Criação de Arquivos REG

O registro é um banco de dados hierárquico no Windows que armazena informações importantes sobre hardware do sistema, programas instalados e configurações, além de perfis de cada uma das contas de usuário no computador.

Os dados do registro são armazenados em chaves (compartimentos, como se fossem “pastinhas”), e dentro deles tem subchaves, que funcionam da mesma forma. As configurações que aparecem do lado direito são chamados de valores. Os valores sempre possuem um nome, o tipo de dados e o conteúdo dos dados (como se fossem variáveis). Tudo isso são parâmetros que ficam armazenados dentro das chaves, e os valores são itens de configurações.

Esses são os tipos de dados mais comuns em entradas de registro, que são utilizados para configurar os valores que guardamos dentro das chaves:

ID do Tipo	Nome Simbólico	Significado
0	*REG_NONE*	Sem tipo definido
1	*REG_SZ*	Valor de cadeia de caracteres UTF-16
2	*REG_EXPAND_SZ*	Valor de cadeia de caracteres expansível
3	*REG_BINARY*	Dados binários
4	*REG_DWORD*	Valor DWORD, inteiro sem sinal de 32 bits
7	*REG_MULTI_SZ*	Cadeia de caracteres múltipla (lista ordenada)
11	*REG_QWORD*	Valor QWORD, inteiro de 64 bits

O registro tem cinco chaves principais (chaves raiz ou de alto nível):

A chave *HKEY_CLASSES_ROOT* contém informações relativas a associações de nomes de arquivos, objetos OLE, associações com objetos COM, e associações de arquivos de classe. Parâmetros contidos nessa chave são na verdade um link (atalho) para a chave HKEY_LOCAL_MACHINE\SOFTWARE\Classes. Abreviada normalmente como HKCR.

A chave *HKEY_CURRENT_USER* contém as configurações do usuário logado no sistema no momento, incluindo variáveis de ambiente, configurações de desktop, de redes e de aplicações. É um link para HKEY_USERS\<SID-DO-USUÁRIO-ATUAL>. Abreviada normalmente como HKCU.

A chave *HKEY_LOCAL_MACHINE* contém todas as informações globais e de hardware e sistema operacional. A informação nessa chave é aplicável a todos os usuários que se logam no sistema local. Abreviada normalmente como HKLM.

A chave *HKEY_USERS* contém dados de todos os perfis de usuários no sistema, incluindo HKEY_CURRENT_USER e o perfil de usuário padrão. No geral, usamos a chave HKCU para configuração do usuário atual. Abreviada normalmente como HKU.

A chave *HKEY_CURRENT_CONFIG* armazena todos os dados sobre a configuração atual de hardware da máquina. É um link para HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware\Profiles\Current. Não é muito utilizada no geral. Abreviada normalmente como HKCC.

Uma coisa que podemos fazer, por exemplo, é criar uma entrada de registro onde um comando, BAT ou programa é executado ao inicializar (não funciona com aplicações Java), para isso, procure a chave RUM em HKCU ou HKLM (essa última é para todos os usuários), localizadas em *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* e *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*.

Sabendo disso, podemos também usar isso para excluir programas que inicializam com o sistema, principalmente malwares e semelhantes, cujas entradas são colocadas justamente em run.

PS: Variáveis do sistema não funcionam para adicionar chaves por esse método, só são possíveis utilizando o CMD ou BAT para isso.

Limpeza e Segurança Básica no Windows

Procurar vírus e malware (em pastas, registro, tarefas agendadas e serviços, usar Msconfig, Regedit, Prompt e Gerenciador de Tarefas (tasklist) pra isso).

Resetar navegadores. Lembrando que Chrome tem uma ferramenta própria pra limpar navegadores. Todos os navegadores deverão ter atalhos, extensões, plugins, websearch e página inicial verificadores.

Verificar se o acesso remoto está desativado (vá em Propriedades do Sistema, Remoto e desative “Permitir Conexões de Assistência Remota para este Computador”, no firewall do roteador bloquei as portas 135, 139, 445 e 3389).

Alguns aplicativos úteis para limpar ou verificar arquivos maliciosos.

- Adwcleaner.
- JRT.
- ZHPCleaner
- Combofix.
- Rkill.
- Malwarebytes Anti-Rootkit.
- Kaspersky Virus Removal Tool.
- Norton Power Erase.

Para remover esses e outros aplicativos após a limpeza (exceto o Malwarebytes Anti-Rootkit e o Spydetected Free), use o KpRm.

Aplicativos para limpeza como Ccleaner e ASC são úteis nesses casos. O próprio Windows tem a ferramenta de Limpeza de Disco, que é acessada digitando *cleanmgr* no executar.

Manter o antivírus atualizado (tanto o programa quanto as definições). Não manter mais de um antivírus ou antispyware ativos no PC. Mantenha o firewall ativo. Executar verificação periodicamente.

Mantenha o sistema operacional atualizado, o Windows lança atualizações toda segunda Terça do mês e quando tem alguma vulnerabilidade crítica. Também mantenha o antivírus e os programas (como navegadores, plugins e drivers) atualizados.

A Diferença Entre Arquivos .exe e .msi

Arquivos EXE podem ser tudo. Quase tudo que você roda em seu computador é iniciado por um arquivo EXE (exceto o próprio Windows e os drivers).

Eles contém códigos executáveis que fazem o computador funcionar, e podem ser de todo tipo.

Tudo sobre MSI

MSI são arquivos de base de dados, usados pelo instalador do Windows. Eles contém informação sobre um aplicativo necessária para executar recursos e componentes, e cada componente pode trazer arquivos, dados de registro, atalhos, etc.

O arquivo MSI também contém o UI, que é usado para instalações, e vários outros dados como pré-requisitos a buscar, ações personalizadas a executar, o procedimento de uma instalação, quando oferecer suporte a instalações administrativas, etc. Assim como arquivos reais a ser instalados automaticamente (não é sempre, mas os arquivos podem estar embutidos num arquivo CAB externo ou como arquivos comprimidos comuns num local onde o MSI possa encontrá-los).

Arquivos MSI são atualmente o meio recomendado de se instalar programas no Windows.

Os MSI são executados por um arquivo EXE que é parte do Windows, chamado MSIEXEC.EXE. Este aplicativo lê os dados no arquivo MSI e executa a instalação.

Tudo sobre EXE

O instalador do Windows é bem recente, principalmente a versão mais nova (3.0). Geralmente instalações que usam MSI ainda vêm com um EXE (SETUP.EXE, por exemplo). Este EXE é chamado de “bootstrapper”. Ele não realiza a instalação, apenas checa se a versão correta do Windows Installer está presente no sistema, se não ele inicia o “MSI Redistributable” (MSIINSTA.EXE ou MSIINSTW.EXE, dependendo da plataforma) e então inicia o arquivo MSIEXEC.EXE contido no arquivo MSI. Em alguns casos (sobretudo em downloads da internet), o arquivo MSI e o MSI Redistributable são empacotadores dentro do arquivo EXE, por isto você não não os vê.

Resumindo: Instalações podem ser feitas de 3 maneiras:

- Personalizada – Sistema de instalação de terceiros em um arquivo EXE.
- Usando o instalador do Windows em um arquivo MSI.
- Arquivo EXE que inicia um arquivo MSI (que podem vir embutidos em um EXE).

Arquivos MSI servem apenas para instalações. Arquivos EXE podem ser qualquer coisa que possa rodar em seu computador.

Sistema de Pastas do Windows

O sistema de pastas do Windows é como um arquivo metálico de escritório, com algumas gavetas e várias pastas dentro de uma gaveta. O ponto de montagem no Windows é identificado por uma letra, geralmente C, e outros discos (removíveis ou não) costumam ser identificados por outras letras, como D, E, F e assim por diante.

As pastas mais importantes do Windows são essas:

Usuários

A pasta Usuários é onde encontramos as pastas para todas as contas criadas no Windows. Ao acessá-la vemos pastas padrões para músicas, imagens, vídeos e documentos, entre outros arquivos pessoais.

Dentro da pasta de usuário também tem a pasta AppData (geralmente oculta), que contém os arquivos especificados do seu perfil de usuário do Windows. Dentro dela tem três pastas: Local, LocalLow e Roaming, onde temos várias pastas de arquivos de programas, e também a Temp, onde ficam os arquivos temporários.

Arquivos de Programas (Program Files)

A pasta Program Files é onde praticamente todos os programas instalados são inseridos. Geralmente dentro dela tem pastas com o nome dos programas ou desenvolvedores (como por exemplo, a pasta Mozilla Firefox, onde é encontrado o executável do navegador firefox.exe e outros componentes necessários para o funcionamento do mesmo, como arquivos de configuração, bibliotecas compartilhadas, etc.).

Nos sistemas Windows de 64 bits temos duas pastas: A *C:\Program Files(x86)* é onde por padrão, são instalados os programas de 32 bits, enquanto os programas de 64 bits são instalados na pasta que é apenas *C:\Program Files*. Nos sistemas 32 bits apenas têm a Program Files padrão.

Windows

Essa é a pasta mais importante do computador, onde se encontra toda a estrutura do sistema operacional, onde não se deve mexer em absolutamente nada, a menos que você saiba o que está fazendo.

Dentro dela também tem uma pasta Temp, onde são inseridos arquivos temporários, mas usados pelo Windows.

Outra pasta importante é a Prefetch, onde estão arquivos com extensão .pf, que indicam os programas usados com mais frequência.

Mas a pasta mais importante dentro dela é a System32, que tem as partes mais importantes do sistema, como o Kernel, as DLLs e os programas padrões do Windows. Ela nunca deve ser deletada, ao contrário do que dizem alguns tutoriais mentirosos da internet.

O que é uma DLL?

Uma DLL é uma biblioteca que contém código e dados que podem ser usados por mais de um programa ao mesmo tempo. Por exemplo, em sistemas operacionais Windows, a DLL Comdlg32 executa funções comuns relacionadas à caixa de diálogo. Cada programa pode usar a funcionalidade contida nessa DLL para implementar uma caixa de diálogo Abrir. Isso ajuda a promover a reutilização de código e o uso eficiente de memória.

Usando uma DLL, um programa pode ser modularizado em componentes separados, o que faz o carregamento do programa ser mais rápido, e um módulo só é carregado quando essa funcionalidade é solicitada. Além disso, as atualizações são mais fáceis de aplicar a cada módulo sem afetar outras partes do programa, sem a necessidade de compilar ou instalar o programa inteiro novamente.

Grande parte das funcionalidades do sistema operacional são fornecidas pela DLL. Quando executamos programas no Windows, grande parte das funcionalidades deles podem ser fornecidas por DLLs. O uso de DLLs ajuda a promover a modularização e reutilização de código, uso eficiente da memória e espaço em disco reduzido.

Programas instalados no Windows podem usar tanto as DLLs nativas do Windows como ter suas próprias DLLs.

Quando um programa usa uma DLL, um problema chamado dependência pode fazer com que o programa não seja executado. Além disso, uma DLL nunca deve ser editada.

Com a introdução do .NET Framework, a maioria dos problemas de dependência foram eliminadas usando assemblies.