KillDisk, un malware contra financieras latinas

El equipo de investigación de Trend Micro ha descubierto una nueva variante de KillDisk, un malware que tiene la capacidad de borrar por completo el disco duro de la máquina afectada y que, inicialmente, se dirige a organizaciones financieras latinoamericanas. Trend Micro lo detecta como TROJ_KILLDISK.IUB.

Según un comunicado de prensa, "el análisis inicial (y que todavía está en curso) revela que puede ser un componente de otra carga útil, o parte de un ataque más grande. **La compañía todavía está analizando esta nueva variante de KillDisk** y mantendrá la información actualizada a medida que descubra más detalles sobre esta amenaza".

KillDisk, junto con BlackEnergy, el malware polivalente relacionado con el ciberespionaje, **se utilizó en los ciberataques de finales de diciembre de 2015 contra el sector energético de Ucrania y su industria bancaria, ferroviaria y minera,** como explican los expertos de trend Micro. Desde entonces, el malware se ha metamorfoseado transformándose en una amenaza utilizada para la extorsión digital, que afecta a plataformas Windows y Linux.

¿Cómo llega al sistema? P**arece que esta variante de KillDisk es lanzada intencionalmente por otro proceso o atacante.** Su ruta de archivo está codificada (hard-coded) en el malware (c:\windows\dimens.exe), lo que significa que está estrechamente relacionada con su instalador o es parte de un paquete más grande.

KillDisk también tiene una función de autodestrucción, aunque en realidad no se elimina, sino que se cambia el nombre de su archivo renombrándose como c:\windows\0123456789 mientras se ejecuta. Esta cadena está codificada o hardcoded en la muestra analizada por Trend Micro. Espera que su ruta de archivo sea c:\windows\dimens.exe (también hardcoded). En consecuencia, si se realiza un análisis forense del disco y se busca dimens.exe, el archivo que se recuperará será el archivo recién creado con contenido de 0x00 bytes.

¿Qué pueden hacer las organizaciones? Las capacidades destructivas de KillDisk, y puesto que podría ser solo una parte de un ataque más grande, ponen de relieve la importancia de la defensa en profundidad: asegurar los perímetros, desde gateways a endpoints, redes y servidores, para reducir aún más la superficie de ataque. Trend Micro recomienda mantener el sistema y sus aplicaciones actualizados/parcheados para evitar que los atacantes aprovechen las lagunas de seguridad; tener en cuenta el parcheo virtual para sistemas heredados y hacer copias de seguridad de los datos con regularidad y asegurarse de su integridad, entre otros asuntos. La firma ofrece una herramienta al mercado para aplacar los efectos de este malware.