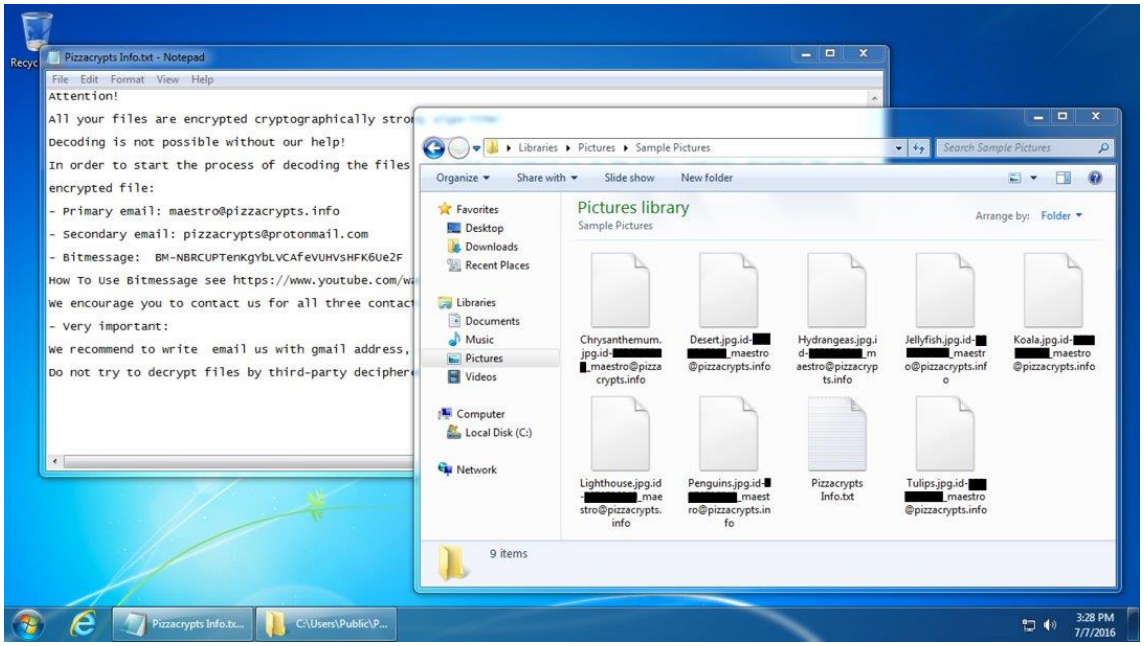
Alguns Exemplos de Telas do Ataque do vírus:

O Cryptolocker sequestra documentos. E pede resgate por eles!

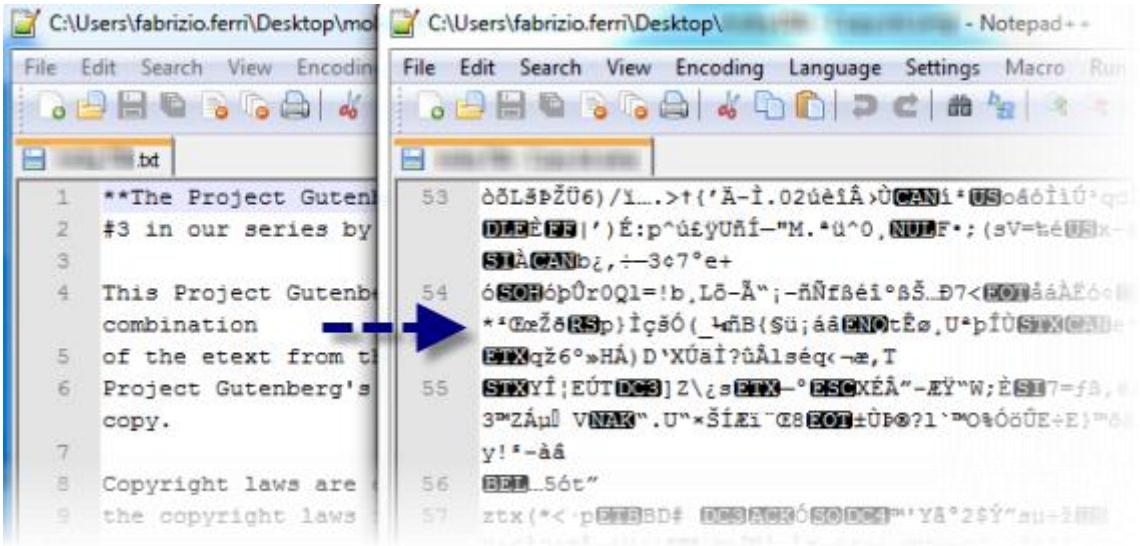
O CryptoLocker é um malware também conhecido como "**Ransomware**" basicamente criptografa todos os arquivos do computador Windows da vítima. Isto inclui as fotos, vídeos e músicas, documentos, além de certos arquivos nas mídias de armazenamento local ou de rede. Um resgate, pago através de **Bitcoin** ou **MoneyPak**, é exigido como pagamento para receber uma chave que desbloqueia os arquivos criptografados e os decriptografa.

Com Base em algumas ocorrências nos EUA, Europa e no Brasil em média as vítimas tem 72 horas para pagar cerca de 200 dólares ou mais. Depois deste prazo, o resgate sobe para mais de 2.200 dólares assim como o prazo também decresce.



Como é a infecção pelo CryptoLocker?

Quando executado, o Cryptolocker se instala na pasta de programas e começa a encriptar os documentos do Office e LiveOffice, arquivos PDF, fotos e ilustrações, **tornando-as inacessíveis ao proprietário do PC**. Os arquivos são encriptados com uma senha que apenas os autores do Cryptolocker possuem.

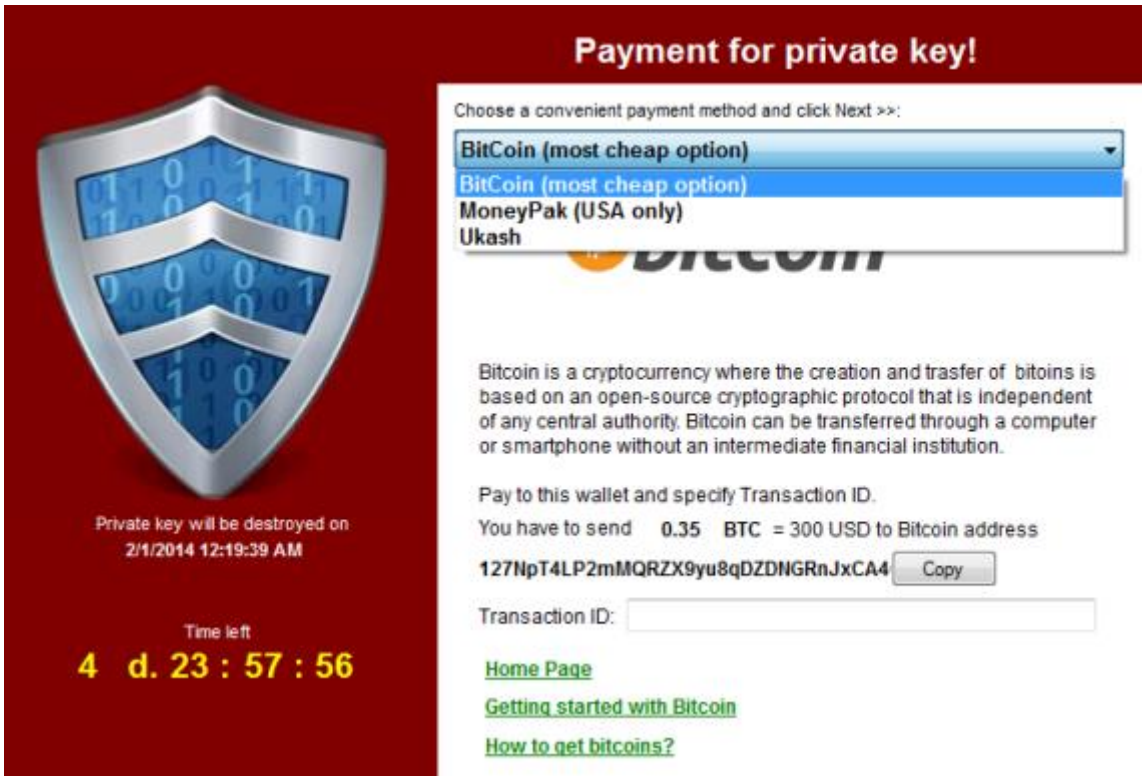


Os arquivos infectados pelo Cryptolocker se tornam ilegíveis devido à encriptação

Ao mesmo tempo, o Cryptolocker **lança sua terrível ameaça**: se o proprietário não pagar uma quantia de dinheiro no prazo de três a quatro dias, a senha usada para bloquear os arquivos será apagada para sempre, e os arquivos já não poderão ser resgatados. É como trancafiar alguém em uma cela indestrutível e jogar a chave fora.

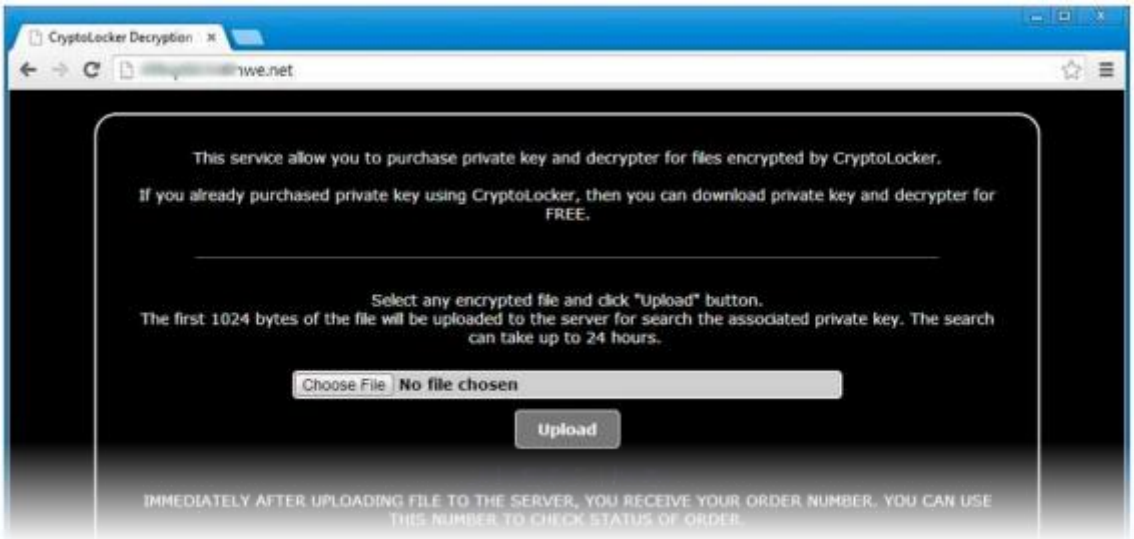
Os arquivos não podem ser resgatados sem pagar

Caso o pobre usuário pague o resgate – que pode chegar até 300 dólares – o Cryptolocker decifra os arquivos. Algo que, mesmo assim, não é garantido. O pagamento pode ser efetuado através do MoneyPak (apenas para os EUA), Ukash e -a novidade- Bitcoin, a moeda virtual cujas transações são feitas sem controle algum. (não é possível rastrear sua origem e destino).



Formas de pagamento do vírus Cryptolocker dificultam a identificação dos autores

Toda tentativa de pagamento errada **diminui o tempo disponível** para salvar os arquivos. Para "ajudar", os autores do vírus até disponibilizaram um endereço de suporte técnico no fundo da tela que o Cryptolocker ativa no PC infectado. Cara de pau pouca é bobagem.



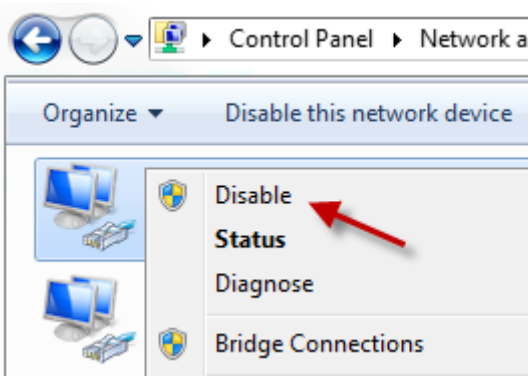
A página do "suporte" do Cryptolocker

O sistema idealizado pelos criminosos é perfeito: **se o usuário não paga**, os arquivos não poderão ser recuperados. A encriptação usada é muito forte, e mesmo um programa

especializado em quebrar senhas demoraria muito tempo para decifrar qualquer um dos arquivos capturados. Então, se você não tiver uma cópia de segurança, terá que pagar aos bandidos.

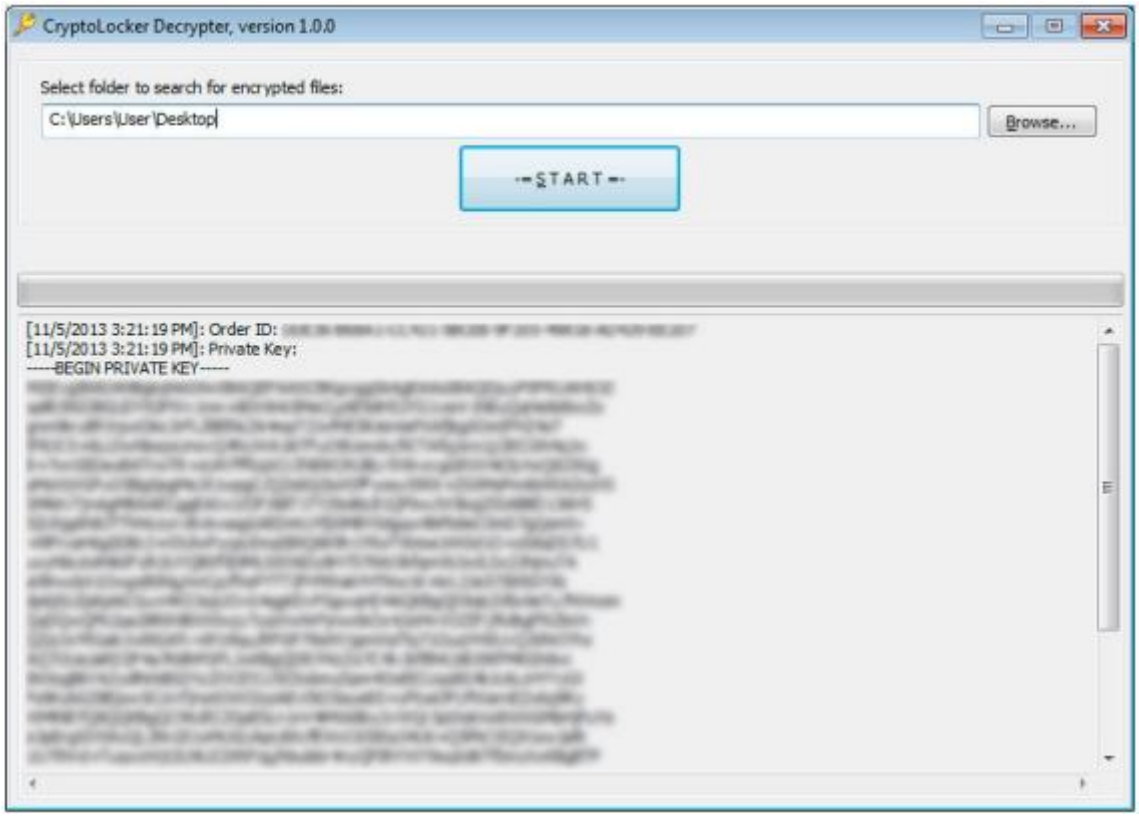
O que fazer no caso de infecção do Cryptolocker

Se você ver a tela do Cryptolocker, **desconecte o equipamento da rede** para que o vírus não possa encriptar mais arquivos, nem se comunicar com os criminosos. Desabilitar a conexão da Internet também evita que seus arquivos no Dropbox ou no Google Drive sejam infectados pelo arquivo.



Uma forma rápida de desativar a conexão é ir ao painel de Rede e desativar os dispositivos

O próximo passo é **se perguntar o que você quer fazer:** se pagar a soma do resgate, ou eliminar o vírus e tentar recuperar os arquivos. Caso você opte pelo pagamento, estará à mercê dos criminosos, e a recuperação não é garantida. Há muitos relatórios que comentam que a liberação dos arquivos começa poucas horas depois do pagamento ter sido efetuado. Outros comentam que o processo de recuperação está cheio de falhas. **Logo, recomendamos que você não pague.**



O utilitário para decodificar o Cryptolocker só funciona se você pagar o resgate…

Seja qual for sua escolha, o melhor que você pode fazer é **obter uma lista dos arquivos infectados e encriptados.** Para isso, execute a ferramenta ListCrilock, que cria um arquivo TXT com todos os arquivos codificados pelo vírus. Outro programa tão eficiente quanto, o CryptoLocker Scan Tool, procura os arquivos sequestrados pelo vírus e analisa se eles conseguem ser recuperados.

CryptoFinder analisa os arquivos para dizer se podem ser recuperados ou não

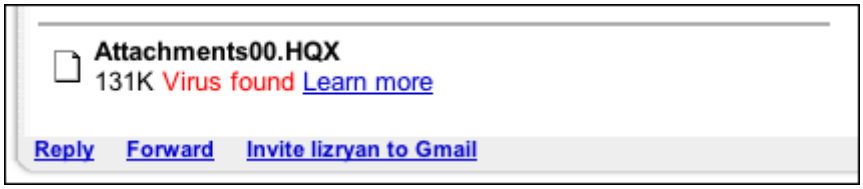
A **opção manual** consiste em abrir o Editor do Registro do Windows (Inicio > Executar > Regedit) e ir até a senha HKEY_CURRENT_USER\Software. Lá você verá uma pasta com número e uma subpasta que contém os nomes dos arquivos: é o Cryptolocker. Pode ser que alguns desses arquivos ainda não estejam encriptados e podem ser recuperados. Para os demais, só se você tiver cópias de segurança.

Extensões que o Cryptolocker ataca: .odt, .ods, .odp, .odm, .odc, .odb, .doc, .docx, .docm, .wps, .xls, .xlsx, .xlsm, .xlsb, .xlk, .ppt, .pptx, .pptm, .mdb, .accdb, .pst, .dwg, .dxf, .dxg, .wpd, .rtf, .wb2, .mdf, .dbf, .psd, .pdd, .pdf, .eps, .ai, .indd, .cdr, .jpg, .jpe, .jpg, .dng, .3fr, .arw, .srf, .sr2, .bay, .crw, .cr2, .dcr, .kdc, .erf, .mef, .mrw, .nef, .nrw, .orf, .raf, .raw, .rwl, .rw2, .r3d, .ptx, .pef, .srw, .x3f, .der, .cer, .crt, .pem, .pfx, .p12, .p7b, .p7c.

Como prevenir infecções por Cryptolocker

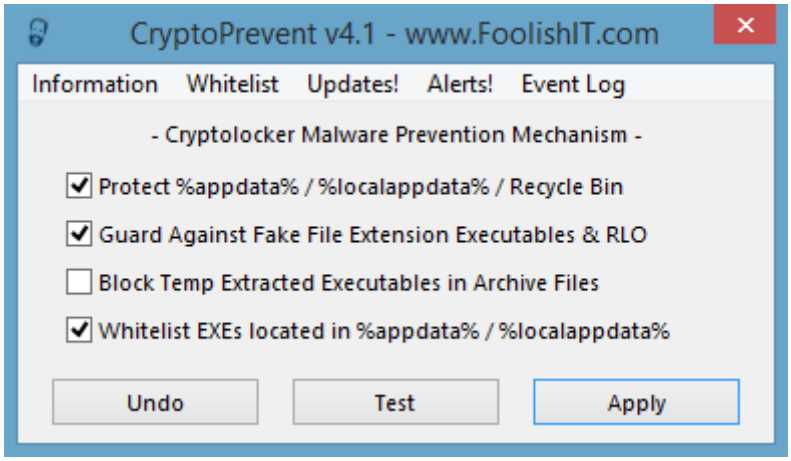
Os autores do Cryptolocker desenharam seu vírus com dois preceitos em mente: que todos abrimos anexos desconhecidos e que ninguém faz cópia de segurança recente de seus documentos. É seu dever desconstruir esse mito. Para isso, você tem que reforçar suas políticas de segurança (ou escolher uma empresa para fazer isso por você).

Para começar, desconfie dos e-mails suspeitos. Se você não os espera, não abra os anexos de forma nenhuma. O mesmo pode ser aplicado se você está usando um e-mail: **se você não pediu nada**, não clique. Essa regra evitará a maioria das infecções oportunistas, a maneira principal da propagação do vírus.



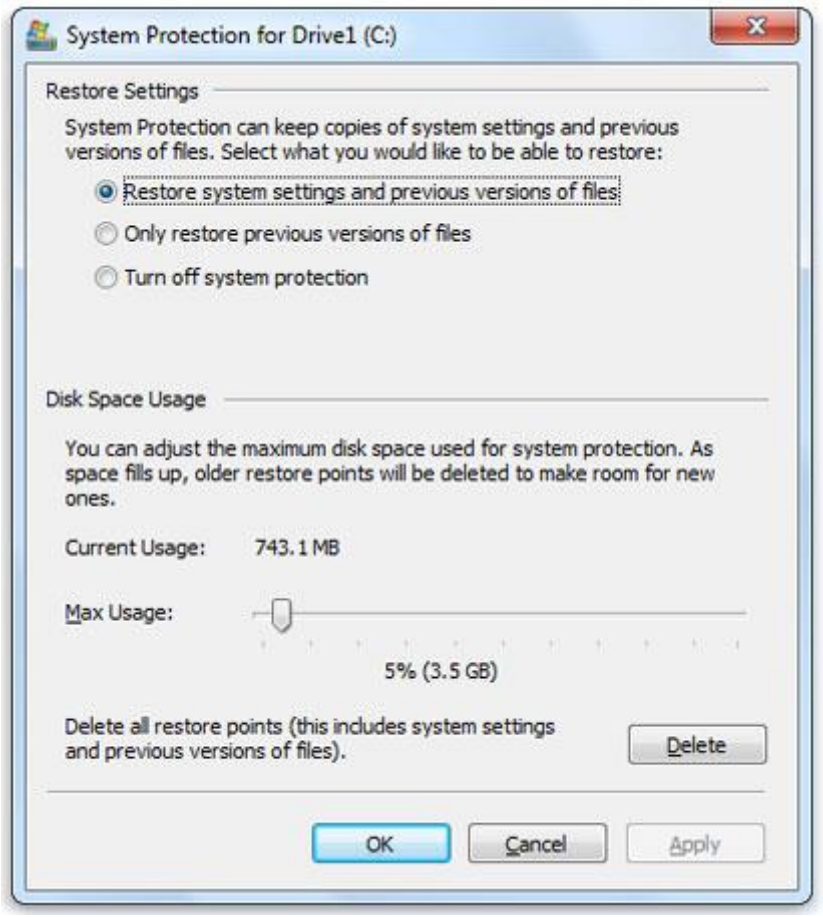
< Um vírus detectado pelo Gmail, que o impede de baixá-lo (imagem de AskDaveTaylor)

Os mais preocupados podem usar a ferramenta CryptoPrevent para desabilitar os tipos de permissões que o vírus aproveita para se instalar. O utilitário modifica as políticas de segurança do Windows para evitar que um programa possa ser executado na pasta de dados do programa (AppData).



Ao executar o CryptoPrevent, marque a **primeira, segunda e quarta opção** para que os programas já existentes nas pastas continuem a ser executados. O botão “Desfazer” permite desfazer a manobra, útil se você tiver que agregar algum programa novo ou se esse procedimento cria mais incômodos que segurança.

Finalmente, se ainda não o tiver feito, convém que você crie seu próprio plano de cópias de segurança. Segundo os dados da firma BlackBlaze, mais de 30% dos usuários trabalham sem cópias de segurança de documentos, e só 10% fazem cópias diárias. Você deve configurar um sistema de cópias, pelo menos, para seus documentos mais vitais.



As **cópias de segurança do Windows** são ativadas no menu de Propriedades de Sistema, que pode ser acessado com um clique direito sobre o ícone do Meu Computador, ou pelo Painel de Controle, dentro da sessão Sistema. A seção Proteção do sistema é o que permite habilitar o backup dos arquivos e definir quanto espaço destinar a elas.

O Cryptolocker é mais perigoso que o "Vírus da Polícia"

Lembramos todos do terrível Reveton, o vírus da polícia, que semeou o pânico em milhões de lares e escritórios. O vírus mostrava uma mensagem que parecia ter sido escrito pela polícia e incitava as vítimas a pagarem uma soma em troca de não serem perseguidos por crimes horríveis. Mas esse vírus não tocava nos arquivos.

O Cryptolocker é mais perigoso. No final de 2013, calcula-se que ele já tenha infectado mais de 250 mil PCs. Visto que as transações com a Bitcoin podem ser analisadas, alguns especialistas descobriram que os criminosos estão ganhando dezenas de milhões de dólares graças a esse vírus.

A forma que o Cryptolocker infecta os PCs é convencional, **e pode ser prevenida se você tomar as precauções que indicamos acima.** A lição mais importante, contudo, é que você precisa atualizar sempre suas cópias de segurança. Seus dados são um pequeno tesouro, e que agora os ladrões querem seus arquivos como forma de chantagem.

Fonte: Softonic