ALERTA TÉCNICA

TLP:CLEAR

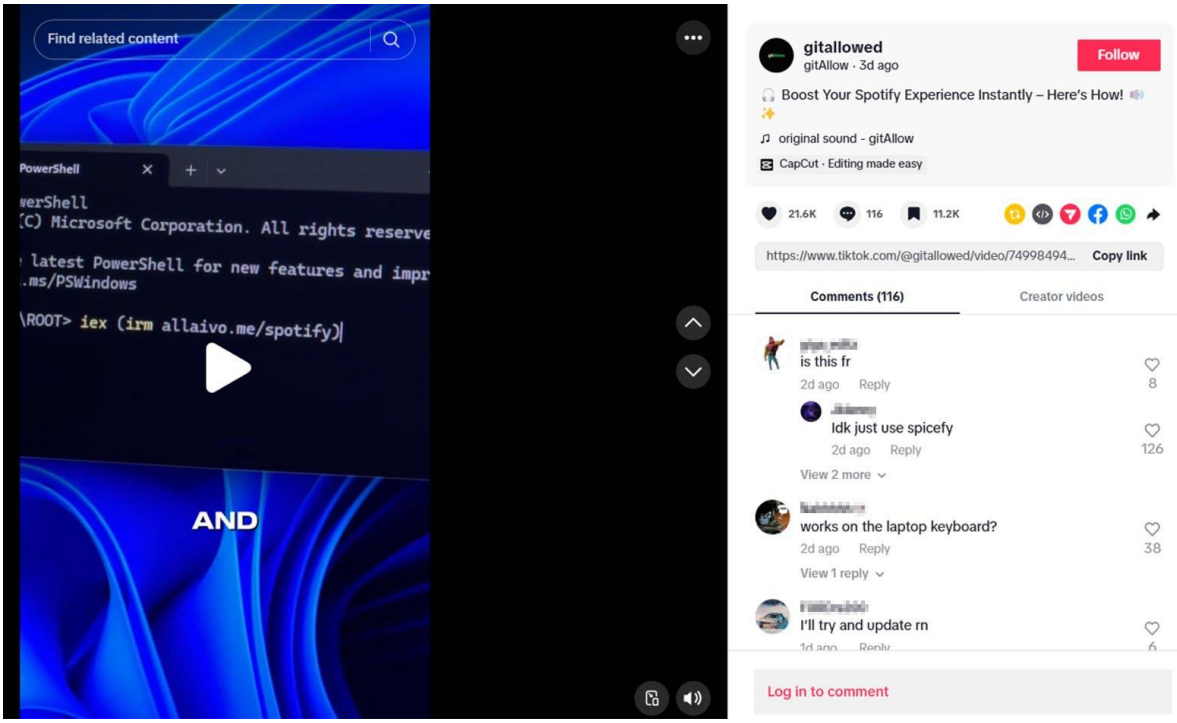
MICITT-DC-CSIRT-AT-1056-2025

Difusión de Vidar y StealC vía TikTok usando Ingeniería Social

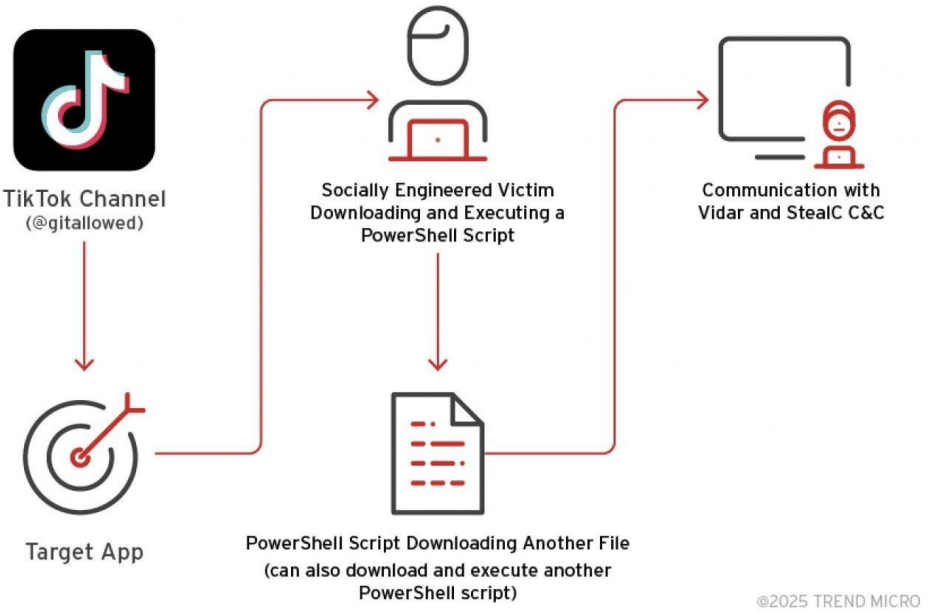
Se les comunica a los Directores (as) /jefes (as) de Tecnologías de Información y a los enlaces de Ciberseguridad, para que tomen las medidas necesarias.

Investigaciones recientes han identificado una campaña en TikTok donde videos, aparentemente generados con herramientas de inteligencia artificial, instruyen a los usuarios para ejecutar comandos de PowerShell bajo el pretexto de activar funciones premium en aplicaciones populares como Spotify, CapCut y Microsoft Office. Al seguir estas instrucciones, los usuarios descargan e instalan malware del tipo infostealer, específicamente las variantes Vidar y StealC, que están diseñadas para robar información sensible como credenciales, datos bancarios y otros datos personales.

Esta técnica, denominada "ClickFix", explota la ingeniería social al presentar soluciones falsas a problemas inexistentes, incitando a los usuarios a ejecutar comandos maliciosos. La campaña ha logrado una amplia difusión gracias al algoritmo de TikTok, con videos que han alcanzado cientos de miles de visualizaciones.



Vídeo de ClickFix en TikTok (Trend Micro)



Flujo de ataque (Trend Micro)

Impacto y Riesgos:

- Robo de Información Sensible: Las variantes Vidar y StealC están diseñadas para extraer credenciales, datos bancarios y otra información personal.
- Ampliación de Plataformas Afectadas: Inicialmente dirigida a sistemas Windows, la campaña ha evolucionado para afectar también a dispositivos macOS, Android e iOS mediante redirecciones en el navegador que pueden iniciar descargas maliciosas sin interacción del usuario.
- Difusión Automatizada: El uso de videos generados por IA permite a los atacantes crear y distribuir contenido malicioso de manera masiva y eficiente.

Medidas de Mitigación:

- Educación y Concienciación: Informar a los usuarios sobre los riesgos de seguir instrucciones de fuentes no verificadas en redes sociales.
- Restricción de Privilegios: Limitar la capacidad de los usuarios para ejecutar scripts o comandos que puedan comprometer la seguridad del sistema.
- Monitoreo de Actividades: Supervisar el tráfico de red y las actividades del sistema para identificar comportamientos anómalos que puedan indicar una infección.

Recomendaciones:

- Se recomienda monitorear su red para detectar actividad anormal e investigar cualquier actividad inesperada en la red.
- Estar atento a las noticias que emita la empresa proveedora del servicio.
- Mantener todos los sistemas actualizados.

Referencias:

Trend Micro. (2025, May 21). TikTok videos promise pirated apps, deliver Vidar and StealC infostealers instead. https://www.trendmicro.com/en_us/research/25/e/tiktok-videos-infostealers.html

Gatlan, S. (2025, May 23). TikTok videos now push infostealer malware in ClickFix attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/tiktok-videos-now-push-infostealer-malware-in-clickfix-attacks/

En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico csirt@micitt.go.cr

JASON CASTRO MARTINEZ (FIRMA)
Fecha: 2025.06.03 17:51:51 -06'00'

Analista de Ciberseguridad

JOSE ALONSO ROCHA VILLALOBOS (FIRMA)
Firmado digitalmente por JOSE ALONSO ROCHA VILLALOBOS (FIRMA)
Fecha: 2025.06.03 17:54:02 -06'00'

Analista de Ciberseguridad