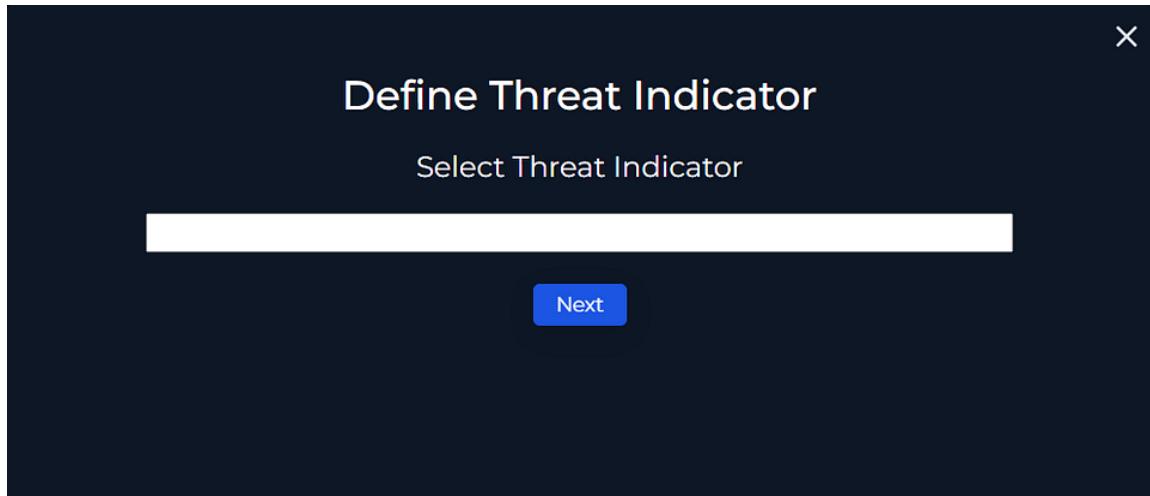


SOC138 - Detected Suspicious Xls File [Let's Defend – Write-up]

The alert for Detected Suspicious Xls File served as a key starting point for the investigation. It provided the necessary visibility to initiate the analysis process and helped in identifying the subsequent activities within the environment. This detection was essential for understanding the sequence of events during the incident response.

| Start Investigation

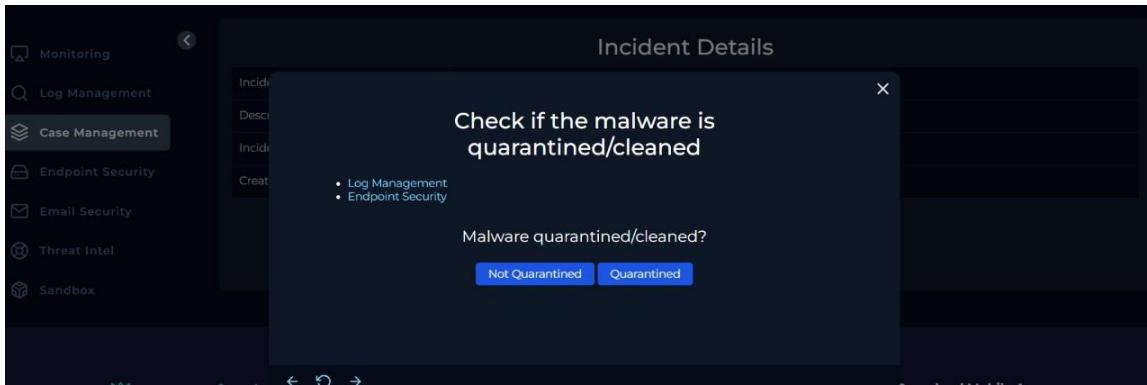
At the beginning of the analysis and closing of the alert, we use Playbook.



And to define Threat indicator I just saw the Log management.

A screenshot of a dark-themed Log Management interface. On the left, a sidebar menu includes "Monitoring", "Log Management" (which is selected and highlighted in blue), "Case Management", "Endpoint Security", "Email Security", "Threat Intel", and "Sandbox". The main area shows a table of log entries. The columns are: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. A filter bar at the top of the table allows for filtering by "Show Filter" and "Basic" or "Pro" view. A specific row in the table is highlighted with a blue background, showing the source IP as 172.16.17.56 and destination IP as 177.53.143.89. The "Basic" tab is selected in the top right corner of the interface.

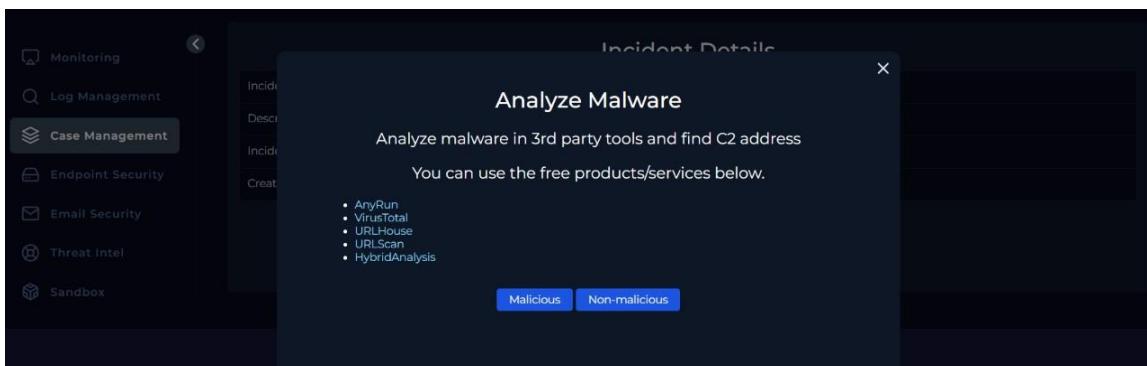
And I saw that the ip 172.16.17.56 which is outgoing traffic, So the answer is **Unknown or unexpected outgoing internet traffic**.



The answer to this question is inside the alert;

EventID :	77
Event Time :	Mar, 13, 2021, 08:20 PM
Rule :	SOCT38 - Detected Suspicious Xls File
Level :	Security Analyst
Source Address :	172.16.17.56
Source Hostname :	Sofia
File Name :	ORDER SHEET & SPEC.xlsx
File Hash :	7ccf88c0bbe3b29bf19d877c4596a8d4
File Size :	2.66 Mb
Device Action :	Allowed
File (Password:infected) :	Download

So, the answer is **Not quarantined** because the Device action is allowed



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 13, 2021, 08:20 PM	Firewall	172.16.17.56	52155	177.53.143.89	443	
Oct, 19, 2020, 10:17				189.10.17	80	
Mar, 13, 2021, 08:20				177.53.143.89	443	

I Analysis this Url to see whether it is Malicious or not

3 / 94 security vendors flagged this URL as malicious

Status: 404 | Last Analysis Date: 1 day ago

DETECTION DETAILS COMMUNITY 13

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?	
BitDefender	Malware	Fortinet	Malware
Sophos	Malware	CyRadar	Suspicious
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean

I analyzed it in VirusTotal and it turned out to be harmful (Malware).

47 / 66 security vendors flagged this file as malicious

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

ORDER SHEET & SPEC.xlsx

xlsx detect-debug-environment checks-user-input executes-dropped-file macros run-file run-dll auto-open exploit long-sleeps macro-run-file exe-pattern calls-wmi clipboard write-file open-file cve-2017-11882

Size: 2.66 MB | Last Analysis Date: 1 day ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 22+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Code insights
This macro exhibits several behaviors commonly associated with malicious intent:
1. Obfuscation:
The code uses heavily obfuscated variable and function names, making it difficult to understand its true purpose.
[Show more](#)

Crowdsourced AI
Hispacse flags this file as [malicious](#)
↳ The macros extracted from the document exhibit several signs of malicious intent, as outlined below:

I also analyzed the file's hash, and it turned out to be malicious.

Analysis Overview

Submission name: ORDER SHEET & SPEC.xlsx
Size: 2.7MiB
Type: [xlsx](#) [office](#) application/octet-stream
Mime: SHA256: 7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813
Submitted At: 2021-03-12 14:37:07 (UTC)
Last Anti-Virus Scan: 2026-01-16 01:20:15 (UTC)
Last Sandbox Report: 2025-07-24 06:01:01 (UTC)

Analysis Overview

Request Report Deletion Show Sample Content

malicious
Threat Score: 100/100
AV Detection: 69%
Labeled As: Trojan.Generic
#bitdefender #evasive
#macros-on-open #exploit

Back to top

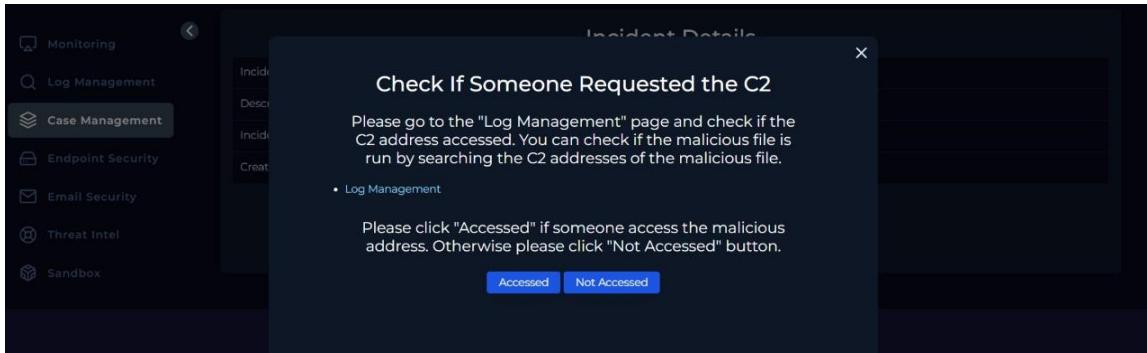
Anti-Virus Results

CrowdStrike Falcon Static Analysis and ML
Malicious (100%)
No Additional Data

MetaDefender Multi Scan Analysis
Malicious (10/26)
More Details

Updated 13 days ago - Click to Refresh

Ans I also used HybridAnalysis for duple check and appear as malicious.



Log Management							
Show Filter		DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT
Mar, 13, 2021, 08:20 PM		Firewall	172.16.17.56	52155	177.53.143.89	443	Q
Oct, 19, 2020, 10:17 PM		Proxy	172.16.17.56	32212	35.189.10.17	80	Q
Mar, 13, 2021, 08:20 PM		Firewall	172.16.17.56	52155	177.53.143.89	443	Q

I saw that ip 172.16.17.56 connect to ip 177.53.143.89 which is the attacker's ip
So the answer is Accessed.

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Apr 10, 2023 08:21:41	54.192.87.239
Apr 10, 2023 08:24:41	52.254.114.65
Apr 10, 2023 08:25:19	13.85.23.206
Apr 10, 2023 08:26:41	146.75.52.81
Apr 10, 2023 08:31:41	177.53.143.89

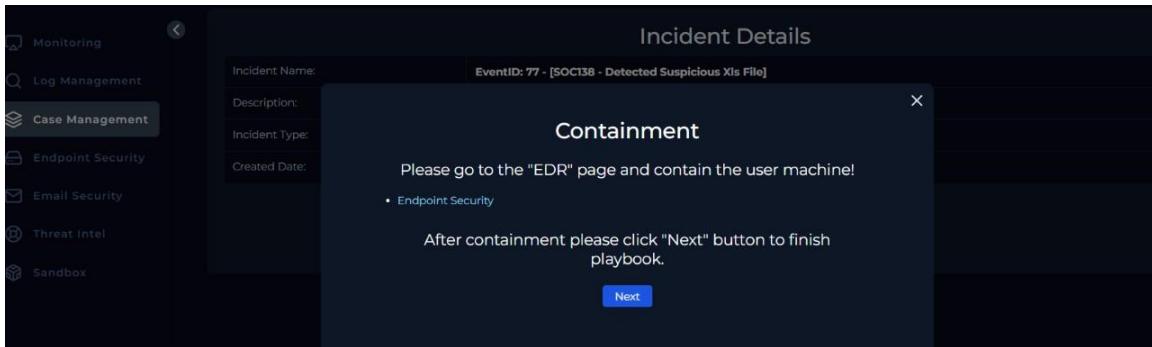
Ans I saw also that the ip 177.53.143.89 connect with Nolan, and for more investigation I checked the email section to see if there any communication.

From: jack@aventeach.io
To: nolan@letsdefend.io
Subject: Order Sheet and Specifications
Date: Apr, 10, 2023, 08:30 AM
Action: Allowed

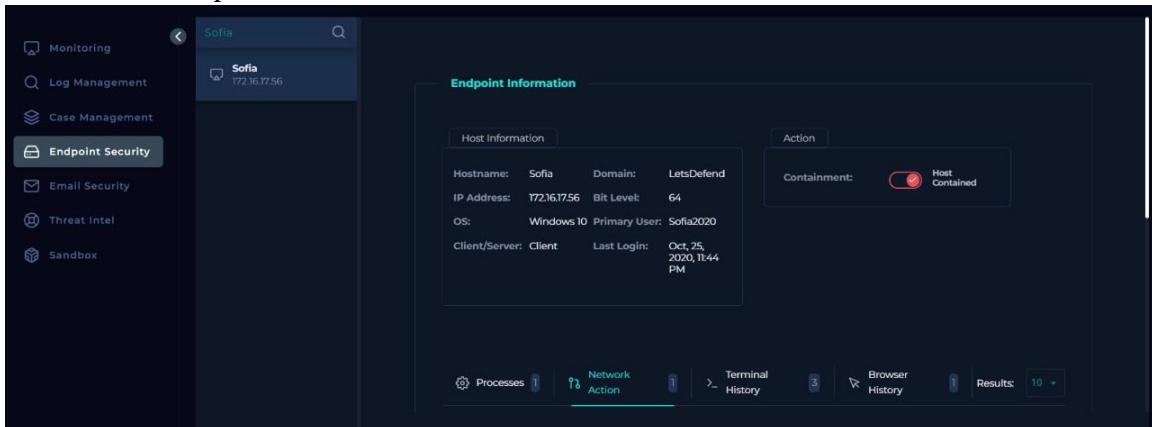
Dear Nolan, To place an order, please fill out the form provided below. Please review the specifications carefully and ensure that they are accurate before finalizing your order. You can download the order form in the attached file named ORDER SHEET & SPEC.xlsx.zip. Please fill out the form completely with all the necessary information. Before placing your order, please check the following specifications: *Price *Expire Date *Performance Please verify these specifications and complete the order form accordingly. Once you have completed your orders, a AvenaTech sales representative will contact you. If you have any questions, please do not hesitate to contact us. Best regards, Jack

Attachments
ORDER SHEET & SPEC.xlsx.zip
Password: infected

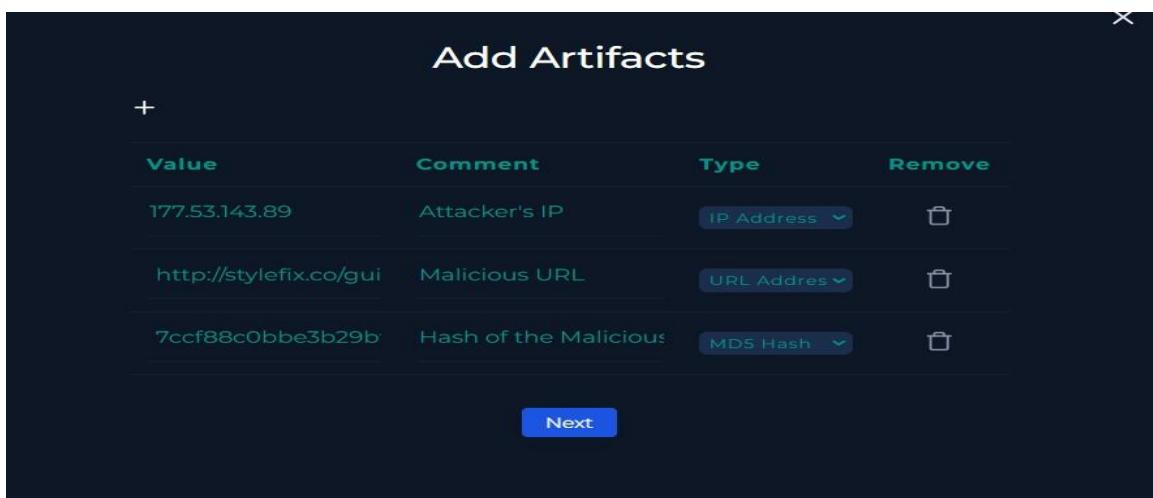
So, it seems that email jack@avenatech.io sent to nolan@letsdefend.io malicious email that contains the same malicious file that appears on the Alert. So at the end Yes there is communication to malicious address (177.53.143.89).



After that it's required to isolate the device.



After I fished these artifacts;



And yes, it is **True Positive**.

Summary

The investigation of the SOC138 – Detected Suspicious XLS File alert confirmed a True Positive security incident. Analysis revealed that the XLS file was malicious, as verified through multiple threat intelligence platforms including VirusTotal, Hybrid Analysis, and hash reputation checks. Log analysis showed unexpected outbound traffic from the internal host 172.16.17.56 to the external IP 177.53.143.89, identified as the attacker's infrastructure.

Further investigation confirmed that the malicious file was delivered via phishing email, establishing communication between internal users and the malicious external address. Although the device action was initially allowed and the file was not quarantined, the evidence clearly indicated malicious activity. As a result, device isolation was required, and the alert was correctly classified as a True Positive.