FACULTAD DE CIENCIAS MÉDICAS.
DR. FAUSTINO PÉREZ HERNÁNDEZ.
SANCTI SPÍRITUS.

XXVI JORNADA NACIONAL DE BIBLIOTECOLOGIA

Título: Tool - Malware como alternativa para eliminar virus informáticos.

Autores:

Lic. Adams Fernández Barrera.

Lic. Miguel Angel Herrera González.

Lic. Michel Soto García.

Ms.C. Yaima Rodríguez Peña.

Introducción:

En la actualidad, la tecnología forma parte esencial de la vida cotidiana:

En este trabajo se aborda un tema de gran relevancia en el ámbito de la seguridad informática: los virus - malware.

¿Qué es un Virus Informático?

Es un tipo de software malicioso, o malware, que se propaga entre las computadoras y causa daños a los datos y al software, tienen como objetivo interrumpir los sistemas, causar problemas operativos importantes y provocar la pérdida y filtraciones de datos.

En la Universidad de Ciencias Médicas Sancti Spíritus, los equipos informáticos se vieron afectados por múltiples infecciones de virus que, sorprendentemente, no fueron detectadas por el antivirus Segurmatica, reglamentado en el Plan de Seguridad Informática. Al probar otras soluciones comerciales, se obtuvo el mismo resultado: ninguna logró identificar las amenazas.

Objetivo:

Ante esta situación, se estableció en el presente trabajo:

Implementar dos herramientas informáticas que permitan detectar, eliminar y restaurar los efectos del virus-malware no identificado por el antivirus Segurmatica ni por otras soluciones comerciales en los equipos de la Universidad.

Desarrollo:

Con el propósito de la limpieza en las computadoras afectadas por múltiples virus informáticos propagados principalmente a través de memorias USB y discos extraíbles, lo cuales no fueron detectados por el antivirus institucional, se implementaron dos herramientas con la ayuda de la inteligencia artif icial **DeepSeek.**

➤ Herramienta 1 OnlyUSB.bat:

Es un script batch diseñado específ icamente para limpiar memorias USB y Discos extraíbles sin afectar el sistema operativo.

➤ Herramienta 2 OnlyPC.ps1:

Es un script de **PowerShell** que realiza una limpieza más profunda del **sistema completo**, complementando la acción de OnlyUSB.bat.

OnlyUSB.bat

Funciones principales:

- Elimina archivos sospechosos comunes (autorun.inf, *.lnk maliciosos, *.vbs, *.ps1 en la raíz).
- Restaura archivos y carpetas que fueron ocultados por el virus usando el comando (attrib -h -r -s /s /d).
- No requiere instalación; se ejecuta directamente desde la unidad USB limpia o desde una carpeta segura del sistema.

Fragmento representativo del código (ejemplo real)

```batch
@echo off
echo Limpiando unidad USB...
attrib -h -r -s /s /d %~d1\*.*
del /f /q %~d1\autorun.inf
del /f /q %~d1\*.vbs
del /f /q %~d1\*.ps1
echo Hecho.
pause
```

OnlyPC.ps1

Funciones principales:

- Escanea y elimina procesos maliciosos en memoria.
- Limpia tareas programadas, entradas de registro y servicios creados por virus USB.
- Elimina variantes de malware que se replican desde el USB al disco local (carpetas System Volume Information, Recycler, etc.).

Fragmento representativo del código (ejemplo real)

```powershell
Write-Host "Limpiando PC completa..." -ForegroundColor Green
Get-Process | Where-Object {$_.Name -match "virus|worm|malware"} | Stop-Process -Force
Remove-Item -Path "C:\ProgramData\*.tmp" -Recurse -Force -ErrorAction SilentlyContinue
Get-ScheduledTask | Where-Object {$_.TaskName -match "usb|worm"} | Unregister-ScheduledTask -Confir
m:$false
# ... más reglas de limpieza
```

Valoración Económica y Aporte Social:

En un país donde el acceso a software de seguridad es limitado y la conectividad es intermitente, estas dos herramientas representan una solución soberana, gratuita y efectiva para el problema cotidiano de los virus - malware. No solo ahorran recursos escasos, sino que protegen lo más valioso que tiene una universidad o centro: la información, los datos y el tiempo,evitando que se propague a través de la red.

Pueden generalizarse con otras instituciones como: el **MINED**, **MINSAP**, **MINCIN** y otras entidades que manejan información sensible en USB.

Conclusiones:

Como resultado del presente trabajo se implementaron dos herramientas propias con el apoyo del asistente inteligente artif cial DeepSeek, las cuales permitieron soluciones efectivas que resolvieron completamente el brote de virus - malware en la Universidad de Ciencias Médicas Sancti Spíritus, que no fueron detectados por el antivirus Segurmatica, ni por otras soluciones comerciales evaluadas.

Este trabajo demuestra, en la práctica, cómo la inteligencia artif cial acelera el desarrollo de soluciones de ciberseguridad efectivas, de bajo costo y adaptadas a las necesidades reales de una institución cubana, cubriendo brechas que las herramientas convencionales no logran identificar.

Recomendaciones:

Como cierre del presente trabajo, se recomienda formalizar la incorporación de las herramientas **OnlyUSB.bat** y **OnlyPC.ps1** al Plan de Seguridad Informática de la Universidad de Ciencias Médicas Sancti Spíritus, no como un reemplazo del antivirus Segurmatica, sino como un complemento especializado ante amenazas que este no logra detectar. Además, se sugiere capacitar al personal técnico y no técnico en su uso, y extender su aplicación a otras facultades y centros de la provincia, garantizando así una respuesta rápida, efectiva y soberana ante futuros brotes de virus - malware propagado por dispositivos extraíbles.

MUCHAS GRACIAS