INFECTAREA FIȘIERELOR DE SISTEM CU UN VIRUS DE TIP BACKDOOR

Arina LACHI

Universitatea Tehnică a Moldovei

Abstract: *A device driver is a program that controls a particular type of device that is attached to your computer. There are device drivers for printers, displays, CD-ROM readers, diskette drives, and so on. A device driver essentially converts the more general input/output instructions of the operating system to messages that the device type can understand. To secure the device driver can be a critical process. It is a lot of malicious programs that can infect them. Device drivers have been known to contain security flaws, which can be exploited, so it's important to keep these secured.*

Cuvinte cheie: *fișier de system, driver,rootkit, BackDoors, Trojan, virus informational,system.*

1. Introducere

Driver-ul este o componentă software care permite sistemului de operare să profite la maximum de funcționalitatea oferită de o componentă hardware. Deseori se întâmplă să apară în Device Manager un dispozitiv ascuns în spatele numelui de „generic device" sau „Unknown Device". Într-o astfel de situație, până când nu este instalat driverul potrivit, Windows-ul nu va folosi o placă de sunet, un modem, placa video, o placă de rețea, o placă de captură, un webcam sau orice altceva. Salvarea driverelor de sistem, recuperarea, actualizarea şi ştergerea acestora din sistemul de operare Windows reprezintă un proces complex care de cele mai multe ori necesită utilizare software-ului specific. Însă de cele mai multe ori anume securitatea acestor fișiere devine una critică pentru sistemul informațional deoarece efectele infectării ar fi unele cu adevărat dezastruoase. Controlul asupra fișierelor de sistem, utilizatorii neautorizați îl obțin de cele mai dese ori prin programele de rootkit. Un soft tip rootkit este în general un program ce reușește printr-o vulnerabilitate a sistemului gazdă să capete drepturi depline pe un sistem, sistem pe care îl modifică pentru a-i putea folosi resursele nedetectat.

Rootkit-urile sunt diferite față de un virus, mai ales prin modalitatea de propagare: în general acestea sunt "implantate" de un atacator și nu sunt interesate de propagarea pe alt sistem. Ca și un virus, un rootkit va încerca să păstreze sistemul sub controlul său, ceea ce poate însemna de exemplu că face verificări constante asupra modulelor prin care rootkit-ul își menține controlul și reaplicarea modificărilor dacă acestea au fost "reparate" pentru ca sistemul să poată în continuare să fie controlat. Rookit-urile în marea majoritate pun la dispoziția atacatorului un **backdoor** prin care acesta poate intra în sistem oricînd dorește și poate efectua orice operațiuni asupra datelor. Rootkit-urile rar sunt distructive, pentru că scopul lor este de a căpăta și menține controlul asupra unui sistem cu scopul folosirii capacității sale de procesare în alte scopuri sau în ideea accesului la eventual informații importante (parole, coduri PIN, numere cărți credit, etc).

2. Infectarea fișierului Atapi.sys

Atapi.sys este un driver Windows localizat în C:\Windows\system32\drivers, care permite comunicarea cu unitățile periferice: CD-ROM, HDD,etc. Coruperea acestui fișier sau a fișierelor asociate acestuia are drept efect BSOD (*Blue Screen of Death*) sau restartarea calculatorului la cîteva minute după pornire.

Aceste situații apar în cazul ștergerii fișierului Atapi.sys care a fost catalogat de antivirus ca fiind infectat. De cele mai multe ori însă sistemul informațional va funcționa doar că cu o performanță net inferioară. Un astfel de virus este BackDoor.Tdss.565 care folosindu-se de tehnica backdoor obține acces la un calculator aflat la distanță. Specificul acestui virus este utilizarea unei tehnici rootkit prin care-și

maschează prezența în sistem infectînd driver-ul Atapi.sys. BackDoor.Tdss.565 își injectează codul în procesul sistemului de instalare și apoi îl utilizează pentru a crea un serviciu temporar – tdlserv:

[HKLM\system\currentcontrolset\services\tdlserv]
Imagepath=" \??\C:\DOCUME~1\\LOCALS~1\Temp\3.tmp"
Type=1

Pentru a-și asigura încărcarea viitoare în mod automat, driver-ul infectează driverele de sistem pe drive-ul fizic unde se află localizat sistemul de operare (spre exemplu, atapi.sys). Biții originali ai driver-ului infectat și ai codului rootkit-ului sunt păstrate în ultimele sectoare ale discului. De asemenea, ultimele sectoare ale discului servesc drept partiție criptată ascunsă, folosită pentru a stoca componentele tdlcmd.dll și tdlwsp.dll și de asemenea fișierul de configurare config.ini.

Rootkit-ul ascunde modificările aduse sistemului de operare și implementează injectarea celor două biblioteci de date amintite (.dll-uri) în acord cu instrucțiunile fișierului de configurare. Metoda non-tipică de injectare într-un proces de sistem în timpul instalării este una complet neașteptată. Ceea ce permite rootkit-ului de a ocoli cele mai multe blocante de comportament, instalînd driverul și rămînînd nedetectate. Metoda constă în omiterea din stiva de dispozitive ale driver-ului ATAPI care funcționează cu unitatea de sistem care intenționează să fie folosită.

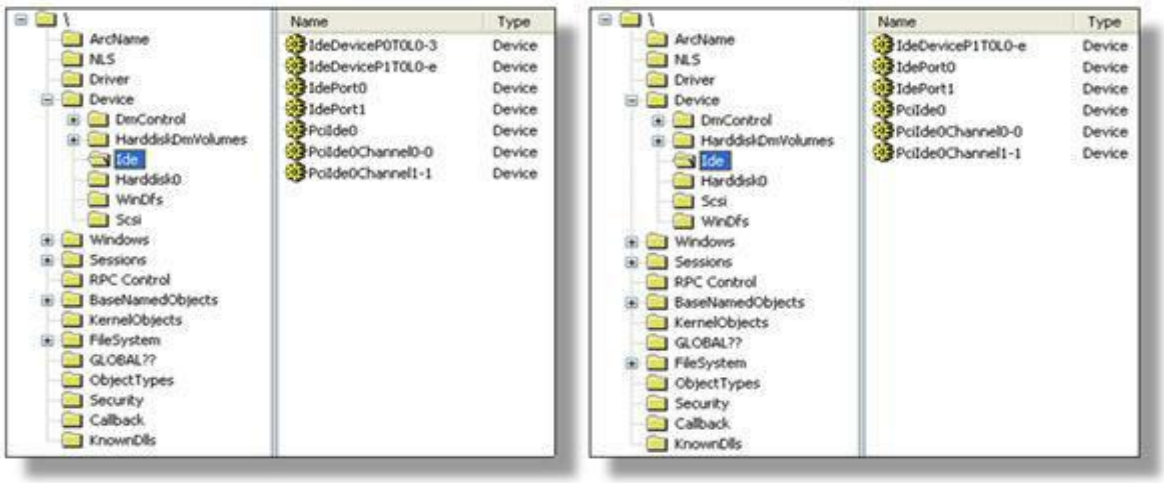

Figura 1 Partea stîngă reprezintă o stivă neinfectată. Partea dreaptă are lipsă un dispozitiv

3. Corectarea erorilor din sistemul informational

Funcționarea corectă a sistemului informațional poate fi recuperate utilizînd următoarele tehnici:

- Utilizarea opțiunii sfc/scannow atunci cînd rulează Command Prompt. Această comandă va inspecta toate fișierele Windows din sistemul de calcul, inclusive fișierele DLL. Dacă File System Checker va depista o problemă la oricare din fișierele de sistem va încerca să-l trateze.

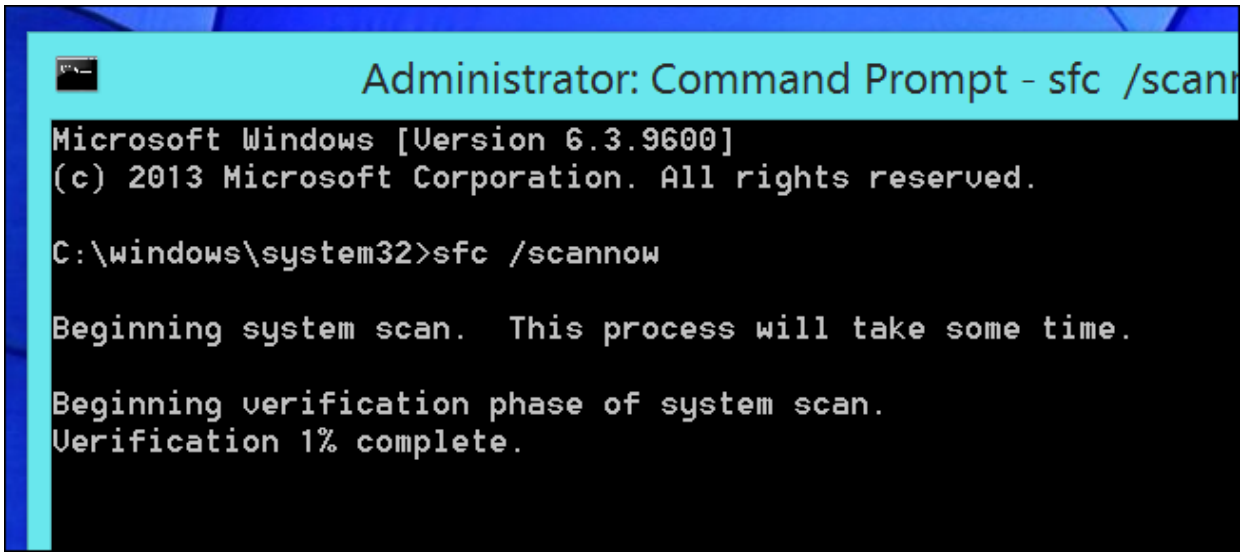

Figura 2 Comanda sfc/scannow

- Dezinstalarea programelor ce nu au mai fost utilizate de mult timp, verificînd Programele Autostart (prin opţiunea msconfig).

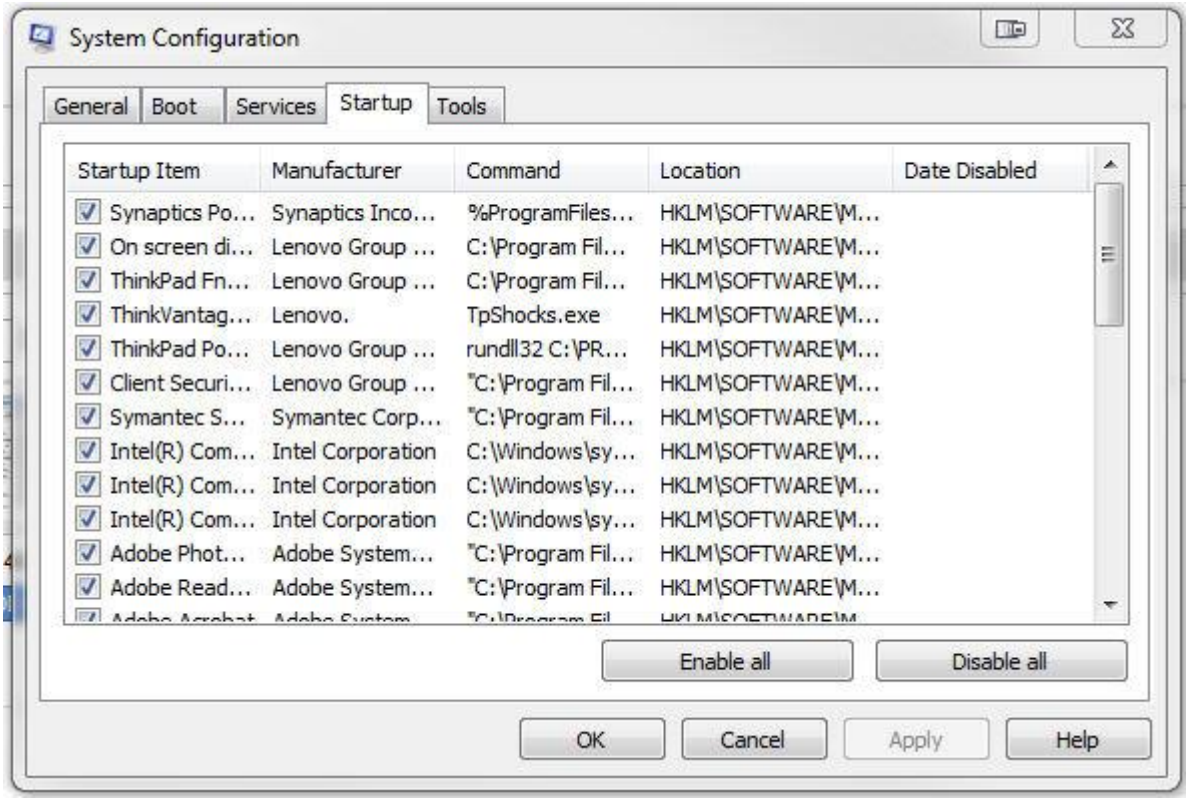

Figura 3 Utilitara msconfig.exe

- Crearea de backup la date precum și setarea punctelor de restaurare în caz de necesitate. Astfel dacă sistemul nu mai funcționează cu aceiași performanță să existe posibilitatea de restaurat sistemul din punctul în care el funcționa normal.
- Pentru a analiza procesele din atapi.sys pot fi utilizate următoarele programe:

- Security Task Manager care va identifica toate procesele Windows care rulează inclusiv și procesele ascunse așa ca: procese de monitorizare a browser-ului sau intrările AutoStart. Security Task Manager arată toate procesele active de pe calculator. Astfel pot fi ușor recunoscute procesele ilicite care ulterior vor fi plasate în carantină pentru o perioadă de timp. Security Task Manager este compatibil cu toate programele Antivirus. De asemenea una din opțiunile sale este ștergerea istoriei și atenționarea cînd are loc vreo modificare în regiștri.

- Malwarebytes AntiMalware ce detectează și șterge toate programele ascunse Spyware, Trojan, Keyloggers de pe hard disc. Malwarebytes Anti-Malware are o funcție de scanare rapidă pentru a verifica zonele critice ale sistemului și de a plasa malware într-o zonă de carantină. Software-ul permite să se adauge fișiere sau foldere într-o listă, care este ignoratăn, atunci când scanează. Malwarebytes Anti-Malware are o caracteristică care permite rularea unui program, chiar și atunci când este blocat ca fiind malware.

4. Concluzie

Tehnologiile informaționale reprezintă cel mai dinamic sector cu o dezvoltare anuală care impresionează. Întreaga lume este digitalizată ceea ce impune involuntar utilizatorilor cunoștințe cel puțin minimale despre buna funcționare a unui sistem informațional. Dar este știut și faptul că un dispozitiv ca calculatorul, telefonul mobil sau tableta practic va fi imposibil de utilizat fără un sistem de operare viabil și sigur care ar asigura funcționarea acestora. Driver-ele sistemului de operare sunt programe ce asigură legătura cu diferite periferice și de buna funcționare a cărora depinde accesul pe care îl vom avea la sistemul dat. Dar cu cît mai mult s-au dezvoltat tehnologiile informaționale cu atît mai accelerat au crescut și pericolele. Dacă cu 10 ani în urmă existau doar virușii informaționali care aveau un cod malițios static, atunci actualmente codurile de viruși sunt polimorfizați asigurîndu-se un cod diferit la fiecare infestare ceea ce îi face greu detectabili de către programele Antivirus. Pe lîngă problema cu virușii informaționali a apărut una și mai complexă: cea a programelor de rootkit care fac detectarea proceselor periculoase și ilicite și mai dificilă. Astfel reieșind din cele relatate mai sus pot să afirm ca și soluțiile care ar trebui întreprinse în situațiile critice sunt unele complexe, adică nu mai este suficient de a utiliza un produs software care să rezolve problemele de securitate dar este necesar de a întreprinde o serie de măsuri care vor include de asemenea și programe de protecție doar că în ansamblu cu alte procedee.

Bibliografie

1. Carnegie Melon Software Engineering Institute, Security of the Internet, Froehlich/Kent Encyclopedia of Telecommunications, vol. 15
2. Reka A. e.a., The Internet Achilles' Heel: Error and attack tolerance of complex networks, Physica A, Elsevier Science B.V., 2000
3. https://support.microsoft.com/ru-ru
4. http://www.securitatea-informatiilor.ro