Gislene Noronha Messias

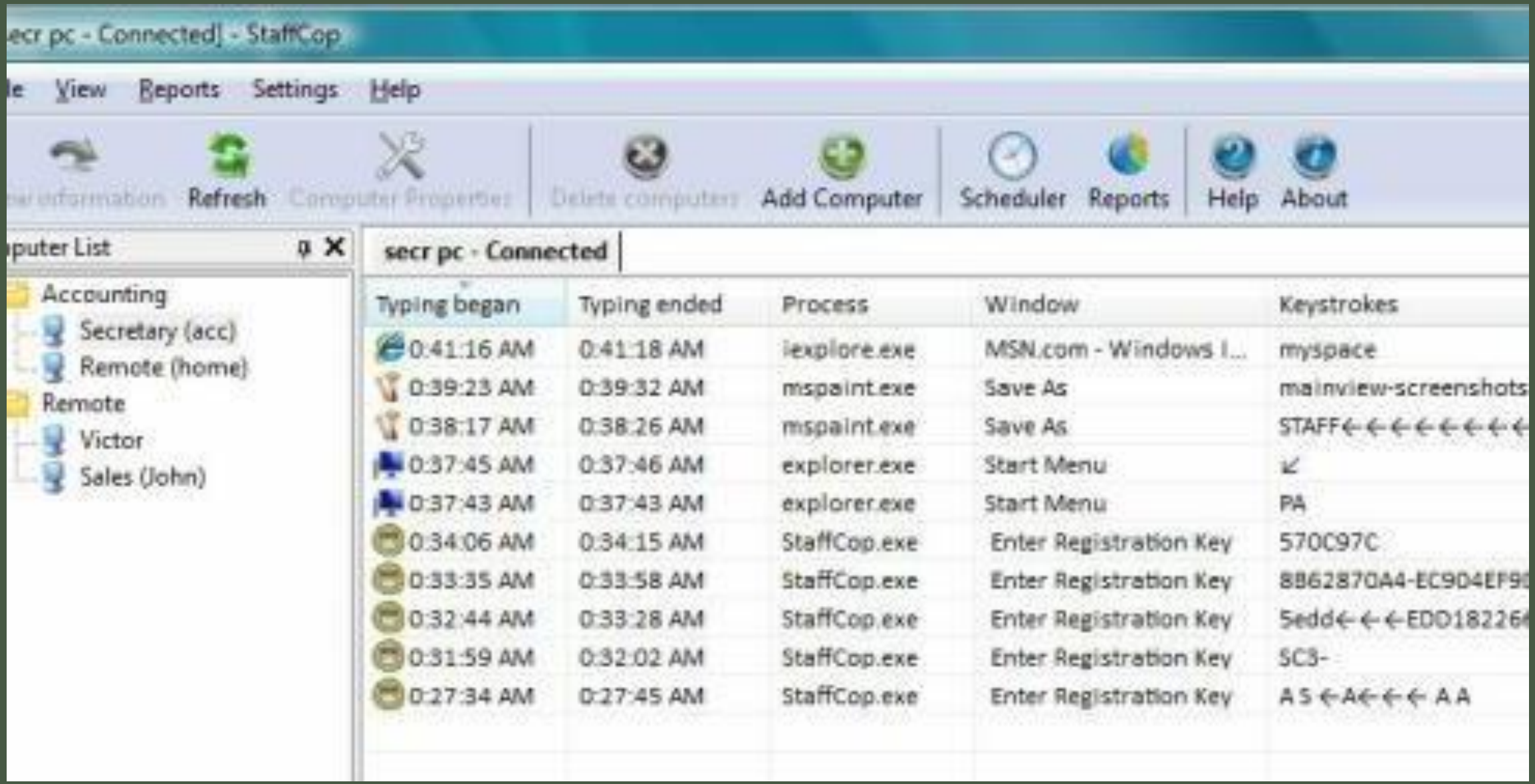
Diego Silva

O que é keylogger?

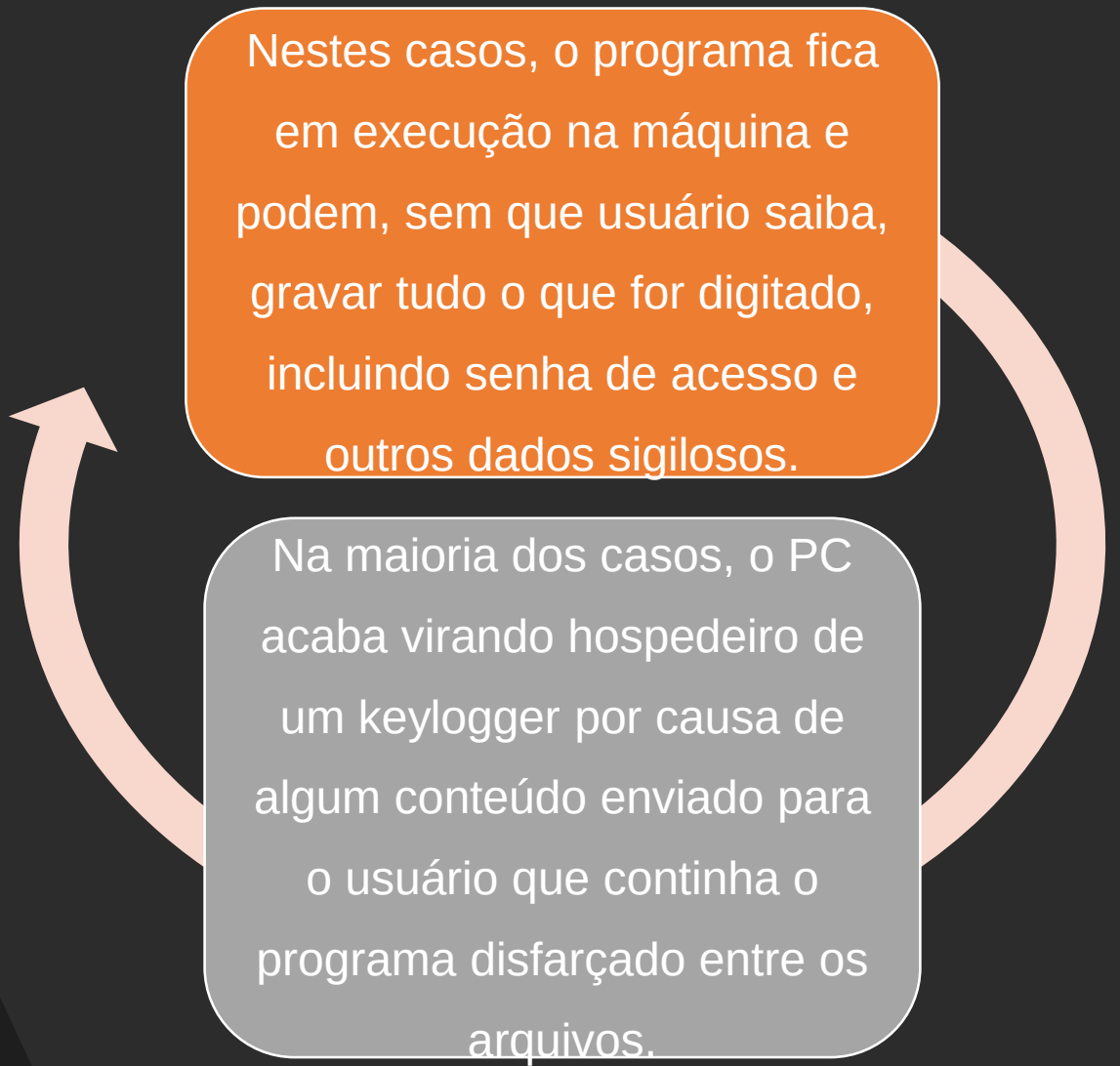
- Entre os “truques” mais utilizados pelos crackers está o keylogger, um programinha capaz de gravar tudo o que uma pessoa desavisada digitar no teclado, incluindo senhas de acesso a sites bancários.

Para que serve?

- Keyloggers são aplicativos ou dispositivos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado.
- Esse tipo de função também está inclusa em boa parte de outros tipos de aplicativos, como jogos que precisam monitorar o teclado para saber quando uma combinação de teclas de atalho foi acionada durante uma partida.


ecr pc - Connected] - StaffCop
le View Reports Settings Help
Refresh
Add Computer
Scheduler
Reports
Help
About
puter List
Accounting
Secretary (acc)
Remote (home)
Remote
Victor
Sales (John)
secr pc - Connected
Typing began
Typing ended
Process
Window
Keystrokes
0:41:16 AM
0:41:18 AM
iexplore.exe
MSN.com - Windows I...
myspace
0:39:23 AM
0:39:32 AM
mspaint.exe
Save As
mainview-screenshots
0:38:17 AM
0:38:26 AM
mspaint.exe
Save As
STAFF
0:37:45 AM
0:37:46 AM
explorer.exe
Start Menu
0:37:43 AM
0:37:43 AM
explorer.exe
Start Menu
PA
0:34:06 AM
0:34:15 AM
StaffCop.exe
Enter Registration Key
570C97C
0:33:35 AM
0:33:58 AM
StaffCop.exe
Enter Registration Key
0:32:44 AM
0:33:28 AM
StaffCop.exe
Enter Registration Key
0:31:59 AM
0:32:02 AM
StaffCop.exe
Enter Registration Key
SC3-
0:27:34 AM
0:27:45 AM
StaffCop.exe
Enter Registration Key

O perigo que representam



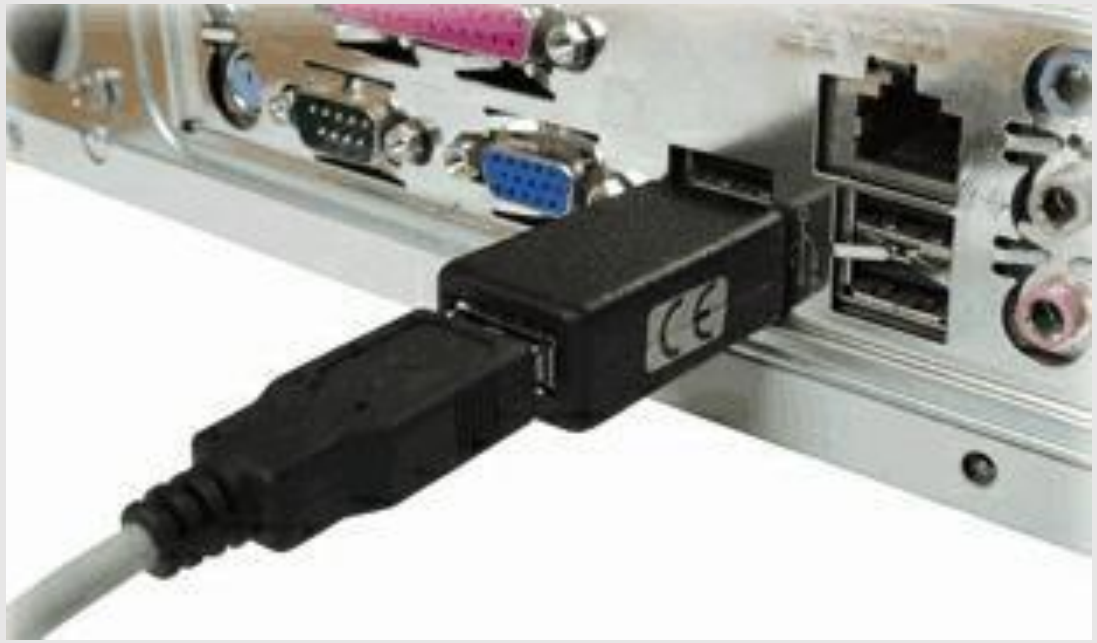
Como evitar?

- Manter um bom antivírus sempre ativo na máquina é um bom meio de detectar e eliminar este tipo de aplicação;
- As contas bancárias são os principais alvos dos keyloggers, praticamente todos os aplicativos de webbanking adotaram medidas preventivas, sendo o teclado virtual uma das mais efetivas.

*Teclado virtual do Windows (Fonte da imagem: **Tecmundo***

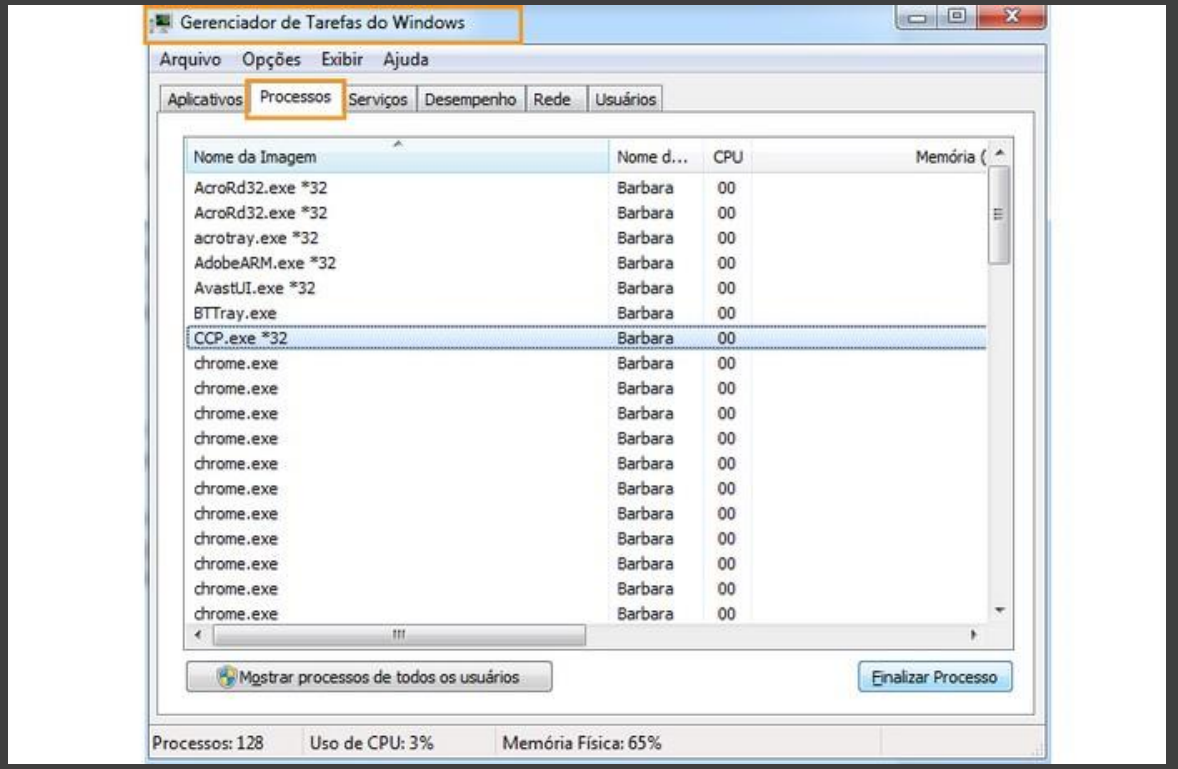
Keyloggers em forma de hardware

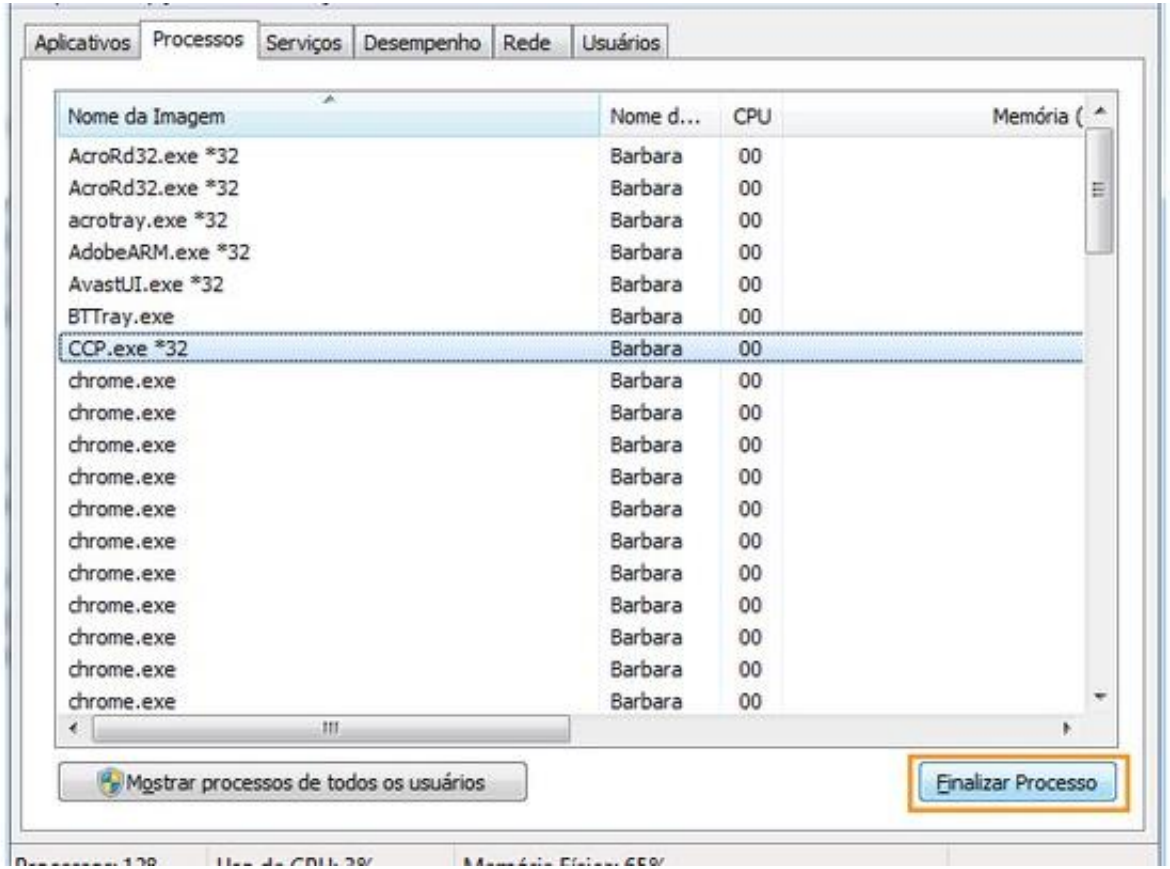
- Lembre-se que keyloggers também podem estar na forma física!



Como descobrir e remover keylogger do PC

- Passo 1. Abra o Gerenciador de Tarefas no computador. Para isso, aperte os atalhos no teclado CTRL+ALT+ESC e acesse a aba “Processos”;

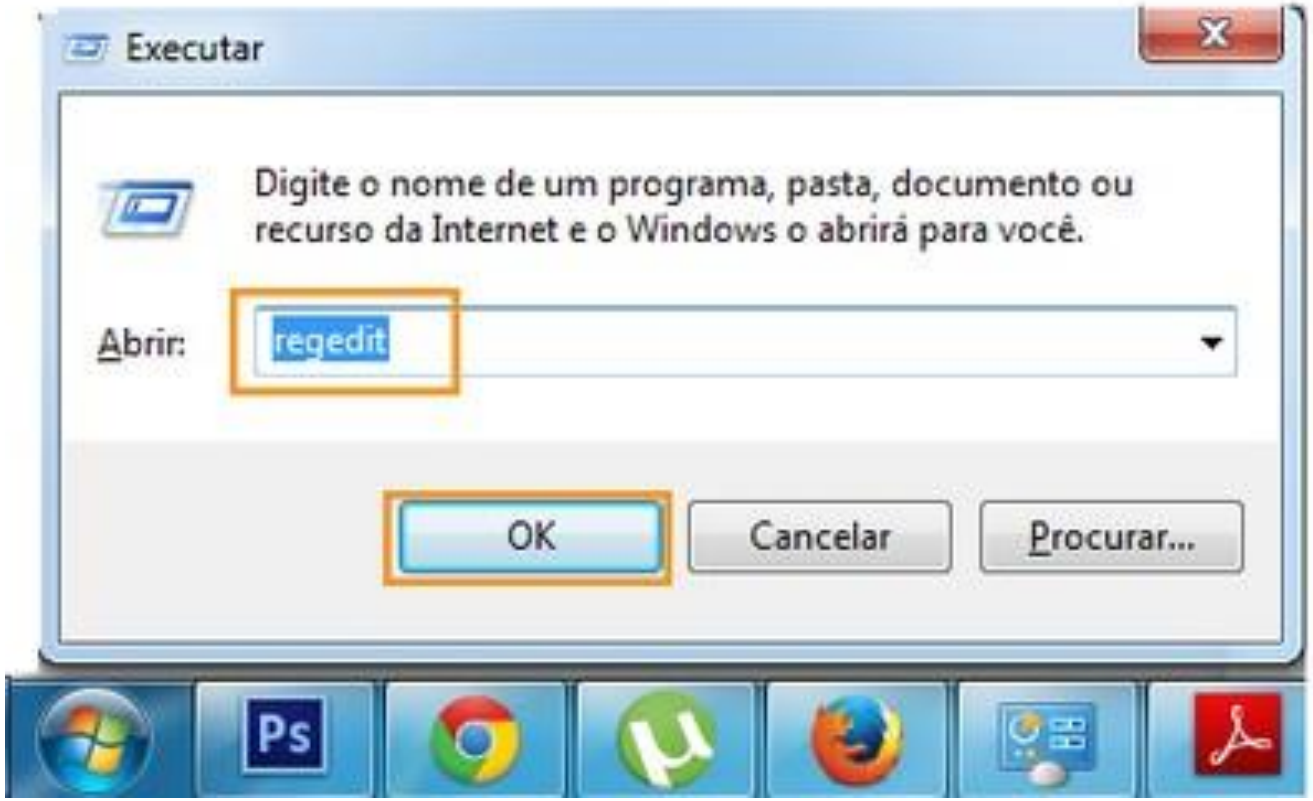


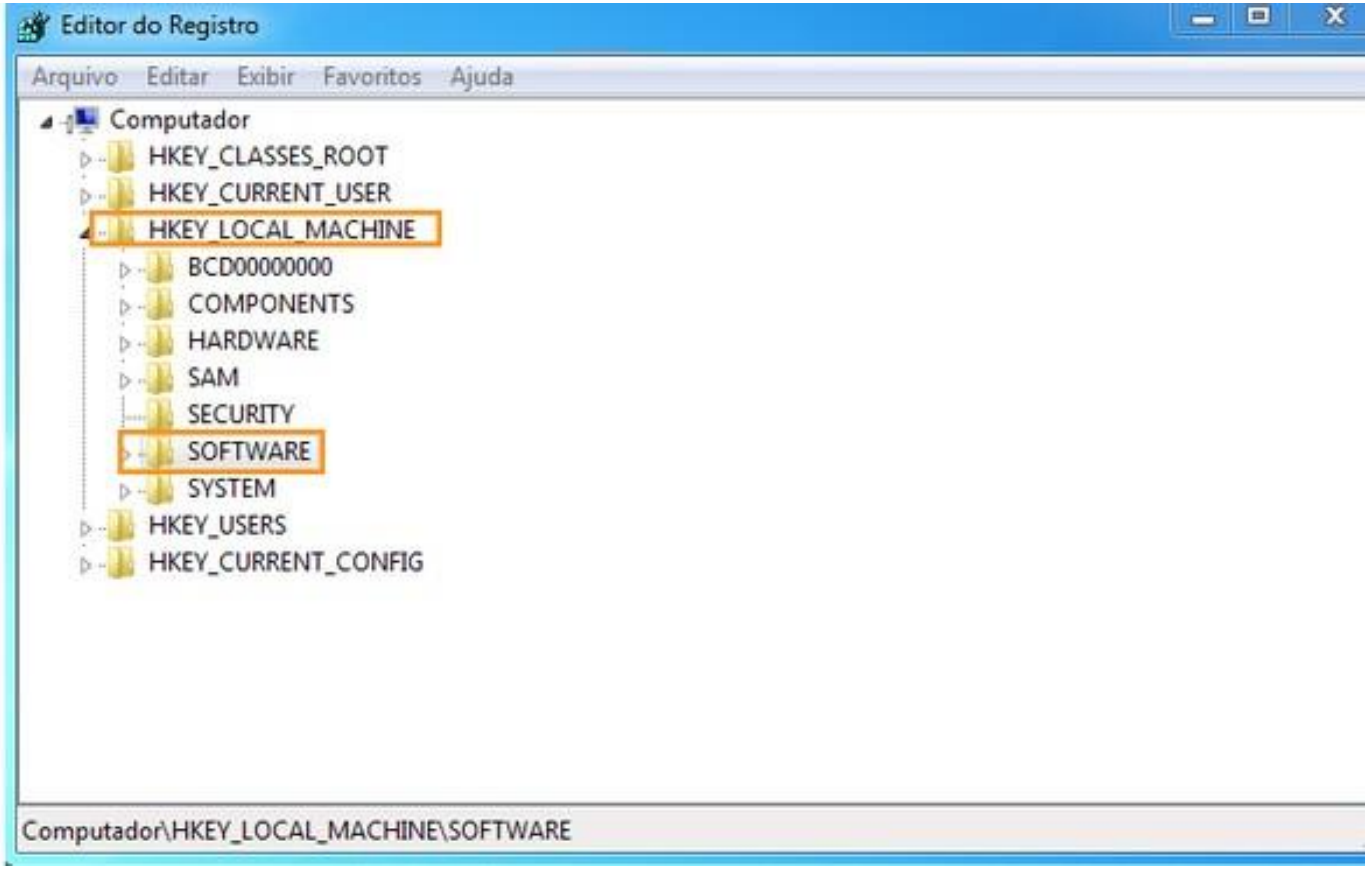


- Passo 2. Em seguida, procure por itens executáveis que contenham três ou quatro letras maiúsculas seguidas por (.exe), como POL.exe, YIO.exe, BKP.exe e AKL.exe. Se encontrar um deles, clique em “Finalizar Processo”.

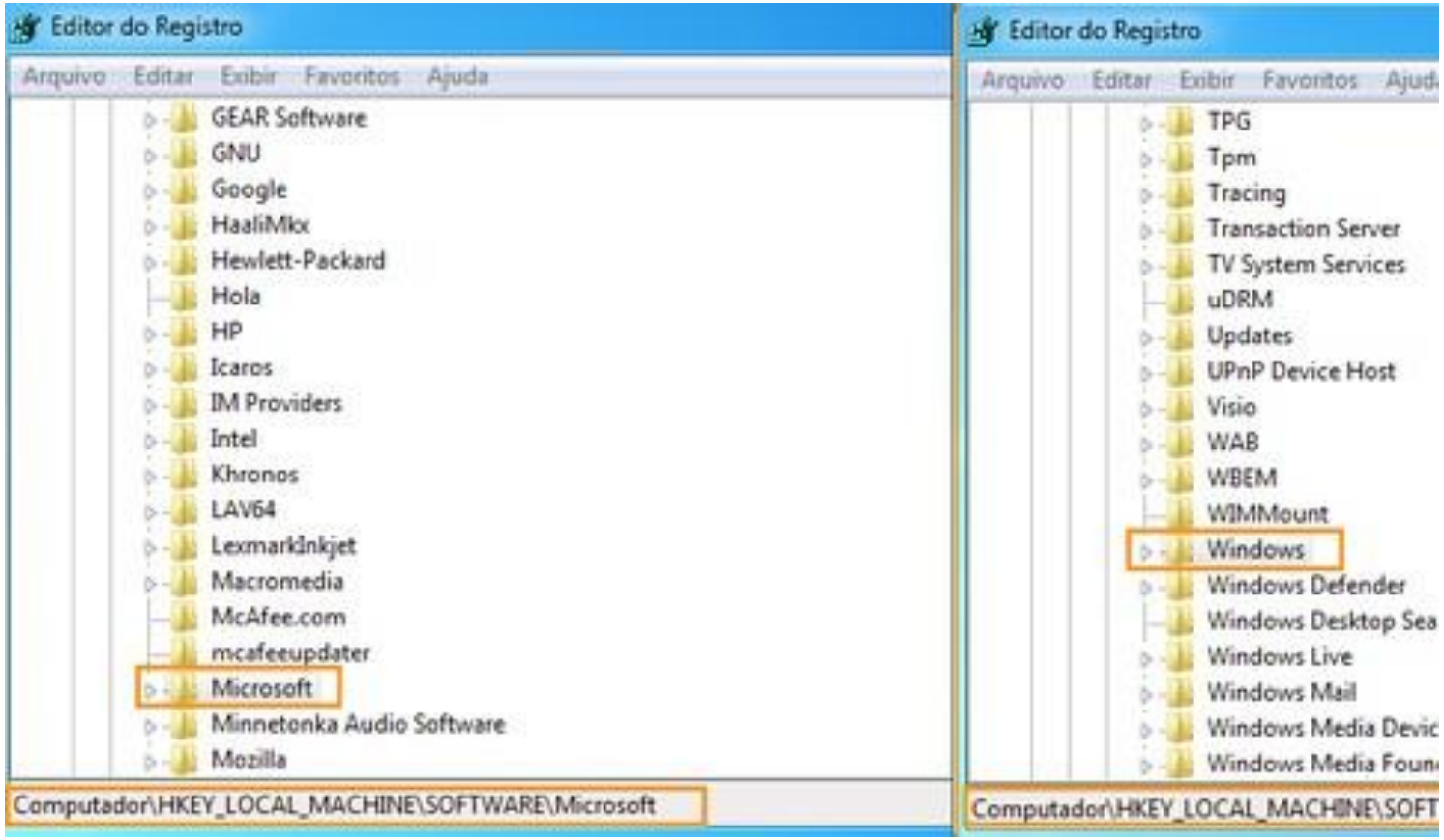
Removendo keylogger

- Passo 1. Aperte o atalho no teclado “Win +R” para abrir o “Executar”. Em seguida, digite “regedit” (sem aspas) e conclua em “Ok”;

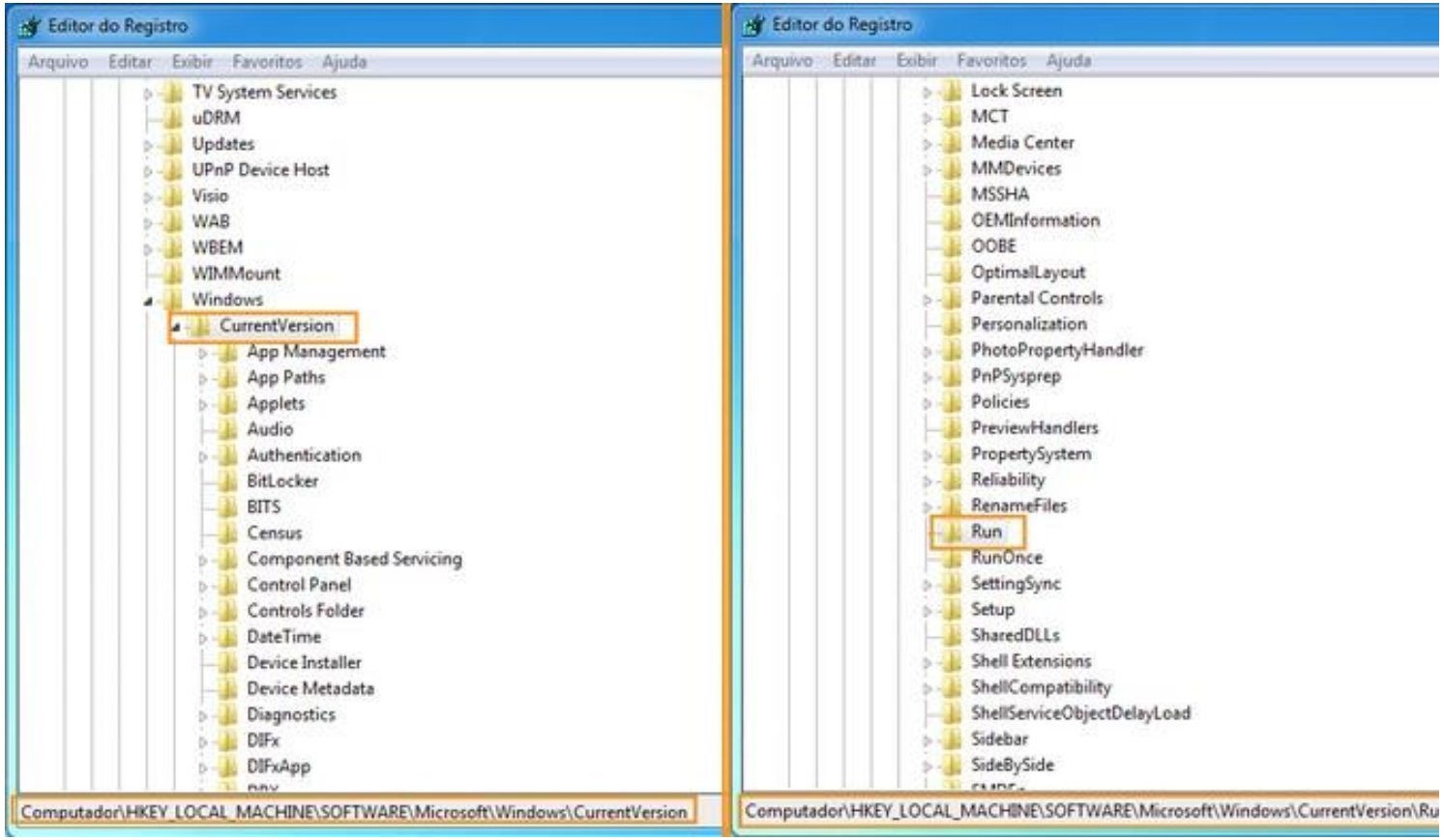




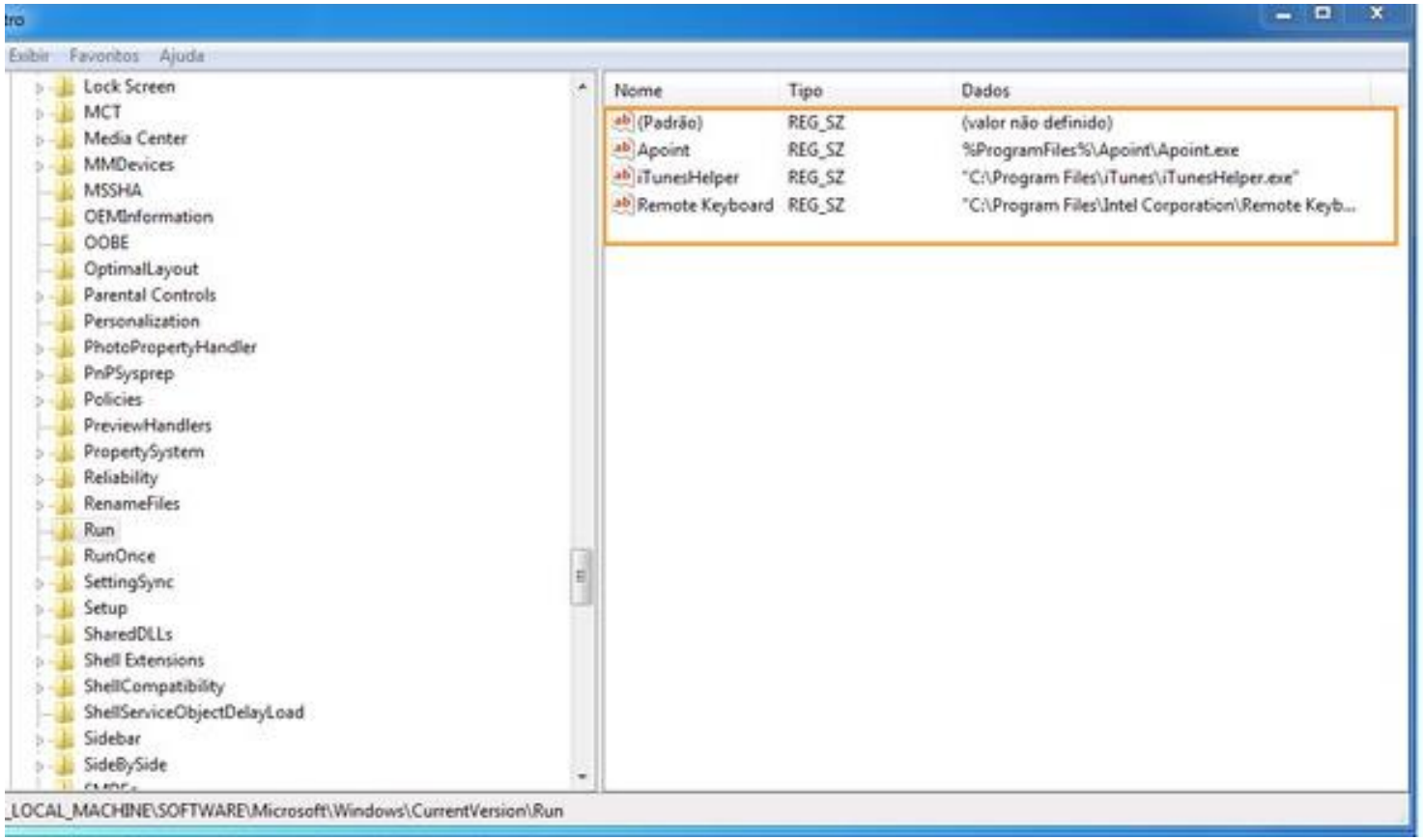
- Passo 2. Depois, você vai abrir essas pastas e subpastas em cascata, uma dentro da outra. Inicie pelo item “HKEY_LOCAL_MACHINE” e depois selecione “Software”;



- Passo 3. Selecione “Microsoft” e depois “Windows”;



- Passo 4. Busque pela pasta “Current Version” e selecione “Run”;



- Passo 5. Agora busque pelo keylogger e delete o arquivo. Ele está representado por três ou quatro letras maiúsculas, seguidas de (.exe), como POL.exe, YIO.exe, BKP.exe e AKL.exe.

- Pronto. Agora você estará livre do recurso malicioso. É recomendado passar seu antivírus antes e após o processo para conferir se ele captura algum malware.
  O Combofix e Spybot também são boas opções para detectar programas espiões.

Conclusão

Fontes:

- https://www.tecmundo.com.br/spyware/1016-o-que-e-keylogger-.htm

- http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2015/07/como-descobrir-e-remover-keylogger-do-pc.html