ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 09 DE FEBRERO 2022

PRESIDENCIA DE LA REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

ALERTA DE SEGURIDAD

- **TLP** Blanco
- **Tipo de incidente** Ransomware
- **Categoría** Código Malicioso
- **Nivel de peligrosidad CRITICO**

DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes (CSIRT- RD), comparte los Indicadores de Compromiso (IoC) conocidos del Ransomware LockBit 2.0, el cual funciona a través de diversas TTPs y con ayuda de afiliados.

Funcionamiento

LockBit es una pandilla de Servicios Ransomware (RaaS) que utiliza diversas tácticas, técnicas y procedimientos (TTPs), en conjunto con el acceso inicial proporcionado por afiliados, los cuales son reclutados para escribir y distribuir el código malicioso del LockBit 2.0.

LockBit 2.0 utiliza herramientas muy conocidas como Mimikatz y otras herramientas hechas por los atacantes para la escalación de privilegio y la persitencia.

Mensaje de Rescate

Nota que explica a los usuarios el procedimiento para pagar el rescate de los datos comprometidos:

INDICADORES DE COMPROMISO (IoC)

Comandos

- cmd.exe /c vssadmin Delete Shadows /All /Quiet
- cmd.exe /c bcdedit /set {default} recoveryenabled No
- cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
- cmd.exe /c wmic SHADOWCOPY /nointeractive
- cmd.exe /c wevtutil cl security
- cmd.exe /c wevtutil cl system
- cmd.exe /c wevtutil cl application
- cmd.exe "C:\Windows\System32\cmd.exe" /C ping 127.0.0.7 -n 3 >Nul&fsutil file setZeroData offset=0 length=524288 "C:\Users\fred\Desktop\Lsystem-234-bit.exe" & Del /f /q "C:\Users\fred\Desktop\Lsystem-234-bit.exe"
- cmd.exe "C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no

Llaves de Registro Utilizadas

- Llaves de Registro Utilizadas
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\ICM\Calibration
- HKEY_CLASSES_ROOT\Lockbit\shell\Open\Command
- HKEY_CLASSES_ROOT\Lockbit\DefaultIcon
- HKEY_CURENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{GUID}
- HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Private
- HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Public
- HKEY_LOCAL_MACHINE\Software\Classes\.lockbit\DefaultIco
- HKEY_CURRENT_USER\Control Panel\Desktop

INDICADORES DE COMPROMISO (IoC)

Archivos Creados

- C:\Users\<Username>\Desktop\LockBit_Ransomware.hta
- C:\Windows\SysWOW64\<First 6 characters of Decryption ID>.ico
- C:\Users\<username>\AppData\Local\Temp\<LockBit 2.0 wallpaper> .tmp.bmp

Powershell

- owershell.exe -Command “Get-ADComputer -filter * -Searchbase ‘%s’ | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}”

Otros IoCs

- Restore-My-Files.txt
- *.lockbit

RECOMENDACIONES

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso (IoC) citados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces suministrados mediante medios de mensajería.
3. Mantener actualizadas las plataformas y sistemas de información según las recomendaciones del proveedor y en especial priorizar las actualizaciones para aplicaciones externas y servicios de acceso remoto.
4. Realizar contacto inmediato con el Equipo Nacional de Respuesta a Incidentes Ciberneticos (CSIRT-RD), a través del correo incidentes@csirt.gob.do, para reportar cualquier acción sospechosa o posible incidente de ciberseguridad antes de realizar una acción.
5. Realizar campañas de concientización periódica a todos los usuarios de la institución.