



ICS202 – Algoritmos Maliciosos  
Prof.: Ing. Harold Marzán

# Proyecto Final

## Ransomware

1098139 – Vladimir González

# TABLA DE CONTENIDO

01

## Introducción

Concepto de ransomware y métodos de infección.

02

## Diseño del virus

Objetivo, entorno operativo y proceso de ataque.

03

## Demostración

Ejecución del virus en una máquina virtual de Windows 10 Home.



01

# Introducción

# RANSOMWARE

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal.

Según su comportamiento, al ransomware se le puede denominar:

- Scareware.
- Bloqueadores de pantalla.
- Ransomware de cifrado.



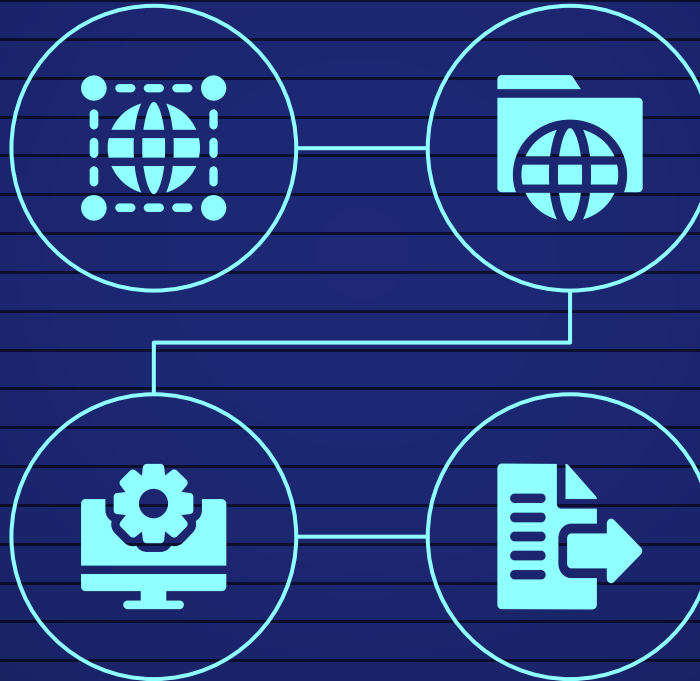
# MEDIOS DE INFECCIÓN

## Malspam

Es un correo electrónico no solicitado que se utiliza para distribuir malware.

## Spear phishing

Email dirigido a un individuo dentro de una organización que parece provenir de una fuente confiable.



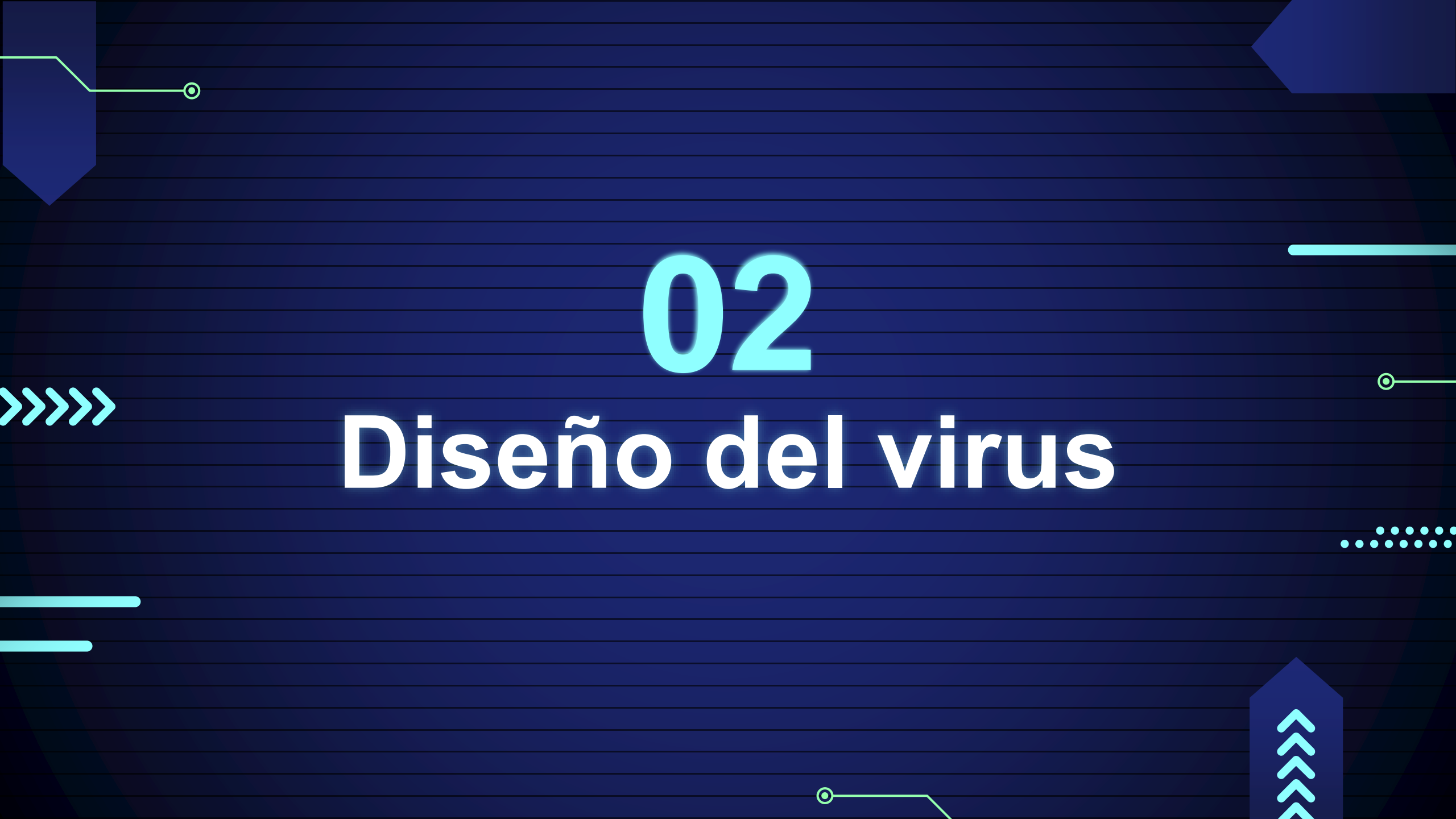
## Malvertising

Publicidad online para distribuir malware sin interacción del usuario.

## Ingeniería social

Los hackers la usan para asustar a los usuarios y hacerles pagar una suma de dinero para desbloquear sus archivos.





02

>>>>>>

# Diseño del virus

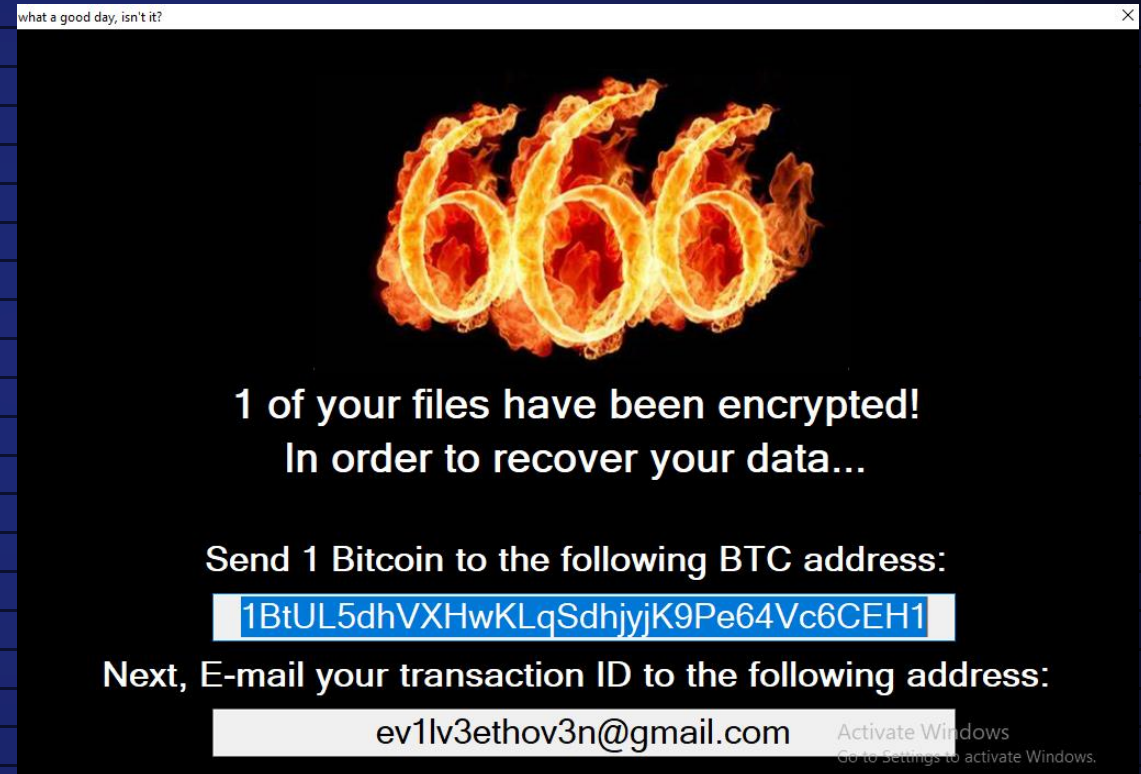




# WHAT A GOOD DAY, ISN'T IT?

Desarrollado en **C#** utilizando Windows Forms, el ransomware, cuyo irónico nombre es “What a good day, isn’t it?” está diseñado para:

- Operar en el ambiente de **Windows 10**.
- Encriptar los archivos localizados en el **Escritorio**, **Descargas** y **Documentos** del computador.
- Eliminar los archivos base y mostrarle al usuario archivos encriptados, no interpretables a simple vista.
- Guardar un registro de los archivos encriptados.
- Mostrar una pantalla para consumo del usuario.



# PROCESO DE ENCRYPTADO



## Paso 1

Llena un array de 32 bytes con una secuencia criptográfica fuerte de números aleatorios.



## Paso 2

Crea un archivo con el mismo nombre del que se pretende encriptar con la extensión .jcrypt.



## Paso 3

Convierte la contraseña definida como constante en el programa a un array de bit.



## Paso 4

Aplica el algoritmo de encriptado simétrico de Rijndael, indicándole sus propiedades

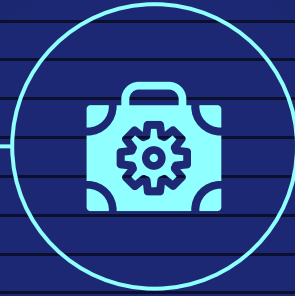


# PROCESO DE ENCRYPTADO



## Paso 5

Para el objeto de encriptado Rijnjael, le asigna una llave (usando el método Rfc2898DeriveBytes) y la encripta en dos ocasiones.



## Paso 6

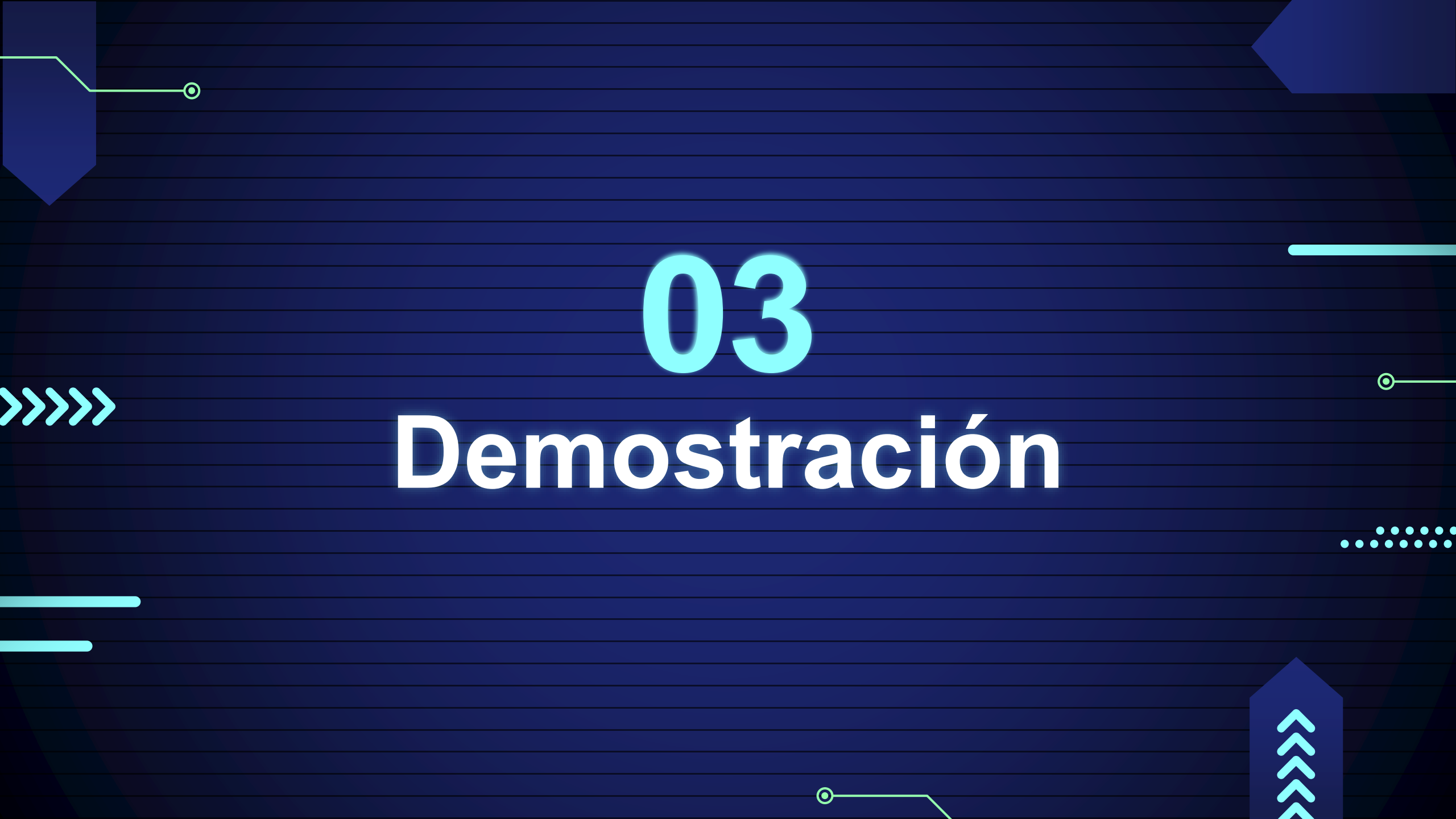
Crea un buffer de un mega (1 MB) para solo asignar esta cantidad de memoria y no el tamaño completo del archivo.



## Paso 7

En un archivo .txt, se agregan iteradamente los archivos encriptados y se eliminan los originales de la ruta del ordenador que está siendo intervenida.





03

Demostración



# Proyecto Final

## Ransomware

# REFERENCIAS BIBLIOGRÁFICAS

- Kamaruzzaman, M. (2021, 11 diciembre). *Microservice Architecture: A brief overview and why you should use it in your next project*. Medium. <https://towardsdatascience.com/microservice-architecture-a-brief-overview-and-why-you-should-use-it-in-your-next-project-a17b6e19adfd>
- Kamaruzzaman, M. (2022, 12 abril). *Microservice Architecture and its 10 Most Important Design Patterns*. Medium. <https://towardsdatascience.com/microservice-architecture-and-its-10-most-important-design-patterns-824952d7fa41>
- Malwarebytes. (s. f.). *What is Ransomware? | How to Protect Against Ransomware*. <https://www.malwarebytes.com/ransomwar>
- Microsoft. (s. f.-a). *Rfc2898DeriveBytes Class (System.Security.Cryptography)*. Microsoft Docs. <https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rfc2898derivebytes?view=net-6.0>

# REFERENCIAS BIBLIOGRÁFICAS

- Microsoft. (s. f.-b). *RNGCryptoServiceProvider Class (System.Security.Cryptography)*. Microsoft Docs.  
<https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rngcryptoserviceprovider?view=net-6.0>
- Microsoft. (s. f.-c). *RNGCryptoServiceProvider.GetBytes Method (System.Security.Cryptography)*. Microsoft Docs.  
<https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rngcryptoserviceprovider.getbytes?view=net-6.0>
- Microsoft. (s. f.-d). *System.Security.Cryptography Namespace*. Microsoft Docs. <https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography?view=net-6.0>
- Quanti. (2022, 25 enero). *La historia del ransomware: Historia, tipos de ransomware y futuros impactos*. Quanty.  
<https://quanti.com.mx/articulos/la-historia-del-ransomware-historia-tipos-de-ransomware-y-futuros-impactos/>
- Tarek, A. (2022, 8 enero). *.NET C# Covariance & Contravariance - Ahmed Tarek - Medium | Level Up Coding*. Medium.  
<https://levelup.gitconnected.com/covariance-and-contravariance-in-net-c-c2b8576b2155?gi=46e3d55892>