Kaspersky: deliencuentes se enriquecen con software de mining

Un grupo de investigadores de Kaspersky Lab ha descubierto un grupo de ciberdelincuentes que han comenzado a **utilizar métodos avanzados de infección y técnicas tomadas de ataques dirigidos para instalar software de extracción de datos** (mining) en PCs atacadas dentro de las organizaciones. El grupo más exitoso observado por **Kaspersky Lab** obtuvo al menos 7 millones de dólares estadounidenisescon la explotación de sus víctimas en solo seis meses durante 2017.

Dice un comunicado de prensa que **aunque el mercado de la criptomoneda está experimentando muchas variaciones,** el fenómeno del año pasado con aumentos en el valor de Bitcoin ha cambiado considerablemente no solo la economía global, sino también el mundo de la ciberseguridad. Con el objetivo de **obtener criptomonedas,** los delincuentes han comenzado a utilizar un **software malicioso de extracción** (minería), que, como el **ransomware**, tiene un modelo simple de monetización. Pero, a diferencia del ransomware, "no daña destructivamente a los usuarios y puede permanecer sin ser detectado durante mucho tiempo al usar silenciosamente la potencia de la PC".

En septiembre de 2017, Kaspersky Lab registró un aumento de programas mineros (buscadores de criptomonedas) que comenzaron a propagarse activamente por todo el mundo y predijo su mayor desarrollo. Las investigaciones más recientes revelan que este crecimiento no solo ha continuado, sino que también se ha incrementado y ampliado.

El ataque funciona de la siguiente manera: **la víctima se ve tentada a bajar e instalar un software de publicidad que tiene el instalador del programa extractor de datos escondido en su interior**. Este instalador elimina un utensilio legítimo de Windows con el objetivo principal de bajar el software minero desde un servidor remoto. Después de su ejecución, se inicia un proceso legítimo del sistema y el código genuino de este proceso se convierte en código malicioso. Como resultado, el programa minero funciona bajo la apariencia de una tarea segura, por lo que será imposible que un usuario reconozca si hay una infección para extracción de datos.