

Outlook

RE: Analisis de alertas windows defender Cloud - Moodle Azure

Desde Ingrid Silvana, Escobar Castro <ISEscobar@saludcapital.gov.co>

Fecha Jue 10/07/2025 9:30 PM

Para Carlos Andres, Olarte Cardoso <CAOlarte@saludcapital.gov.co>; Adlay, Cuello Villarreal <A1Cuello@saludcapital.gov.co>

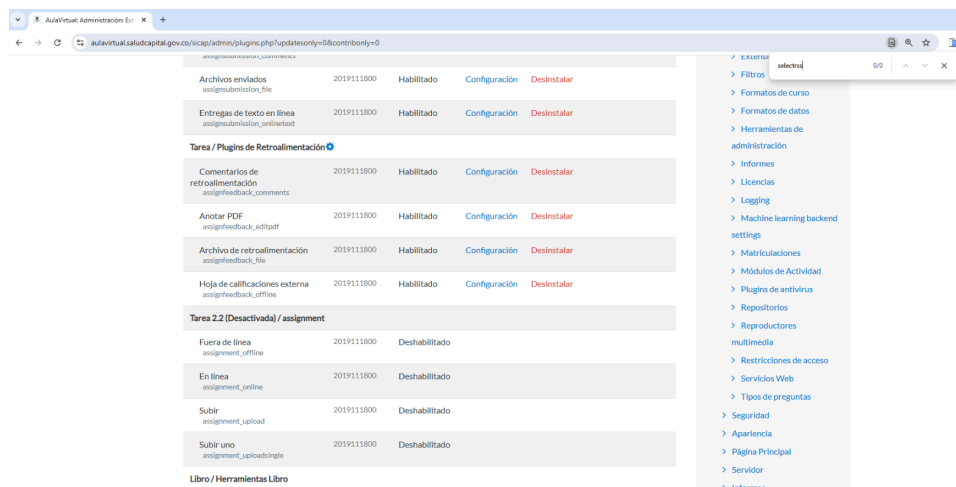
CC Juan Sebastian, Martinez Martinez <JSMartinez@saludcapital.gov.co>; Erlington, Salcedo Benavides <E1Salcedo@saludcapital.gov.co>

Cordial saludo ingeniero Carlos

Realice las validaciones frente a la información enviada y tengo lo siguiente:

1.El plugin selectrss no está instalado actualmente en la Moodle y no hace parte del sitio

- No aparece listado como bloque, filtro, módulo ni herramienta.
- Esto implica que no está activo ni accesible desde el sistema web.
- Los archivos relacionados con selectrss no se desplegaron en producción, es decir no se están ejecutando en ninguna aula virtual.
- Se puede eliminar el ZIP y su carpeta


2. En cuanto a los archivos detectados con nombres como:

- 17f7cde062dfc1820c37aadac411c2b805f91cb9
- 1346cef4b38d7a629f8664e14fc713041d60a07
- e320fb79266d8d88bee555356be771fca7fd86c07

para poder validar solicito realizar la siguiente consulta SQL en la base de datos de Moodle para obtener información detallada sobre los archivos detectados, incluyendo quién los subió, cuándo, dónde se usaron y su nombre original:

```
SELECT
  f.id AS file_id,
  f.contenthash,
  f.filename,
  f.filepath,
  f.filesize,
  f.mimetype,
  f.timecreated,
  f.timemodified,
  f.userid,
  u.firstname,
  u.lastname,
  f.contextid,
  c.contextlevel,
  c.instanceid,
  f.component,
```

```
f.filearea,
f.itemid
FROM mdl_files f
LEFT JOIN mdl_user u ON f.userid = u.id
LEFT JOIN mdl_context c ON f.contextid = c.id
WHERE f.contenthash IN (
    '17f7cde062dfc1820c37aadac411c2b805f91cb9',
    '1346cef4b38d7a629f8664e14fc713041d60a07',
    'e320fb79266d8d88bee555356be771fca7fd86c07'
)
AND f.filename <> '.';
```

los campos hacen referencia:

- **contenthash:** Identifica el archivo físico (el mismo que viste en /filedir/xx/yy)
- **filename:** Nombre original del archivo subido
- **filepath:** Ruta relativa dentro del área de archivos (por ejemplo /)
- **component:** Módulo de Moodle donde se utilizó (mod_assign, mod_forum, core, etc.)
- **filearea:** Subzona dentro del componente (submission_files, attachment, intro, etc.)
- **userid / firstname / lastname:** Usuario que subió el archivo
- **timecreated:** Fecha/hora de subida
- **contextid/contextlevel/instanceid:** Ubicación lógica (curso, módulo, bloque, etc.)

Quedo atenta a sus comentarios

Silvana Escobar Castro

Secretaría Distrital de Salud

Dirección TIC

De: Carlos Andres, Olarte Cardoso <CAOlarte@saludcapital.gov.co>
Enviado: miércoles, 9 de julio de 2025 11:31 a. m.
Para: Ingrid Silvana, Escobar Castro <ISEscobar@saludcapital.gov.co>
Cc: Juan Sebastian, Martinez Martinez <JSMartinez@saludcapital.gov.co>; Erlington, Salcedo Benavides <E1Salcedo@saludcapital.gov.co>
Asunto: Analisis de alertas windows defender Cloud - Moodle Azure

Buen día Ing. Silvana,

en relación con los eventos de seguridad que se han reportado por el Defender for Cloud de Azure, seguimos recibiendo alertas con diferentes directorios de la plataforma Moodle, como por ejemplo la siguiente que llego el 8 de julio:

Security alert

5e53befc-42aa-6da7-eb43-07738c3c446a

'Kepavll' malware was detected (Agentless)

High
Severity

Active
Status

07/07/25, 07:22 PM
Activity time

Alert description

Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.

This detection might indicate that the malware was stopped from delivering its payload. However, it is prudent to check the machine for signs of infection.

Last updated time
07/07/25, 07:22 PM

Threat Information

Trojan:Win32/Kepavllrln

Threat Category

Trojan

Machine Name

SdsMoodleReplOnPremise

Related entities

Azure resource (1)

File (3)

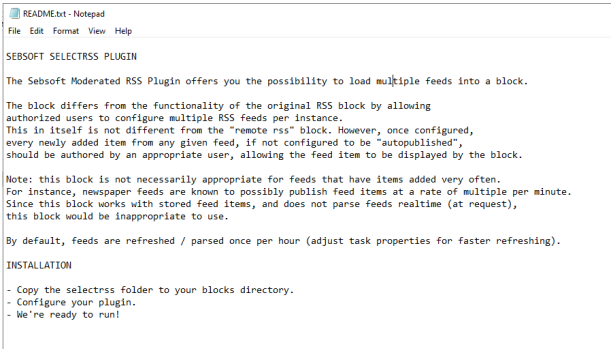
Name	Directory	Host	File hashes	Threat Intelligence
17f7cde062dfc1820c37aadac411c2b805f91cb9	/var/moodledata/filedir/17/17	SdsMoodleReplOnPremise	17f7cde062dfc1820c37aadac411c2b...	
1346cef4b38d27a629f8664e14c713041d60a07	/var/moodledata/filedir/13/46	SdsMoodleReplOnPremise	1346cef4b38d27a629f8664e14c713...	
e320fb79266d8d88bee555356be771fca7fd86c07	/var/moodledata/filedir/e3/20	SdsMoodleReplOnPremise	a4e6840c94a7789ad01a1a6fdc7bf53...	

Adicionalmente, con el ingeniero Sebastián Martínez se realizo el analisis de los comprimidos en virus total en una maquina aislada donde dse evidencia que efectivamente estos cargues en la plataforma contienen Malware.

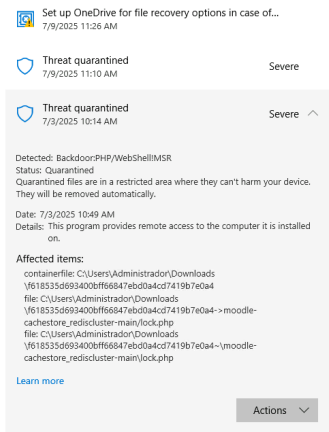
Con lo anterior necesitamos validar de tu parte de donde provienen este cargue de archivos y si existen plug-ins adicionales ya que tambien se pudo ver que el contenido del Zip afectado uno de los archivos menciona lo siguiente:

https://outlook.office.com/mail/sentitems/id/AAkALgAAAAAAHYQDEapmEc2byACqAC%2FEWg0AEe%2FkzRIFE0eGrxeRe6j%2FMgAHw2%2FLaAAA

2/3

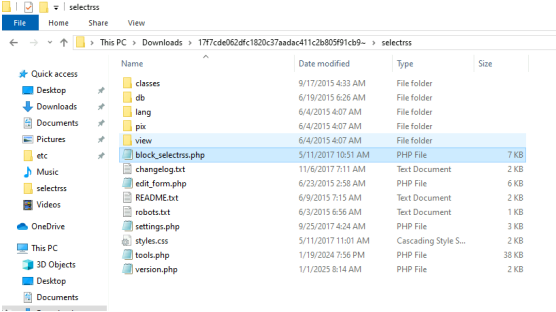


El defender de windows lo detectó como una amenaza en riesgo mayor por tal motivo lo eliminó en el momento de abrir el contenido del zip:



Agradecemos nos des la mayor información posible, siendo que no sabemos si esto hace parte la aplicación Moodle o si corresponde a cargue de archivos de otra fuente.

El contenido de la Zip afectada es el siguiente:



Quedamos atentos a tu respuesta.

Cordialmente,



SECRETARÍA
DISTRITAL DE SALUD

Carlos Andres Olarte Cardoso
Dirección TIC
Secretaría Distrital de Salud
Teléfono: 364 9090 Ext.: 9001