Virtualização do UAC

Conceitos básicos

Um determinado caminho de programa no Windows 10 (em princípio, já desde o Windows VISTA) pode não estar gravado com direitos de usuário normais. Esta restrição, que significa esses arquivos e caminho apenas podem ser alterados com direitos de administrador, faz parte do conceito de segurança do Windows e é denominada Controle de Conta de Usuário (User Account Control, UAC).

Os seguintes caminhos estão especialmente envolvidos

- C:\Windows
- C:\Program Files
- C:\Program Files (x86)

e talvez outros caminhos críticos do sistema.

Além disso, alguns tipos de arquivo apenas podem ser alterados com direitos de administrador, portanto, entre muitos outros

- EXE
- VBA
- BAT

que são principalmente arquivos executáveis, que podem conter código malicioso. Para obter informações mais detalhadas, consulte o documento de Mark Russinovich.

O problema

Seguindo este conceito, não é possível tirar proveito da prática estabelecida para salvar os dados do usuário, tais como configurações básicas e opções do caminho do programa, uma vez que o programa não é executado com direitos de administrador. A solução amplamente utilizada para salvar as configurações no registro está relacionada ao mesmo princípio. Não é suficiente estar conectado como administrador, mas o programa tem que ser explicitamente iniciado com direitos elevados clicando com o botão direito do mouse e "executando como administrador".

Para o programa Metric, é impossível salvar as configurações básicas, como sistemas de medição, calibração, tempo de exposição ou a ligação de tabelas de medição ou acionadores de motor - tudo salvo em Metric.opt no caminho do programa - com uma exceção: Tem que ser iniciado com direitos elevados. Isto, por sua vez, prejudicaria a segurança do sistema, se o usuário normal pudesse iniciar o programa com direitos de administrador.

Para se livrar desses problemas, a Microsoft estabeleceu uma técnica chamada “virtualização do UAC”. Se um programa não tiver o direito de escrever ou alterar um arquivo no caminho desejado, uma cópia deste arquivo é armazenada em um local especial e esta cópia (ou até mesmo o arquivo não existente no diretório de destino) é apresentada virtualmente no diretório de destino.

Exemplo: Você está conectado como "YouAsAUser" com direitos de usuário normais e deseja salvar as configurações em Metric.opt. Como você não tem permissão para fazer isso em "C:\Program files (x86)\Metric \Metric.opt", o Windows salva uma cópia deste arquivo em

C:\Users*YouAsAUser*\AppData\Local\VirtualStore\Program Files (x86)\Metric\Metric.opt

A virtualização do UAC salva o arquivo em um local completamente diferente.

Não há nenhuma diferença se o administrador tiver alterado sua permissão de gravação em "C:\Program files (x86)\Metric". O Windows reconhece automaticamente o caminho crítico e faz a virtualização por você. Conforme mencionado acima, a única exceção é quando você inicia explicitamente o Metric com direitos elevados, o que é proibido por motivos de segurança.

Se você carregar seu arquivo a partir de "C:\Program files (x86)\Metric\Metric.opt", o Windows carrega este arquivo a partir da loja virtual.

Para você, enquanto usuário único, isto é fantástico. Por um lado, você tem um nível de segurança elevado pela virtualização do UAC e, por outro, você pode manter sua prática e salvar seus arquivos e configurações onde o programa está instalado.

Se, nesta situação, um outro usuário fizer login como “YourCollegue”, duas coisas acontecerão:

> Seu colega lerá, no primeiro início do Metric, o arquivo Metric.opt originalmente instalado,
>
> Ao salvar, seu colega criará um novo Metric.opt em sua própria VirtualStore, e essa cópia apenas é visível para ele.

Você tem agora três Metric.opt diferentes: O que foi instalado a partir do CD, sua cópia privada e a cópia privada de seu colega, embora todos vocês apenas vejam um único Metric.opt no caminho do aplicativo. A única diferença será presumivelmente o tamanho e o tempo de criação.

Você tem agora a vantagem de que o seu colega não pode alterar suas configurações. No entanto, se algumas configurações básicas como a calibração tiverem que ser alteradas, isso tem que ser feito para todos os trabalhadores em separado, o que pode dar muito trabalho se muitos trabalhadores fizerem seu trabalho nesta máquina.

Se, no seu caso, esta virtualização do UAC for um problema, você pode dar a volta à situação da seguinte forma.

A solução Excluir Arquivo do UAC

Conforme mencionado acima, existem tipos de arquivo que não são virtualizados pelo UAC. Se você adicionar OPT à lista destes tipos de arquivo, a virtualização para Metric.opt (e todos os outros arquivos com a extensão opt) deixará de ocorrer.

Um usuário simples não deve alterar mais as configurações. Apenas o administrador que inicia explicitamente o Metric com direitos elevados pode alterar as configurações. Se esta for a solução desejada no seu caso, então está tudo concluído. O arquivo "uac opt exclusion.reg" contém a entrada de registro, que faz o trabalho por você e adiciona a extensão de arquivo OPT às extensões excluídas.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\luafv\Parameters]
"ExcludedExtensionsAdd"=hex(7):6f,00,70,00,74,00,00,00,00,00
```

Código de caracteres hexadecimais para a string "OPT" em formato DBCS e uma string vazia. Clicando duas vezes nesse arquivo e aceitando todas as questões do UAC, esta entrada é feita no registro e uma reinicialização final do sistema permite que os efeitos sejam executados em seu sistema.

A solução ampliada "permissão de escrita"

Se os usuários normais forem autorizados a alterar as configurações do Metric, eles têm que obter permissão de gravação no caminho de instalação do Metric ("C:\Program files (x86)\Metric"). Neste caso, "alterar/mudar" seria suficiente, pois salvar um novo conjunto completo de configurações em um arquivo diferente não é necessário. O administrador pode então conceder direitos mínimos e não precisa conceder acesso total ao caminho.