Informe técnico sobre análisis

***Autor**: Valentina Alcubillas Arango / **Fecha**: 25/01/25*
***Evidencia**: "debian-disk001.vmdk"*

Introducción

El presente documento detalla el análisis digital sobre la imagen del servidor clave Debian **"debian-disk001.vmdk"** proveniente de la empresa **4Geeks Academy.**

El objetivo en el que se indica el análisis se basa en **identificar** el **origen del ataque**, el **método** que se ha empleado y **el alcance** del compromiso que se ha detectado el **30 de Septiembre de 2024.** El atacante consiguió **elevar privilegios, establecer múltiples mecanismos de persistencia (SSH, Base de Datos, FTP)** y **optimizar el sistema** para el alojamiento de servicios **no autorizados**.

Herramientas relevantes

Para completar de manera exitosa el análisis forense, se ha hecho uso de las siguientes herramientas:

- **Autopsy** (análisis digital)
- **Navegador web** (búsquedas de información)
- **FTK Imager** (conversión de archivos raw.img a .E01)
- **VBoxManage** (herramienta de conversión vmdk a raw.img)
- **rkhunter** (programa para análisis de rootkits y malware)

Evidencias relevantes

Servicios que fueron comprometidos

Servicio	Nombre	Descripción
22/tcp SSH	Secure Shell (OpenSSH 9.2p1)	Instalado y activado manualmente por el atacante (openssh-server). Fue utilizado como túnel para evadir el firewall y permitir el acceso remoto persistente.
MariaDB/MySQL	Base de Datos	El motor de base de datos fue manipulado para crear cuentas administrativas paralelas y almacenar la configuración del sitio web comprometido.
21/tcp FTP	vsftpd 3.0.3	Vector potencial de exfiltración de información y carga de malware.
80/tcp HTTP	Apache 2.4.62, servidor Web	Comprometido para alojar una instancia de WordPress instalada de forma no autorizada. Sirvió como interfaz para la ejecución de scripts y gestión de contenidos maliciosos.
Systemd	Gestor de Servicios	Utilizado por el atacante para detener y deshabilitar servicios legítimos de accesibilidad (speech-dispatcher, espeakup) con el fin de optimizar recursos para el ataque.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.1.63
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 07:50 EST
Nmap scan report for 192.168.1.63
Host is up (0.000092s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:9A:1F:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Usuarios y privilegios

Se identificó la manipulación de las siguientes cuentas:
Usuario del sistema ***debian*** (UID 1000): Vector principal de entrada. Se detectó el uso de sudo para escalar a root.

- **Escalación de privilegios**: El usuario escaló privilegios a root el **30/09/24.** Utilizó sudo para añadirse a los grupos **root (GID 0), sudo (GID 27) y adm (GID 4)** en el archivo **/etc/group**, obteniendo **control total** del sistema de archivos y acceso a los **logs de administración**.

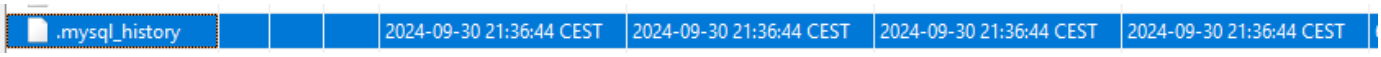
```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:debian
floppy:x:25:debian
tape:x:26:
sudo:x:27:
```

- **Modificaciones críticas**: Manipuló el archivo **visudo** para eliminar **restricciones de seguridad**. Se identificó la inserción de la directiva **NOPASSWD: ALL,** permitiendo ejecutar **cualquier comando** como **superusuario** sin necesidad de **autenticación**.
- **Persistencia**: Realizó modificaciones en **/etc/sudoers** para asegurar la ejecución de comandos sin contraseña y configuró el servicio SSH para permitir el **acceso remoto permanente**, estableciendo un canal de **control externo independiente**.

```
# Cmnd alias specification

# User privilege specification
root            ALL=(ALL:ALL) ALL
debian  ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo           ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

Usuario de la Base de Datos ***user***: Creado manualmente a partir de MariaDB/MySQL utilizando la contraseña trivial de ***password***.

- **Privilegios:** Se le otorgaron **permisos globales** mediante la sentencia **GRANT ALL PRIVILEGES ON *.* WITH GRANT OPTION**. Esto le permite controlar **todas las bases de datos del servidor** de forma independiente a los accesos del sistema operativo.
- **Evidencia de creación (MySQL History):** Se localizó la sentencia exacta de su creación en el archivo **.mysql_history** del usuario **debian**, lo que vincula directamente la actividad del atacante en la terminal con la **manipulación de la base de datos**.



.mysql_history				2024-09-30 21:36:44 CEST	2024-09-30 21:36:44 CEST	2024-09-30 21:36:44 CEST	2024-09-30 21:36:44 CEST			

- **Identidad Web:** Vinculado al administrador de **WordPress** creado durante la ejecución del **script install.php**.

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Domain	Text
places.sqlite				File	Unknown					Administrator role (WordPress platform)

Cronología: La creación de este usuario web fue en agosto de 2024, mientras que el último acceso registrado fue en octubre del mismo año.

Archivos manipulados/abiertos/accedidos recientemente

En esta sección se detallan las alteraciones detectadas en el sistema de archivos y las evidencias encontradas en los registros de transacciones:

- **Servicios Web:** Creación y modificación del archivo /var/www/html/wp-config.php (contiene credenciales expuestas).

Metadata

Name:	/img_debian-disk001.vmdk/vol_vol2/var/www/html/wp-config.php
Type:	File System
MIME Type:	text/x-php
Size:	3017
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-09-30 18:02:41 CEST
Accessed:	2024-10-08 22:49:45 CEST
Created:	2024-09-30 17:56:21 CEST
Changed:	2024-10-08 22:20:04 CEST

- **Persistencia Web:** Creación de directorios en /wp-content/uploads/2024/10/, evidenciando actividad que se prolongó hasta octubre. El atacante eliminó el instalador original en /tmp tras la migración para limpiar rastros.

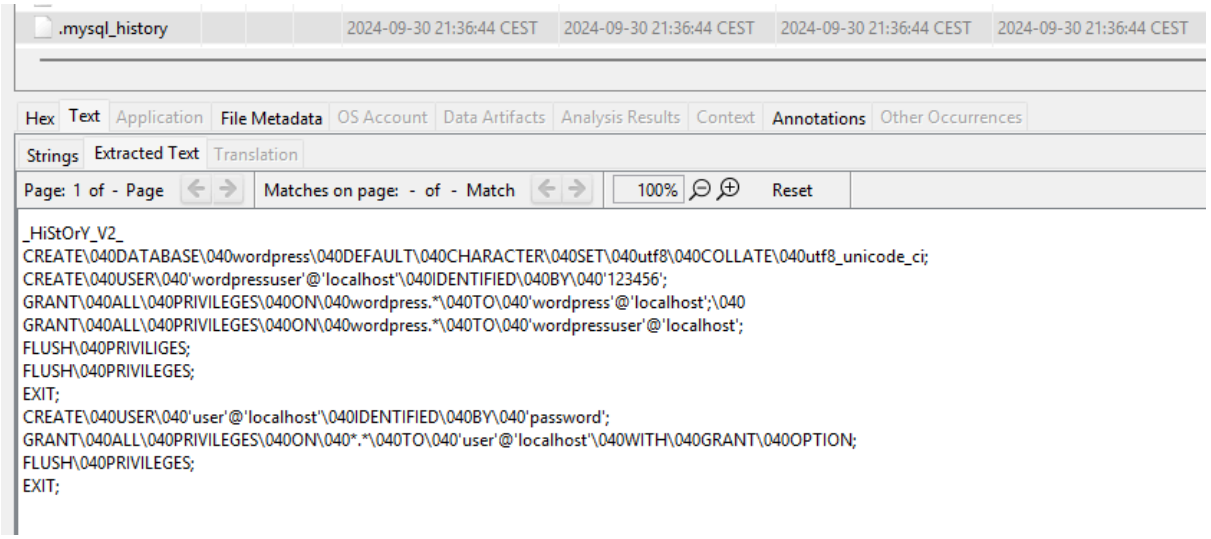
Listing

/img_debian-disk001.vmdk/vol_vol2/var/www/html/wp-content/uploads/2024/10

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST
[parent folder]				2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:18:00 CEST	2024-09-30 18:23:13 CEST

- **Historial de MySQL (.mysql_history):** * Se confirma la ejecución de comandos para la creación del usuario ***user*** con la contraseña ***password*** encontrado en /root.



- **Historial de Terminal (.bash_history):** Documenta la instalación de paquetes (apt install), la descarga de WordPress y el borrado de archivos temporales en /tmp.

```
cd /tmp
curl -O https://wordpress.org/latest.tar.gz
sudo apt install curl
curl -O https://wordpress.org/latest.tar.gz
tar xzvf latest.tar.gz
sudo cp -a /tmp/wordpress/. /var/www/html/
sudo chown -R www-data:www-data /var/www/html/
sudo chmod -R 755 /var/www/html/
cd /var/www/html/
sudo mv wp-config-sample.php wp-config.php
sudo nano wp-config.php
ip a
sudo systemctl restart apache2
sudo systemctl status apache2
sudo apt install php libapache2-mod-php php-mysqli php-gd php-xml php-mbstring php-curl -y
cd ..
sudo nano /etc/apache2/sites-available/000-default.conf
```

- Evidencia de la ejecución de **GRANT ALL PRIVILEGES ON *.***, otorgando control total sobre el motor de base de datos de forma independiente al CMS.
- **Rastros técnicos de la actividad del sistema**: Se encuentran en la ruta /tmp/ los archivos siguientes:

Carpeta	Archivo	Significado
ssh-XXXXXXGZYLks	agent.946	Refuerza el hecho de que hubo una sesión SSH activa dónde se utilizó un agente para gestionar llaves de autenticación.
.X11-unix	X0	Indica que el sistema inició un entorno gráfico o que alguien había intentado exportar una interfaz gráfica de manera remota.
.ICE-unix	946	Protocolo para que las aplicaciones del entorno se comuniquen entre sí, confirmando que se ejecutaron procesos en un entorno de escritorio interactivo el **08 de octubre** del mismo año.

Ruta de archivo agent.946

/img_debian-disk001.vmdk/vol_vol2/tmp/ssh-XXXXXXGZYLks

Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
agent.946				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST
[current folder]				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST
[parent folder]				2024-10-08 23:39:27 CEST	2024-10-08 23:39:27 CEST	2024-10-08 23:28:39 CEST	2024-07-31 18:13:51 CEST

Ruta de archivo X0

/img_debian-disk001.vmdk/vol_vol2/tmp/.X11-unix

Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
X0				2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST
[current folder]				2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST
[parent folder]				2024-10-08 23:39:27 CEST	2024-10-08 23:39:27 CEST	2024-10-08 23:28:39 CEST	2024-07-31 18:13:51 CEST

Ruta de archivo 946

/img_debian-disk001.vmdk/vol_vol2/tmp/.ICE-unix

Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
946				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST
[current folder]				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST
[parent folder]				2024-10-08 23:39:27 CEST	2024-10-08 23:39:27 CEST	2024-10-08 23:28:39 CEST	2024-07-31 18:13:51 CEST

*Notas: "Se analizó el archivo de configuración de shell **.bashrc** del usuario debian, confirmando que el atacante no inyectó scripts de ejecución automática ni modificó los parámetros del historial para ocultar su actividad".*

Registro de inicio de sesión

Se confirma el inicio de dos sesiones gráficas **MATE** el **08 de octubre de 2024** a las 04:48 Pm y 05:28 PM, ambos vinculados al usuario **debian**.

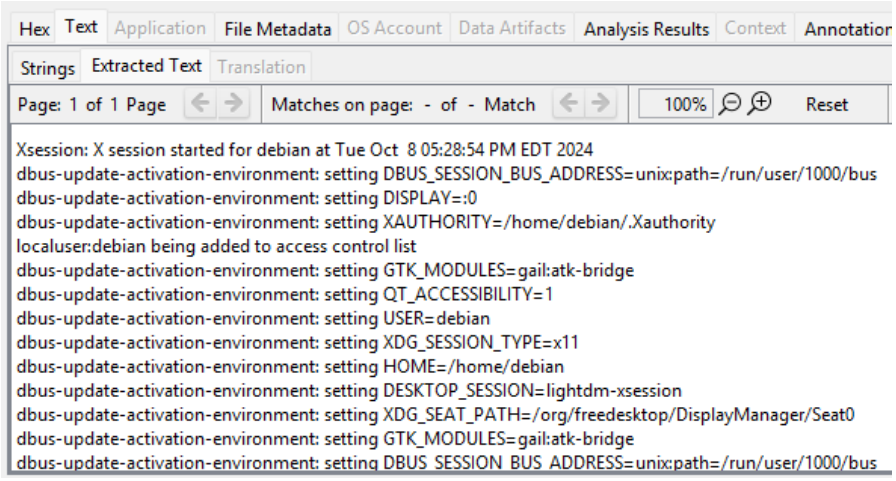
.xsession-errors		0
.xsession-errors.old		

- Primera conexión (.xsession-errors.old):

Page: 1 of - Page | Matches on page: - of - Match | 100% | Reset

```
Xsession: X session started for debian at Tue Oct  8 04:48:15 PM EDT 2024
dbus-update-activation-environment: setting DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
dbus-update-activation-environment: setting DISPLAY=:0
dbus-update-activation-environment: setting XAUTHORITY=/home/debian/.Xauthority
localuser:debian being added to access control list
dbus-update-activation-environment: setting GTK_MODULES=gail:atk-bridge
dbus-update-activation-environment: setting QT_ACCESSIBILITY=1
dbus-update-activation-environment: setting USER=debian
dbus-update-activation-environment: setting XDG_SESSION_TYPE=x11
dbus-update-activation-environment: setting HOME=/home/debian
dbus-update-activation-environment: setting DESKTOP_SESSION=lightdm-xsession
dbus-update-activation-environment: setting XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
```

- Segunda conexión (.xsession-errors):

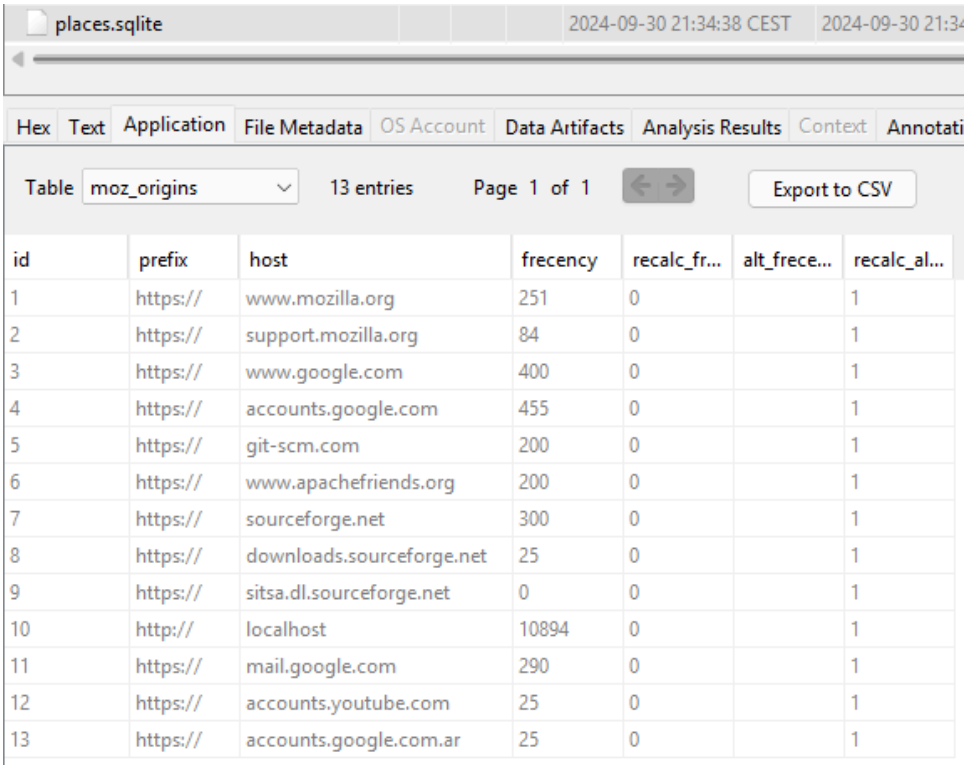


Navegación sospechosa

Durante el análisis se encuentran movimientos por los dominios de [apachefriends.org](), [sourceforge.net](), [git-scm.com]()

- **Fase de Preparación (28/09/2024):** Descarga de instaladores de XAMPP desde sourceforge.net y consultas a [apachefriends.org]().

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
places.sqlite			0	https://git-scm.com/downloads	2024-08-01 00:16:32 CEST	https://www.google.com/search?client=firefox-b-e&...	Git - Downloads
places.sqlite			0	https://git-scm.com/download/linux	2024-08-01 00:16:37 CEST	https://git-scm.com/downloads	Git
places.sqlite			3	https://www.google.com/search?client=firefox-b-e&...	2024-09-28 22:51:04 CEST		xammp - Buscar con Google
places.sqlite			1	https://www.apachefriends.org/es/download.html	2024-09-28 22:51:13 CEST	https://www.google.com/search?client=firefox-b-e&...	Download XAMPP
places.sqlite			1	https://www.apachefriends.org/es/download_success....	2024-09-28 22:52:27 CEST	https://www.apachefriends.org/es/download.html	XAMPP Download Success
places.sqlite			1	https://sourceforge.net/projects/xampp/files/XAMPP...	2024-09-28 22:52:31 CEST	https://sourceforge.net/projects/xampp/files/XAMPP...	Download xampp-osx-8.0.28-0-installer.dmg (XAMPP)
places.sqlite			1	https://sitsa.dl.sourceforge.net/project/xampp/XAMP...	2024-09-28 22:52:48 CEST	https://sourceforge.net/projects/xampp/files/XAMPP...	xampp-osx-8.0.28-0-installer.dmg
places.sqlite			1	https://sourceforge.net/projects/xampp/postdownload	2024-09-28 22:52:58 CEST	https://sourceforge.net/projects/xampp/files/XAMPP...	Find out more about XAMPP | SourceForge.net
places.sqlite			1	https://sourceforge.net/projects/xampp/	2024-09-28 22:53:16 CEST	https://sourceforge.net/projects/xampp/postdownload	XAMPP download | SourceForge.net

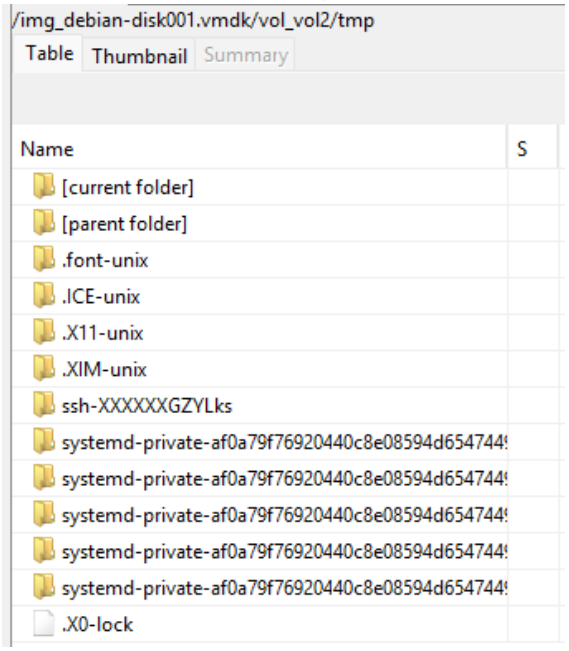


id	prefix	host	frecency	recalc_fr...	alt_frece...	recalc_al...
1	https://	www.mozilla.org	251	0		1
2	https://	support.mozilla.org	84	0		1
3	https://	www.google.com	400	0		1
4	https://	accounts.google.com	455	0		1
5	https://	git-scm.com	200	0		1
6	https://	www.apachefriends.org	200	0		1
7	https://	sourceforge.net	300	0		1
8	https://	downloads.sourceforge.net	25	0		1
9	https://	sitsa.dl.sourceforge.net	0	0		1
10	http://	localhost	10894	0		1
11	https://	mail.google.com	290	0		1
12	https://	accounts.youtube.com	25	0		1
13	https://	accounts.google.com.ar	25	0		1

- **Obtención de Herramientas**: Uso de git para clonar repositorios y curl para la descarga del CMS WordPress (latest.tar.gz) en el directorio /tmp.

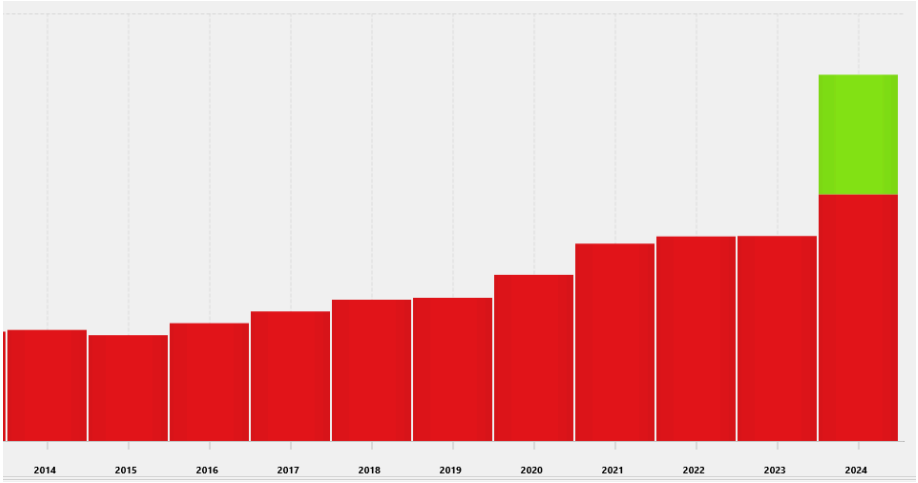
```
cd /tmp
curl -O https://wordpress.org/latest.tar.gz
sudo apt install curl
curl -O https://wordpress.org/latest.tar.gz
tar xzvf latest.tar.gz
sudo cp -a /tmp/wordpress/. /var/www/html/
sudo chown -R www-data:www-data /var/www/html/
sudo chmod -R 755 /var/www/html/
cd /var/www/html/
sudo mv wp-config-sample.php wp-config.php
sudo nano wp-config.php
ip a
sudo systemctl restart apache2
sudo systemctl status apache2
sudo apt install php libapache2-mod-php php-mysqli php-gd php-xml php-mbstring php-curl -y
cd ..
sudo nano /etc/apache2/sites-available/000-default.conf
```

- **Interacción Web**: Acceso a install.php y wp-admin desde la dirección 127.0.0.1, confirmando el uso de un túnel SSH para evadir controles de red.
- **Historial de Navegador**: Localización de accesos en places.sqlite a SourceForge y ApacheFriends (28/09/2024).
- **Descargas**: Evidencia del uso de curl para descargar latest.tar.gz (WordPress) en el directorio /tmp.
- **Limpieza**: El atacante eliminó los instaladores originales en /tmp, aunque los historiales de terminal quedaron intactos.

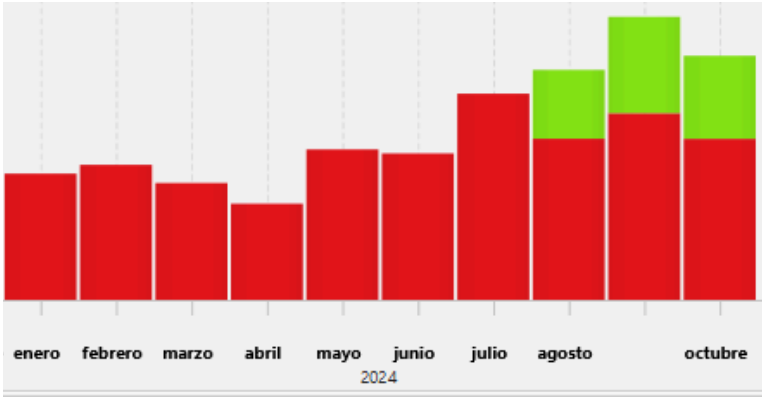


Línea de tiempo (TimeLine)

Bajo una comparativa de la actividad de la última década registrada, cabe recalcar un alto movimiento en el último año (2024), triplicando al año 2014 y casi duplicando al año 2023. Así, dando lugar a que la premeditación del ataque no fue tan extensa para años de preparación.



El mayor pico de actividad se sitúa entre agosto y octubre, dando más protagonismo a diciembre, lo que encamina de que fue el mes concreto del ataque.



Resultados de escaneo del servidor

El escaneo tiene como objetivo identificar la aparición de rootkits o malware presente en el servidor:

- Haciendo el escaneo con el comando **rkhunter --check --sk:** Se obtiene un listado extenso sobre los rootkits analizados. De todos modos, los rootkits pueden ser falsos positivos debido a que en los listados cómo *found*, de lo contrario suele ser porque son alertas de cambios de propiedades de archivos.

```
Rootkit checks ...
    Rootkits checked : 497
    Possible rootkits: 3
```

Vulnerabilidades identificadas

Durante el análisis, se encontraron diferentes vulnerabilidades que han comprometido la información total de la base de datos:

- **Configuración de sudo permisiva:** Se permitió al usuario inicial tomar el control total del sistema.
- **Servicios innecesarios:** La instalación de un servidor SSH no supervisado facilitó el túnel para hacer el ataque web.
- **Contraseñas débiles:** El uso de credenciales como “123456” y “password” en servicios críticos.
- **Falta de Hardening (fortalecimiento de sistemas):** El historial de MySQL (.mysql_history) quedó evidenciado en texto plano, dando lugar a reconstruir la creación de usuarios maliciosos.
- **Protocolos Inseguros**: Uso de FTP, que transmite datos y claves sin cifrado.

Fase de erradicación

La fase de erradicación tiene como finalidad **revertir** los **cambios** realizados por el **atacante** y evitar que se siga propagando la escalación de privilegios al servidor.

Eliminación de los usuarios DB

Dado que el atacante conoce los usuarios de la base de datos (user y wordpressuser), es necesario borrarlos ya que de esta manera no tendrá acceso a ellos y no podrá comprometer la información.

```
MariaDB [(none)]> DROP USER user@localhost ; FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.004 sec)

Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> DROP USER 'wordpressuser'@'localhost'; FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.014 sec)

Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> SELECT User FROM mysql.user;
+-------------+
| User        |
+-------------+
| mariadb.sys |
| mysql       |
| root        |
+-------------+
3 rows in set (0.001 sec)
```

Eliminación de privilegios al usuario debian

Para evitar la escalación de privilegios del usuario debian, será necesario hacer los siguientes pasos:

- Limpieza de sudoers en /etc/sudoers con “nano” (eliminar a debian de esa lista)

```
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

- **Expulsar de grupos:** Debido a que se ha borrado a **debian** del archivo **sudoers**, al ejecutar el comando éste **rechaza al usuario**, dando así a la aplicación del **principio de menor privilegio**.

```
debian@debian:~$ sudo deluser debian adm
debian is not in the sudoers file.
This incident has been reported to the administrator.
debian@debian:~$ groups debian
debian : debian cdrom floppy audio dip video plugdev users netdev bluetooth lpadmin scanner
debian@debian:~$
```

- **Eliminar persistencia de /tmp:** Debido a que se ha revocado a debian de sudoers, se tendrá que acceder a root para aplicar los comandos restantes. Así con el comando de rm se da lugar a la **eliminación de rastros** del inicio de sesión del **8 de octubre**.

```
root@debian:~# rm -rf /tmp/.X11-unix /tmp/.ICE-unix /tmp/ssh-*
```

```
root@debian:~# ls -la /tmp
total 40
drwxrwxrwt  9 root root 4096 Jan 25 05:52 .
drwxr-xr-x 19 root root 4096 Sep 30  2024 ..
drwxrwxrwt  2 root root 4096 Jan 24 12:22 .font-unix
drwx------  3 root root 4096 Jan 24 12:22 systemd-private-12a548da56204d06b99e94f0fff6ec28-apache2.service-zG5aiz
drwx------  3 root root 4096 Jan 24 12:22 systemd-private-12a548da56204d06b99e94f0fff6ec28-ModemManager.service-MmfGLr
drwx------  3 root root 4096 Jan 24 12:22 systemd-private-12a548da56204d06b99e94f0fff6ec28-systemd-logind.service-yIf0le
drwx------  3 root root 4096 Jan 24 12:22 systemd-private-12a548da56204d06b99e94f0fff6ec28-systemd-timesyncd.service-5AE3mN
drwx------  3 root root 4096 Jan 25 05:24 systemd-private-12a548da56204d06b99e94f0fff6ec28-upower.service-M3pMxp
-r--r--r--  1 root root   11 Jan 24 12:22 .X0-lock
drwxrwxrwt  2 root root 4096 Jan 24 12:22 .XIM-unix
```

Acciones correctivas y medidas preventivas

Para remediar de manera temporal y corregir de manera permanente las vulnerabilidades encontradas, se hará lo siguiente:

Para las acciones correctivas:

- Aislamiento del servidor de la red.
- Eliminación de los usuarios de base de datos wordpressuser y user.
- Revocación de permisos de sudo para el usuario debian.
- Desactivación del servicio SSH y eliminación de servicios no autorizados.

Para las medidas preventivas:

- **Principio de Menor Privilegio**: Restringir la modificación de grupos de administración.
- **Hardening de SSH:** Cambiar el puerto por defecto y usar solo llaves públicas (desactivar contraseñas).
- **Monitoreo de Integridad:** Implementar herramientas para detectar cambios en archivos críticos y centralizar logs en un servidor externo.

Conclusiones

Aunque no se haya localizado una evidencia de una exfiltración de archivos de gran volúmen, existe la presencia del servicio FTP (vsftpd) activo y el compromiso total de la **Base de datos MariaDB** implican que toda la información del servidor fue accesible. Este riesgo de fuga se considera crítico debido al control total que ha habido sobre las tablas de datos.

El ataque ha sido confirmado como una configuración forzada local. Es decir, el atacante no explotó ningún fallo del kernel, sino que hizo provecho del acceso inicial a la shell del usuario ***debian*** para escalar privilegios mediante configuraciones permisivas en ***sudoers***. Una vez obtenida la identidad de root, el atacante montó una infraestructura **LAMP** propia para asegurar su acceso y control.

¿Qué usuarios estuvieron involucrados en el incidente?

- **Usuario debian (UID 1000)**: Fue la puesta principal de entrada y el ejecutor a nivel de sistema.
- **Usuario user (DB)**: Fue la identidad creada para mantener un control de los datos a largo plazo.

La intención que ha supuesto este ataque ha sido alta y premeditada. El atacante desactivó servicios de accesibilidad del sistema para ahorrar recursos, instaló varias herramientas de persistencia y realizó varias tareas para la limpieza de archivos temporales para así dificultar el análisis.