

מקומות שכדי לשים לב אליהם בעת חקירה - registry

סיכום בר

מפתחות Run:

מדובר במפתחות שיש בהם תוכניות שירצו בעת חיבור של המשתמש, משמע תוקף יכול לשים במפתחות הללו ערך של נתיב זמני ובכך גם אם הלקוח יכבה את המחשב ברגע שידליך אותו הקבצים הדונינים ירצו 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 בתתיים אלה על מנת להפעיל את התוכנות שלו ובכך לגרום לכך שיורכו גם אם סוגרים אותם.

HKLM\SOFTWARE\Microsoft\Command Processor

מפתח של תוכניות שירצו בכל פעם שנריץ cmd.

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

מפתח של תוכניות שירצו בכל פעם שהלן ה- winlogon (חלון ההתחברות).

מפתחות שיעזרו לנו בעת חקירה:

HKLM\SYSTEM\MountedDevices

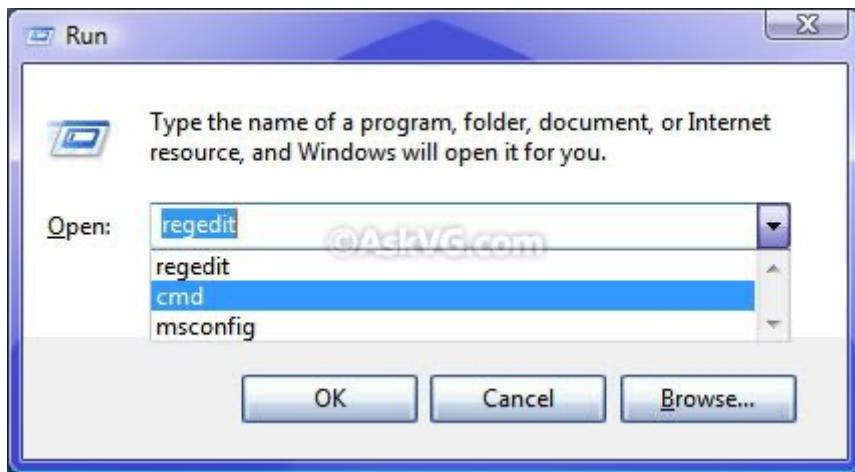
מפתח שמציג מכשירים אחרונים שוחבו למחשב ובוצע להם mount (אתחול כוכן עם אותן כמו E (C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z) מכשירים אלה יכולים להיות גם rom, floppy, cd, usb ועוד

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

רשימה של האתרים האחרונים שבוצעו עליהם חיפוש באינטרנט אקספלורר

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

רשימה של חיפושים אחרונים ב- run (חלון z+winkey), יכול לעזור מאד להבין מה ניסו להריץ.



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

מציג מסמכים אחרונים שנפתחו (כמו דוגמה שנכנסים ב- word ושיש 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 מאד! מראה את ה- SSID (שם הרשת) של הרשות האחרון שהתחברנו אליו!

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 לחת את ה- IP ולהמישר לתקן ב- fw, wireshark ועוד.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

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

זהו רק רשימה חלקית וניתן לראות כמה מידע ניתן להשיג ברגיסטרי בעת חקירה על מנת להשלים את הפאל של החקירה, מאייה דיסק אוון קיוס הכניסו למחשב, לאיזה רשות הוא היה מחובר, אילו פקודות ניסו לבצע, האם ניסו לתפוא persistence ועוד.

שים לב! לעיתים ערכיהם ברגיסטרי נראהים לנו כמו גיבריש, אל תפחדו חפשו את המפתח בגוגל ותראו איך מנתחים את אותו ערף, בנוסף יהיו מקרים בהם נראה ערכים רבים בדר"כ יהיה מדובר במידע ביןארי, כך לדוגמה אם נחפש כוננים או מסמכים אחרים נוכל לראות שמדובר במידע ביןארי נטען אותו ל- DxH ונבדוק.