

# מקומות שכדאי לשים לב אליהם בעת חקירה - registry

## סיימון בר

### מפתחות Run:

מדובר במפתחות שיש בהם תוכניות שירוצו בעת חיבור של המשתמש, משמע תוקף יכול לשים במפתחות הללו ערך של נתיב זדוני ובכך גם אם הקורבן יכבה את המחשב ברגע שידליק אותו הקבצים הזדוניים ירוצו שוב (מה שנקרא persistence - התמדה).

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

### מפתחות הרצה אוטומטיים:

מדובר על מפתחות שונים שיריצו תוכניות ותהליכים כאשר דברים יקרו (event-driven) באופן אוטומטי, גם כאן תוקף יכול להשתמש בנתיבים אלה על מנת להכניס את התוכנות שלו ובכך לגרום לכך שירוצו גם אם סוגרים אותן.

HKLM\SOFTWARE\Microsoft\Command Processor

מפתח של תוכניות שירוצו בכל פעם שנריץ cmd.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

מפתח של תוכניות שירוצו בכל פעם שחלון ה-winlogon עולה (חלון ההתחברות).

### מפתחות שיעזרו לנו בעת חקירה:

HKLM\SYSTEM\MountedDevices

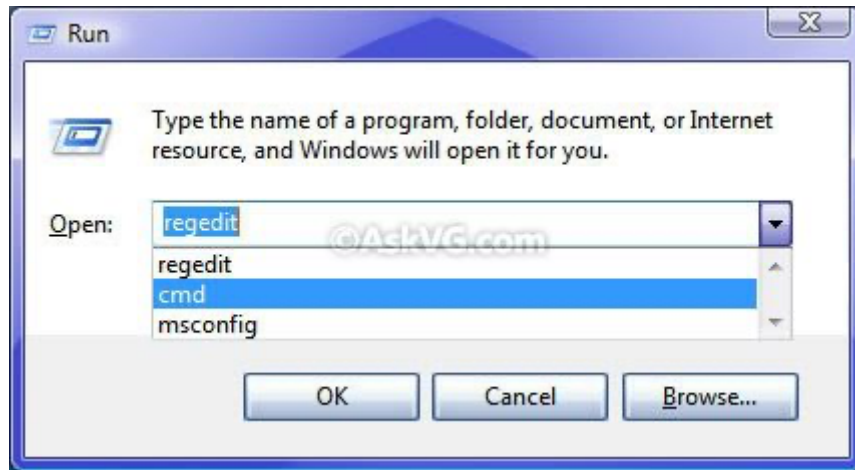
מפתח שמציג מכשירים אחרונים שחוברו למחשב ובוצע להם mount (אתחול ככונן עם אות C, D, E) מכשירים אלה יכולים להיות גם cd rom, floppy, usb ועוד

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

רשימה של האתרים האחרונים שבוצע אליהם חיפוש באינטרנט אקספלורר

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

רשימה של חיפושים אחרונים ב-mru (חלון winkey+r), יכול לעזור מאוד להבין מה ניסו להריץ.



HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

מציג מסמכים אחרונים שנפתחו (כמו דלוגמה שנכנסים ב- word ושי אפשרות לראות רשימה של המסמכים האחרונים שנערכו)

HKEY\_LOCAL\_MACHINE\SYSTEM\controlset001\Enum\USBSTOR

שומר רשימה של USB אחרונים

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Currentversion\Search\RecentApp

s

שומר רשימה של תוכנות אחרונות שבוצע בהן שימוש

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\NetworkList\Profiles

מפתח שימושי מאוד! מראה את ה- SSID (שם הרשת) של הרשתות האחרונות שהתחברנו אליהן

HKEY\_LOCAL\_MACHINE\System\Services\CurrentControlSet\services\Tcpip\Parameters\Interfaces

מפתח בו רואים את ה- ip ופרטים נוספים על תקשורת המחשב כאשר בוצע האירוע ונוכל לקחת את ה- ip ולהמשיך לתחקר ב- fw, wireshark, ועוד.

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services

מפתח שמכיל נתונים על סרוויסים שעולים בעת עליית המחשב, סרוויסים עם הערך 2 עולים בצורה אוטומטית כאשר מדליקים את המחשב.

זוהי רק רשימה חלקית וניתן לראות כמה מידע ניתן להשיג ברגיסטרי בעת חקירה על מנת להשלים את הפאזל של החקירה, מאיזה דיסק און קייס הכניסו למחשב, לאיזה רשתות הוא היה מחובר, אילו פקודות ניסו לבצע, האם ניסו לתפוס persistence ועוד.

שימו לב! לפעמים ערכים ברגיסטרי נראים לנו כמו ג'יבריש, אל תפחדו חפשו את המפתח בגוגל ותראו איך מנתחים את אותו ערך, בנוסף יהיו מקרים בהם נראה ערכים רבים בדר"כ יהיה מדובר במידע בינארי, כך לדוגמה אם נחפש כוננים או מסמכים אחרונים נוכל לראות שמדובר במידע בינארי נעתיק אותו ל-HxD ונבדוק.