our first vm !

בתרגיל הקודם הכנו את הקרקע וכתבנו דרייבר בסיסי שמשחק קצת עם ההגדרות והאוגרים של VMX.
כעת, אנחנו נהפוך את הדרייבר הזה ל Hypervisor, ובעצם ניצור את ה "VM" הראשון שלנו !

APP

אין שינוי עיקרי, בדיקה של היצרן והתמיכה ב VTX, לאחר מכן יוצרים את ה device על מנת לטרגר את פונקציית ה Initiate_VMX בדרייבר. בסוף יש משחק עם ה IOCTLs לדרייבר שהוא פחות מעניין, אך נחמד להבנה (בהערה).

DRIVER

PAGED_CODE - מאקרו שמוודא שה thread שמריץ את הקוד הנוכחי רץ ב IRQL מספיק נמוך על מנת לאפשר paging.
ניתן לראות את המימוש של ה IOCTLs בשיטת השונות METHOD_OUT_DIRECT, METHOD_IN_DIRECT,
METHOD_BUFFERED or METHOD_NEITHER לא אכנס להבדלים - מוזמנים לקרוא על דרייברים.
בסופו של דבר הקוד שמעניין אותנו עדיין נמצא ב DrvCreate שקורא לפונקציה Initiate_VMX.

Initialize_VMX

חשוב לזכור שבסופו של דבר רוב המחשבים בעולם הם מרובי מעבדים, ולכן יש לוודא שאנחנו גורמים לדברים לעבוד בכל המעבדים ביחד. על מנת לעשות זאת, windows עוזרים לנו בעזרת סט של APIs המספק את מספר המעבדים, והרצת קוד על מעבד ספציפי בהינתן האינדקס שלו (KeQueryActiveProcessorCount, KeSetSystemAffinityThread).

סה"כ, נבדוק ש VMX נתמך באופן כללי במחשב עליו אנו רצים כפי שכבר ראינו (CPUID, IA32_FEATURE_CONTROL).
לאחר מכן, נעבור מעבד מעבד ונגרום ל VMX להיות דלוק בעזרת CR4, ונקצה VMXON Region + VMCS ל VM שלנו.

Terminate_VMX

רצים על כל מעבד שוב, אך הפעם קוראים ל VMXOFF ומשחררים את המשאבים שהקצנו (VMXON Region, VMCS).

Allocate_VMXON_Region

כפי שהסברנו, מבנה נתונים פר מעבד פיזי שעלינו לאלקץ ולשלוח את הכתובת הפיזית שלו ל VMXON.
ראשית, הופכים את ה IRQL ל DISPATCH_LEVEL (מצורף קובץ המסביר על IRQLs) על מנת שה scheduling של windows לא יציק לנו באמצע וישנה לנו דברים תוך כדי שאנחנו מנסים לשמור אותם, שנית מקצים זיכרון רציף ומאופס שהוא aligned כמבוקש, לאחר מכן כותבים בהתחלת ה VMXON Region את ה revision ID אותו מקבלים מ AI32_VMX_BASIC_MSR, ולבסוף קוראים ל VMXON עם הכתובת פיזית של VMX Region שזה עתה אתחלנו.

Allocate_VMCS_Region

כפי שכבר הצגנו ל VMXON Region ול VMCS אותו מבנה בכך שהם aligned ומכילים בהתחלה revision ID.
לכן, נבצע בדיוק אותו קוד, רק שהפעם נקרא ל VMPTRLD במקום ל VMXON עם הפרמטר VMCS שאתחלנו.

כעת, הריצו ובדקו שלא מקבלים BSOD, ושמקבלים את ההודעות דיבוג המתאימות...
יש לנו VM בסיסי ביותר (שעוד לא רץ), לעת עתה הוא לא באמת עושה משהו :(