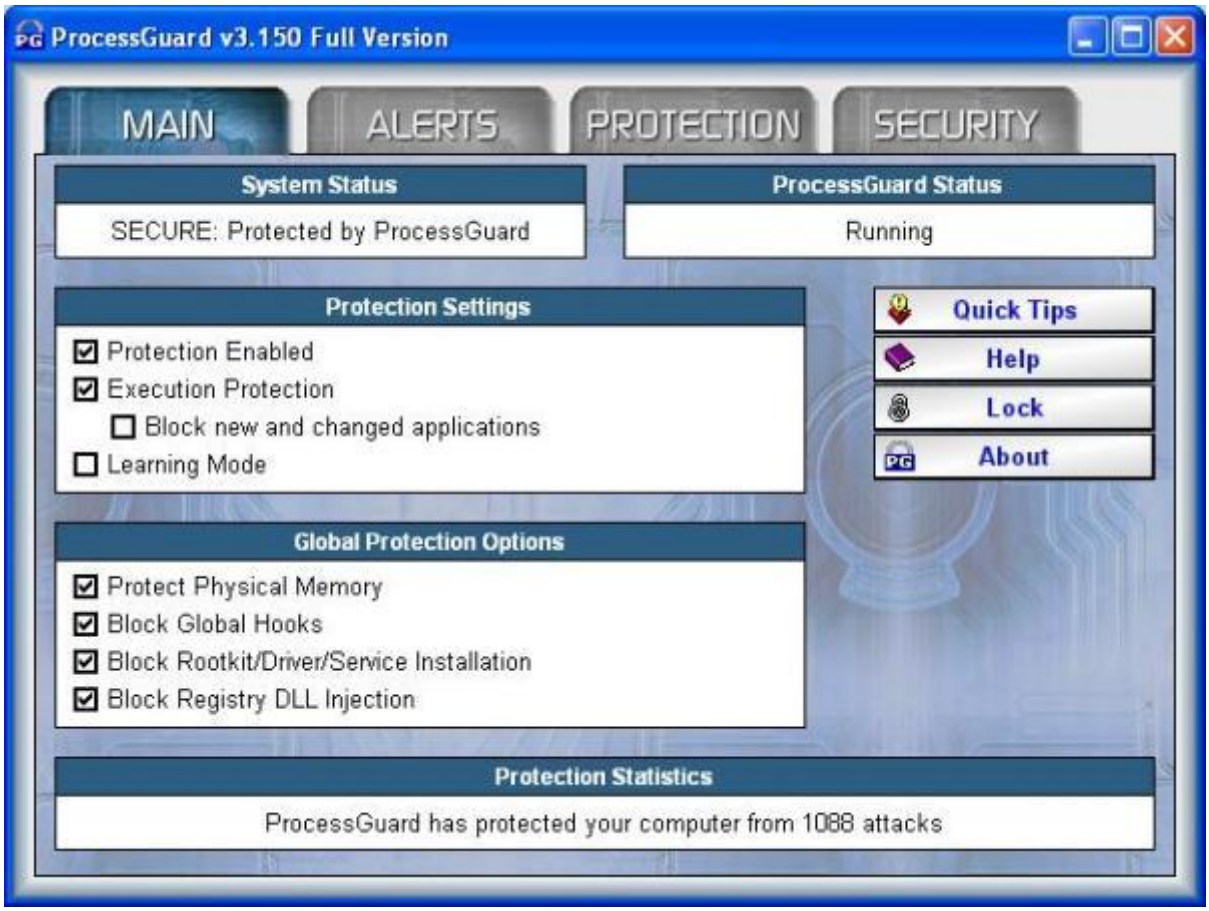
DiamondCS ProcessGuard



ProcessGuard is an australian product from DiamondCS, a small business but dynamic enterprise specialized on security softwares for home users.

"ProcessGuard was created out of the need for a solution to be found for a very big problem that has been troubling developers of security software for years: how to prevent their software from being attacked by malicious software and others programs running on the same system."

This sentence extracted from the help file explains the origin of ProcessGuard which is currently at the 3.150 version.

The target of ProcessGuard is to protect the integrity of the system.

It's not only an application firewall which can help the user to control the activity.

ProcessGuard uses a behaviour approach to prevent from running many kind of attacks which can be used by malicious codes and malwares.

Some of the most interesting features are the ability:

-to protect any program/application from termination or modification,

-to prevent access to physical memory,

-to prevent driver/service installation.

ProcessGuard provides a high degree of security against advanced threats and attacks and is one of the most effective products to integrate on a line defense.

TEST:

Configuration:

-all options (see above the first image) are enabled except "block new and changed applications" (if enabled, any unknown application will be blocked),

-procguard.exe, pgaccount.exe and DCSUserProt.exe (service) are protected from all attacks, are protected from reading and have maximum privileges.

The majority of the test files are:

-run as unknown files (for the first time),

-launched from a CDRom (except Kapimon, APISpy32, BufferOverflow test files),

- allowed to run once,

- not integrated in the protection list.

NB: For some tests, ProcessGuard associated processes are allowed to be read.

Any other similar security software is disabled.

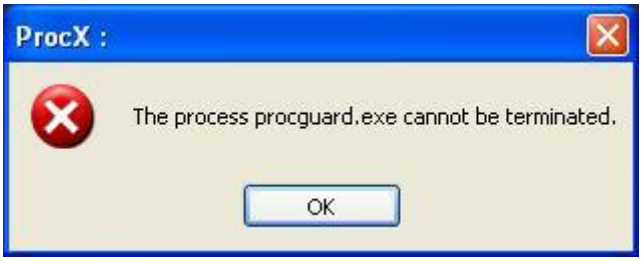
***** Execution control/protection with Leaktests:**

ProcessGuard is the winner (can detect and block Copycat, DNSTester and Ghost).

*****Process Termination:**

ProcX and APT are allowed to read procguard.exe.

-with ProcX: ProcessGuard is the winner .



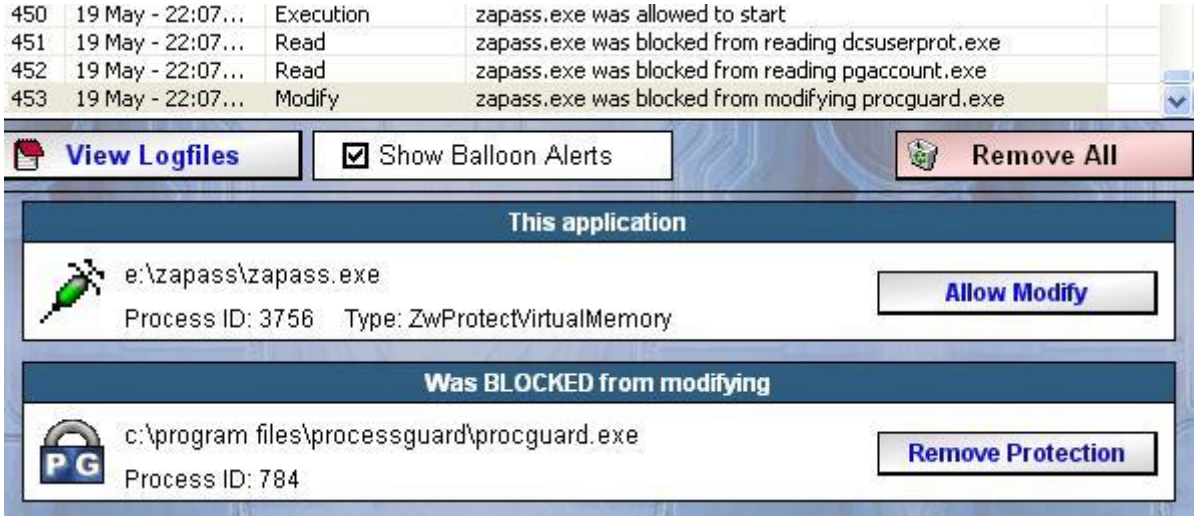
-with APT: ProcessGuard is the winner.

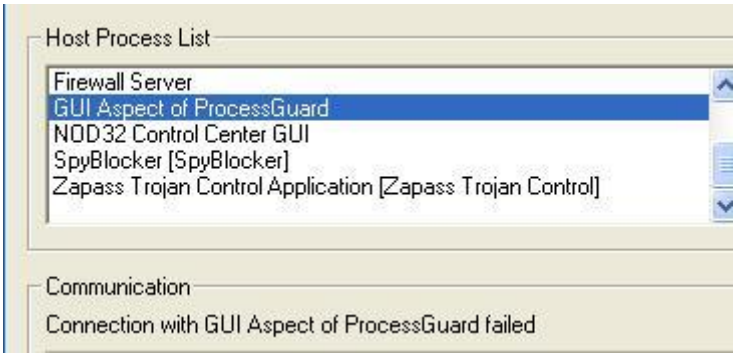
-with Copylock: PG is the winner.

ProcessGuard is the winner against process termination test.

*****Dll injection/implant:**

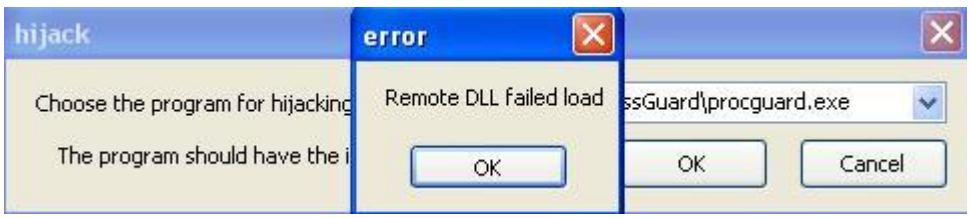
ProcessGuard is the winner against Zapass or Copycat.





*****Process Hijacking:**

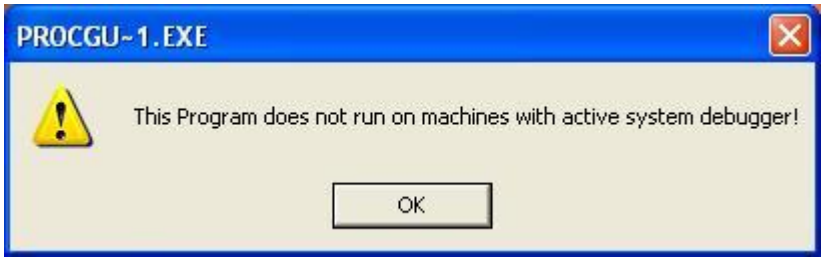
ProcessGuard is the winner.

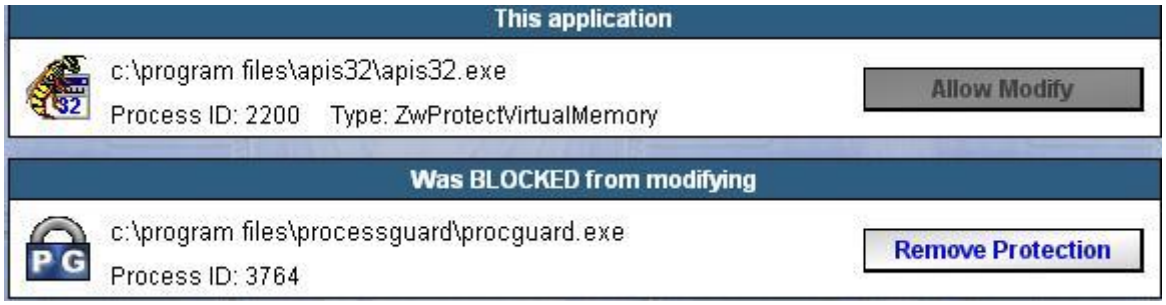


*****API Manipulation test:**

-with APISpy32: another instance of procguard.exe can't be run.

ProcessGuard is the winner (the same result for any other protected application).



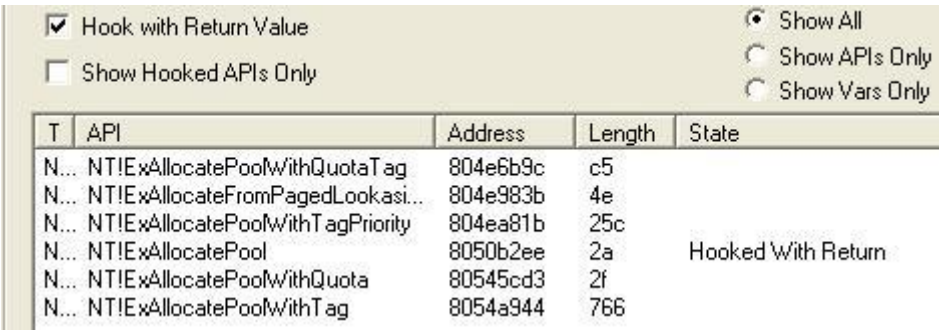


-with ExecuteHook: PG (ProcessGuard) detects any hooks (global or notepad's one).

ProcessGuard is the winner.

-with Kapimon: PG does not detect the API hook with return value on the system.

ProcessGuard failed.



I consider that ProcessGuard is the winner (2/3) against API Manipulation test.

NB: service.exe is allowed to load the Trace.sys driver (needful for this test).

*****Finjan Tests:**

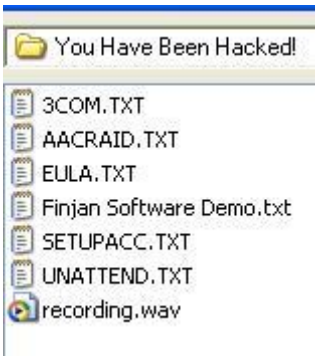
-F.Demo: PG does not detect the creation of the folder: PG failed.

-F.VBS: ProcessGuard detects the Windows Scripting Host, but not folders access.

PG failed.

-F.JPG: PG detects the packager and its first action (access to Temp file) but not the creation of the folder: ProcessGuard failed.

ProcessGuard failed against Finjan Tests.



*****Registry Tests:**

-with Regtest 1: ProcessGuard failed.

Registry Item	Status
HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SESSION MANAGER\BootExecute	Modification Successful
HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\!1_ProcessGuard_Sta...	Modification Successful
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\JeticoPFStartup	Modification Successful
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\SpyBlocker	Modification Successful
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\OGCC	Modification Successful
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\KAVPersonal50	Modification Successful

-with Regtest 2: this test has been done twice and if the system was blocked without a reboot, the action of Regtest is real and is confirmed by [this pop up] after the reboot.

ProcessGuard failed.

NB. ProcessGuard detects the call to the driver but can't prevent the shutdown and the reboot with or without a specific rule for Windows\System32\Service.exe.

```
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
regtest.exe [568] Tried to install a driver/service named 1RegTest
```

-with Scoundrel Simulator: ProcessGuard failed (0/5).

RegHide and RegTick pro tests are unnecessary.

ProcessGuard failed against Registry Tests.

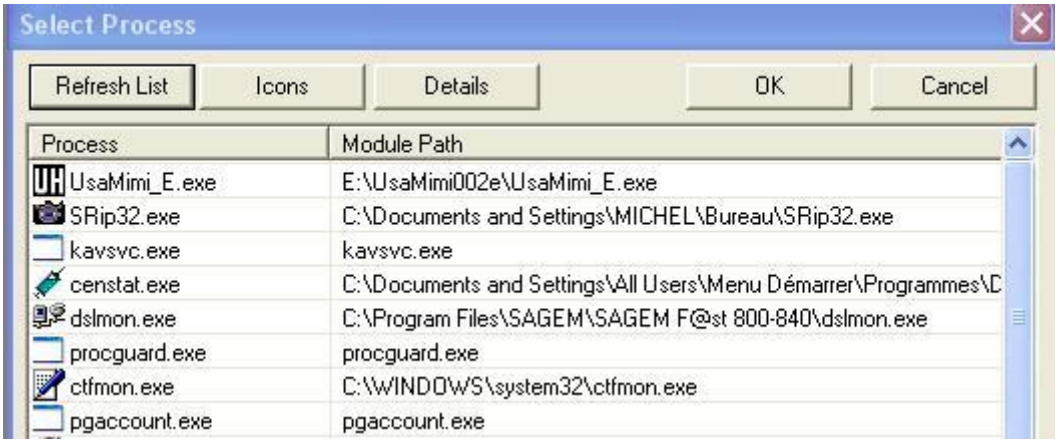
*****Simulate a Trojan with Trojan Simulator:**

ProcessGuard detects the server and can allow the user to block it.

ProcessGuard is the winner.

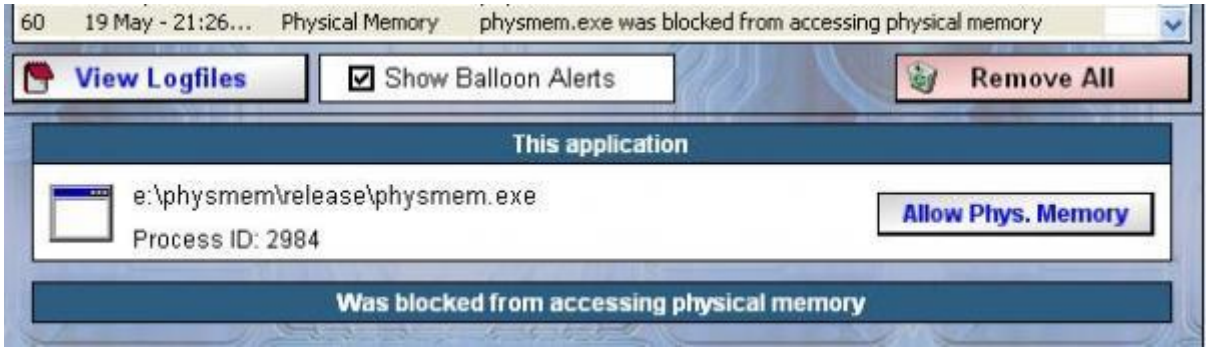
*****Memory Manipulation test:**

-with UH: PG is the winner (same result with pgaccount.exe and dcsuserprot.exe).



NB: Even if we allow UH to read procguard.exe, the modification of processguard memory (or another protected application) is not possible.

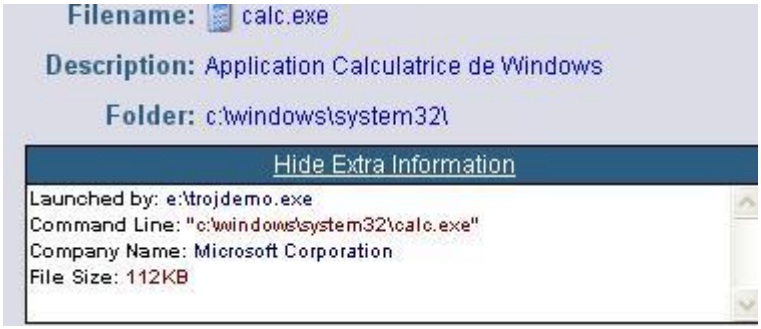
-with PhysMem: PysMem is blocked instantaneously from accessing to the physical memory.

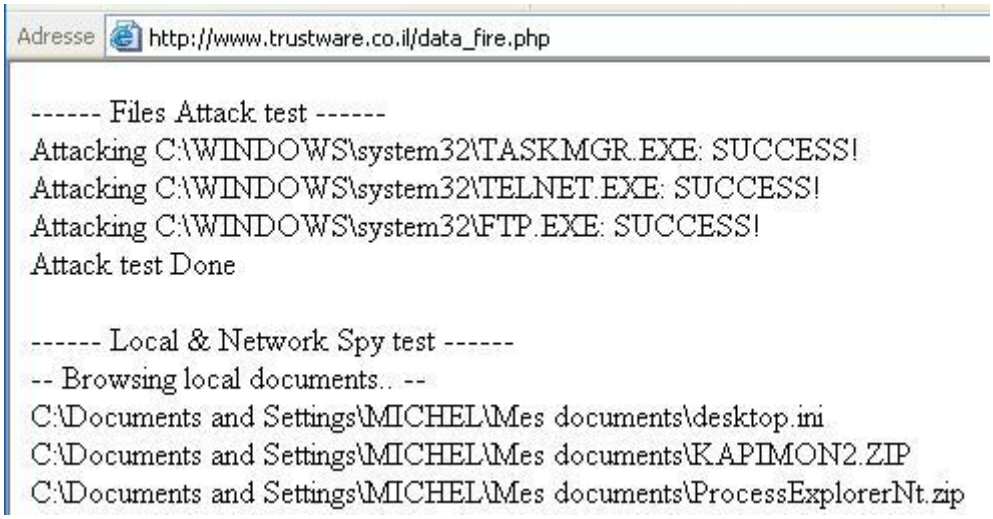


ProcessGuard is the winner against Memory Manipulation tests.

*****Data Theft with Trojan Demo:**

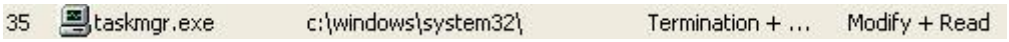
ProcessGuard just detects that calc.exe is launched, but not others access to the taskmanager or the folders.





ProcessGuard failed against Data Theft test.

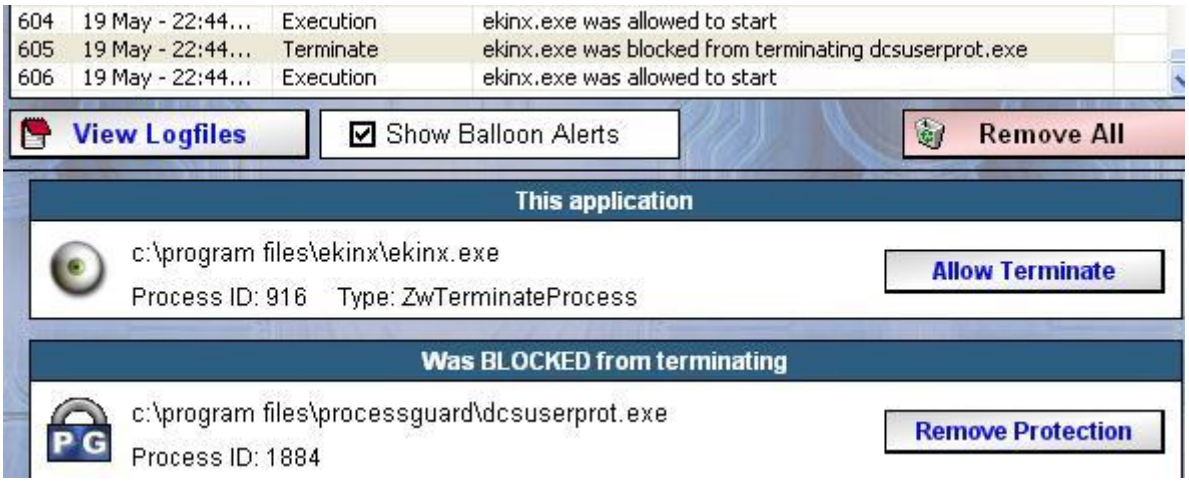
NB. Even with specific rules (protecting taskmgr.exe or telnet.exe from reading), PG can't prevent data from being copied and stolen.



*****Service/driver Manipulation:**

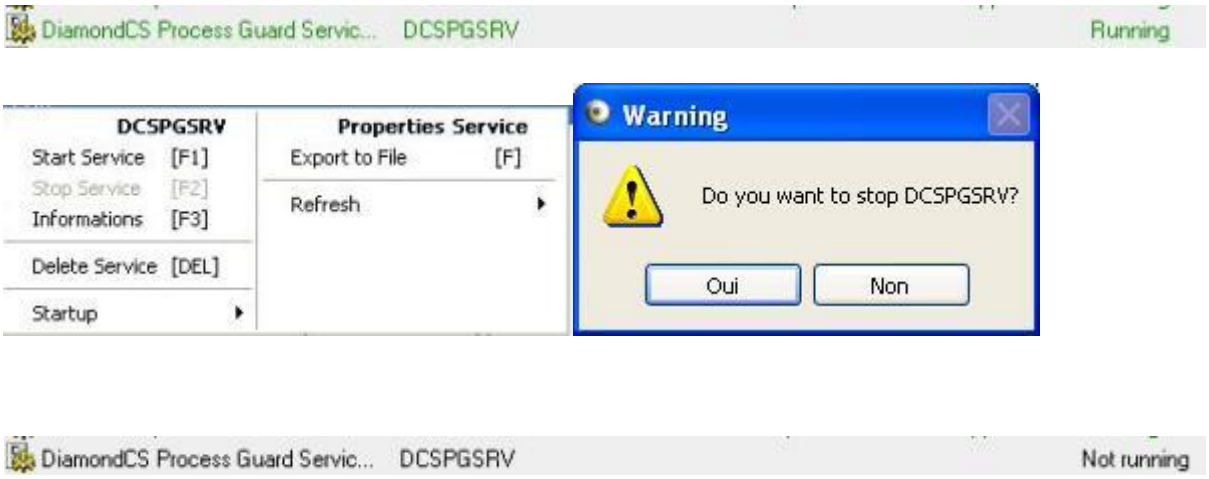
-installation: ProcessGuard is the winner (blocks automatically any service installation if the option is enabled).

-termination: ProcessGuard is the winner (against ProcX, APT, TakeControl or EkinX).

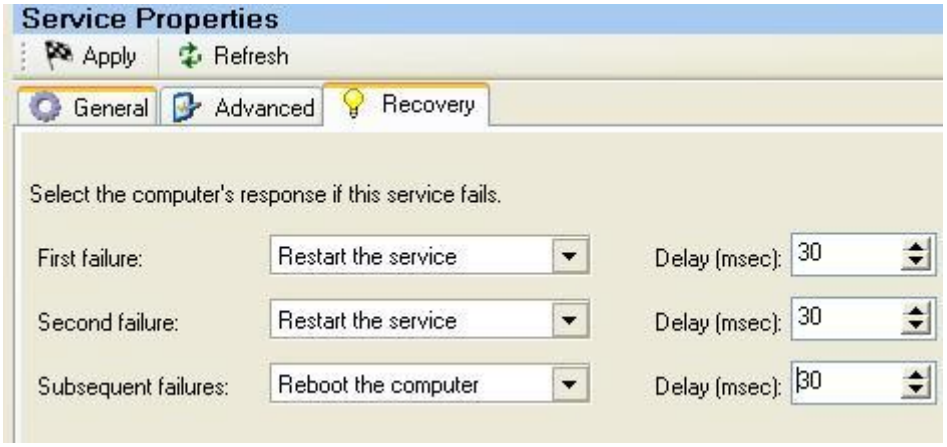


NB. ProcessGuard service and driver can be stoped and removed by using EkinX.

It's strongly suited to configure ProcessGuard/security programs services in the Control Panel (recovery): just choose "restart the service" for the three failures.



Configure the recovery service manually or with [ServiceView]:



Plugin name	Services.dll
Object	DCSPGSRV\DiamondCS Process Guard Service v3.000
Action	Remove
New value	272*2*"C:\Program Files\ProcessGuard\dcsuserprot.exe"

System Status	ProcessGuard Status
Unknown	Error in initialization. Check dcsuserprot.exe

-modificaction: ProcessGuard is the winner.

-unloading a driver: ProcessGuard failed if Windows Service has the permission to allow driver/service : then PG does not detect (or prevent) that Kapimon needs to load its Trace.sys driver to work

PG is the winner if we deny this permission to Windows\System32\service.exe.

NB. ProcessGuard has the ability to intercept API calls, but in this case, usual APIs used to load device drivers (DeviceIoControl/ReadFile/WriteFile) were not intercepted.

ProcessGuard is the winner against service/driver manipulation test.

*****CDRom autorun:**

ProcessGuard is the winner.

*****Fake/Jokes test:**

-open/close the CDRom drive: ProcessGuard detects the action but can't prevent it from being opened: the result can't really be specified.

-launching several windows applications at the same time: ProcessGuard detects all launched executables: ProcessGuard is the winner.

ProcessGuard is the winner against Jokes Tests.

*****Buffer/Heap Overflow:**

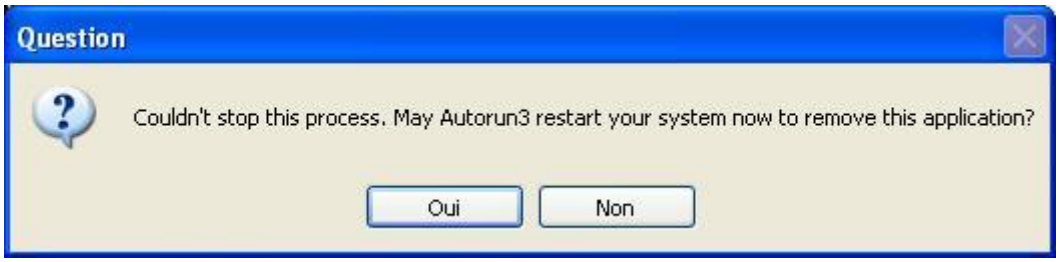
ProcessGuard can't detect shell atempts to the stack but just test files activities.

ProcessGuard failed against Buffer Overflow tests.

*****Deactivation Methods:**

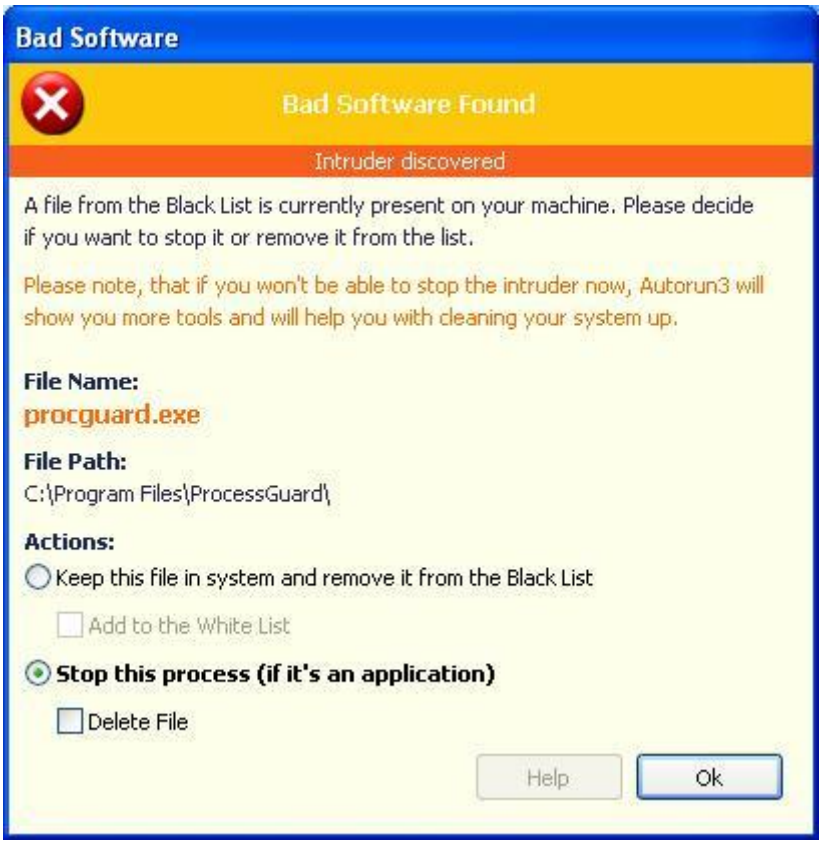
-trashcan: PG is the winner.

-blacklisting: PG is the winner.



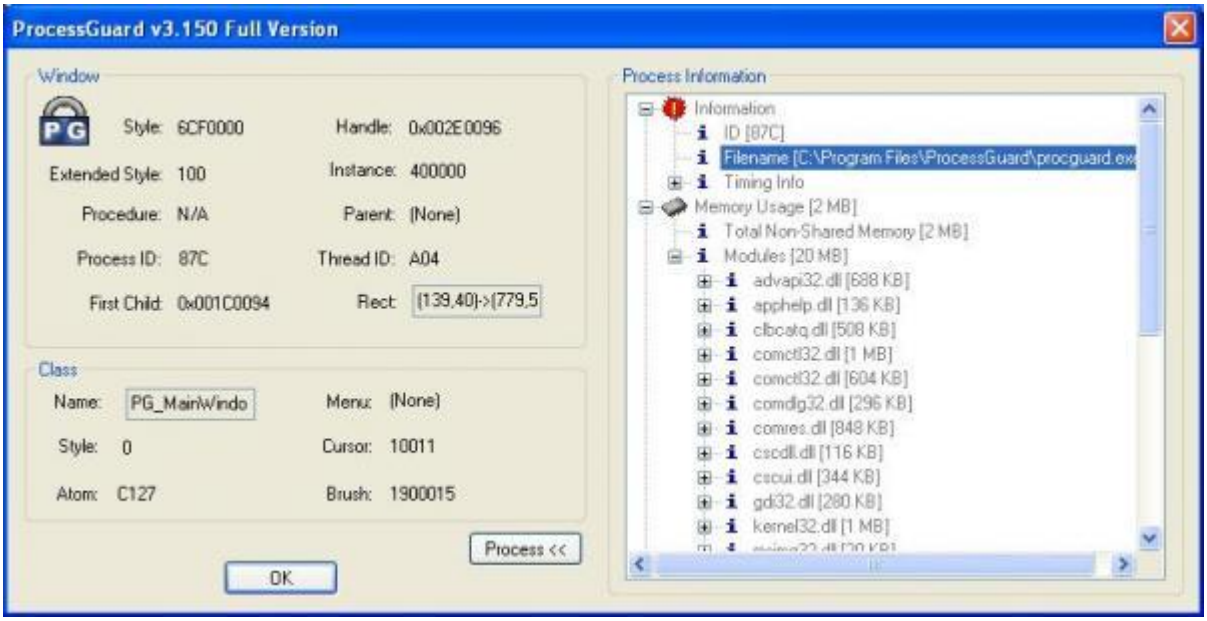
NB: procguard.exe can't be read by Autorun3, then ProcessGuard can't be disabled.

But if we allow procguard to be read by A3, then PG (procguard.exe) can be wiped in Program Files folder.



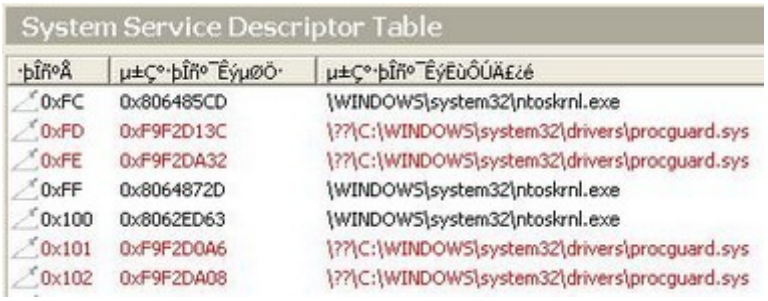
ProcessGuard is the winner against deactivation methods.

CONCLUSION:



The Pros:

-effective defense against various threats and attacks: global hooks (keyloggers), driver/service installation (rootkits), dll injection (CWS trojans) especially due to the integration on kernel low level (see the image),



-ability to protect the integrity of the system and programs processes (especially security applications which can be a target for some malwares),

-effective self-protection and also for associated files (pghash.dat, pguard.dat) which are protected by Windows Protection Service and PG service),

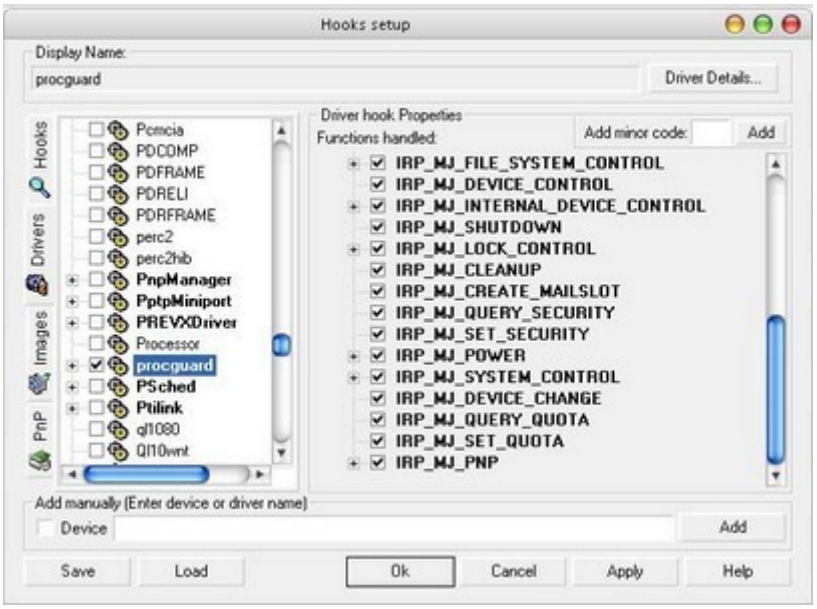
-execution activity control (application firewall),

-very intuitive in using (especially the "learning mode" phase),

-secure mode ("block new and changed applications") to prevent unknown and suspect changed files executions,

-MD5 integrity control for detecting modifications in an executable,

-runs as a service (dcsuserprot.exe),



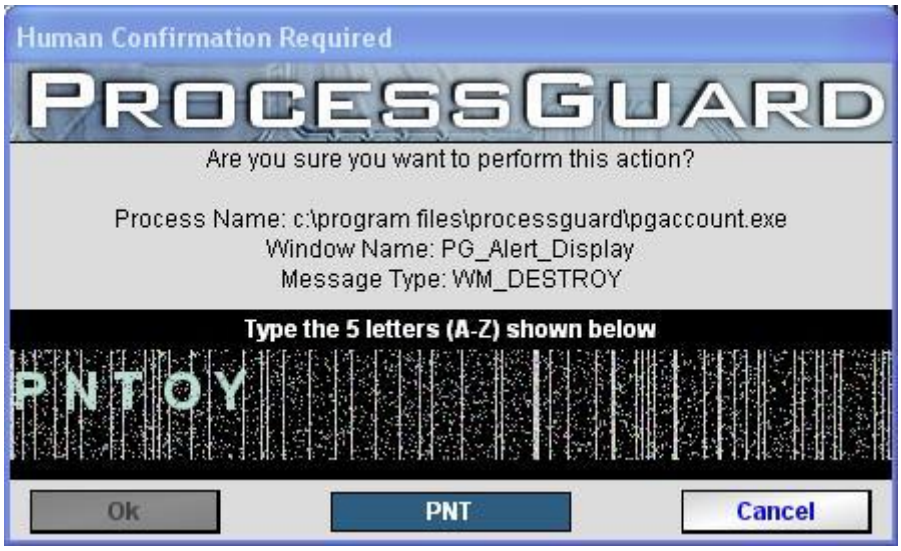
-does not require to be experienced for a high degree of protection: the user just needs to check boxes options,

-"pro and clean package": easy and quick set up, size, quality of the help file (...),

-good support and very helpful forum,

-nice graphic interface,

-human verification control / "secure message handling" (very rare feature), more secure than a simple password, and can prevent unauthorized / suspect activity,



-excellent mix between prevention and detection features,

-competitive price and good value for money.

The Cons:

-takes too much time to load and to initialize :then the protection is limited during the boot (the PG's driver / service is just an autostart, not a system start or better: a boot start one) and an application or a driver / service can start and load without control,

-no registry monitoring features (but not intended to),

-limited protection against worms (does not cover scripts, files access or buffer overflows), but it's quite normal considering WormGuard, a specialized product from the same firm,

-very talkative with its log file: after a month, the log file can take a significant size on the hard drive (>10 Mo), and i can't imagine after a year...

-no maintenance or install mode: for installing a program or an update (Windows, antivirus etc), ProcessGuard must be disabled or set up to learning mode; then the system's still vulnerable and can be infected by spywares for instance (which are often added with legitimate programs) or any other malware by an installer (from P2P files for instance),

-very limited online process database (PerfectProcess is a freeware which can be helpful for classical users: integrates a database and can launch a google search),

Here's the "info" on Diamondcs web site for an usual process:

-not compatible (due to the kernel mode DRIVER) with old Windows versions (95/98),

-only available in english language.

COMMENTS:

ProcessGuard is currently one of the most effective product that a home user can deploy on his line defense.

Coded by a team who is well-informed about new attaks used by malwares, ProcessGuard provides a high degree of security against all kinds of threats (trojans, keyloggers, rootkits, spywares etc).

Its protection covers all system's processes and programs applications.

And the secure mode can prevent the majority of infections during a surf's session.

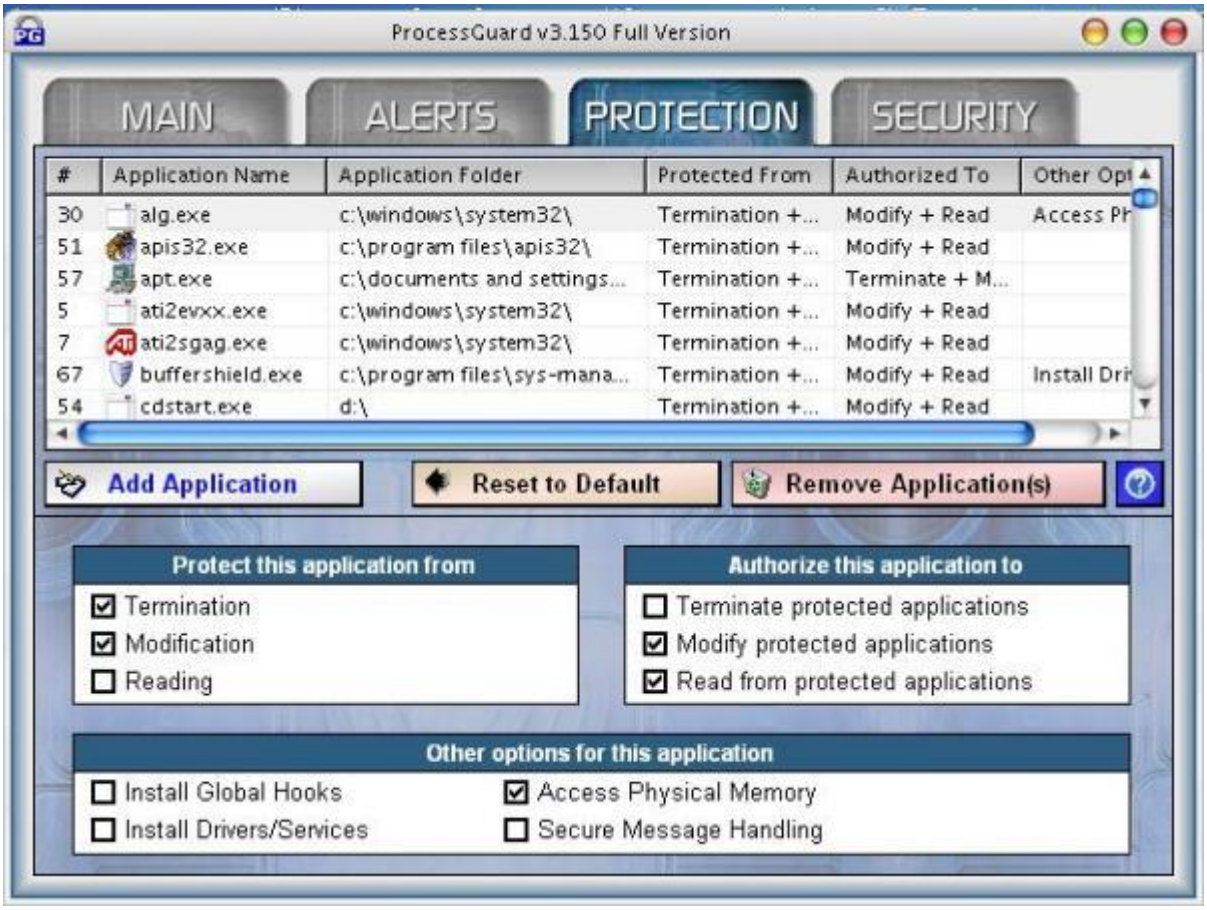
Very intuitive, pleasant and comfortable to use, ProcessGuard does not require too much time for the configuration or for answering to alerts, especially if the "learning" phase was taken seriously into consideration.

With a level-headed mix between prevention and detection features, ProcessGuard is one of the rare product which can be used by beginners and classical users, and can satisfy advanced and experienced ones.

But ProcessGuard appears less exhaustive as a muli-layered defense than some others products, especially regarding the registry: in this case, a specific registry protection (RegRun/RegDefend) can be suggested to increase the line defense.

In all cases, with its best value for money, ProcessGuard is certainly a must have in a single computer.

ProcessGuard with a Mac theme:



NB. A big thanks to Wayne, chief manager / Head of R.D, for his cooperation (special full license of Processguard).

COMMENTAIRES:

ProcessGuard est un logiciel edité par Diamondcs, une petite société australienne basée à Perth depuis 1986 et spécialisée dans la protection des ordinateurs individuels (l'anti-trojan TDS est son produit le plus connu).

Integré au kernel de Windows, lui permettant ainsi d'intercepter les appels de bas-niveaux (mémoire, driver / service etc), ProcessGuard utilise une approche comportementale afin de détecter divers types d'attaques et de malveillances.

Il peut ainsi prevenir l'injection de code, empêcher l'accés à la mémoire physique, bloquer l'installation de drivers ou alors protéger les processus système et les programmes de toute tentative de modification ou de désactivation (les antivirus par exemple sont souvent des cibles de ce type d'attaques).

Aprés son installation, juste au redémarrage de l'ordinateur, ProcessGuard prend une empreinte du système et des applications installées (avec hashage MD5) et tente par la suite d'en préserver l'intégrité.

C'est la raison pour laquelle cette phase de "learning mode" ou "lecture du systeme" doit étre prise trés au sérieux en lançant tous les programmes usuels afin que ProcessGuard les intégre dans sa base de donnée.

ProcessGuard dispose également d'une fonction de contrôleur d'activités qui permet d'octroyer des droits et permissions pour chaque exécutable.

Il peut également fonctionner en "mode sécurisé" grâce à sa fonction de blocage des applications modifiées ou inconnues (mode conseillé lors d'une séance de surf).

Il convient également de noter la fonction trés rare de contrôle visuel ou de "vérification humaine": une boite de dialogue peut apparaître pour autoriser ou non une fermeture de fenêtre Windows et l'utilisateur doit insérer une série de lettres toujours aléatoires.

Cette fonction permet de s'assurer qu'il ne s'agit pas d'une activité suspecte lancée par un programme malveillant.

ProcessGuard est un logiciel intuitif qui procure un haut niveau de sécurité tout en étant confortable et agréable à utiliser.

Il peut ainsi convenir aussi bien à l'utilisateur avancé qu'à l'utlisateur classique; seul les permissions spéciales allouées aux applications peuvent poser quelques difficultés à celles et ceux qui ne seraient pas familiers de ce type de produits.

Toutefois, si ProcessGuard apporte une protection trés efficace contre les malwares avancés (rootkits, enregistreurs de frappes, trojans), il ne ne comporte pas de module de surveilleillance du registre, des fichiers ou services vitaux.

Vendu avec un trés bon rapport qualité-prix (30 euros environ), ProcessGuard aurait tout pour lui, si ce n'est l'inconvénient majeur de n'être disponible qu'en anglais.

NB. Un grand Merci à Wayne, directeur de project chez Diamondcs, pour sa coopération (activation d'une version complète de ProcessGuard).