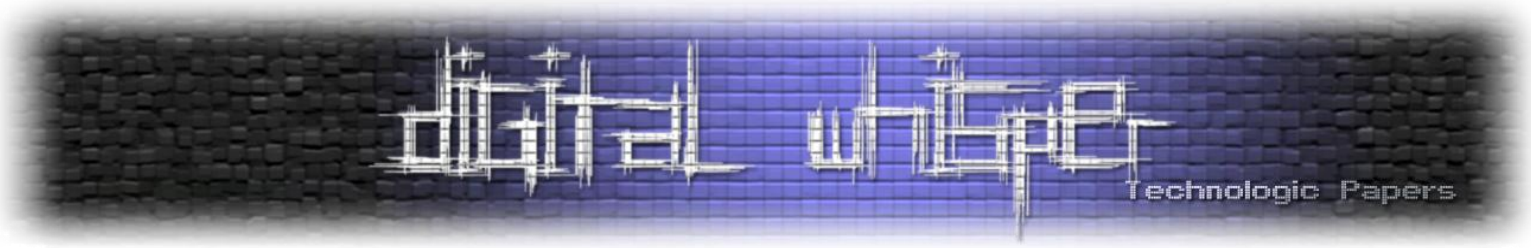


וירוסים - שיטות טעינה

מאת אפיק קסטיאל (cp77fk4r)

לאחר שוירוס או תולעת מצליחים להריץ את עצמם על מחשב-קורבן, אחד הנושאים הקריטיים מצד כותב הוירוס היא לדאוג לפעם הבאה בה הוירוס ירוץ. כאן קיים tradeoff מצד כותב הוירוס. מצד אחד מטרת כותב הוירוס היא להשתמש בדרכים אפקטיביות ורבות ככל שניתן לדאוג שהוירוס ירוץ שוב ושוב על המחשב, כך שלמשתמש יהיה קשה יותר להפטר מהוירוס, והוירוס יצליח לשמור על אורך חיים ארוך יותר. מצד שני, ככל שהוירוס משנה יותר דברים במערכת ההפעלה - כך יגדל הסיכוי שהוא יתגלה.

במאמר זה נסקור מספר דרכים, או "טכנולוגיות", שבהן הוירוסים והתולעים משתמשים בכדי לגרום למערכת/למשתמש לטעון את עצמם מבלי ידיעת המשתמש. בנוסף נסקור דרכים ופעולות אותן ניתן לבצע בכדי להתמודד נגד וירוסים המשתמשים בדרכים אלו, בכדי לגרום למחשבכם להיות מאובטח יותר מפני האיומים.

Startup

הדרך הפשוטה וגם המוכרת ביותר להפעלת תוכנה עם עליית המחשב היא שימוש בתיקיה Startup. מערכת ההפעלה Windows מאפשרת למשתמש לקבוע תוכנות שירוצו בעת טעינתה ע"י הוספת קובץ ההפעלה של התוכנה (או קיצור דרך אליו) בתיקיה Startup.

ב-Windows XP המיקום של התיקיה הוא:

```
C:\Documents and Settings\[User]\Start Menu\Programs
```

ובמערכת Vista מיקומה של התיקיה הוא:

```
C:\Users\[User]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
```

כל קובץ הממוקם בתיקיה הנ"ל בזמן טעינתה של מערכת ההפעלה יורץ לאחר שהמערכת תעלה.כיום השימוש בתיקיה זו אינו רב, וכמעט ולא ניתן למצוא וירוסים או תולעים אשר משתמשים בה לצורך

טעינתם - קל מאוד לאתר שימוש בה, תוכן התיקיה מופיע בתפריט ה-"Program Files" הממוקם תחת תפריט ה-"Start" ונגיש מאוד אף למשתמש הממוצע.

System Configuration Loading Files

השיטה הבאה שנציין בה וירוסים וטרויאנים משתמשים היא שימוש במספר קבצי האצווה וקבצי ה-ini בהם Windows משתמשת. קבצים אלה כוללים קבצים או פקודות שעל מערכת ההפעלה לבצע בעת עלייתה. שמות הקבצים הנקראים באופן אוטומטי:

```
%homedrive%\Autoexec.bat
%homedrive%\Config.sys
%windir%\Win.ini
%windir%\Wininit.ini
%windir%\System.ini
```

- %homedrive% זהו הכונן בו מותקנת מערכת ההפעלה.
- %windir% זו הספריה בה מצוייה מערכת ההפעלה (בד"כ C:\Windows).

שיטה זו מעט קשה יותר לאיתור למשתמשי המחשב הממוצעים מאשר שימוש בספריה Startup, ואפשר למצוא שימוש בה בוירוסים ישנים, אך כיום לא ניתן למצוא וירוסים המשתמשים בה.

שימוש בקבצים Autoexec.bat ו-Config.sys:

שני הקבצים Autoexec.bat ו-Config.sys הם קבצי אצווה רגילים. כדי לגרום להם להריץ אפליקציות אפשר להשתמש בפקודה הקריאה Call. דוגמא לשימוש:

```
Call %temp%\virus.exe
```

בשאר הקבצים ניתן להשתמש רק במערכת הישנות מ-XP, כגון 98 ודומותיה. על מנת להתגונן מוירוסים הנמצאים בקבצים אלו ניתן לסרוק תקופתית קבצים אלה לשינויים או תוספות חשודות.

שימוש בקבצים Win.ini ו-Wininit.ini.

הקבצים win.ini, Wininit.ini הם קבצי ini. קבצים אלו מחולקים על ידי תוויות (Labels). תחת [Windows] נמצאות תכונות שנקראות על ידי מערכת ההפעלה עם עלייתה, באופן הבא:

```
[windows]
LOAD=%temp%\virus.exe
```

או באופן הבא:

```
[windows]
RUN=%temp%\virus.exe
```

מערכת הקבצים מבצעת שימוש בקובץ Wininit.ini כדי לטעון הגדרות ושירותים לאחר התקנת מערכת ההפעלה - קבצים והגדרות שהמערכת לא יכולה לטעון בעת ההתקנה.

לאחר שמערכת ההפעלה תטען את המידע הקיים ב-Wininit.ini היא תשנה אותו מיד ל-Wininit.BAK, כך שבפעם הבאה המערכת לא תמצא שום קובץ "Wininit.ini" ולכן לא תבצע שום הרצה של התוכן הקיים בו.

שימוש בקובץ-System.ini.

מערכת הקבצים משתמשת בקובץ הנ"ל בכדי לטעון דרייברים נחוצים להפעלה תקינה של מערכת ההפעלה, הקובץ עצמו הוא גם קובץ ini, וה-label שממנו נטענים הדרייברים הוא: "[386enh]", והשימוש בו הוא בדיוק כמו השימוש בקבצי ה-ini הקודמים.

מעקב והתגוננות

בכדי לעבוד באופן נח ומסודר עם הקבצים הנ"ל מייקרוסופט הוסיפו למערכת ההפעלה עורך קטן בשם "System Configuration Editor", והוא ממוקם ב:

```
%windir%\System32\sysedit.exe
```

אפשר להשתמש בכלי כדי לבדוק במהירות את כל הקבצים שהצגנו ולאתר בהם שינויים חשודים.

Startup Regedit Values

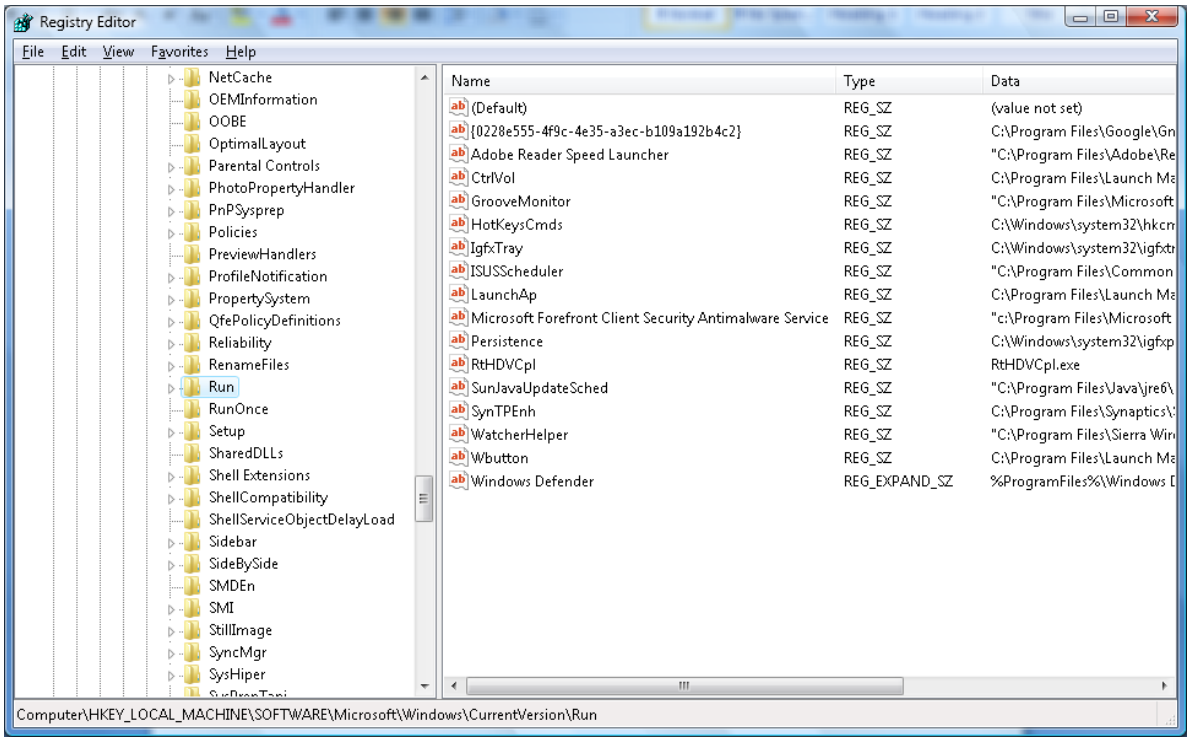
עורך הרישום של מערכת ההפעלה (registry editor) טומן בחובו הרבה מאוד נסתרות. כחלק מאפיונו הוא גם אחראי על טעינת קבצים בעת מספר אירועים, אירועים כגון טעינת מערכת ההפעלה, התחברות משתמש מסויים, כניסה לכונן מסויים, ואף אירועים חיצוניים כגון - חיבור התקן USB ליציאת ה-USB במחשב, שימוש בפרוטוקולים ועוד נושאים רבים. נציג מעט ערכים הנוגעים להפעלה אוטומטית של תוכנות.

טעינת מערכת ההפעלה:

זהו אולי המפתח שוירוסים משתמשים בו לעיתים הקרובות ביותר:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

כל ערך שיופיע תחת המפתח הנ"ל יטען בעת טעינת מערכת ההפעלה.



וירוס המעוניין להוסיף את עצמו למפתח זה משתמש בפקודה "Reg" עם המתג-"add", למשל:

```
Reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Virus /d %temp%\virus.exe
```

הפקודה תוסיף עוד ערך בשם "Virus" המכיל את מיקום הקובץ שיש להריץ-"%temp\virus.exe" אשר יטען כל פעם בעת טעינת מערכת ההפעלה.

כמובן שוירוסים ושאר מזיקים ישתמשו בשמות פחות חשודים כגון-"svchosts.exe" או "explorer.exe", ולכן חשוב מאוד לבדוק מה הערך המוכנס ל-Data (מיקום הקובץ אותו המערכת תריץ) ולברר האם הקובץ הנ"ל אכן שייך למערכת ההפעלה או לא.

קיימים עוד מפתחות כאלה בעורך הרישום, השימוש בהם נפוץ פחות, אך פעולתן זהה (ברב המקרים), המפתחות הם:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup
```

במערכת ההפעלה-XP, קיים גם המפתח הבא:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
```

כל הערכים אשר ימוקמו תחת המפתחות הנ"ל יטענו בעת טעינת מערכת ההפעלה, הערכים הבאים יטענו רק בעת טעינת משתמש ספציפי (המשתמש תחתיו הריצו את הפקודה):

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
```

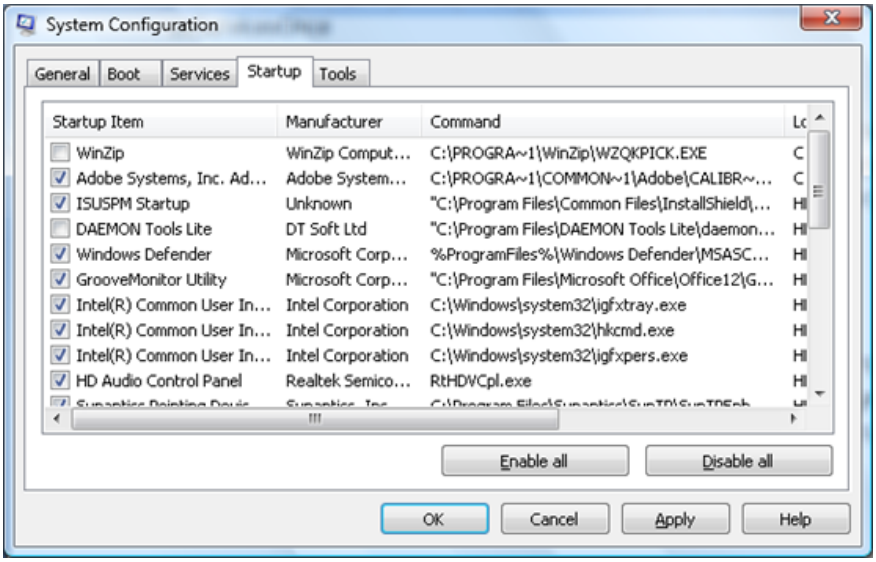
בעורך הרישום תחת מערכות ההפעלה-NT, XP ו-Server2003, ישנו מפתח המתנהג באופן זהה, אשר תפקידו לטעון את הקובץ userinit.exe המקושר לקביעת תצורת המשתמש, המפתח הוא:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
```

ובכדי לטעון בעזרתו אפליקציות שונות, פשוט מאוד מוסיפים "," (פסיק) לאחר המיקום של הקובץ userinit.exe ומוסיפים בו את המיקום של האפליקציה שברצוננו לטעון, לדוגמא:

```
%windir%\system32\userinit.exe,%temp%virus.exe
```

לאחר טעינת כל הערכים מהמפתחות שציוינו עד כה מערכת הקבצים תרכז את כולם לתוך רשימה מסודרת בכדי להקל על ניהול המערכת, את הרשימה הנ"ל אפשר למצוא תחת החוצץ "Startup" באפליקציה Msconfig.exe:



Autorun Auto&Play

עורך הרישום מנהל עוד מספר מפתחות וערכים אשר תולעים ווירוסים "מתקדמים" מנצלים בכדי לשפר את אורך חייהם, ערכים אלה לא נטענים בעת עליית מערכת ההפעלה או התחברות משתמש מסויים, אך ערכים אלה מנהלים אירועים המתקיימים מספר רב של פעמים המספיק בכדי לשמור על פעילות "תקינה" של אותה התולעת, לדוגמא:

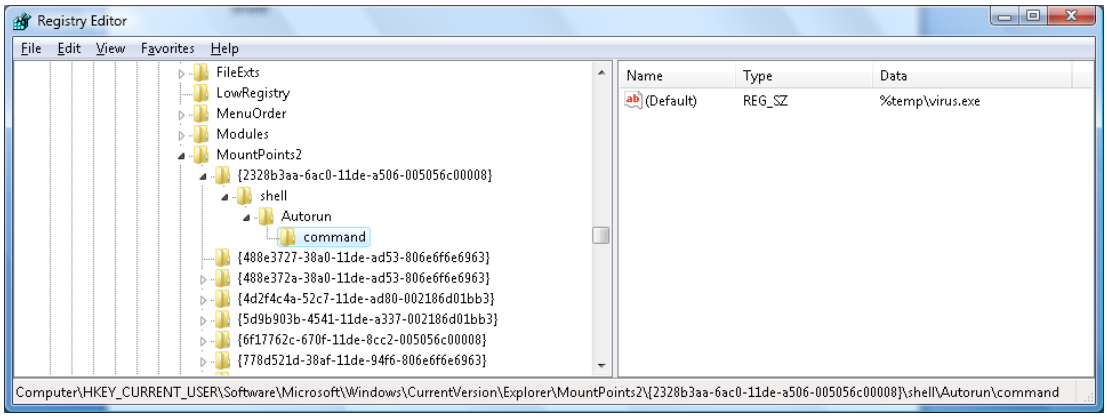
בעת הכנסת התקן USB או כל כונן (אפילו קשיח) עורך הרישום "זוכר" באיזה תצורת טעינה המשתמש בחר בכדי לפתוח אותו (טעינת המידע לנגן ה-Media, פתיחת הכונן בעזרת סייר החלונות, ביצוע סינכרון בעזרת ה-WinSync וכו'), וכך, בפעם הבאה שהמשתמש יחבר את אותו ההתקן - עורך הרישום יידע להגיד למערכת איזו פעולה לבצע וכך להקל על המשתמש ולהגדיל את "חווית השימוש" במערכת ההפעלה, פעולה זאת נקראת-"Autorun". המפתח האחראי על "זכירת" תצורת הטעינה הוא:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoint
s2
```

תחת מפתח זה, עורך הרישום מנהל תת-מפתחות עם שמות זיהוי ייחודיים לאותו התקן, כגון:

```
{2328b3aa-6ac0-11de-a506-005056c00008}
{5d9b903b-4541-11de-a337-002186d01bb3}
{9916dd74-653d-11de-b8be-002186d01bb3}
{ae9a98c3-3f2b-11de-ae4c-002186d01bb3}
```

כל המפתח אחראי על התקן שונה, וירוסים משנים ערכים של מפתחות אשר אחראים על התקנים דומיננטים, כגון כונן מערכת ההפעלה, או מחיצות שונות על הכוננים הקשיחים. על מנת להשתמש בפונקציה זו, יש להוסיף למפתח תת-מפתח בשם: Shellעם ה-data: "Autorun", ובו תת-מפתח בשם: Autorun או Autoplay עם ה-data: "Auto&Play", ובו עוד תת-מפתח בשם: Commandובו, בערך ה-(Default) יש להוסיף את מיקום האפליקציה אותה יש לטעון בעת כניסה לאותו הכונן .התוצר הסופי אמור להראות באופן הבא:

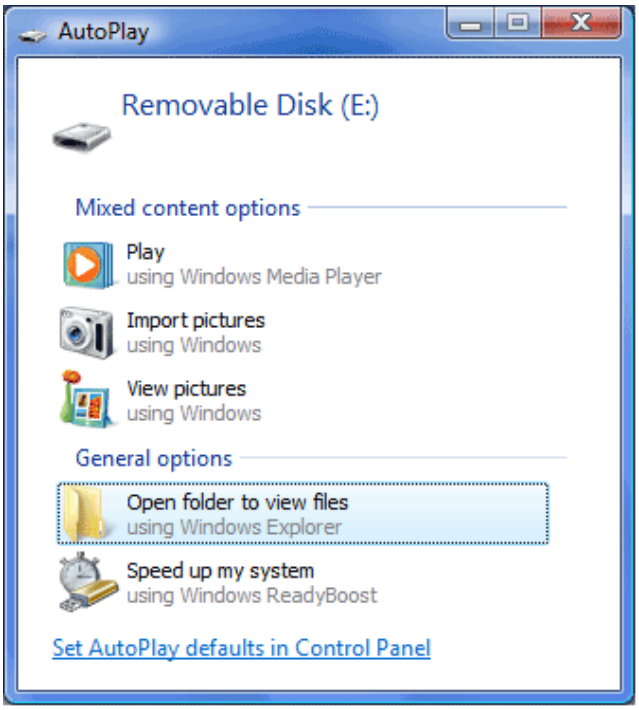


כך, בכל כניסה של משתמש לכונן C ירוץ הוירוס. חשוב לציין כי כניסה משמעה לחיצה פעמים על הכונן "C" במחשב שלי, כל כניסה בדרך אחרת לא תגרום להרצה של הוירוס, לדוגמא ע"י לחיצה כפתור ימני ו-"explore" או כניסה ל-Start משם ל-Run ושם ל-"C:\" לא תגרום להרצה של הוירוס.

אין דרך לבטל את הפיצ'ר הזה באופן גורף, ולכן וירוסים ותולעים נוהגים להשתמש בטכנולוגיה זאת באופן תדיר, מה שאפשר לעשות זה ליצור קובץ אצווה שמוחק את כל המפתחות הקיימים ב-Mountpoint2 ולבקש מהמערכת לטעון אותו בכל פעם שהמערכת עולה, בכל אופן, בכל פעם שיש חשד שהמחשב ננגע באיזה מזיק- מומלץ ללכת למפתחות הקיימות בנקודה זאת, וכך לאתר את היישום הסורר.

AUTORUN.INF

וירוסים ותולעים מנצלים עוד טכנולוגיה שנתמכת ע"י מערכת הקבצים של חלונות, והוא עוד פיצ'ר שמתפעל את ה-Auto&Play, הרעיון הוא שברגע שמחברים התקן USB למחשב, מערכת הקבצים מחפשת בתיקיית השורש שלו קובץ בשם Autorun.inf (לרב הוא יהיה עם מאפייני R+ S+ H+, אך זה לא מחייב) ובקובץ הנ"ל נשמרת הדרך שבה מערכת הקבצים תתייחס לאותו התקן. הקובץ אחראי על תצורתו ותפקודו של תפריט ה-AutoPlay:



מבנה הקובץ בנוי באופן המזכיר קבצי ini, דוגמא לקובץ Autorun.inf:

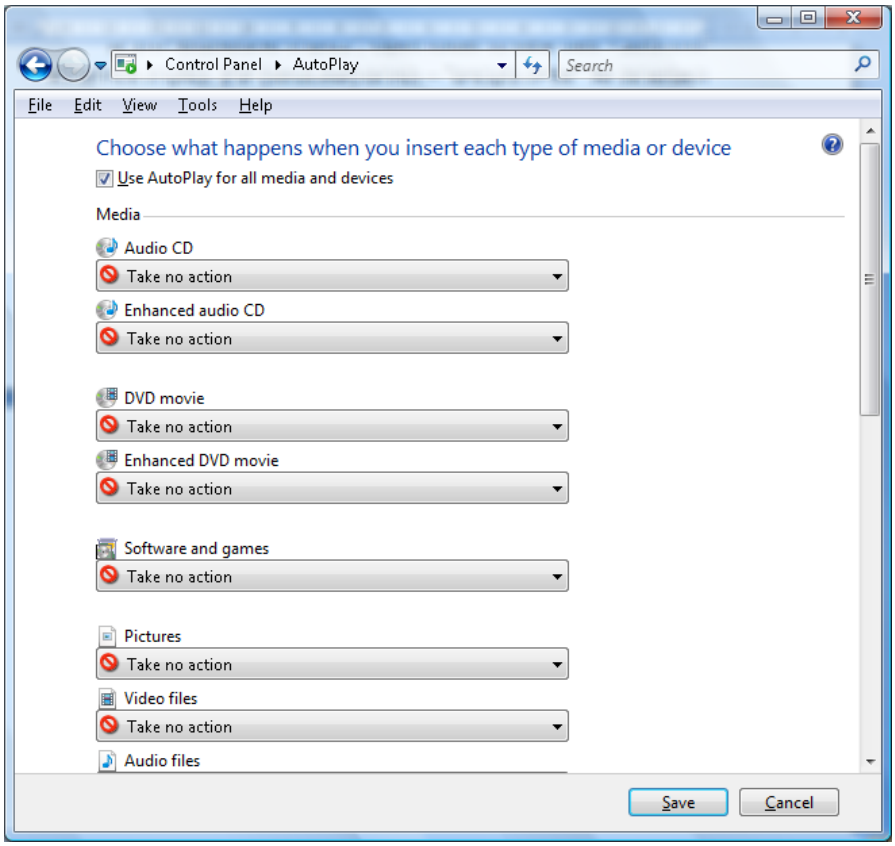
```
[autorun]
open=virus.exe
icon=folder.ico
label="Open folder to view files"
```

התוכן הבא יגיד למערכת הקבצים לטעון את תפריט ה-Autoplay, ולהכניס בו אפשרות לצפייה בקבצים, יקבע איזה אייקון יופיע, וכמובן גם מה יהיה כתוב לידו-"Open folder to view files", במקרה שהמשתמש ילחץ על האפשרות של "צפייה בקבצים" - הוירוס (virus.exe) יורץ. במקרה וכותב הוירוס לא רוצה ליצור חשד הוא יגיד לוירוס גם לפתוח את כונן ה-USB לצפייה בקבצים בכדי שהפעולה תהיה חלקה והמשתמש לא יוכל לשים לב לשינויים.

בכדי לבטל אפשרות זאת יש למנוע ממערכת ההפעלה להשתמש בתפריט ה-Autoplay, לכל התקני הקבצים (כולל CD, FLOOPY, USB, SMARTCARD וכו'). אפשר לבצע זאת ע"י:

<u>ב-Vista:</u>

כניסה ל-"Control Panel" ושם כניסה ל-"Autoplay", ושם בחירת "Take no action" לכל ההתקנים.



ב-XP:

כניסה ל-"My computer", ושם כפתור ימני על כונן ושם בחירה ב-"Properties", בתפריט שהופיע יש לבחור בחוצץ "AutoPlay", תחת התווים "Actions" יש לסמן את "Select an Action to perform" ואז לבחור את "Take no action". לחיצה על "Apply" ואז "OK" יקבעו את התצורה הנוכחית מעכשיו והלך.

שינויים אלה לא מספיקים! הפעולה שהצגנו אומנם תמנע ממערכת הקבצים להקפיץ לנו את תפריט ה-AutoPlay, שזה טוב ויפה, אבל היא לא תמנע ממנה לאתר ולהריץ את קובץ ה-Autorun.inf, כך שהתפריט לא יופיע - אבל הוירוס עדיין ירוץ.

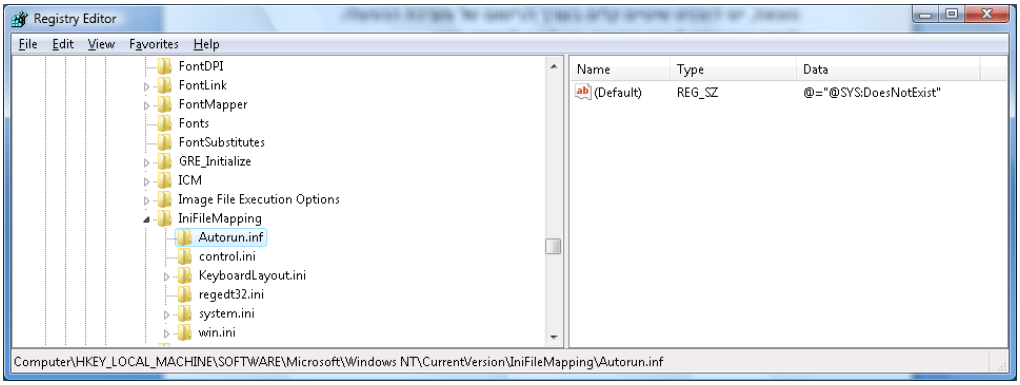
בכדי למנוע ממערכת הקבצים להריץ את כל קבצי ה-Autorun.inf שהיא מוצאת, יש להכניס שינויים קלים בעורך הרישום של מערכת ההפעלה. לאחר שנכנסתם לעורך הרישום, יש לנווט למפתח הבא:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\Autorun.inf
```

אם תת-המפתח "Autorun.inf" לא קיים- יש ליצור אותו. לאחר מכן יש להכניס אליו את הערך הבא:

```
@="@SYS:DoesNotExist"
```

מהפעם הבאה שמערכת ההפעלה תעלה, מערכת הקבצים לא תנסה לאתר את קבצי ה-Autorun.inf בכל ההתקנים אשר יחוברו למחשב.



System Services

מערכת ההפעלה בנויה באופן מודולרי, ומספר רב מאפשרויותיה מבוססות על על "שירותים" אשר היא מריצה. שירותים אלו ("Services") הם יישומים האחראים לנהל או לתת שירות בנוגע לרכיבים או איפיונים ספציפים, כמו למשל רכיבי רשת, רכיבי שמע, רכיבי בקרה וניהול וכו', רכיבים אלו רצים ברקע המערכת וכמעט ולא נראים לעין. וירוסים ותולעים מנצלים לפעמים אופי זה בכדי לטעון את עצמם ביחד עם שירותי המערכת, וכך לדאוג שהם יטענו בכל פעם שהמערכת עולה.

בכדי לראות אילו שירותים נטענים ביחד עם מערכת ההפעלה, מיקרוסופט הוסיפו לנו את היישום Services.msc הממוקם ב: C:\Windows\System32.

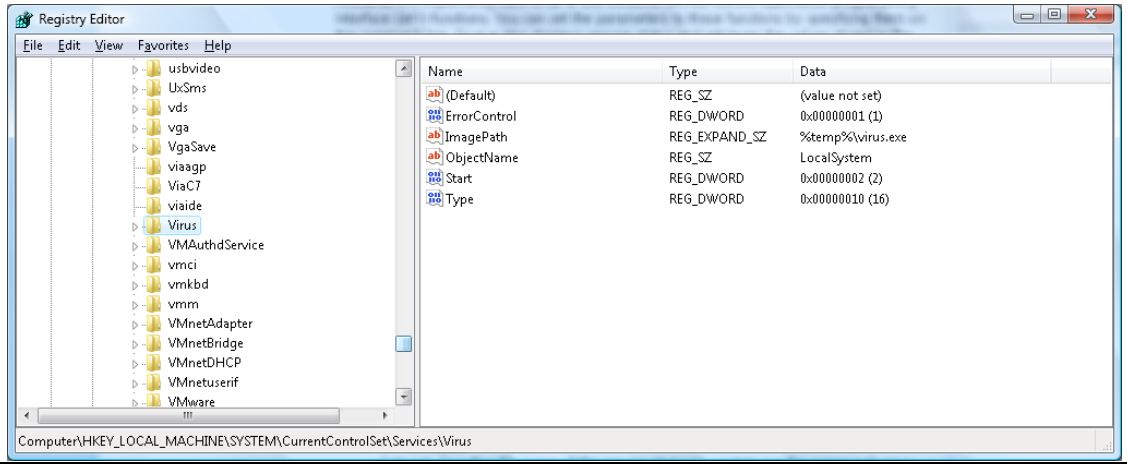
היישום לוקח את הרשימה הנ"ל מעורך הרישום, תחת המפתח:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
```

מבנה המפתח בנוי באופן הבא:

```
ErrorControl  [REG_SZ]
ImagePath     [REG_DWORD]
ObjectName    [REG_EXPAND_SZ]
Start         [REG_DWORD]
Type          [REG_DWORD]
```

- ImagePath - שומר את המיקום של היישום אותו יש להריץ.
- ObjectName - שומר את שמו של השירות אשר יופיע במנהל השירותים.
- Start - סוג הריצה (ידנית, אוטומטית, מבוטל, בעת טעינת המערכת וכו')
- Error - רמת השגיאות (רגיל, בינוני, קריטי).



יש אפשרות להוסיף את השירות באופן ידני, אך מיקרוסופט הוסיפו עוד כלי קטן בשם "SC.exe" המאפשר לבצע הוספה ומחיקה של שירות באופן זריז ויעיל. בכדי להוסיף שירות למערכת ההפעלה יש להשתמש בכלי באופן הבא (דרך שורת הפקודה):

```
sc.exe create "Virus" binPath= "%temp%\virus.exe" start= "auto"
```

מעכשיו, בכל טעינה של מערכת ההפעלה יורץ גם הקובץ %temp%\virus.exe. בכדי למחוק שירות, יש להשתמש בכלי באופן הבא:

```
sc.exe delete "Virus"
```

ושוב- יש לזכור כי לרב וירוסים יקראו לעצמם בשמות קצת פחות מסגירים, שמות של כלי מערכת או בקרים/שירותים אמיתיים עם שינויים קלים.

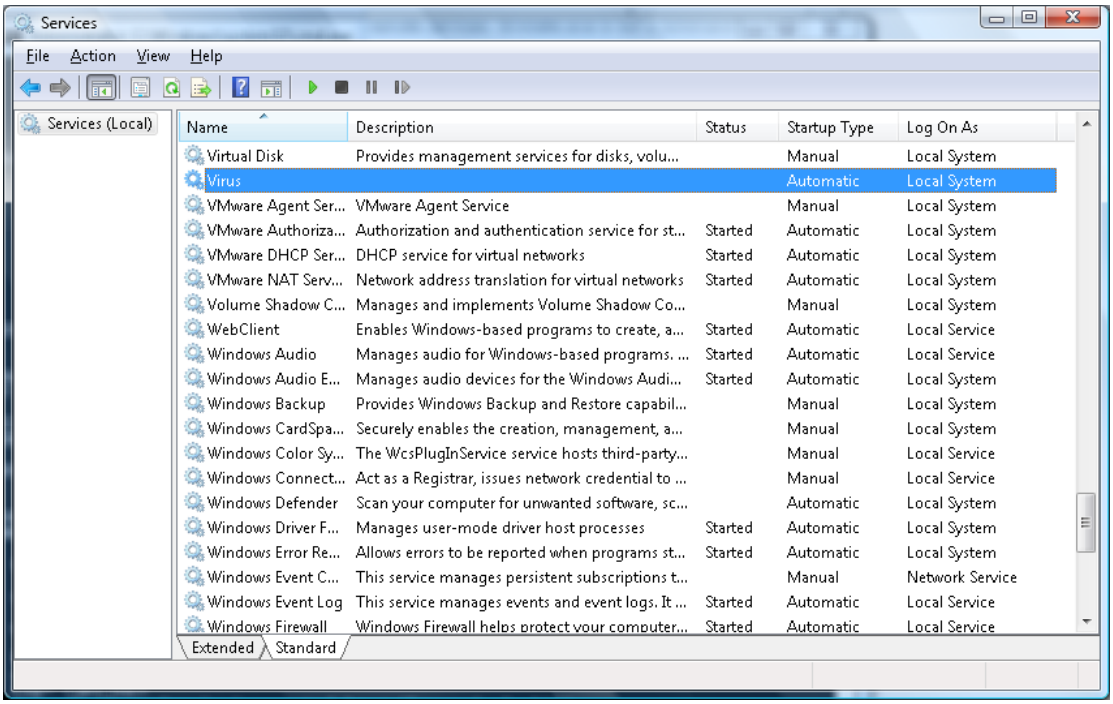


Image File Execution Options

ישנו עוד ערך אשר מנוצל טוב טוב ע"י כותבים התולעים, שימוש נכון בערך הנ"ל מאפשר לכותבי התולעים לבצע השתלטות מלאה על הרצת קובץ מסויים וזאת מבלי להשתמש בשיטות כגון API Hooking או Binary Code Injection אלה ע"י שינוי הערכים ב-Image File Execution Options אותם מנהל עורך הרישום.

בעורך הרישום, קיים המפתח הבא:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options
```

אם נרצה למשל לבצע "השתלטות" על הקובץ Msconfig.exe, כך שכל פעם שמישהו ירצה להריץ אותו-המערכת, במקום להריץ את ה-Msconfig, תריץ את התולעת שלנו - נניח Calc.exe, נוסיף בעורך הרישום מפתח בשם "msconfig.exe", ובתוכו ניצור מחרוזת (String Type) בשם "Debugger", ערכה יהיה המיקום של התולעת שלנו:

```
%windir%\system32\calc.exe
```

מעכשיו, בכל פעם שמישהו יפעיל את ה-Msconfig (כל אופן שהוא) במקומו תרוץ התולעת שלנו-Calc.exe.

יותר מכך, אם למשל "נדביק" תוכניות שמוגדרות להריץ סוג מסויים של קובץ- למשל Notepad מוגדר להריץ קבצים בעלי סיומת ".txt" - בכל פעם שיריצו את אותם קבצים, הקבצים האלה לא ירוצו ובמקומם תרוץ התולעת שלנו.

וירוסים משתמשים בתכונה זו בכדי "להדביק" בעיקר את ה-Taskmgr, Msconfig, Notepad, Cmd ותוכנות דומות.

ישנם תולעים אשר נכתבו באופן כזה שבכל הרצה שלהם הם גם מריצות את הערך שקיים ב-1% וב-2% בדיוק בשביל מקרים כאלה- כך שאם "נדביק" את Notepad.exe, ונרצה להריץ את 1.txt, גם התולעת שלנו תרוץ וגם אותו הקובץ, וכך הדבר מוסיף "לשקיפות" שלה ומאפשר לה להיות פחות מורגשת.

סיכום

שיטות לטעינת הוירוס רק גדלות וגדלות במהלך הזמן החולף, ולכן חשוב להכיר דרכים אלו, כך במקרים ובהם לא ניתן להריץ אנטי-וירוס מעודכן - חיפוש טוב במנגנונים שהצגתי היום יוכל להוביל לאיתור הוירוס או התולעת, וכך להקל בהסרתה.

בטקסט זה הצגתי מספר דרכים וטכנולוגיות אשר קיימות במערכת ההפעלה Windows אשר מנוצלים ע"י וירוסים ותולעים בכדי לשפר את אורך חייהם וכך להגביר את יעילותן. חשוב להזכיר כי "שיטות" אלה נוצרו בכדי להקל על המשתמש ו-"לשפר את חווית השימוש" שלו במערכת ההפעלה, אך כמו שראינו- מספר רב של גורמים "מזיקים" מבצע שימוש נוסף במרכיבים אלו. ניתן לחשוב שככל שהוירוס ישתמש ביותר מנגנוני גיבוי כך סביר להניח כי אורך חייו יגדל, אך חשוב מאוד לזכור - שככל שאותו הוירוס ישנה את סביבתו, כך יגדלו הסיכויים שהוא יתגלה.