Boas práticas em Cibersegurança

Demonstração de invasão a computador pessoal utilizando malware

ATENÇÃO: este documento mostra, sem revelar detalhes técnicos, uma simulação de ataque legitimamente realizada em ambiente de laboratório pelos especialistas da Perallis IT Innovation, portanto em suas próprias dependências e sobre os seus próprios ativos.

Imagine a seguinte situação: você está em casa, bem tranquilo, usando o seu computador normalmente. Ele está funcionado rápido como um raio. Todos os seus arquivos estão disponíveis e tudo, absolutamente tudo, está operando na mais perfeita normalidade. Baseado nisso, você pode dizer que você está seguro? Como você já deve estar pensando, a resposta é um sonoro "não". E por quê? No cenário imaginado aqui, em algum momento, você pode ter feito o download de um programa que você julgava ser legítimo, mas que, na verdade, está "traindo" você e pode estar sendo usado por terceiros para espioná-lo, para roubar sua informação e, pasme, até mesmo para tirar fotos suas usando a sua webcam (e, portanto, é malware). É exatamente esse tipo de ataque extremamente invasivo e sorrateiro que será demonstrado a seguir.

O programa malicioso

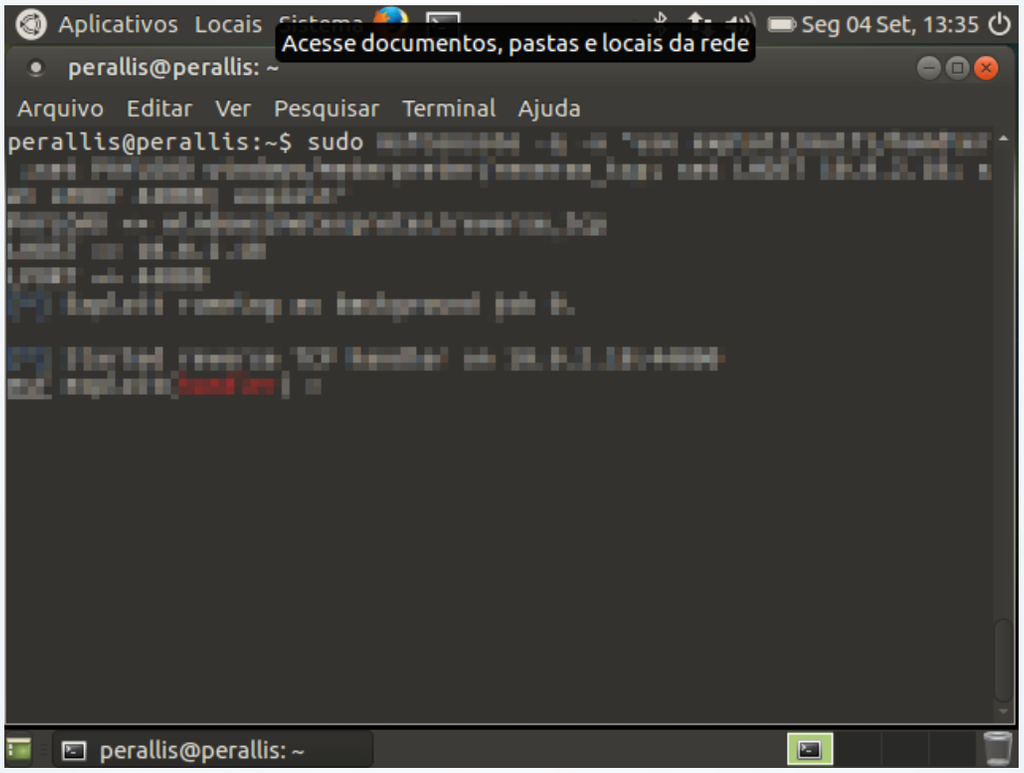
A Internet está cheia de sites de download maliciosos. Com certeza, você já deve ter se deparado com um. Pois bem, um hacker poderia criar e disponibilizar em um destes sites um programa malicioso que permitisse que ele se conectasse ao seu computador e executasse todas as ações hediondas mencionadas acima. Em nosso laboratório, nossos especialistas criaram uma versão maliciosa de um programa muito utilizado em diversos computadores com Windows: o CCleaner. Se você não conhece, o CCleaner é um programa que permite, entre outras coisas, fazer uma "faxina" no seu disco rígido, apagando arquivos que não serão mais utilizados. O programa malicioso se parece em tudo com o programa original, mas, "por debaixo dos panos", cria uma conexão remota com o computador do hacker que o criou. Uma captura de tela do ícone desta versão do programa, na área de trabalho do Windows, é mostrada abaixo:

Perallis IT Innovation

Boas práticas em Cibersegurança

Enquanto isso, nas profundezas do castelo...

Após obter sucesso em fazer uma pessoa baixar o programa malicioso, nosso maldoso hacker está tranquilamente sentado à sua escrivaninha, a muitos quilômetros do epicentro do ataque. Ele já está a postos no que, muito provavelmente, é um terminal Linux, esperando que a vítima clique no CCleaner "bichado" para abri-lo. A tela do nosso hacker é mostrada abaixo (por razões óbvias, os comandos que ele utiliza foram embaçados na imagem):

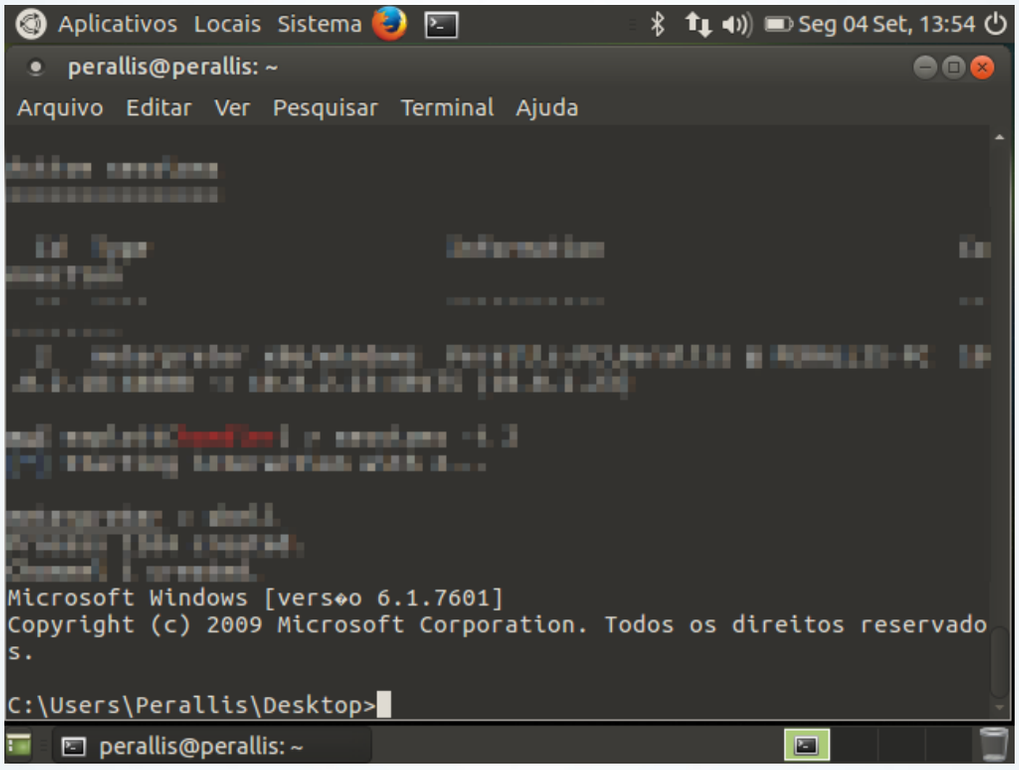


Infelizmente, nossa vítima desavisada clica no CCleaner "bichado":

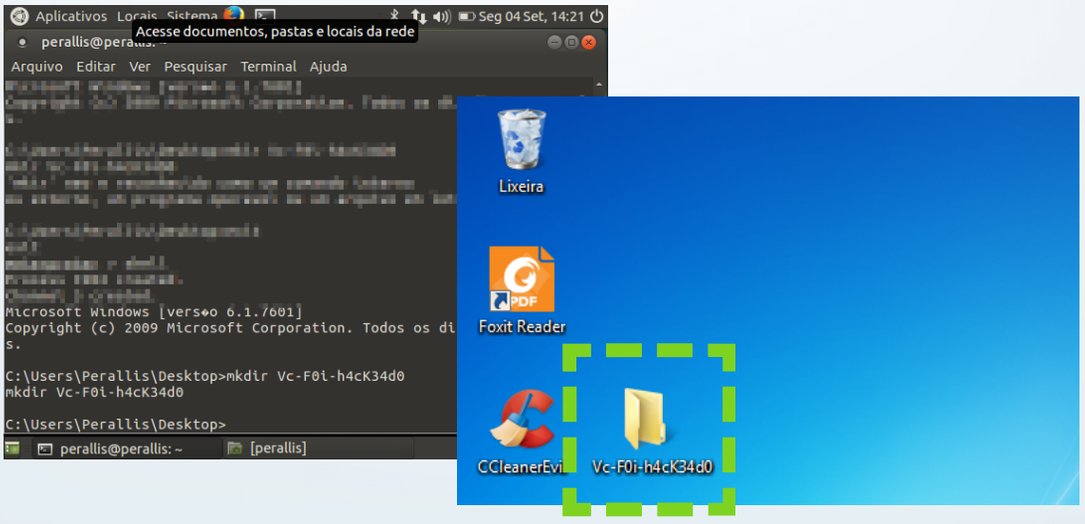
Boas práticas em Cibersegurança

E pronto! O malware agora permite a entrada do hacker...

Assim que o CCleaner "bichado" inicia, ele permite que o hacker tenha acesso a um "prompt de comando do Windows" da vítima, isto é, uma interface textual que permite que ele passe comandos ao computador da vítima:



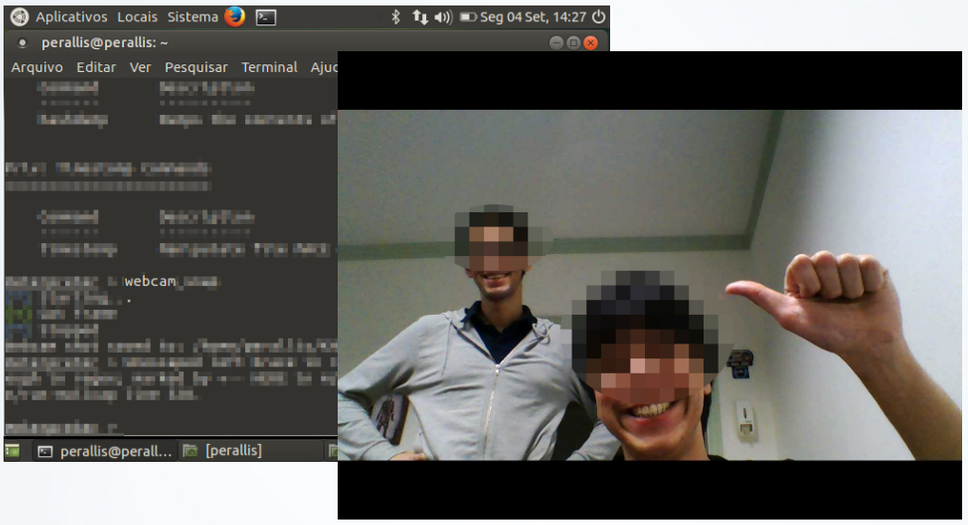
Dentre outras coisas, agora ele pode... Bagunçar, ler, apagar, roubar e sequestrar arquivos...



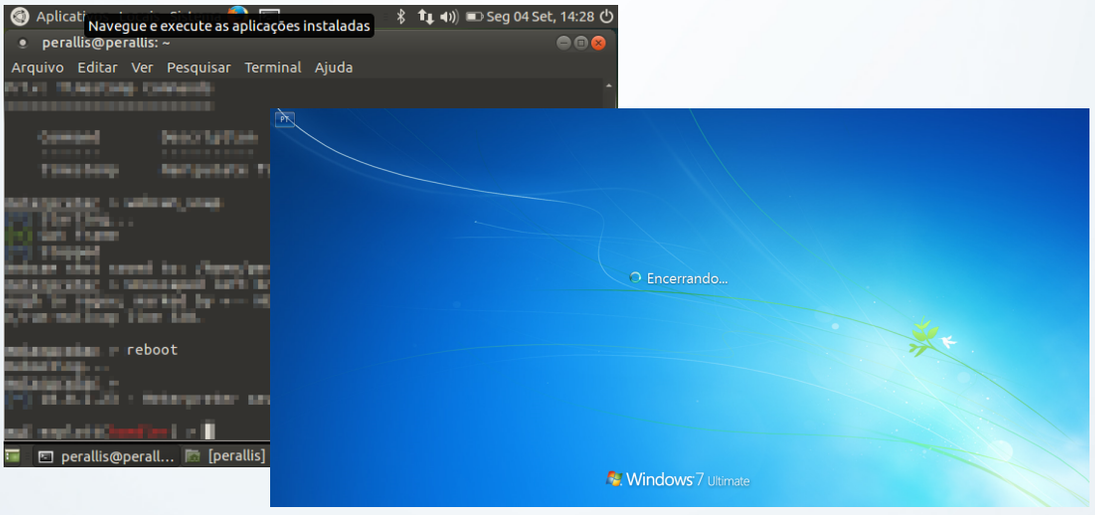
Perallis
IT Innovation

Boas práticas em Cibersegurança

Controlar a webcam da vítima e salvar as fotos que tirar e os vídeos que gravar com ela...



E até mesmo desligar/reiniciar o computador da vítima... Dentre muitas outras operações!



Em suma...

O computador atacado vira uma marionete do hacker que criou o malware, tudo por descuido da vítima, ao baixar um programa malicioso de um site de procedência duvidosa. O melhor conselho que podemos lhe dar é: jamais dê chance ao azar baixando programas de sites cuja procedência é duvidosa. Aliás, até mesmo sites conhecidos podem conter malware. Tenha muito cuidado com o que/quem você deixa "entrar na sua casa" (i.e. os programas - e aplicativos, uma vez que smartphones e tablets também são vulneráveis - que você baixa).

Perallis
IT Innovation