



Comportamentos Seguros e Proativos

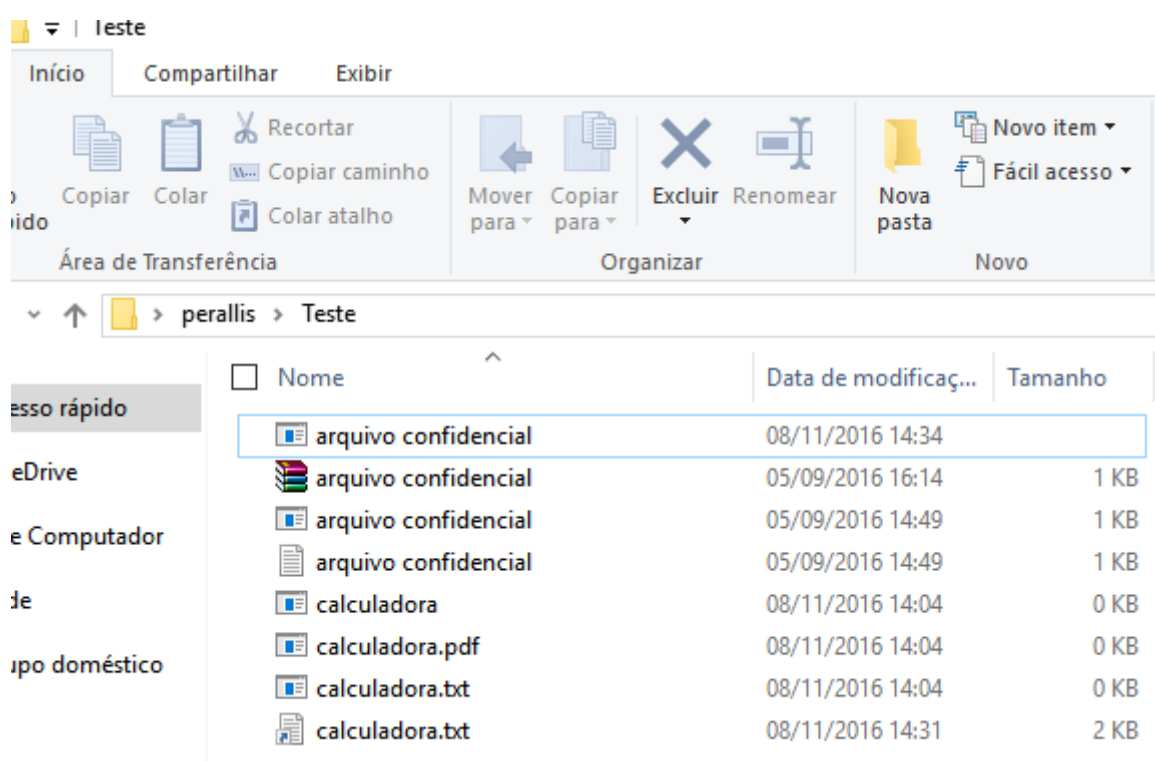
Material Complementar

Perallis IT Innovation
Soluções em Gerenciamento e Segurança de dados
www.perallis.com
contato@perallis.com
+55 19 3203-1002



Extensão de Arquivos

Neste material auxiliar iremos demonstrar como verificar a extensão de arquivos no Sistema Operacional Windows 10 Home.

Vamos imaginar o diretório conforme exibido abaixo:



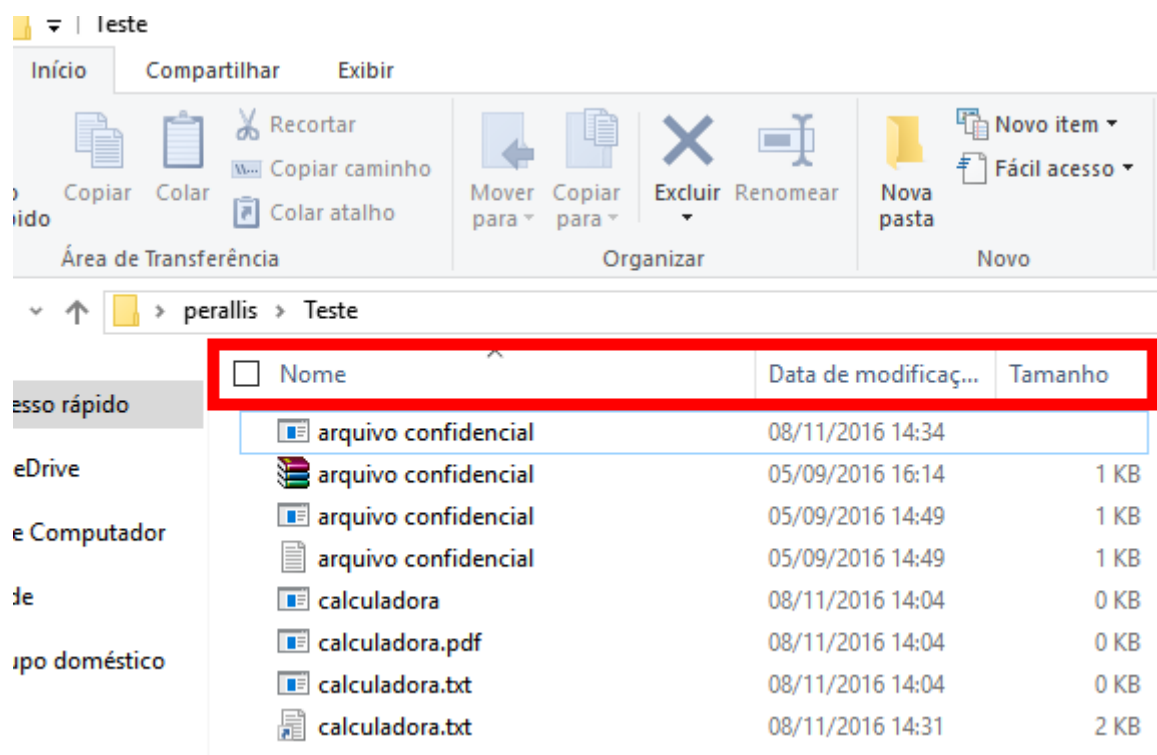
Podemos notar que nesse diretório “Teste”, com base nas imagens ao lado no nome, supostamente temos:

- 5 Executáveis (símbolo );
- 2 Arquivos de Texto (símbolo );

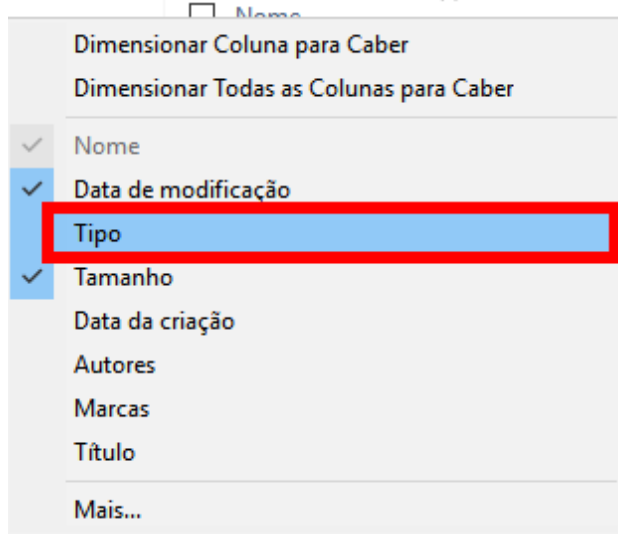
- 1 Arquivo zipado (símbolo .

Mas será que esses arquivos são realmente o que aparentam ser?

Para descobrir o verdadeiro formato do arquivo podemos combinar três metodologias. Primeiro adicione o campo “Tipo” na listagem da descrição do arquivo. Clique com o botão direito do mouse sobre o cabeçalho:



Marque “Tipo” no submenu que irá aparecer, conforme exibido na imagem abaixo:



Data de modificaç...	Tamanho
08/11/2016 14:34	
05/09/2016 16:14	1 KB
05/09/2016 14:49	1 KB
05/09/2016 14:49	1 KB
08/11/2016 14:04	0 KB
08/11/2016 14:04	0 KB
08/11/2016 14:04	0 KB
08/11/2016 14:31	2 KB

Agora aparecerá um campo novo na descrição de cada arquivo, conforme exibido:

<input type="checkbox"/> Nome	Data de modificaç...	Tipo	Tamanho
arquivo confidencial	08/11/2016 14:34	Pasta de arquivos	
arquivo confidencial.7z	05/09/2016 16:14	Arquivo do WinRAR	1 KB
arquivo confidencial.exe	05/09/2016 14:49	Aplicativo	1 KB
arquivo confidencial.txt	05/09/2016 14:49	Documento de Te...	1 KB
calculadora.exe	08/11/2016 14:04	Aplicativo	0 KB
calculadora.pdf.exe	08/11/2016 14:04	Aplicativo	0 KB
calculadora.txt.exe	08/11/2016 14:04	Aplicativo	0 KB
calculadora.txt	08/11/2016 14:31	Atalho	2 KB

Com isso, podemos tirar novas conclusões. O diretório na verdade possui:









- 1 pasta de arquivos;
- 1 arquivo zipado (Arquivo do WinRAR);
- 4 Aplicativos;
- 1 Documento de Texto; e

- 1 Atalho.

Dessa forma, chegamos a conclusão que as imagens exibidas na verdade podem ser **alteradas** para enganá-lo.

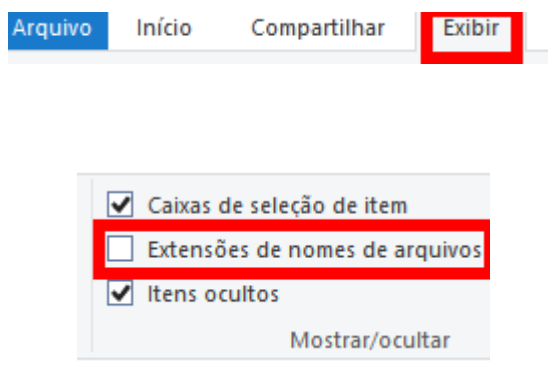
Mas será que só com isso resolvemos nossos problemas?

Preste atenção nos arquivos marcados na imagem abaixo:









<input type="checkbox"/> Nome	Data de modificaç...	Tipo	Tamanho
 arquivo confidencial	08/11/2016 14:34	Pasta de arquivos	
 arquivo confidencial	05/09/2016 16:14	Arquivo do WinRAR	1 KB
 arquivo confidencial	05/09/2016 14:49	Aplicativo	1 KB
 arquivo confidencial	05/09/2016 14:49	Documento de Te...	1 KB
 calculadora	08/11/2016 14:04	Aplicativo	0 KB
 calculadora.pdf	08/11/2016 14:04	Aplicativo	0 KB
 calculadora.txt	08/11/2016 14:04	Aplicativo	0 KB
 calculadora	08/11/2016 14:31	Atalho	2 KB

Como um arquivo pode ter extensão “.pdf” e “.txt” se um arquivo do tipo Aplicativo deveria ser “.exe”?

Para resolver essa questão, temos que exibir as extensões de todos arquivos. No menu superior, selecione “Exibir” e marque o campo “Extensões de nomes de arquivos”:











E no final do nome do arquivo apareceram todas as extensões:

<input type="checkbox"/> Nome	Data de modificaç...	Tamanho
 arquivo confidencial	08/11/2016 14:34	
 arquivo confidencial.7z	05/09/2016 16:14	1 KB
 arquivo confidencial.exe	05/09/2016 14:49	1 KB
 arquivo confidencial.txt	05/09/2016 14:49	1 KB
 calculadora.exe	08/11/2016 14:04	0 KB
 calculadora.pdf.exe	08/11/2016 14:04	0 KB
 calculadora.txt.exe	08/11/2016 14:04	0 KB
 calculadora.txt	08/11/2016 14:31	2 KB

Assim, podemos concluir que na verdade os arquivos que antes demonstravam “calculadora.pdf” e “calculadora.txt” na verdade possuem extensão “.exe”. Um atacante pode colocar **múltiplas extensões para disfarçar** o verdadeiro formato do arquivo.

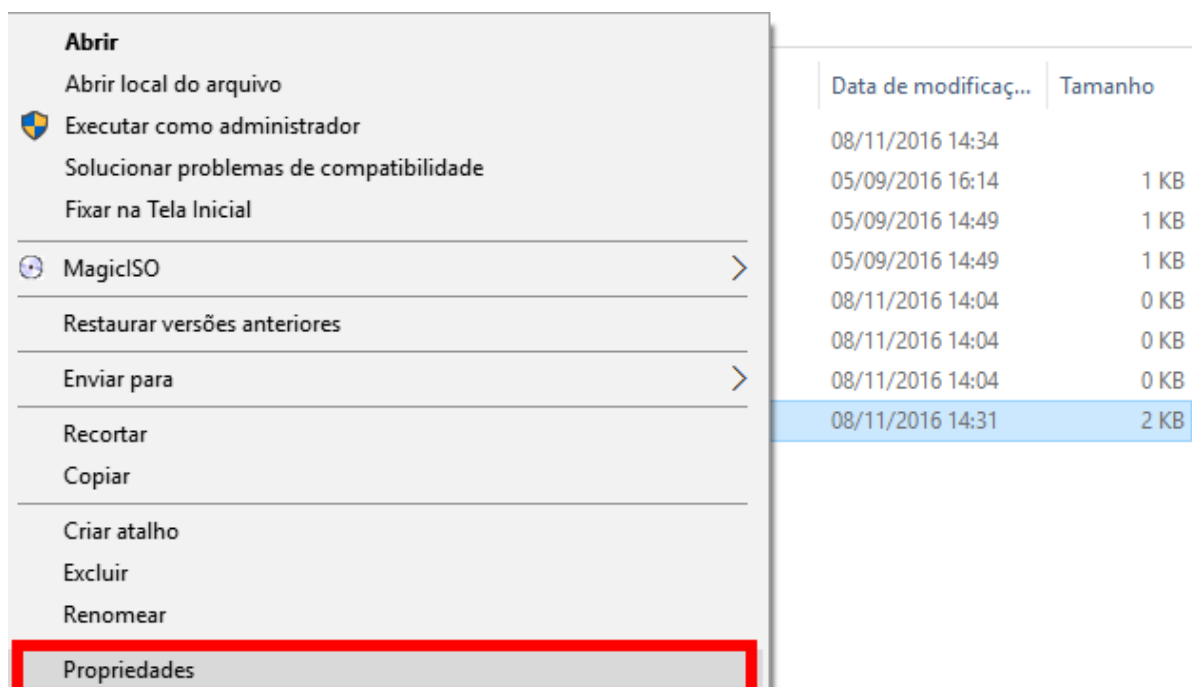
Será que resolvemos todos os nossos problemas então?

Na verdade tem mais um ponto que precisamos ficar atentos. Veja o último arquivo da lista:

<input type="checkbox"/> Nome	Data de modificaç...	Tipo	Tamanho
 arquivo confidencial	08/11/2016 14:34	Pasta de arquivos	
 arquivo confidencial.7z	05/09/2016 16:14	Arquivo do WinRAR	1 KB
 arquivo confidencial.exe	05/09/2016 14:49	Aplicativo	1 KB
 arquivo confidencial.txt	05/09/2016 14:49	Documento de Te...	1 KB
 calculadora.exe	08/11/2016 14:04	Aplicativo	0 KB
 calculadora.pdf.exe	08/11/2016 14:04	Aplicativo	0 KB
 calculadora.txt.exe	08/11/2016 14:04	Aplicativo	0 KB
 calculadora.txt	08/11/2016 14:31	Atalho	2 KB

Podemos ver que o tipo do arquivo é “Atalho” e que, aparentemente, é um arquivo de texto (formato “.txt”). Pois saiba que esse arquivo **não** é um arquivo de texto. Para

verificarmos essa afirmação vamos clicar com o último botão do mouse sobre o arquivo e selecionar “Propriedades”:

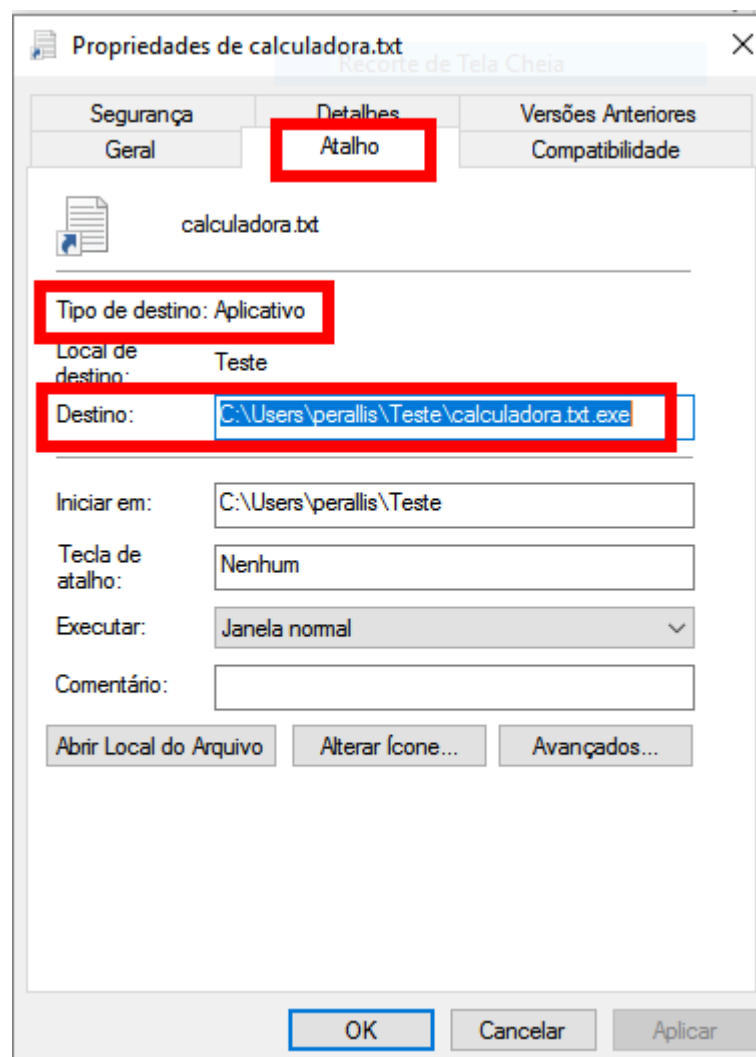


Data de modificaç...	Tamanho
08/11/2016 14:34	
05/09/2016 16:14	1 KB
05/09/2016 14:49	1 KB
05/09/2016 14:49	1 KB
08/11/2016 14:04	0 KB
08/11/2016 14:04	0 KB
08/11/2016 14:04	0 KB
08/11/2016 14:31	2 KB

Abrir

- Abrir local do arquivo
- Executar como administrador
- Solucionar problemas de compatibilidade
- Fixar na Tela Inicial
- MagicISO >
- Restaurar versões anteriores
- Enviar para >
- Recortar
- Copiar
- Criar atalho
- Excluir
- Renomear
- Propriedades**

Irá abrir uma nova janela. Nessa janela, selecione “Atalho” no menu superior:



Como podemos ver, esse arquivo na verdade irá abrir um outro arquivo ("calculadora.txt.exe") que é um executável! Um atacante poderia utilizar o tipo de arquivo "Atalho" para lhe enganar e **disfarçar o arquivo original em outro**. Jamais abra um arquivo Atalho sem verificar qual arquivo será realmente aberto ou executado.