### **SOC336 — Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025–21298)**

### **Event Summary**

**Alert ID —**SOC336

**Event ID —**314

**Detection Rule —**Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025–21298)

**Event Time (UTC) —**Feb, 04, 2025, 04:18 PM

**Source Email —**projectmanagement@pm.me

SMTP Address — 84.38.130.118

**Target Email —**Austin@letsdefend.io

**Email Subject —**Important: Action Required for Upcoming Project Deadline

**Device Action —**Allowed (Email delivered)

Attachment — mail.rtf

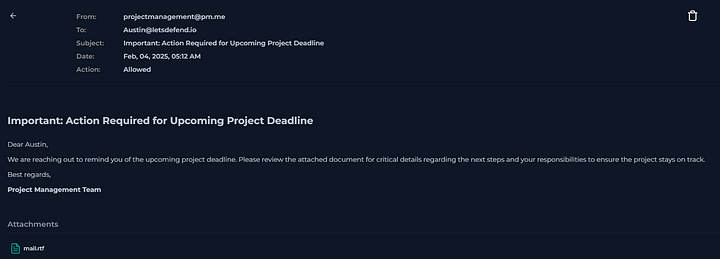
Attachment hash — df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184

**Trigger Reason —**Malicious RTF attachment identified with known CVE-2025–21298 exploit pattern.



### **Analysis**

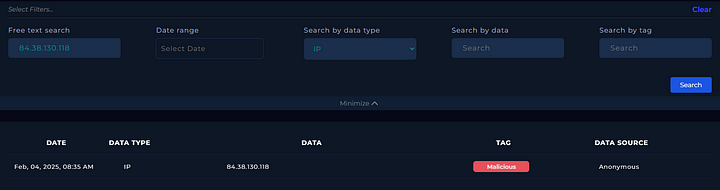
Let us start by investigating the email.



The email seems to instill a sense of urgency in order to trick the user into opening the attachment.

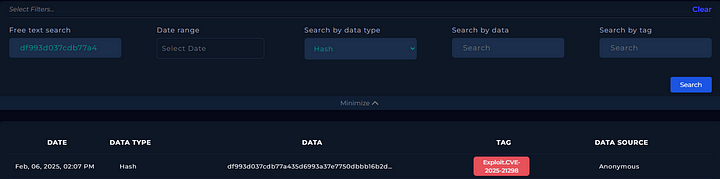
Now, we can check Threat Intelligence to see if there is any known malicious identifiers with this email.

First, we can check with the SMTP address.



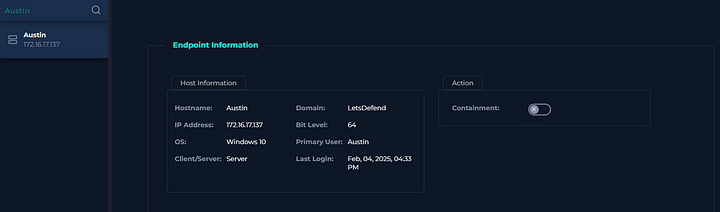
As we can see above, the IP address is a know malicious IP.

Now, we can take a look at the hash of the attachment file.

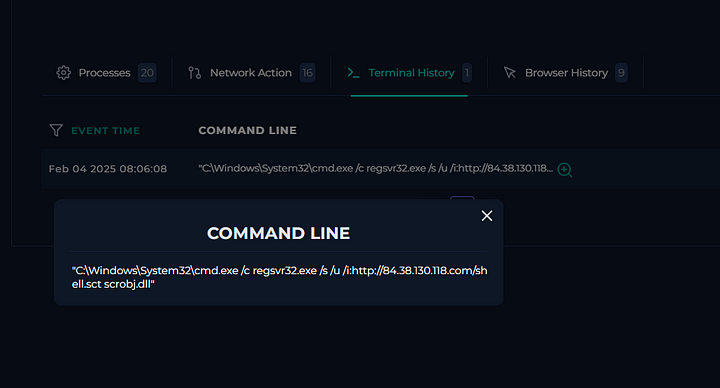


So, it is clear that the email and the attachment are clearly malicious.

With this finding, we need to see if the user had interacted with this email. We can do this by going to the Endpoint Security and having a look at the device of the user Austin.



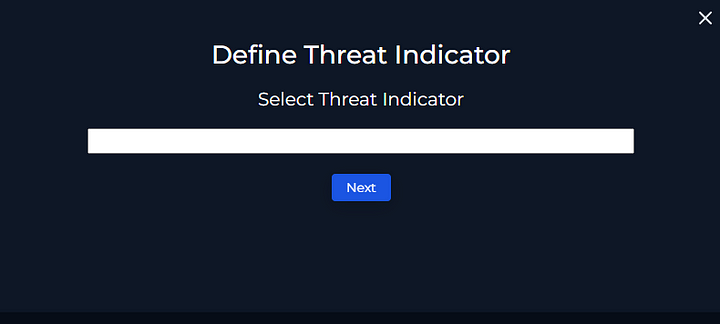
In the terminal history of the user, there is a malicious command which is typically used in LOLBIN exploits.



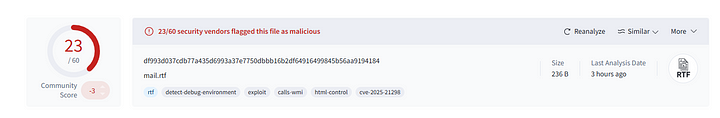
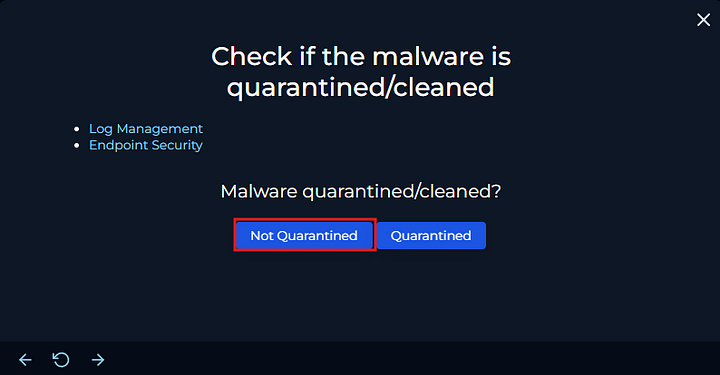
This command downloads and executes remote malicious script without dropping a file to disk. By using regsrv32.exe it bypasses the security as this is a legitimate windows binary. Also the IP address in this command is the same as the SMTP address we checked earlier.

#### **Playbook**

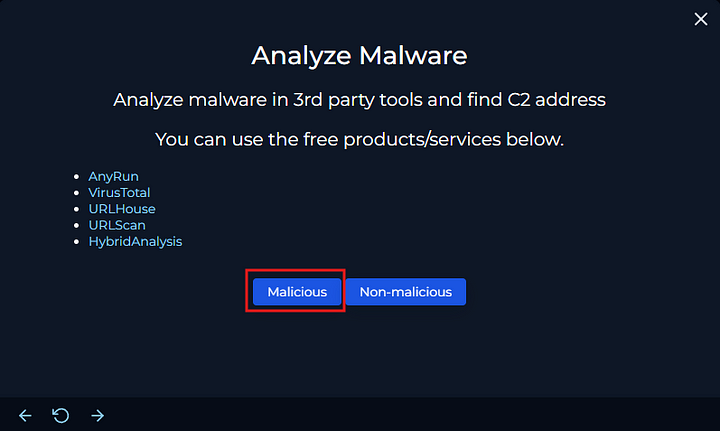
Since we observed malicious network traffic, we can select the first option here.

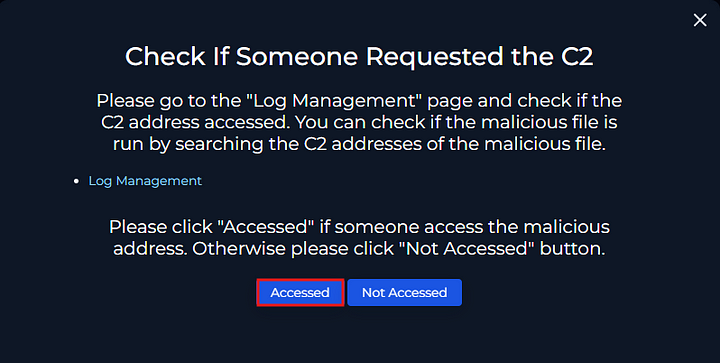


Since the email reached the end user’s endpoint and the user interacted with the email, we can select not quarantined.



We can see above, that the file is indeed malicious.

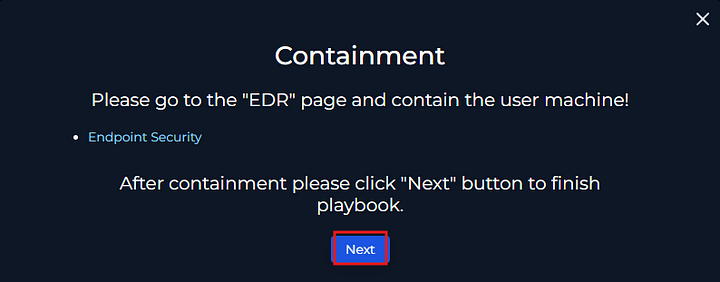


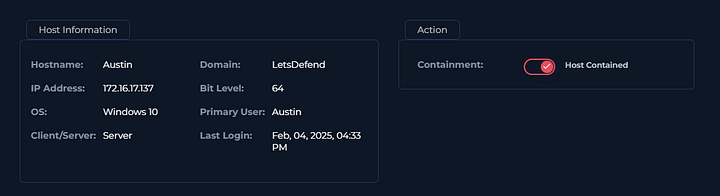


We had already checked the users terminal history that the C2 URL was requested. We can also check this in the Log management.



So, we can confirm that the C2 was accessed.





Now, click next and go to the endpoint section and contain the endpoint.

Now, we can write the report and close the alert as true positive and send it for further analysis.