Nro. Alerta:	AL-2025-020	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	19-may-2025	Ransomware Meow	Pág.: **1** of **1**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de Incidente: Ransomware
Nivel de riesgo: Alto

II. ALERTA

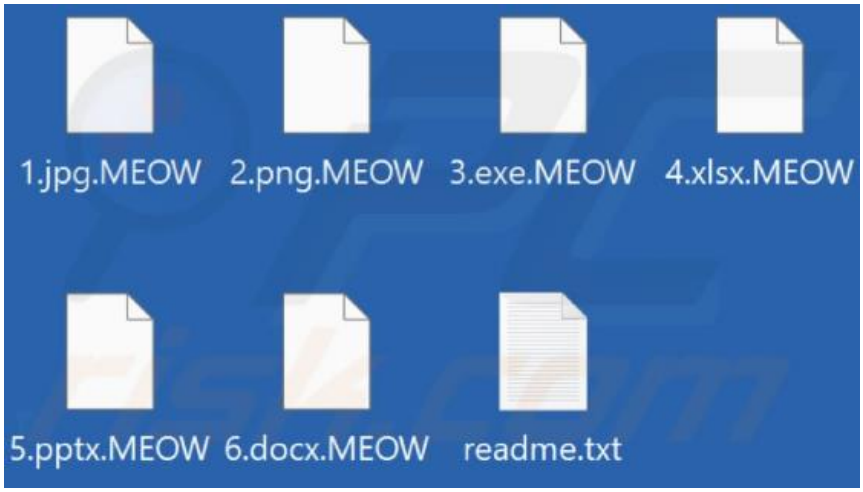

Figura 1.- Ransomware MEOW - figura referencial

Meow es un ransonware considerado una amenaza de cifrado de archivos, modifica los nombres de estos agregándole la extensión .MEOW para dejarlos inaccesibles al usuario.

III. INTRODUCCIÓN

El Ransomware MEOW infecta el dispositivo, cifra los archivos personales y críticos de la víctima, tales como documentos, imágenes, bases de datos, copias de seguridad y archivos ejecutables, tras esta infección los archivos afectados adicionan la extensión .MEOW y crea un archivo de nota de rescate llamado "readme.txt", con instrucciones para que las víctimas se pongan en contacto con los atacantes a través de las direcciones de correo electrónico: meowcorp2022@aol[.]com, meowcorp2022@proton[.]me, meowcorp@msgsafe[.]io y meowcorp@onionmail[.]org y dos nombres de usuario de Telegram (@meowcorp2022 y @meowcorp123) si necesitan descifrar los archivos.

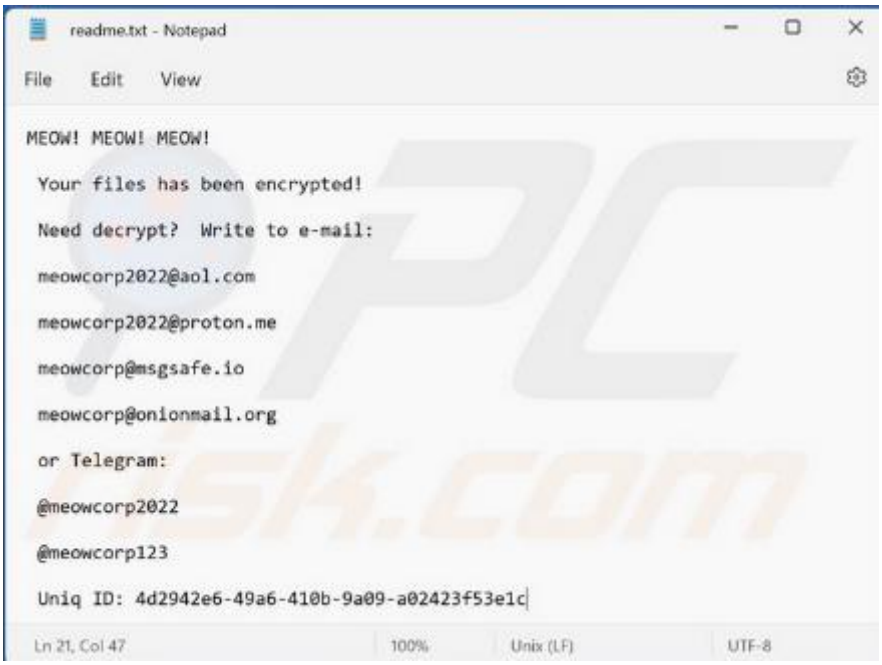

Figura 2.- mensaje de contacto - Ransomware MEOW

IV. VECTOR DE ATAQUE

TTP (Tácticas, técnicas y procedimiento)

Investigación de Bitdefender encontró el modo de actuar del ransomware por ciclos:

Acceso inicial usa correos electrónicos de phishing con un link de descarga, para ejecutar o instalar un archivo malicioso.

Explotación y movimiento lateral, se identificó que un script de Python se usa para lanzar exploits y establecer conexión con host remotos.

Ejecución, usa cifrador de ransomware que estabas asociado al proceso windows.exe que se determinó no es administrado por el host de la víctima.

Exfiltración, añade un ejecutable de MegaSync a una cuenta local en el sistema de la víctima. MegaSync, un cliente de almacenamiento en la nube probablemente fue la aplicación utilizada para la exfiltración.

Persistencia, los ejecutables PowerTool32.exe y PowerTool64.exe se identificaron como recursos disponibles para el atacante que le permitían infiltrarse y modificar procesos en el kernel de un objetivo y ocultar actividades maliciosas. Spoolsv.exe también se identificó como una posible técnica de persistencia; se accedió al ejecutable malicioso desde una carpeta compartida asociada con el atacante.

Evasión de defensa, el atacante intentó crear el archivo truenight.sys. Este archivo de sistema, conocido por interactuar con acciones a nivel de kernel, puede detener procesos EDR.

Se adjunta tabla del TTP con sus respectivos códigos.

Táctica ATT&CK	Técnica ATT&CK
Acceso Inicial (TA0001)	Explotación de Aplicaciones Expuestas al Público (T1190) Servicios Remotos Externos (T1133) Phishing (T1566)
Ejecución (TA0002)	Modulo Compartidos (T1129)
Defensa Evasión (TA0005)	Evasión de Defensa (TA0005) Archivos u Información Ofuscada (T1027) Eliminación de Indicadores de Herramientas (T1027.005) Suplantación (Masquerading) (T1036)
Acceso a Credenciales (TA0006)	Captura de Entrada (T1056)
Descubrimiento (TA0007)	Descubrimiento de Procesos (T1057) Descubrimiento de Información del Sistema (T1082) Descubrimiento de Archivos y Directorios (T1083) Evasión de Entornos Virtuales / Sandbox (T1497) Descubrimiento de Software de Seguridad (T1518.001)
Movimiento Lateral (TA0008)	Contenido Compartido Contaminado (T1080)
Recolección (TA0009)	Captura de Entrada (T1056)
Comando y Control (TA0011)	Protocolo de Capa de Aplicación (T1071) Canal Encriptado (T1573)
Exfiltración (TA0010)	Exfiltración a través de Canal C2 (T1041)
Impacto (TA0034)	Datos Cifrados para Impacto (T1486)

Tabla 1. Resumen de ataque – Ransomware MEOW

V. INDICADORES DE COMPROMISOS

Extensiones de archivo: .MEOW, .CAT, .KITTEN, o. FELINE.

Nota de rescate: "readme.txt"

Claves de Registro:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\MEOW

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser

Tráfico de la red:
meowransomware[.]com
meowransomware[.]net
meowransomware[.]org
185.141.25[.] 241
185.141.25[.] 242
185.141.25[.] 243
185.141.25[.] 244

Tabla 2. Tráfico de Red – Ransomware MEOW

SHA-256:
fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d04444476416f9
7f6421cdf6355edfdcbddadd26bcdfbf984def301df3c6c03d71af8e30bb781f
7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099
5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda5443481922f
222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853
B5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec

Tabla 3. SHA-256 – Ransomware MEOW

SHA-1:
59e756e0da6a82a0f9046a3538d507c75eb95252
987ad5aa6aee86f474fb9313334e6c9718d68daf
94a9da09da3151f306ab8a5b00f60a38b077d594
5949c404aee552fc8ce29e3bf77bd08e54d37c59
578b1b0f46491b9d39d21f2103cb437bc2d71cac
4f5d4e9d1e3b6a46f450ad1fb90340dfd718608b

Tabla 4. SHA-1 – Ransomware MEOW

(MD5)
8f154ca4a8ee50dc448181afbc95cfd7
4dd2b61e0ccf633e008359ad989de2ed
3eff7826b6eea73b0206f11d08073a68
1d70020ddf6f29638b22887947dd5b9c
033acf3b0f699a39becdc71d3e2dddcc
0bbb9b0d573a9c6027ca7e0b1f5478bf

Tabla 5. MD5 – Ransomware MEOW

VI. RECOMENDACIONES:

- Mantenga su sistema operativo y software al día con los últimos parches de seguridad y actualizaciones. Esto puede ayudar a prevenir vulnerabilidades que pueden ser explotadas por los atacantes.
- Utilice contraseñas fuertes y únicas para todas las cuentas y habilite la autenticación de dos factores siempre que sea posible. Esto puede ayudar a evitar que los atacantes tengan acceso a sus cuentas.
- Tenga cuidado con los correos electrónicos, enlaces y archivos adjuntos sospechosos. No abra correos electrónicos o haga clic en enlaces o archivos adjuntos de fuentes desconocidas o sospechosas.
- Utilice software antivirus y antimalware de buena reputación y manténgase al día. Esto puede ayudar a detectar y eliminar el malware antes de que pueda causar daños.
- Utilice un cortafuego para bloquear el acceso no autorizado a su red y sistemas.
- Segmentación de red para dividir una red más grande en subredes más pequeñas con interconectividad limitada entre ellos. Restringe el movimiento lateral atacante y evita que los usuarios no autorizados accedan a la propiedad intelectual y los datos de la organización.
- Limite los privilegios de los usuarios para evitar que los atacantes tengan acceso a datos y sistemas sensibles.
- Educar a los empleados y al personal sobre cómo reconocer y evitar los correos electrónicos de phishing y otros ataques de ingeniería social.
- Utilice herramientas que detecten y bloqueen correos electrónicos maliciosos, enlaces sospechosos y archivos adjuntos peligrosos.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

https://cyberint.com/blog/research/meow-ransomware/

https://socradar.io/dark-web-profile-meow-ransomware/

https://www.bitdefender.com/en-us/blog/businessinsights/meow-meow-leaks-and-the-chaos-of-ransomware-attribution

https://www.pcrisk.es/guias-de-desinfeccion/12413-meow-ransomware

https://csirt.gob.cl/articulo/reaparece-el-ransomware-meow/