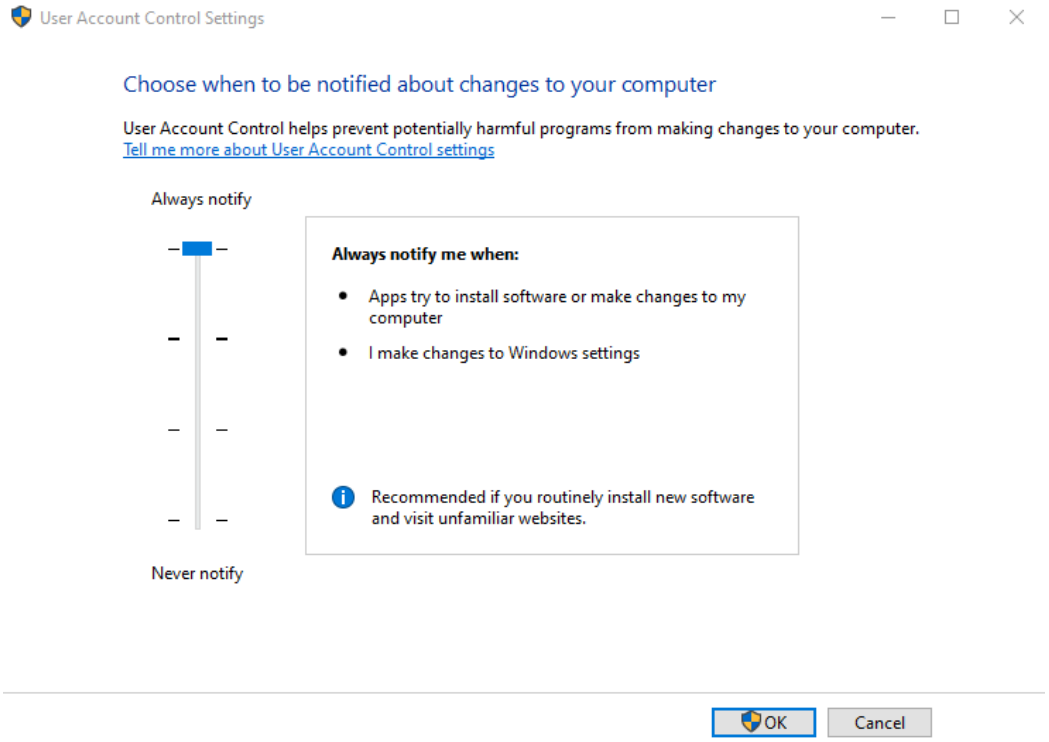
DESAFÍO 16 - INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Miriam Romitelli.

USER ACCOUNT CONTROL

1. Configurar User Account Control para que solicite confirmación siempre.
   Desde el User Account Control Settings se puede configurar que siempre se solicite confirmación cuando se hagan instalaciones de software o cambios en la maquina; o en las configuraciones de Windows.



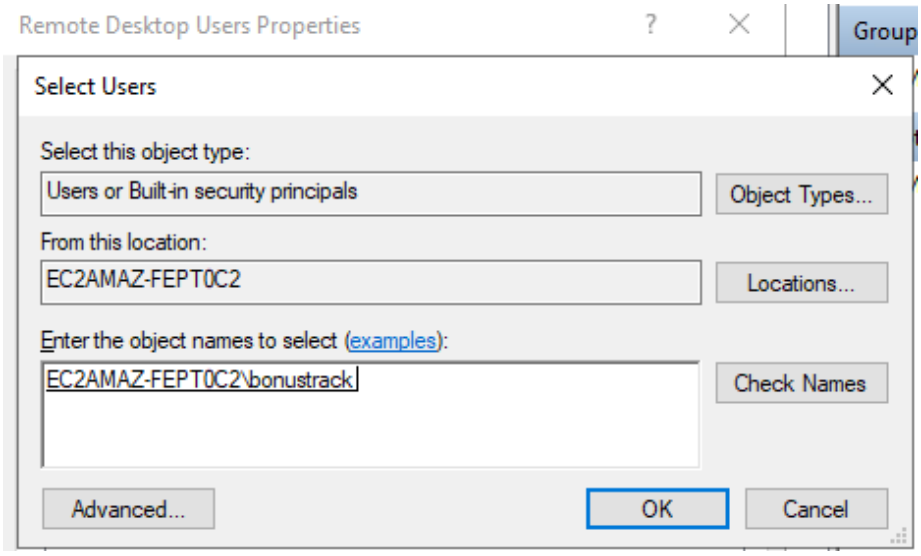
REMOTE DESKTOP

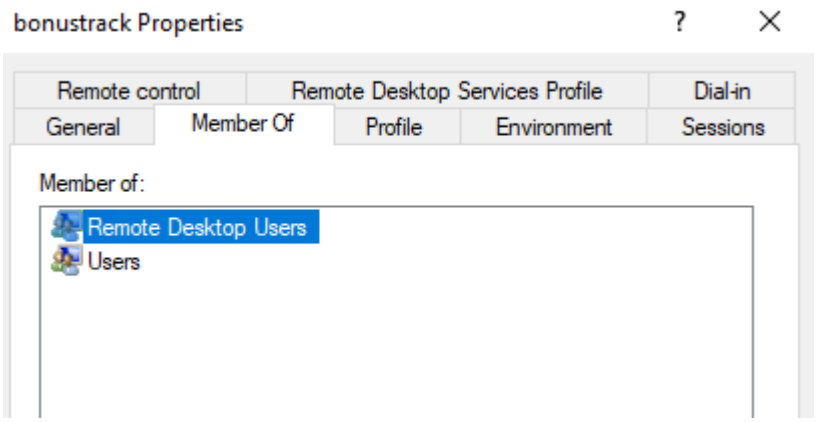
2. Habilitar el acceso por Remote Desktop.

3. Crear una cuenta de usuario llamada bonustrack.

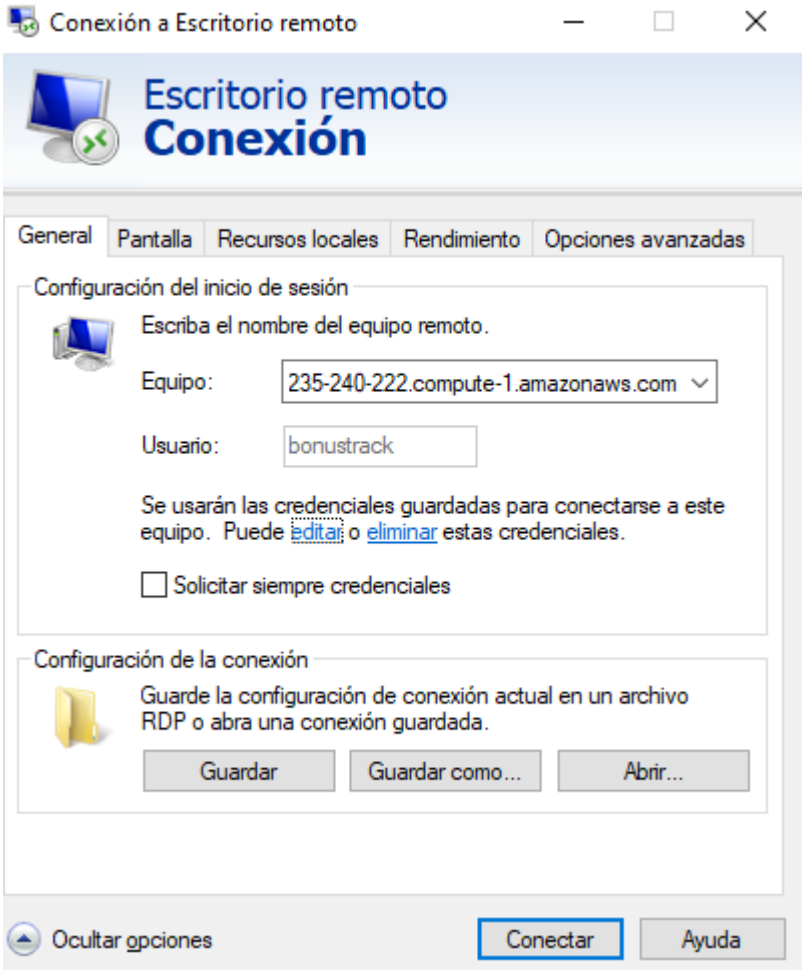
4. Asignar permisos básicos (users) al usuario creado anteriormente.

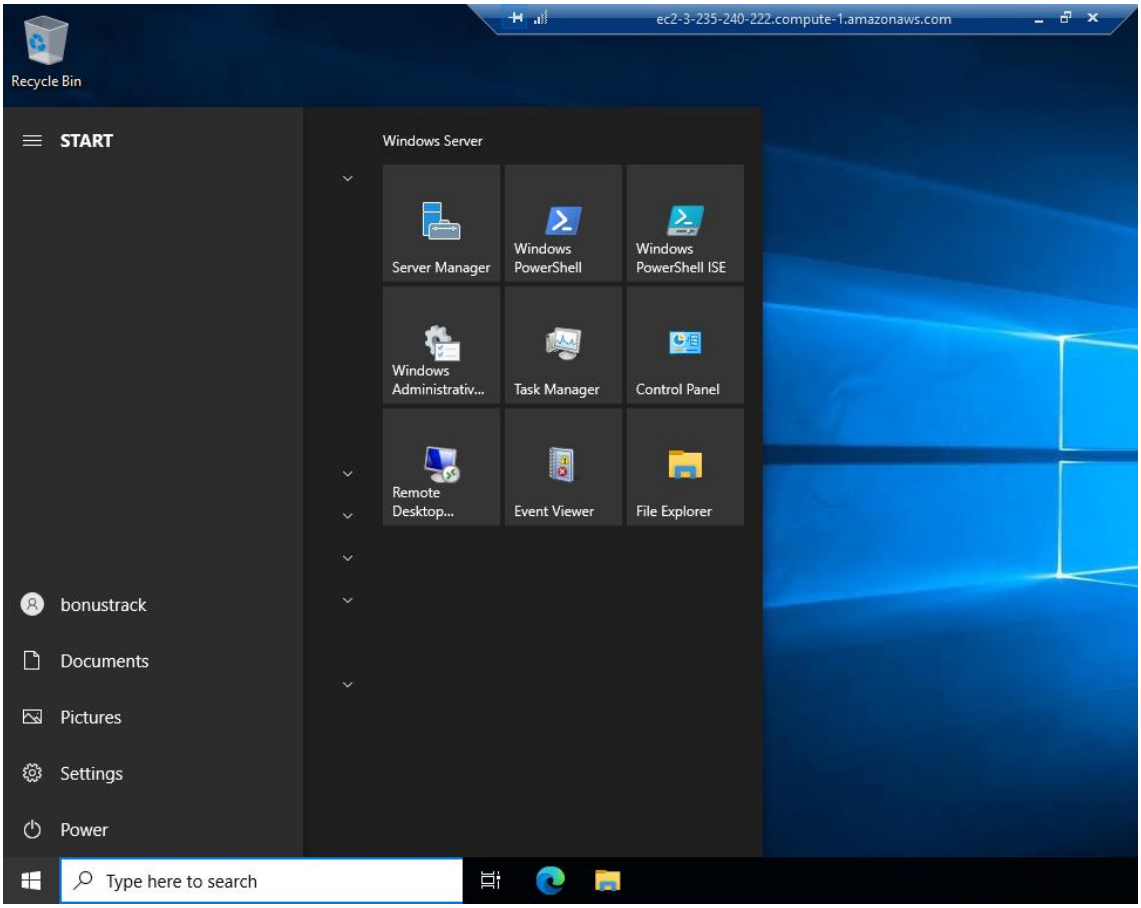
5. Conceder privilegios al usuario bonustrack para tener la posibilidad de iniciar sesión a través de Remote Desktop.





Comprobación del ingreso con el usuario bonustrack por conexión a escritorio remoto:



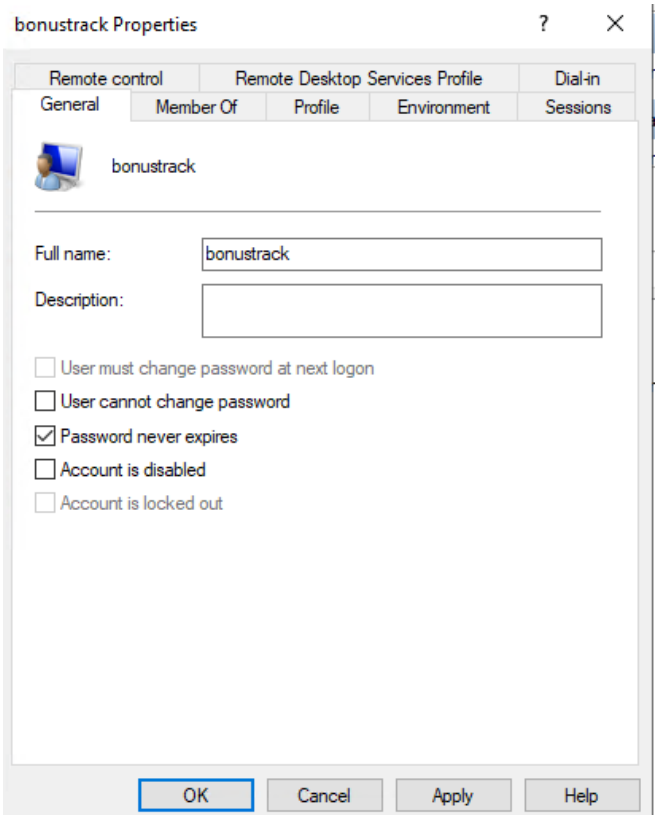


DIRECTIVAS DE SEGURIDAD

6. Habilitar la complejidad de contraseñas.

7. Configurar:

a. No expiren las contraseñas.

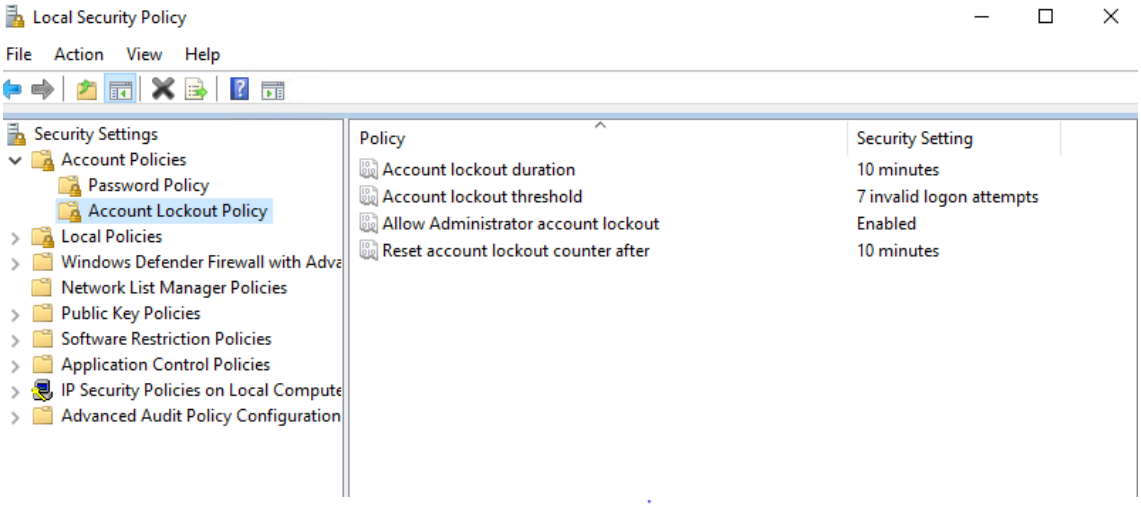


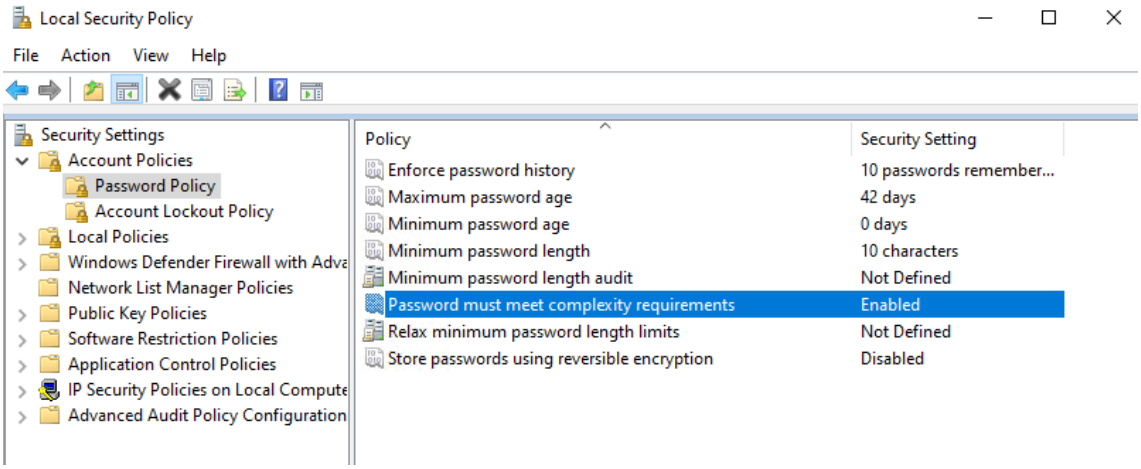
b. Contraseñas con 10 caracteres de longitud.

c. Evitar la reutilización de las últimas 10 contraseñas.

d. Bloqueo de cuentas luego de 7 intentos fallidos.

e. Desbloqueo automático después de 10 minutos.



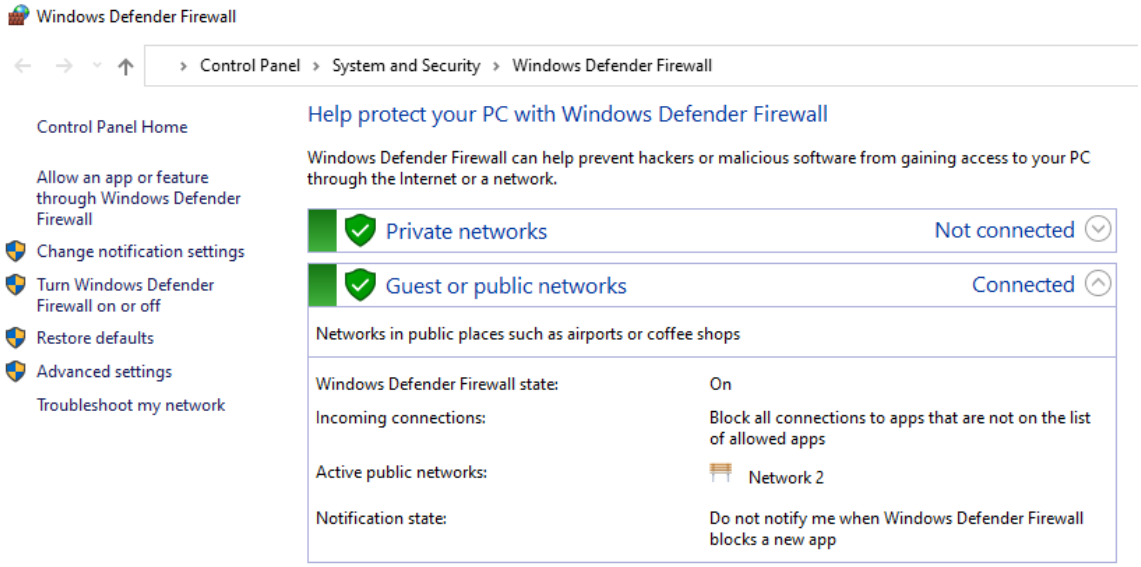


Todas estas configuraciones se hacen desde el Local Security Policy.

<u>WINDOWS DEFENDER</u>

8. Habilitar Windows Defender (en el caso de que no se encuentre presente).

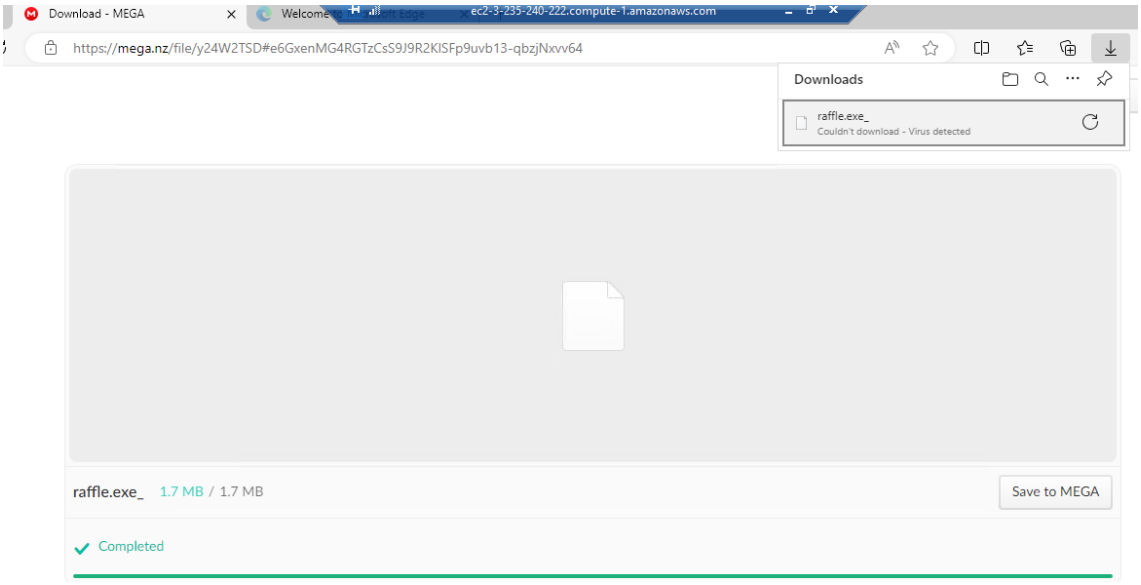
Verificaciones de Windows Defender Firewall desde Control Panel → System and Security



9. Descargar raffle.exe desde:

https://mega.nz/file/y24W2TSD#e6GxenMG4RGTzCsS9J9R2KlSFp9uvb13-qbzjNxvv64.

10.Verificar que Windows Defender lo haya detectado

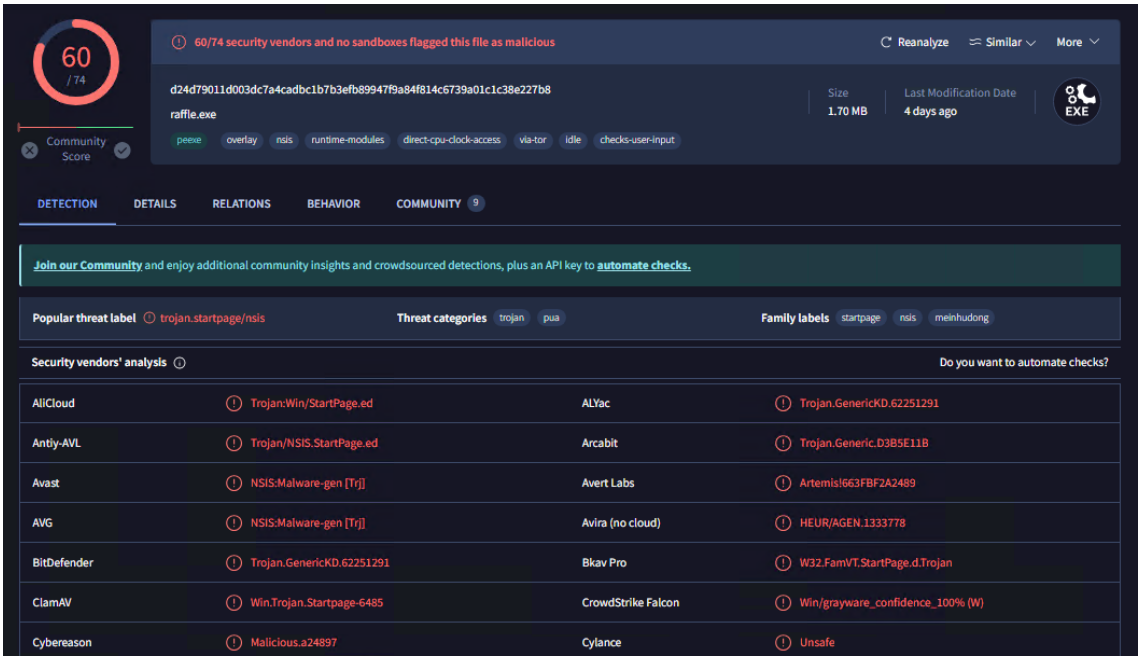


11.Subir el archivo descargado al sitio VirusTotal.

https://www.virustotal.com/gui/home/upload

12.Analizar y mostrar el resultado.

60/74 security vendors and no sandboxes flagged this file as malicious


60
/ 74
Community Score
60/74 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
d24d79011d003dc7a4cadbc1b7b3efb89947f9a84f814c6739a01c1c38e227b8
raffle.exe
peexe
overlay
nsis
runtime-modules
direct-cpu-clock-access
via-tor
idle
checks-user-input
Size
1.70 MB
Last Modification Date
4 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 9
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.startpage/nsis
Threat categories trojan pua
Family labels startpage nsis meinhudong
Security vendors' analysis
Do you want to automate checks?
AliCloud Trojan:Win/StartPage.ed
ALYac Trojan.GenericKD.62251291
Antiy-AVL Trojan/NSIS.StartPage.ed
Arcabit Trojan.Generic.D3B5E11B
Avast NSIS:Malware-gen [Trj]
Avert Labs Artemis!663FBF2A2489
AVG NSIS:Malware-gen [Trj]
Avira (no cloud) HEUR/AGEN.1333778
BitDefender Trojan.GenericKD.62251291
Bkav Pro W32.FamVT.StartPage.d.Trojan
ClamAV Win.Trojan.Startpage-6485
CrowdStrike Falcon Win/grayware_confidence_100% (W)
Cybereason Malicious.a24897
Cylance Unsafe


Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.StartPage.60470
Elastic Malicious (high Confidence)
Emsisoft Trojan.GenericKD.62251291 (B)
eScan Trojan.GenericKD.62251291
ESET-NOD32 Win32/Meinhudong.A Potentially Unwan...
Fortinet W32/StartPage.ED!tr
GData NSIS.Application.Meinhudong.D
Google Detected
Gridinsoft (no cloud) Malware.Win32.Gen.cc!s5
Ikarus Trojan.NSIS
K7AntiVirus Riskware (0040eff71)
K7GW Riskware (0040eff71)
Kaspersky Trojan.NSIS.StartPage.ed
Kingsoft Win32.Troj.Unknown.a
Lionic Trojan.NSIS.StartPage.lVEr
Malwarebytes Generic.Malware.AI.DDS
MAX Malware (ai Score=100)
McAfee Scanner Ti!D24D79011D00
Microsoft Trojan:Win32/Startpage!MSR
NANO-Antivirus Riskware.Nsis.Startpage.ctondj
Palo Alto Networks Generic.ml
Panda Trj/CI.A
Rising Trojan.Generic@AI.88 (RDML:y2DYzq5lejj...
Sangfor Engine Zero PUP.Win32.StartPage.Vwjl
SentinelOne (Static ML) Static AI - Suspicious PE
Skyhigh (SWG) GenDownloader.vb
Sophos Mal/DwnLdr-AJ
SUPERAntiSpyware Trojan.Agent/Gen-StartPage
Symantec Trojan.Gen.MBT
Tencent Nsis.Trojan.Startpage.Simw

Trapmine	Malicious.moderate.ml.score	Trellix (FireEye)	Trojan.GenericKD.62251291
TrendMicro	PUA.Win32.StartPage.NQ	TrendMicro-HouseCall	PUA.Win32.StartPage.NQ
Varist	W32/Trojan.UWRI-1182	VBA32	Trojan.StartPage
VIPRE	Trojan.GenericKD.62251291	VirIT	Trojan.Win32.Genus.CDM
Webroot	W32.Malware.Heur	WithSecure	Heuristic.HEUR/AGEN.1333778
Xcitium	TrojWare.Win32.StartPage.KPY@56k0ea	Yandex	PUA.StartPage.Gen.JK
Zillya	Trojan.StartPage.Win32.20829	ZoneAlarm by Check Point	Trojan.NSIS.StartPage.ed
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	CMC	Undetected
Jiangmin	Undetected	MaxSecure	Undetected
QuickHeal	Undetected	SecureAge	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
ViRobot	Undetected	Zoner	Undetected
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

HASHES

13. Crear un archivo de texto plano con el nombre prueba1.txt en donde el contenido del archivo sea únicamente EducaciónIT.

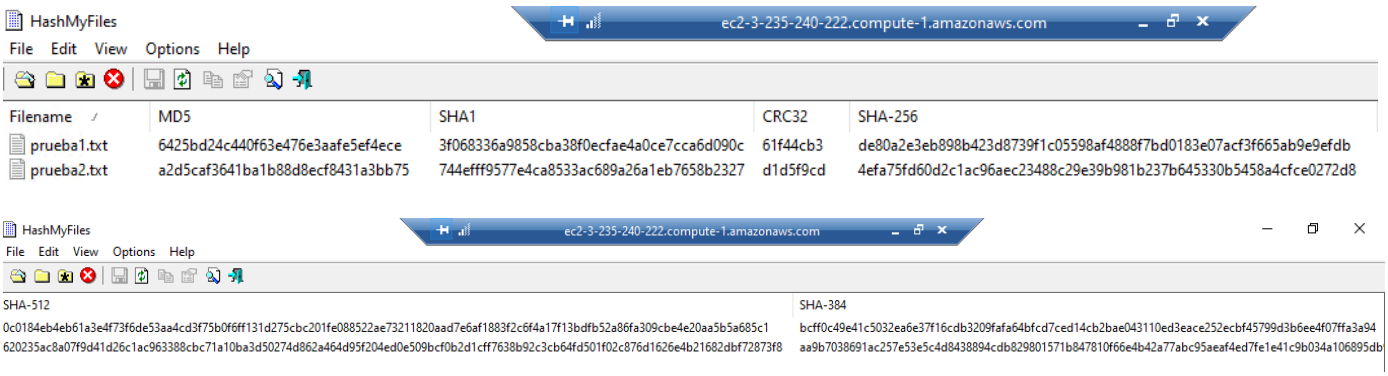
14. Calcular los valores hash del archivo con diferentes algoritmos, utilizando la herramienta HashMyFiles.

https://www.nirsoft.net/utils/hash_my_files.html

15. Crear un segundo archivo, agregar el siguiente contenido EducacionIT1, agregando un 1 (uno) al final, y guardar con el nombre prueba2.txt.

16. Volver a calcular los hashes y verificar si los mismos han cambiado con respecto a los anteriores.

Se descarga e instala la aplicación. Posteriormente con los archivos ya creados se utilizan para el análisis en el HashMyFiles:



Resultado: Los hash del archivo han cambiado con respecto a los anteriores.

VOLÚMENES DE DISCOS CIFRADOS

17. Usar VeraCrypt para crear un volumen de disco cifrado de 10 MB que utilice el algoritmo de Hash SHA 512 y el algoritmo de cifrado AES.

https://www.veracrypt.fr/en/Downloads.html

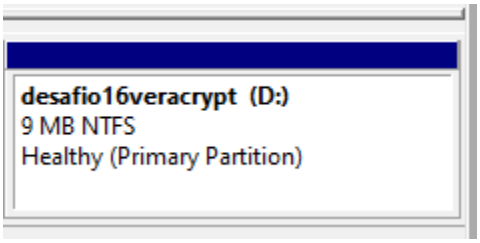
18. Montar el volumen cifrado.

19. Almacenar el archivo prueba1.txt del ejercicio 13 dentro del volumen.

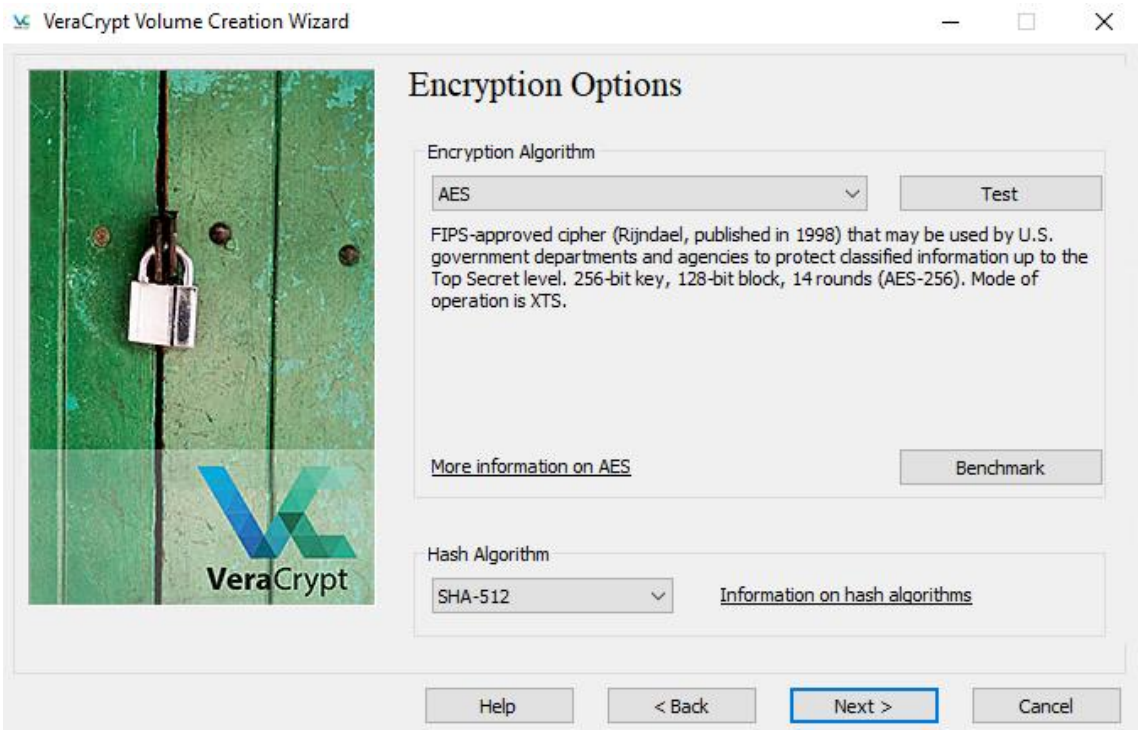
20. Desmontar el volumen, volver a montarlo y verificar si los archivos se encuentren intactos.

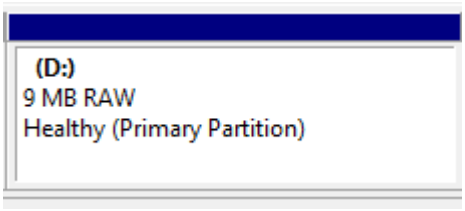
Primero hacemos la partición del disco:

El administrador de discos reconoce el volumen:



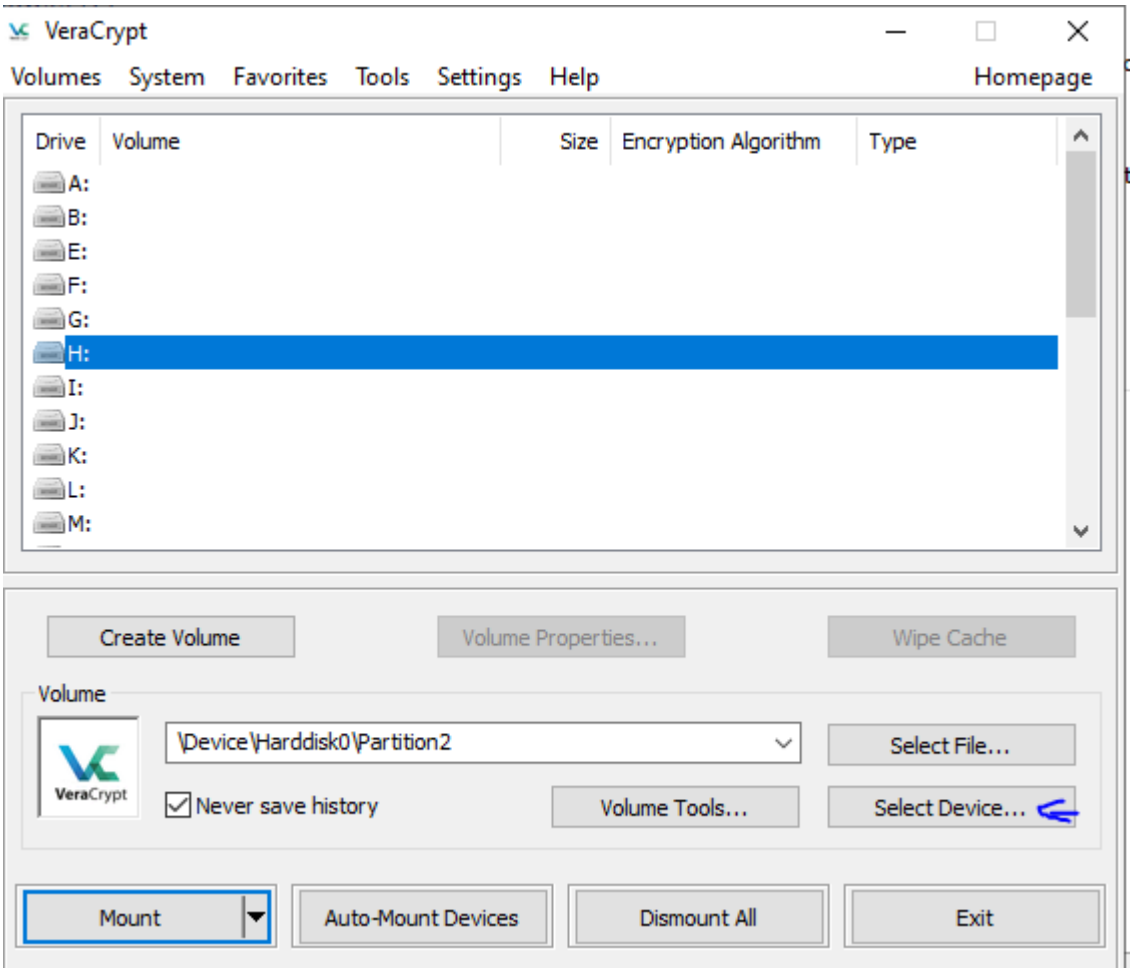
- ✓ *Con la aplicación VeraCrypt instalada ya se puede hacer el proceso de*
- ✓ *Asistente de Creación de Volumenes VeraCrypt: Cifrar partición/unidad secundaria.*
- ✓ *Tipo de Volumen: Volumen VeraCrypt común.*
- ✓ *Modo de creación de volumen: Cifrar partición conservando datos.*
- ✓ *Generar una contraseña de volumen.*
- ✓ *Modo de borrado: Ninguno (configuración rápida).*
- ✓ *Finalmente cifrar.*



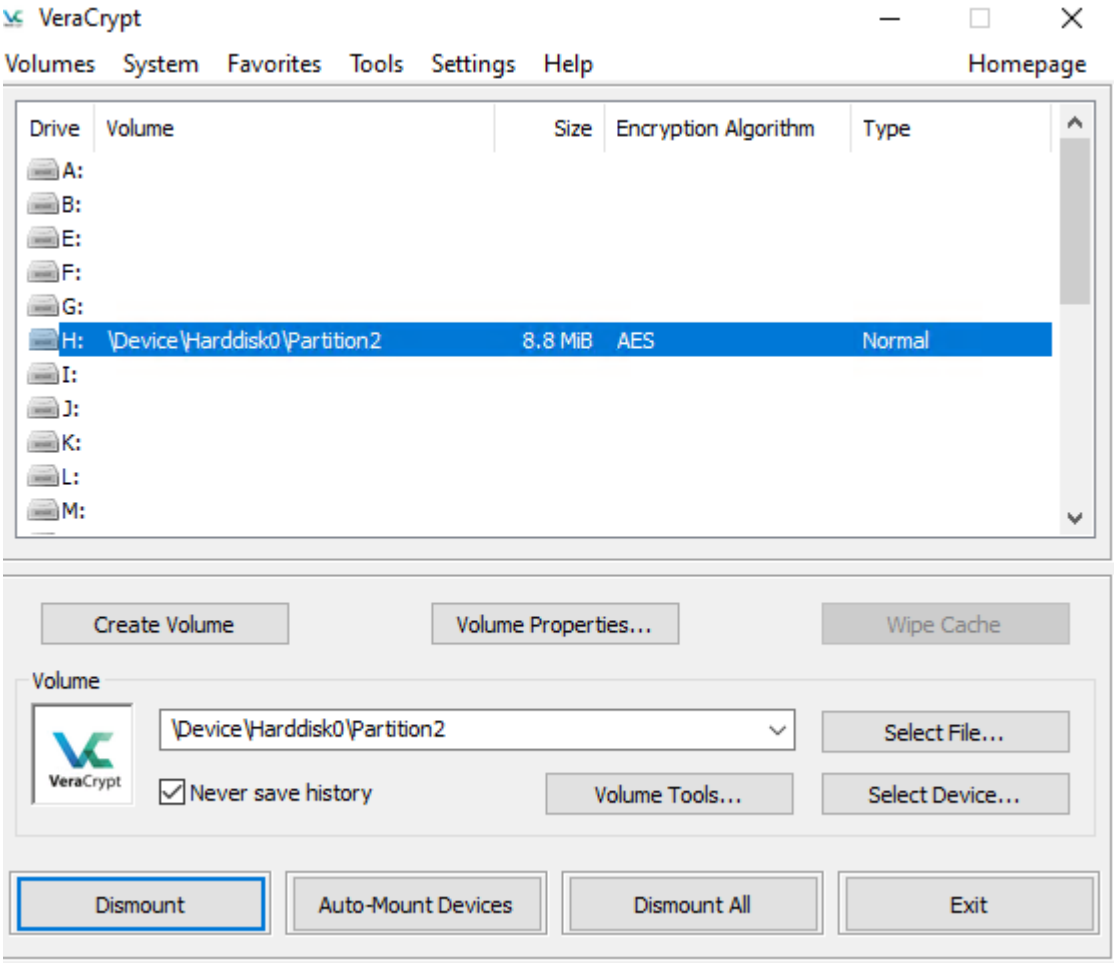


Después de este cambio ya no aparece el nombre que originalmente le habíamos dado al volumen.

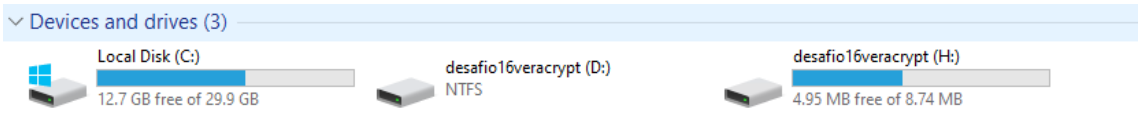
- ✓ *Montado con VeraCrypt:*
- ✓ *Seleccionar un volumen (ej.H)*
- ✓ *Seleccionar dispositivo.*
- ✓ *Seleccionar la partición correspondiente y colocar la contraseña para montar.*



En este caso se montó el D en el H.



Ahora está disponible y los archivos son accesibles:



Al desmontar y montar se mantiene intacto el archivo.

ALMACENAMIENTO DE CONTRASEÑAS

21. Usar KeePassXC para crear una base de datos de contraseñas.

https://keepassxc.org/download/#windows

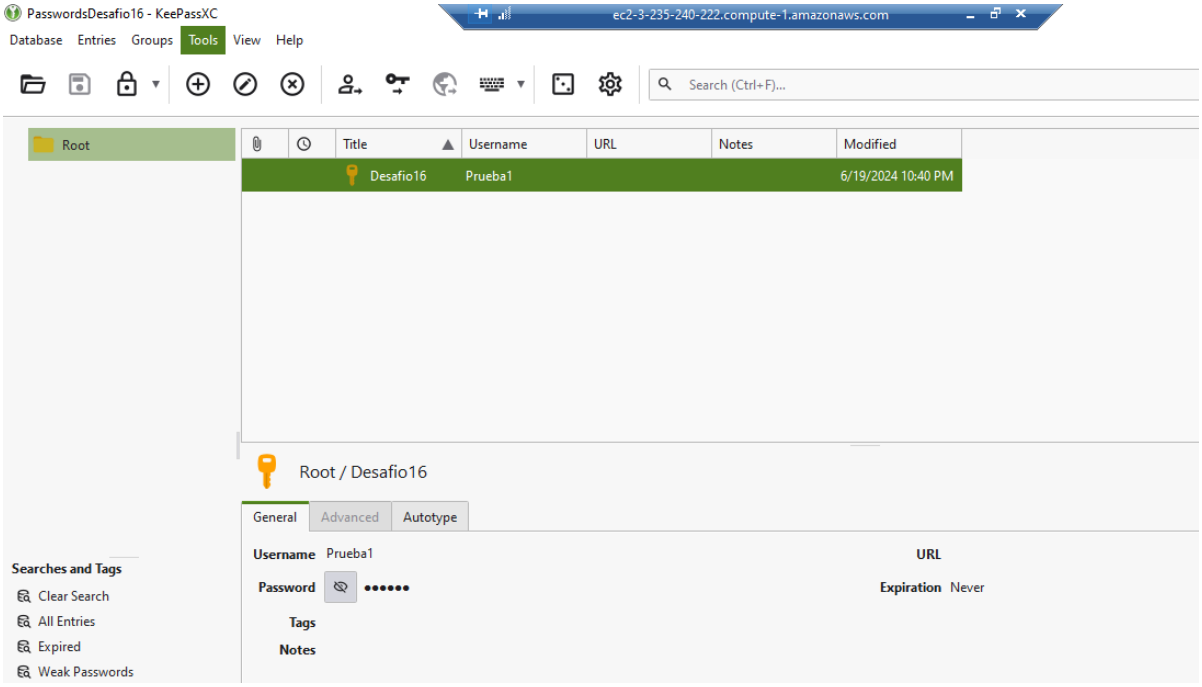
22. Almacenar credenciales con los siguientes datos:

a. Usuario: Prueba1.

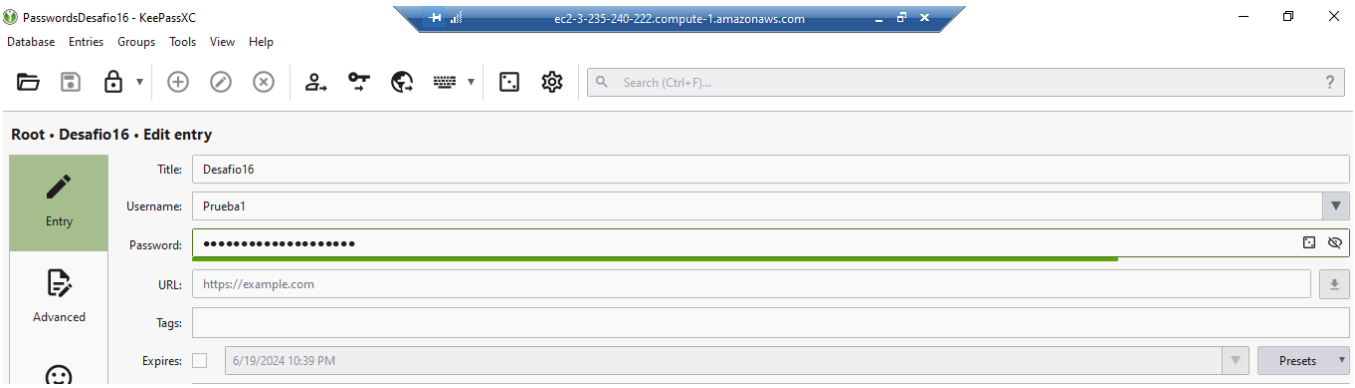
b. Contraseña: “AlgoSuperSeguro.7823”

23. Cerrar KeePassXC y volver a abrir.

24. Verificar si la contraseña que se ha almacenado esté presente en la base



Después de Cerrar KeePassXC y volver a abrir la contraseña que se ha almacenado está presente en la base:



Para el desafío generé una VM (AWS EC2) haciendo las pruebas en un entorno aislado y realizando las configuraciones de seguridad necesarias. Posterior a la práctica eliminé todos los recursos utilizados en AWS.