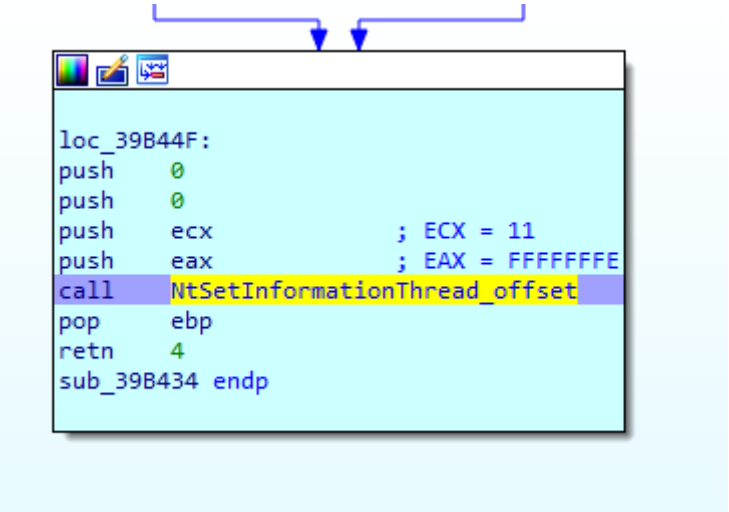
NtSetInformationThread()
Lockbit 3.0

En este artículo analizamos cómo **Lockbit 3.0** utiliza NtSetInformationThread() para esconder un hilo del debugger con un parámetro no documentado. Esta técnica también está explicada en un blog de analista Japonés [1] que ya hemos visto en otras de las fichas. Aquí lo encontrarás resumido por lo que si quieres leer el proceso de análisis completo te aconsejo que leas la entrada del investigador Japonés.

Para nuestras pruebas utilizamos el hash: A7782D8D55AE5FBFABBAAAEC367BE5BE
Esta muestra después de su ejecución despliega en memoria lo que es **Lockbit 3.0** sin token de acceso y al volcarla a disco el PE el hash es: E5A0136AC4FE028FEA827458B1A70124.



Esta técnica es bastante conocida y la podemos leer en diferentes páginas web [2]. Como bien se indica en la referencia de CheckPoint con este API y el parámetro 0x11 se esconde el hilo, desde donde se invoca, del debugger.

[1] https://ameblo.jp/reverse-eg-mal-memo/entry-12775255083.html
[2] https://anti-debug.checkpoint.com/techniques/interactive.html#ntsetinformationthread