Downfall, un mod de renombre para Slay The Spire, fue tomado por ciberdelincuentes. El creador del mod ha compartido ciertos detalles acerca del suceso.

Aunque no es la primera vez que un mod en la plataforma Steam Workshop resulta comprometido, este incidente destaca por ser uno de los más preocupantes relacionados con los mods en esa plataforma. Resulta sorprendente que los piratas informáticos hayan optado por un mod gratuito para esparcir software malicioso. Es comprensible que algunos usuarios se inquieten por la posibilidad de enfrentar problemas similares con otros títulos. Hay quienes se preguntan cómo pudo ocurrir esto y por qué Valve no implementó medidas de seguridad para evitar tales amenazas.

Un desafío recurrente con el software y juegos en Steam son las actualizaciones automáticas. Aunque en muchas ocasiones estas actualizaciones son beneficiosas, ya que permiten recibir correcciones rápidas, en ocasiones pueden causar inconvenientes, como introducir más errores o, como en este caso, exponer a riesgos de seguridad.

Es lamentable que no exista una opción para deshabilitar estas actualizaciones automáticas en Steam. Una vez que un juego o mod se actualiza, la descarga se ejecuta de forma automática en tu equipo. Sin embargo, sin instalar dicha actualización, no podrás iniciar el juego.

Refiriéndonos nuevamente al mod que fue comprometido, parece que el ataque no afectó a todos los usuarios que lo utilizaban. La declaración del creador del mod ofrece detalles sobre cómo los usuarios se vieron afectados por el software malicioso.

El mod Downfall para Slay the Spire fue comprometido para difundir software malicioso

Table 9 Studio, los responsables detrás del mod Downfall, informan que sufrieron un ataque cibernético cerca de las 1:20 PM (18:20 UTC+0) del 25 de diciembre. Los ciberdelincuentes tomaron el control de las cuentas de Steam y Discount del estudio. Aunque se logró

recuperar la cuenta de Steam en la noche, los daños ya estaban consumados (alrededor de las 1:30 PM a 2:30 PM en el horario del Este el 25/12). Los atacantes subieron archivos con software dañino a la biblioteca de Steam del estudio. Se afirma que se actuó rápidamente para contener la situación antes de poder asegurar nuevamente las cuentas.

Los usuarios que no accedieron a Downfall durante el periodo del incidente pueden estar tranquilos, incluso si el mod se renovó automáticamente. Los jugadores que iniciaron Downfall mediante Steam Workshop, es decir, al comenzar Slay the Spire, tampoco se vieron afectados. Básicamente, si el juego funcionaba como de costumbre al iniciarlo, no se registraron problemas.

Si hubo dificultades para abrir Downfall con un mensaje de error indicando la falta de un archivo .exe, no hay motivo de alarma, ya que esto se diseñó para evitar que el software malicioso afectara a los jugadores. Algunos usuarios pudieron visualizar una pantalla similar a un terminal con texto; se trataba del registro de Java que accidentalmente se mostró al restaurar el juego.

No obstante, si apareció una ventana para instalar la biblioteca Unity al abrir Downfall el 25 de diciembre, es posible que hayas sido expuesto. Un comunicado de Table 9 Studio destaca que, aunque el software antivirus no logró evitar la descarga del mod malintencionado, sí pudo bloquear la carga del programa dañino en las computadoras de los jugadores.

El software malicioso busca capturar contraseñas, datos de navegación, información de pagos y más de aplicaciones como Telegram, Discord, entre otras. Se recomienda a los afectados que ajusten sus contraseñas y activen la autenticación de dos factores como medida de precaución.

Hay informes de usuarios que indican que el software malicioso introdujo una herramienta llamada WindowsBootManager en la carpeta AppData del sistema o en usuarios/[nombredeusuario]/AppData/Local/Temp. Uno de estos archivos lleva el nombre epsilon-[nombredeusuario].zip y contiene datos comprometidos. Otro testimonio señala que encontraron el programa dañino en Local\microsoft\windows\0, presentándose como un juego

titulado Windows Boot Manager. Además, se menciona un archivo llamado unitylibmanager en la carpeta local\temp.

Los creadores aseguran que Downfall vuelve a estar seguro para jugar. Table 9 Studio ha presentado el juego Tales & Tactics en la plataforma Steam, un juego táctico en su fase de Acceso Temprano.

Steam está planeando introducir medidas más rigurosas para desarrolladores. Próximamente, implementará un sistema que solicitará a los creadores un número telefónico para recibir códigos de validación de los servidores de Valve. Luego de recibir un código vía SMS, los desarrolladores deberán ingresar ese código para actualizar su juego.

Aunque la autenticación de dos factores es esencial, el uso exclusivo de SMS presenta vulnerabilidades. El protocolo de mensajes de texto en texto sin cifrar es anticuado y presenta riesgos. Varios desarrolladores han manifestado su inquietud a Valve al respecto, por lo que se espera una revisión del sistema, con preferencia hacia aplicaciones de autenticación más seguras.