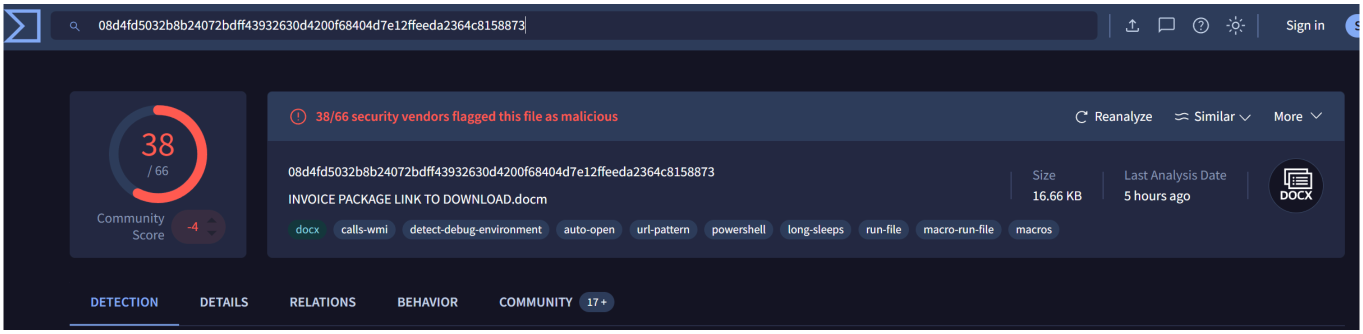
| | | | | |
|---|---|---|---|---|
| **EventID :**<br>**76**<br>**Event Time :**<br>**Mar, 14, 2021, 07:15 PM**<br>**Rule :**<br>**SOC137 - Malicious File/Script Download Attempt**<br>**Level :**<br>**Security Analyst**<br>**Source Address :**<br>**172.16.17.37**<br>**Source Hostname :**<br>**NicolasPRD**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

| | | | | |
|---|---|---|---|---|
| Download | | | | |

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



08d4fd5032b8b24072bdff43932630d4200f68404d7e12ffeeda2364c8158873

38 / 66

Community Score -4

38/66 security vendors flagged this file as malicious

08d4fd5032b8b24072bdff43932630d4200f68404d7e12ffeeda2364c8158873

INVOICE PACKAGE LINK TO DOWNLOAD.docm

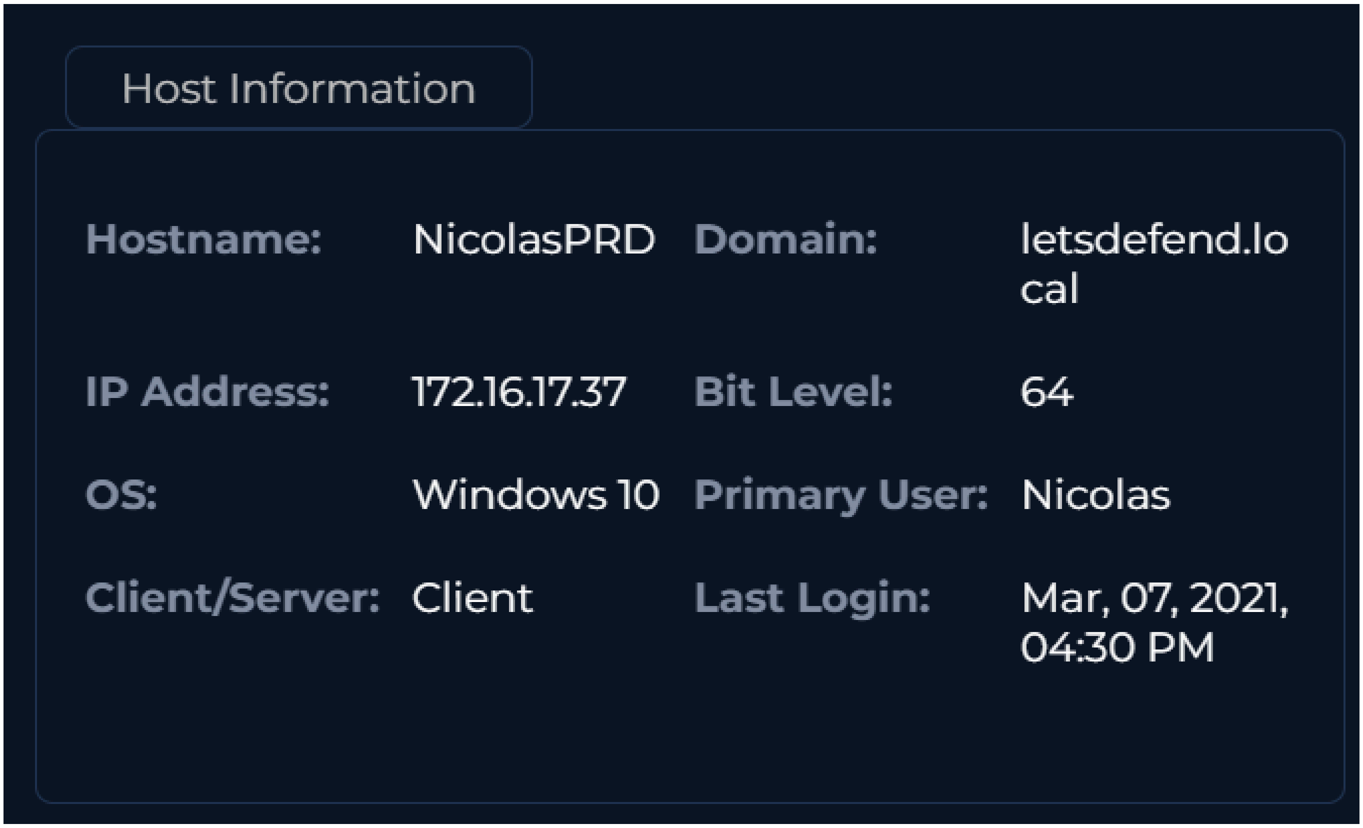
docx calls-wmi detect-debug-environment auto-open url-pattern powershell long-sleeps run-file macro-run-file macros

Size 16.66 KB

Last Analysis Date 5 hours ago

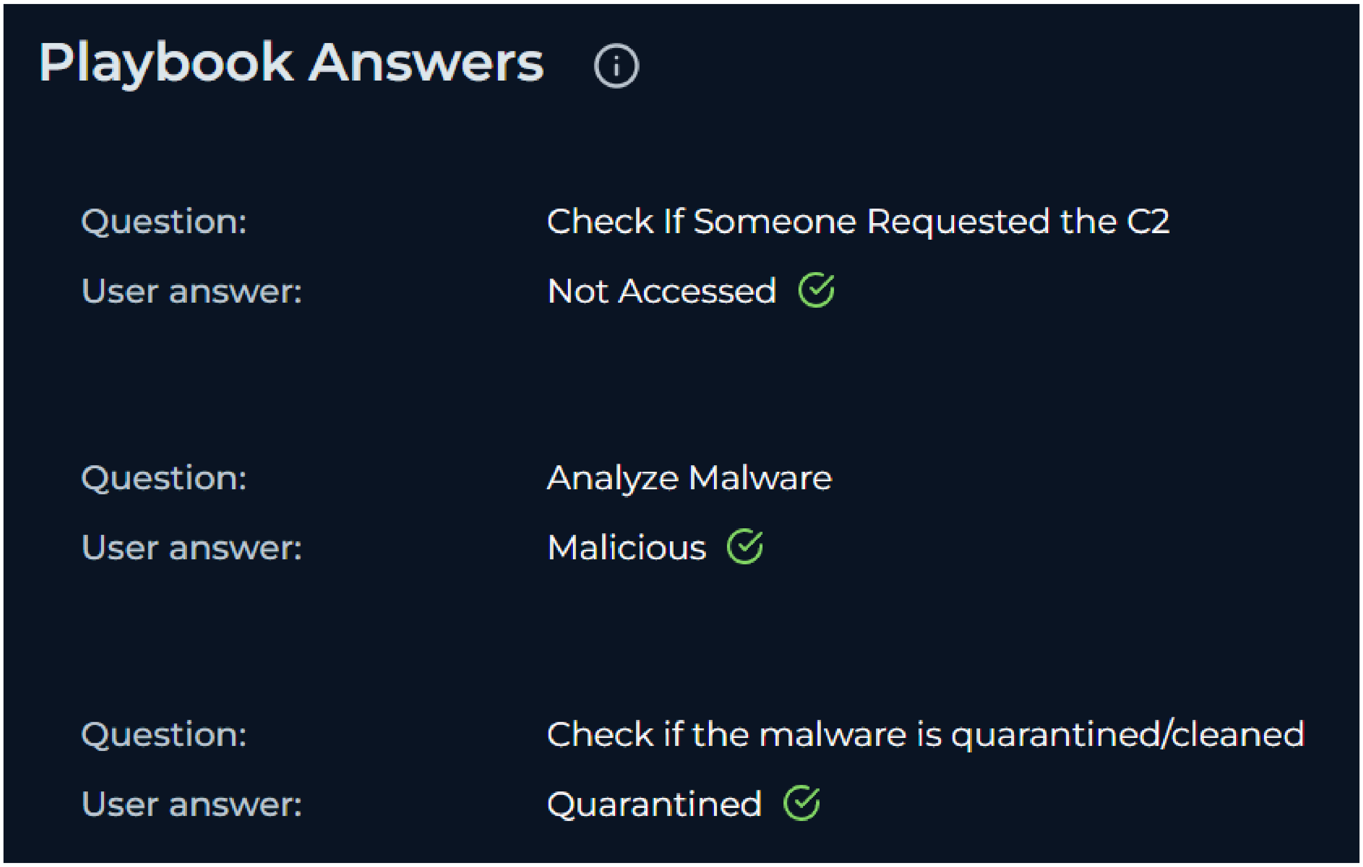
the device action was blocked.

searching the source ip we can see this information :



Host Information

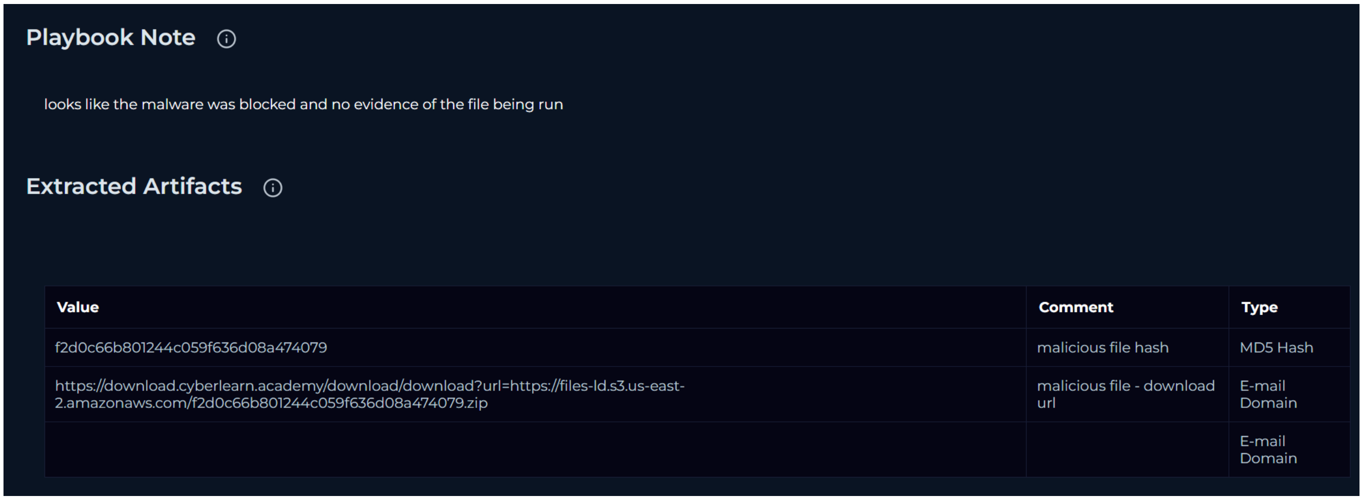
| | | | |
|---|---|---|---|
| Hostname: | NicolasPRD | Domain: | letsdefend.local |
| IP Address: | 172.16.17.37 | Bit Level: | 64 |
| OS: | Windows 10 | Primary User: | Nicolas |
| Client/Server: | Client | Last Login: | Mar, 07, 2021, 04:30 PM |



## 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

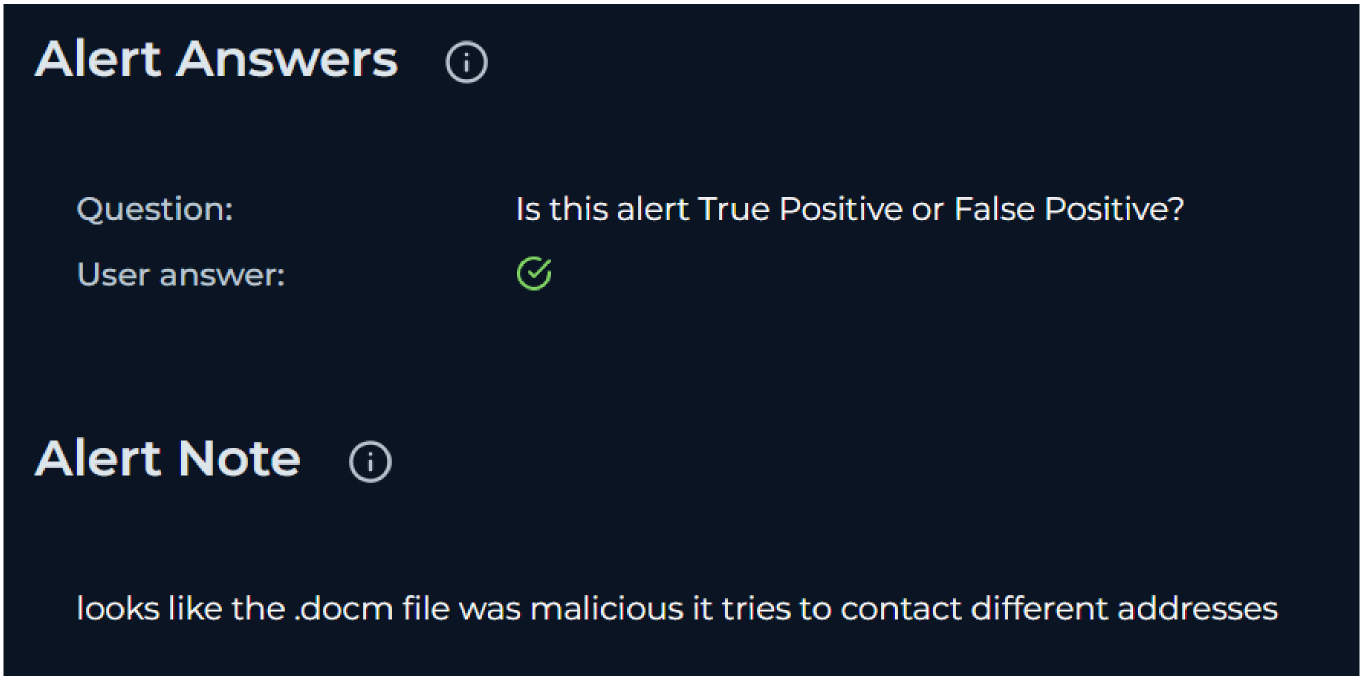


### Playbook Note ⓘ

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