

<b>EventID :</b>  <b>76</b>  <b>Event Time :</b>  <b>Mar, 14, 2021, 07:15 PM</b>  <b>Rule :</b>  <b>SOC137 - Malicious File/Script Download Attempt</b>  <b>Level :</b>  <b>Security Analyst</b>  <b>Source Address :</b>  <b>172.16.17.37</b>  <b>Source Hostname :</b>  <b>NicolasPRD</b>  <b>File Name :</b>  <b>INVOICE PACKAGE LINK TO DOWNLOAD.docm</b>  <b>File Hash :</b>  <b>f2d0c66b801244c059f636d08a474079</b>  <b>File Size :</b>  <b>16.66 Kb</b>  <b>Device Action :</b>  <b>Blocked</b>  <b>File (Password:infected) :</b>	<b>Mar, 14, 2021, 07:15 PM</b>	<b>SOC137 - Malicious File/Script Download Attempt</b>	<b>76</b>	<b>Malware</b>
--	--------------------------------	--	-----------	----------------

[Download](#)

searching the file hash in virus-total we can tell this is a malicious file.

The screenshot shows the VirusTotal interface for a file with hash 08d4fd5032b8b24072bdf43932630d4200f68404d7e12ffeda2364c8158873. The file is identified as 'INVOICE PACKAGE LINK TO DOWNLOAD.docm' and is 16.66 KB in size. It was last analyzed 5 hours ago. The interface shows that 38 out of 66 security vendors flagged this file as malicious. A community score of -4 is displayed. The file's behavior is categorized as follows: docx, calls-wmi, detect-debug-environment, auto-open, url-pattern, powershell, long-sleeps, run-file, macro-run-file, and macros. The bottom navigation bar includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (17+).

the device action was blocked.


searching the source ip we can see this information :

The screenshot displays the 'Host Information' section for the IP address 172.16.17.37. The information is organized into four rows, each with two columns. The first row shows the Hostname as 'NicolasPRD' and the Domain as 'letsdefend.local'. The second row shows the IP Address as '172.16.17.37' and the Bit Level as '64'. The third row shows the OS as 'Windows 10' and the Primary User as 'Nicolas'. The fourth row shows the Client/Server status as 'Client' and the Last Login time as 'Mar, 07, 2021, 04:30 PM'.

Host Information			
<b>Hostname:</b>	NicolasPRD	<b>Domain:</b>	letsdefend.local
<b>IP Address:</b>	172.16.17.37	<b>Bit Level:</b>	64
<b>OS:</b>	Windows 10	<b>Primary User:</b>	Nicolas
<b>Client/Server:</b>	Client	<b>Last Login:</b>	Mar, 07, 2021, 04:30 PM

# Playbook Answers

Question: Check If Someone Requested the C2

User answer: Not Accessed 

Question: Analyze Malware

User answer: Malicious 

Question: Check if the malware is quarantined/cleaned

User answer: Quarantined 

looks like the malware was blocked and no evidence of the file being run

## Playbook Note

looks like the malware was blocked and no evidence of the file being run

## Extracted Artifacts

Value	Comment	Type
f2d0c66b801244c059f636d08a474079	malicious file hash	MD5 Hash
https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/f2d0c66b801244c059f636d08a474079.zip	malicious file - download url	E-mail Domain
		E-mail Domain

## Alert Answers

Question:

Is this alert True Positive or False Positive?

User answer:



## Alert Note

looks like the .docm file was malicious it tries to contact different addresses