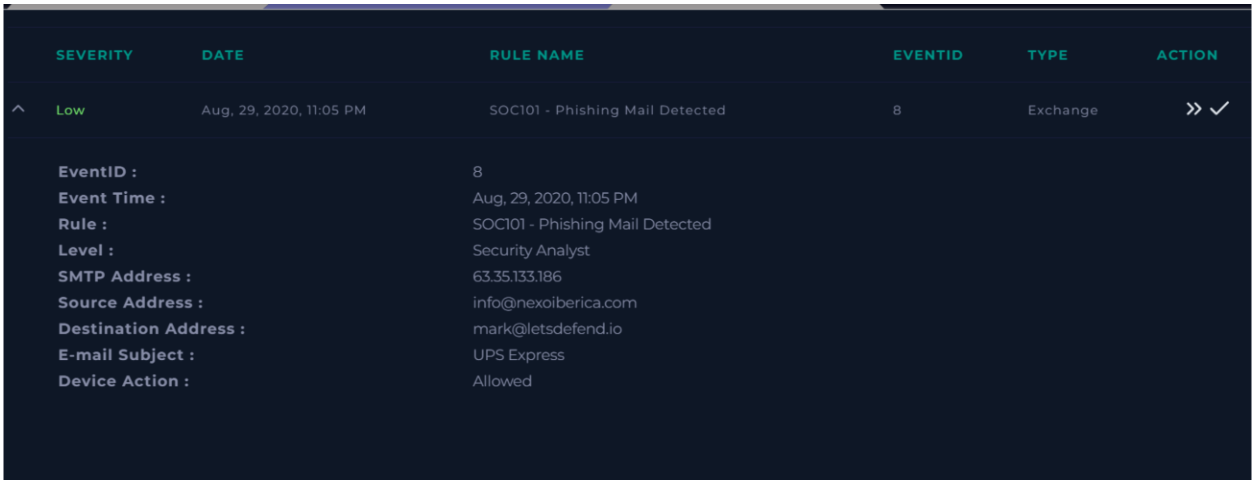
Soc101 – phishing mail Detected

task ID -8



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Low	Aug, 29, 2020, 11:05 PM	SOC101 - Phishing Mail Detected	8	Exchange	» ✓

EventID :	8
Event Time :	Aug, 29, 2020, 11:05 PM
Rule :	SOC101 - Phishing Mail Detected
Level :	Security Analyst
SMTP Address :	63.35.133.186
Source Address :	info@nexoiberica.com
Destination Address :	mark@letsdefend.io
E-mail Subject :	UPS Express
Device Action :	Allowed

Incident Overview:

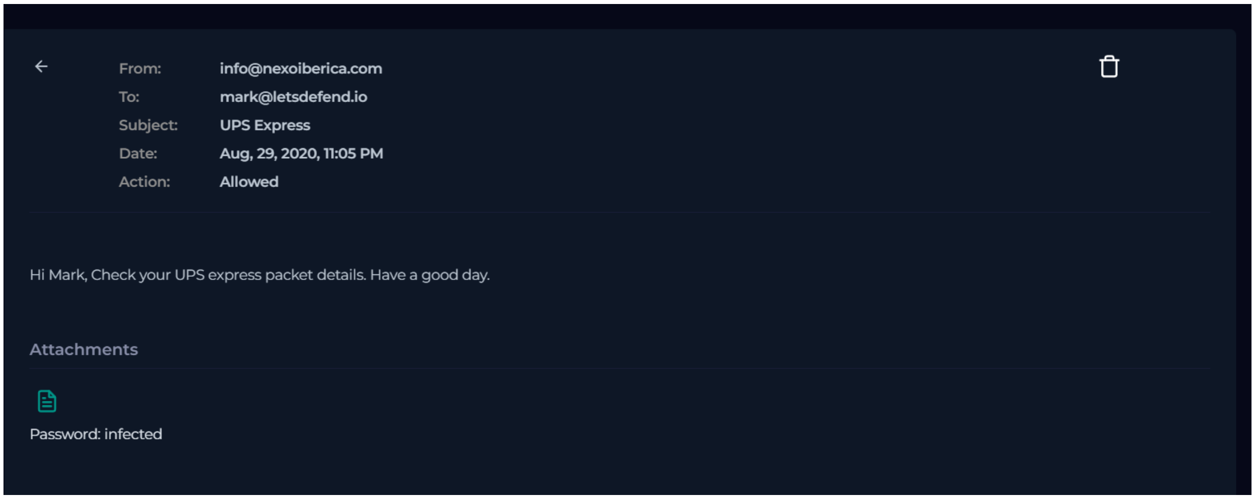
Email Details

SMTP Address: 63.35.133.186

Sender Address: info@nexoiberica.com

Recipient Address: mark@letsdefend.io

Email Subject: UPS Express



From: info@nexoiberica.com
To: mark@letsdefend.io
Subject: UPS Express
Date: Aug, 29, 2020, 11:05 PM
Action: Allowed

Hi Mark, Check your UPS express packet details. Have a good day.

Attachments

Password: infected

The email body contained minimal text intended to appear legitimate and non-suspicious:

"Hi Mark, Check your UPS express packet details. Have a good day."

The message included a password-protected attachment and a download link, a common technique used by threat actors to bypass email security scanning.

Attachment password displayed within the email:

Password: infected

Malicious URL Analysis

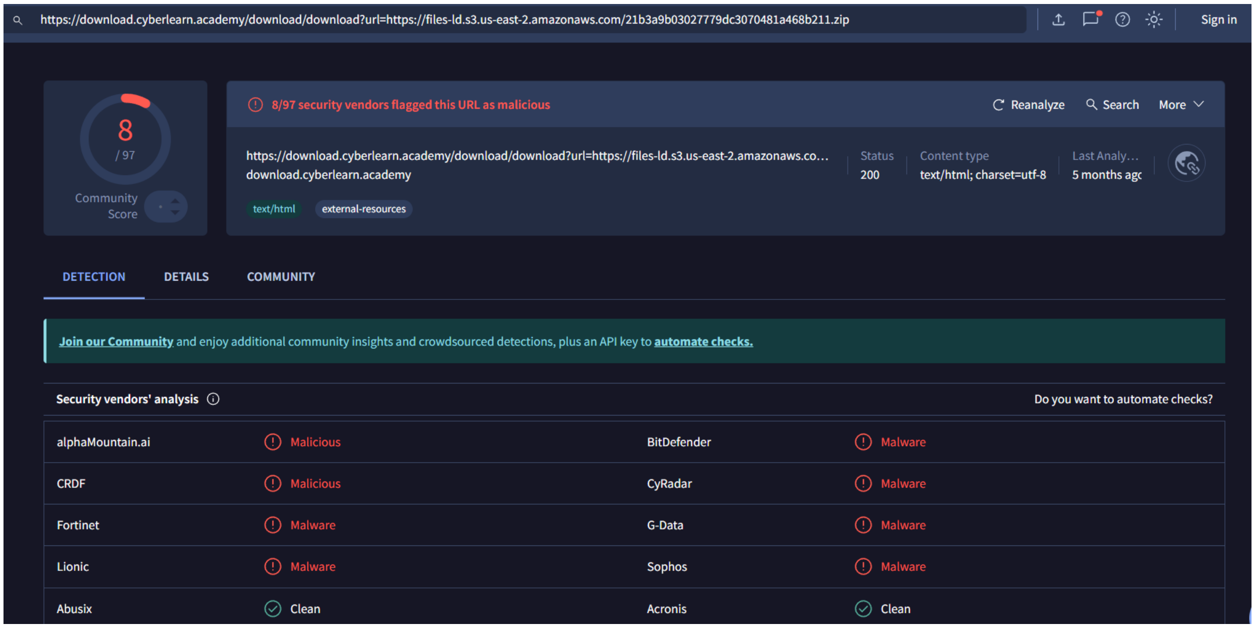
Identified Malicious Download URL

https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/21b3a9b03027779dc3070481a468b211.zip

Threat Intelligence Results

- **Detection Ratio: 8 / 97 security vendors**
- **Verdict: Malware**
- **Content Type: text/html**
- **HTTP Status: 200 OK**

Multiple security vendors including BitDefender, Fortinet, Sophos, CyRadar, and G-Data flagged the URL as malicious.



https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/21b3a9b03027779dc3070481a468b211.zip

8/97 security vendors flagged this URL as malicious

https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.co...
download.cyberlearn.academy

Status	Content type	Last Analy...
200	text/html; charset=utf-8	5 months agc

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	Malicious	BitDefender	Malware
CRDF	Malicious	CyRadar	Malware
Fortinet	Malware	G-Data	Malware
Lionic	Malware	Sophos	Malware
Abusix	Clean	Acronis	Clean

Malware File Analysis

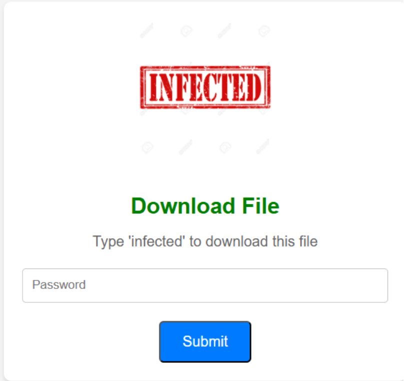
Extracted File Hash (SHA-256)

7dc9821a27cbc29bddb4bb3c708aad0b24a82d9bcb1a2df9cacabf7ca6bd8c06

Additional Payload Hosting

https://files-ld.s3.us-east-2.amazonaws.com/goose_goose_duck_free.rar

Threat intelligence indicates association with SilentBuilder malware, a known dropper and downloader commonly used to deliver secondary payloads.



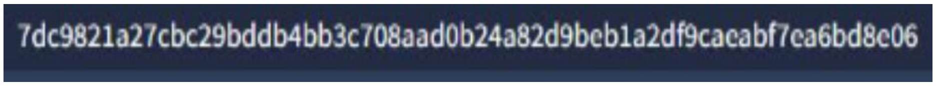
INFECTED

Download File

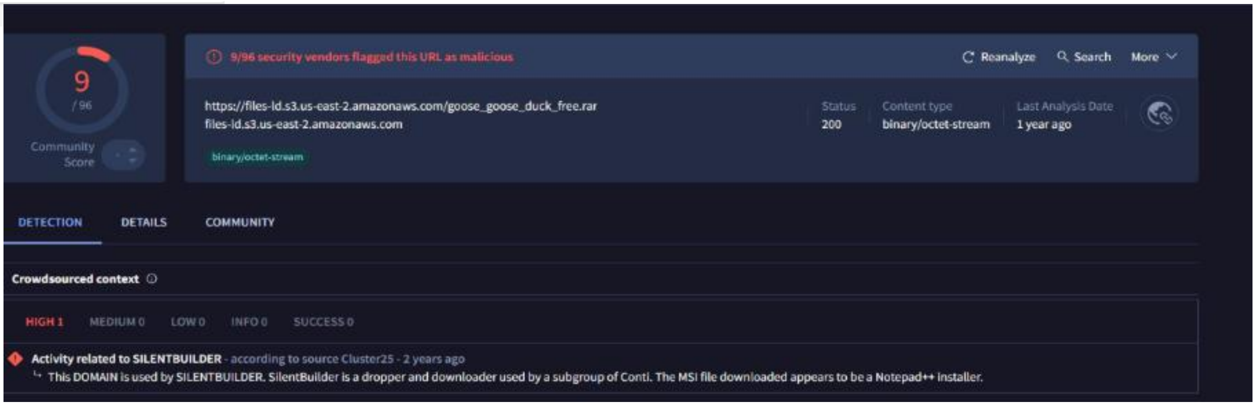
Type 'infected' to download this file

Password

Submit



7dc9821a27cbc29bddb4bb3c708aad0b24a82d9beb1a2df9cacabf7ea6bd8e06



9/96 security vendors flagged this URL as malicious

https://files-ld.s3.us-east-2.amazonaws.com/goose_goose_duck_free.rar
files-ld.s3.us-east-2.amazonaws.com

binary/octet-stream

Status: 200
Content type: binary/octet-stream
Last Analysis Date: 1 year ago

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

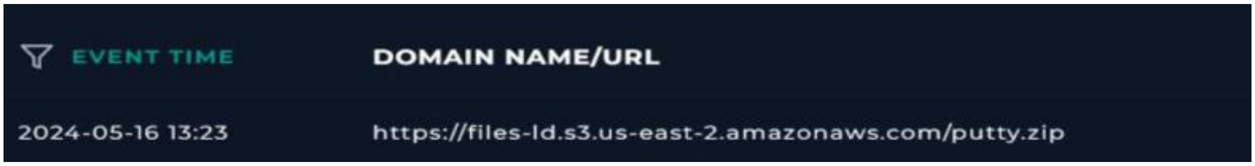
Activity related to SILENTBUILDER - according to source Cluster25 - 2 years ago
↳ This DOMAIN is used by SILENTBUILDER. SilentBuilder is a dropper and downloader used by a subgroup of Conti. The MSI file downloaded appears to be a Notepad++ installer.

Endpoint Telemetry Review

Endpoint visibility confirmed that the email was delivered; however:

- **No confirmed malware execution was observed**
- **No confirmed command-and-control traffic detected**
- **No persistence mechanisms identified**

EDR timeline showed limited activity associated with the downloaded file.

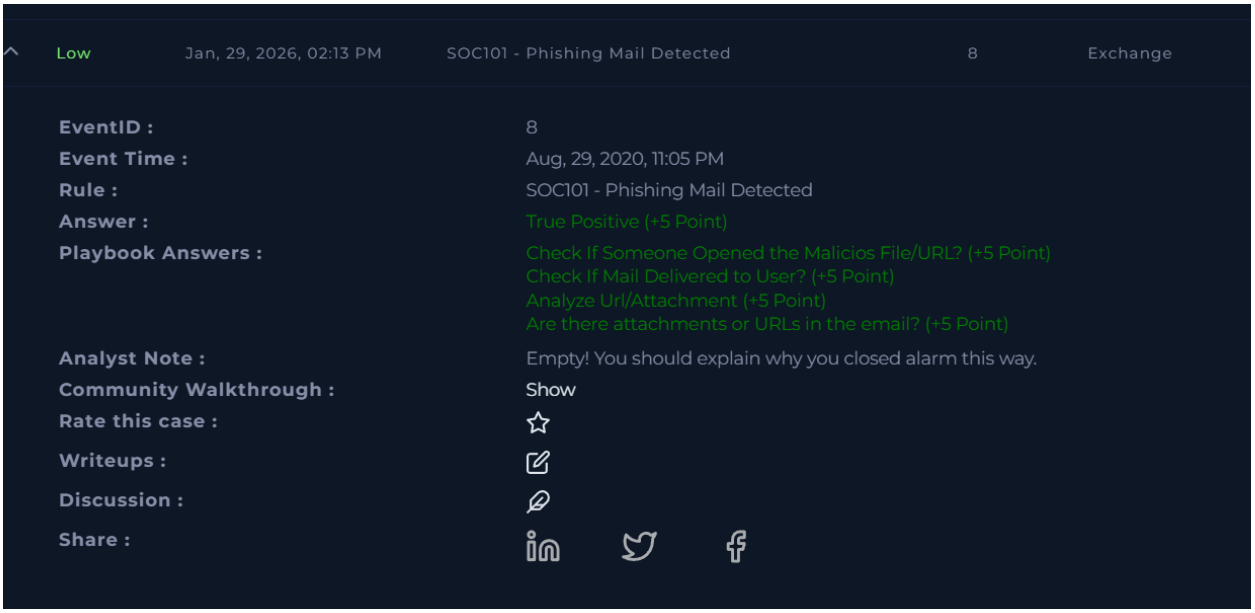


EVENT TIME	DOMAIN NAME/URL
2024-05-16 13:23	https://files-ld.s3.us-east-2.amazonaws.com/putty.zip

Investigation Questions :

When was it sent? Aug 29, 2020, 11:05 PM

- **What is the email's SMTP address?** 63.35.133.186
- **What is the sender address?** info@nexoiberica.com
- **What is the recipient address?** mark@letsdefend.io
- **Is the mail content suspicious?** Yes
- **Are there any attachments?** Yes



Low Jan, 29, 2026, 02:13 PM SOC101 - Phishing Mail Detected 8 Exchange

EventID : 8
Event Time : Aug, 29, 2020, 11:05 PM
Rule : SOC101 - Phishing Mail Detected
Answer : True Positive (+5 Point)
Playbook Answers : Check If Someone Opened the Malicios File/URL? (+5 Point)
Check If Mail Delivered to User? (+5 Point)
Analyze Url/Attachment (+5 Point)
Are there attachments or URLs in the email? (+5 Point)
Analyst Note : Empty! You should explain why you closed alarm this way.
Community Walkthrough : Show
Rate this case : ☆
Writeups :
Discussion :
Share :