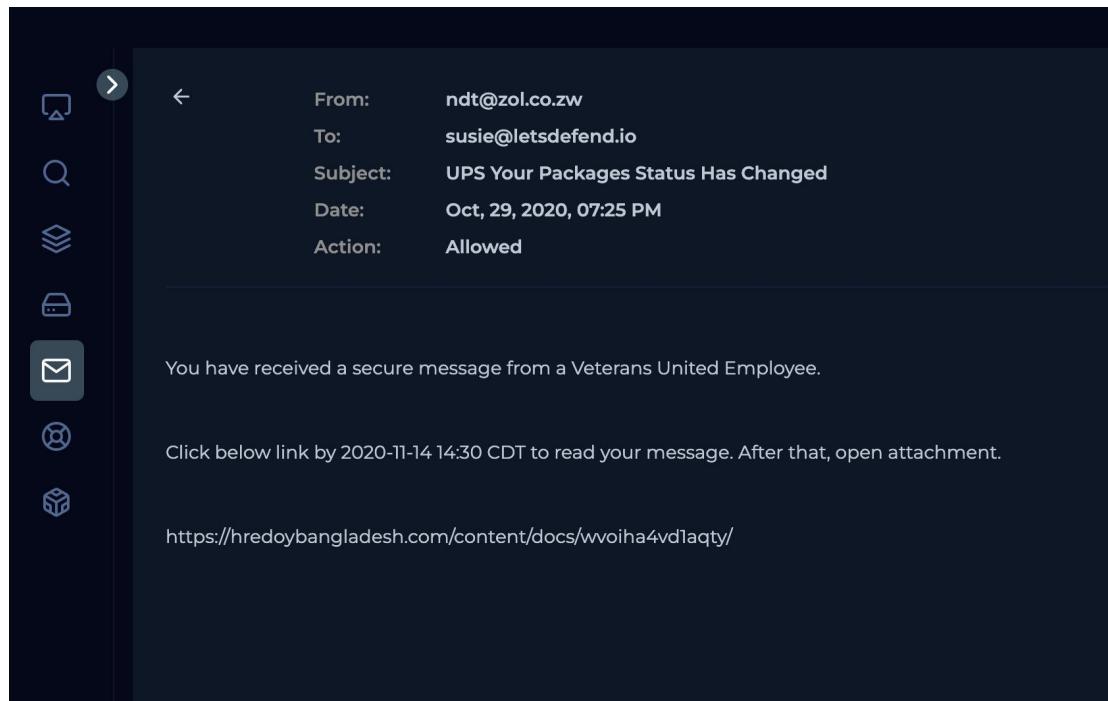
Date: Oct 29, 2020 – 07:25 PM

---

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.



The screenshot shows the VirusTotal analysis page for the URL <https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/>. The page displays a community score of 10/94, indicating 10 out of 94 security vendors flagged the URL as malicious. The last analysis date is 5 days ago. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY (with 6 items). A call-to-action encourages joining the community for additional insights and API keys. Below the main summary, there are sections for Categories (listing various vendor detections like alphaMountain.ai, BitDefender, DrWeb, Sophos, Webroot, and Forcepoint ThreatSeeker) and History (showing first submission on 2020-10-16 and last analysis on 2026-02-01 at 17:24:12 UTC).

The screenshot shows the urlscan.io analysis page for the domain [hredoybangladesh.com](https://hredoybangladesh.com). The domain is identified as malicious. The page shows 13 scans performed by urlscan.io. There is no screenshot available. Detected technologies include LiteSpeed (Web Servers). The page also provides domain and IP information, showing 1 IP/ASN (23.29.122.203) and 1 Autonomous System (29802 (HVC-AS)). Statistics show 1 request, 0 ad-blocked, 0 malicious, 100% HTTPS, 0% IPv6, 1 domain, 1 subdomain, 1 IP, 1 country, and 0 kB 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

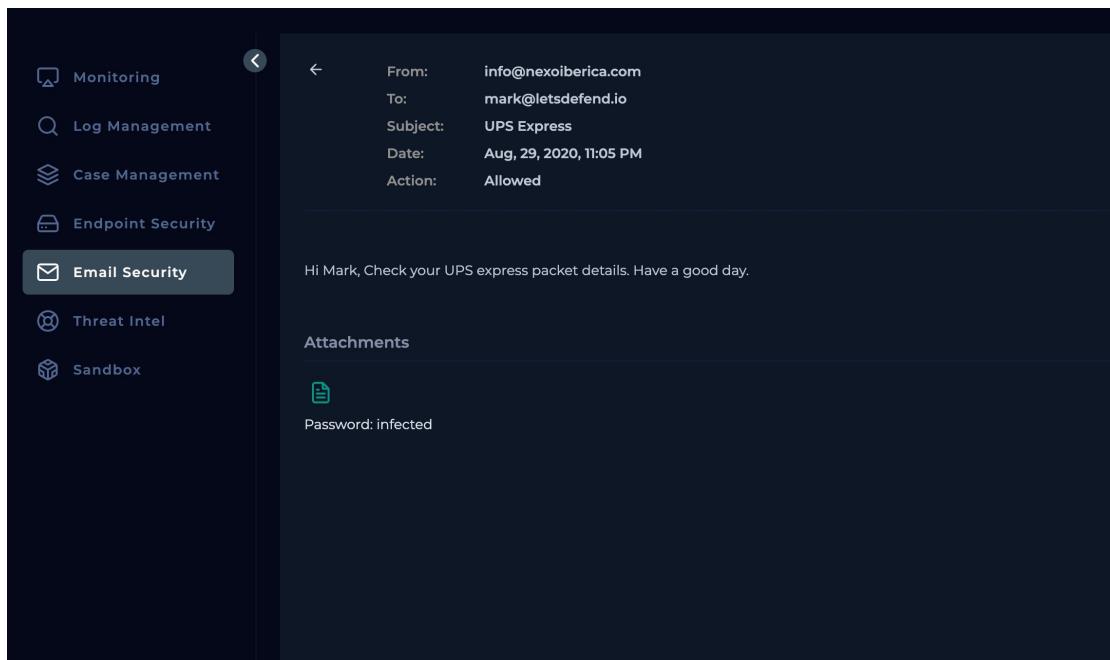
Recipient: mark@letsdefend.io

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.

