CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

# Amenazas cibernéticas

Fecha: 06/11/2023

Problemática: Hackers utilizan paquetes de aplicaciones MSIX para infectar equipos Windows con malware GHOSTPULSE

Correlativo: AC-0093

Institución / Sector: Público y Privado

## CONTEXTO

- Microsoft formuló un comunicado para informar sobre actores de amenazas que utilizan paquetes de aplicaciones MSIX de Windows para el software popular como Google Chrome, Microsoft Edge, Brave, Grammarly y Cisco Webex para distribuir un cargador de malware denominado «GHOSTPULSE».

Nivel de priorización

| Prioridad<br>Urgente / No Urgente | Actualización<br>Seguimiento/Preventiva/Resiliente |
|---|---|
| Urgente | Preventiva |

Matriz de Evaluación

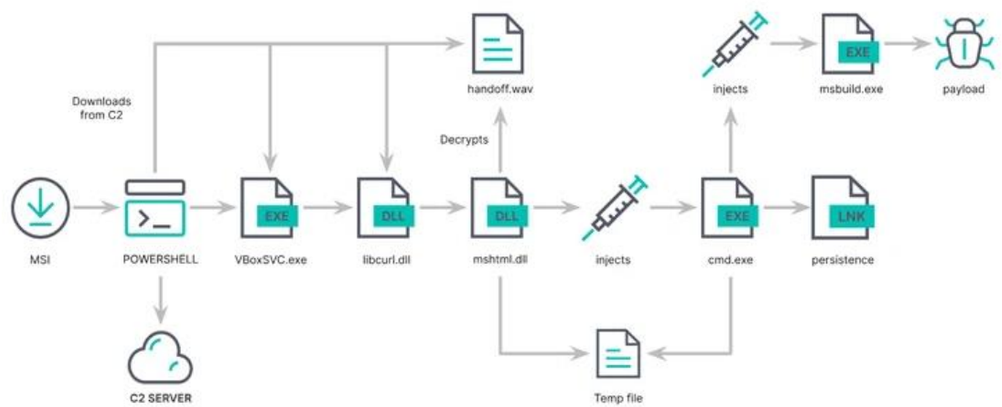
| Riesgo<br>Alto/ Medio/ Bajo | Nivel de Afectación | | |
|---|---|---|---|
| | Integridad | Disponibilidad | Confidencialidad |
| Alto | Alta | Alta | Alta |

## RECOMENDACIÓN

- Deshabilite los protocolos de red heredados que pueden usarse para interceptar el tráfico de red
- Asegúrese de que todo el tráfico cableado y/o inalámbrico esté encriptado adecuadamente.
- Asegúrese de que el tráfico web que pueda contener credenciales esté protegido por SSL/TLS.
- Utilice dispositivos de red y software de seguridad basado en host para bloquear el tráfico de red que no es necesario dentro del entorno
- Limite el acceso a la infraestructura de red y los recursos

## ANEXO

Esquema «Vector de Ataque»




## REFERENCIAS


Microsoft
https://thehackernews.com/2023/10/hackers-using-msix-app-packages-to.html