

# Ransomware - Saiba se proteger de vírus que sequestram arquivos



Que tal estar usando o computador e, de repente, receber uma mensagem que seus arquivos foram "sequestrados" e que você precisa uma quantia para ter de volta o que é seu?

Essa é a ação de pragas digitais chamadas de "ransomware". Elas estão na ativa há muitos anos, mas eram um problema maior em países do leste europeu, principalmente na Rússia. Cada vez mais, porém, há registros de casos nos Estados Unidos e agora também Brasil. Diferente dos ladrões de senhas bancárias (o tipo mais comum de vírus no Brasil), essas pragas são bastante visíveis quando contaminam o computador, já que travam a tela com a mensagem do pedido de "resgate".

Não existe melhor forma de definir os ransomwares do que como "sequestradores digitais. Eles são trojans que invadem o computador e impedem o acesso a documentos, programas, aplicativos e jogos, "engessando" literalmente o usuário.

Os primeiros códigos com esse comportamento eram bem simples, e os antivírus conseguiam não só apagar a praga digital, mas também recuperar os arquivos supostamente "sequestrados". Antes disso, o golpe era ainda mais indireto, porque o "resgate" se dava por meio de um programa antivírus fraudulento criado pelos próprios criminosos e que poderia "limpar" o computador de um vírus. Agora, porém, a fraude não faz rodeios, e recuperar os arquivos é muito difícil.

Quando um desses vírus chega ao computador, ele cifra os arquivos e exibe uma mensagem dizendo que é preciso pagar um valor. Caso o valor não seja transferido dentro um prazo definido pelos golpistas, a


cobrança do "resgate" sobe consideravelmente. Para receber o dinheiro, os sequestradores usam a moeda virtual Bitcoin, o que pode ser feito anonimamente.

**Your files are encrypted.**  
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **02/04/14 - 09:03** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Your system: Windows XP (x32) First connect IP: [REDACTED]

[Refresh](#) [Payment](#) [FAQ](#) [My screen](#) [Test decrypt](#)

We are present a special software - CryptoDefense Decrypter - which is allow to decrypt and return control to all your encrypted files.  
**How to buy CryptoDefense decrypter?**



**1. You should register Bitcon wallet (click here for more information with pictures)**

**2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**  
*Here are our recommendations:*

- [REDACTED] - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
- [REDACTED] - An international directory of bitcoin exchanges.
- [REDACTED] - Recommended for fast, simple service.
- [REDACTED] - Bitcoin exchange based in the United States. (Highly rated).
- [REDACTED] - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
- [REDACTED] - allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.

**3. Send 1.09 BTC to Bitcoin address:** [REDACTED] [Get QR code](#)

**4. Enter the Transaction ID and select amount:**

1.09 BTC ~ 500 USD [Clear](#)

**Note:** Transaction ID - you can find in detailed info about transaction you made.

**5. Please check the payment information and click "PAY".**

[PAY](#)

*Pedido de 'resgate' do Cryptowall (Foto: Reprodução/Symantec)*

## Como proteger os arquivos?

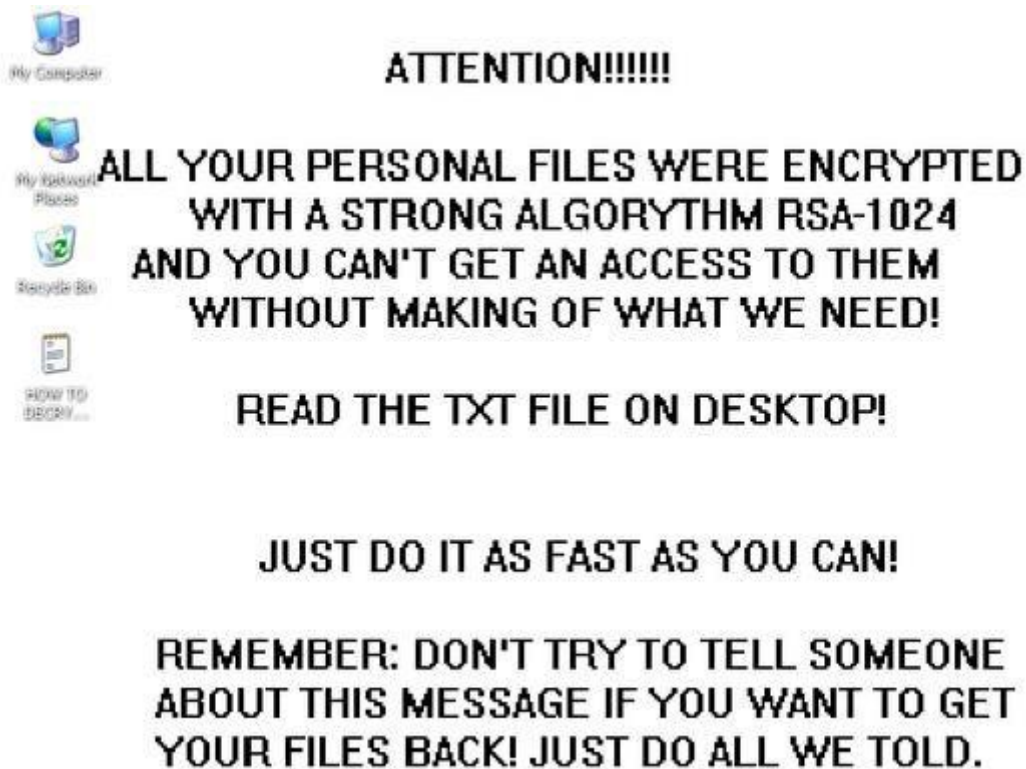
A receita é simples: tenha **backups**.

A melhor prevenção contra os ransomwares é sem dúvida o backup. A cópia periódica de arquivos importantes em uma unidade extra e segura garante que não haverá problemas maiores no caso de uma infecção nos arquivos originais. Com a grande oferta de drives externos existentes, não há desculpa para deixar o backup de lado.

O backup é uma cópia de segurança, extra, dos seus arquivos. Ela deve ficar em uma mídia não acessível. Se você tem a cópia somente em um HD externo que fica o tempo todo ligado ao seu computador ou notebook, não conta.

Cópias em mídias não regraváveis também ajudam a proteger de qualquer alteração, mas elas não são muito práticas.

O backup não serve apenas para proteger desses vírus, mas também de diversos outros problemas, inclusive falhas no hardware de armazenamento.



*GpCode atuando em um computador. (Fonte da imagem: ZDNet)*

## **E se não tiver backup?**

A praga digital precisa criar novas cópias dos arquivos e depois apagar as originais para realizar o seu "trabalho". Isso significa que alguns dados podem ser recuperados com as mesmas ferramentas que recuperam arquivos "apagados" do computador.

Em alguns sistemas, o próprio Windows pode guardar versões anteriores dos arquivos. Mas, se nada disso for possível, o resgate terá de ser pago ou o arquivo foi perdido. E não há garantia de que os criminosos enviarão mesmo a chave para decifrar e recuperar as informações.

## **Quem está por trás dos ransomwares?**

Ao que tudo indica, os desenvolvedores fraudulentos são russos e usam endereços de IP da China — pelo menos é o que serviços de inteligência conseguiram calcular. Através de nomes falsos e contas virtuais hospedadas em serviços como E-Gold e Liberty Reserve, os estelionatários agem sem deixar tantas pistas, comunicando-se com emails aleatórios.

## Como evitar a infecção?

O meio de distribuição mais usado para esse tipo de praga digital hoje em dia são os "kits de ataque" web. Esses kits são inseridos em páginas legítimas que são alteradas pelos hackers com uma invasão ao site. Ou seja, não adianta evitar sites "duvidosos", porque os criminosos fazem com que a infecção chegue até você.

O que funciona é manter o navegador atualizado. Se você usa o Chrome, isso é automático. Para o Internet Explorer, mantenha o Windows Update ativado. E, no Firefox, fique atento aos avisos de atualização.

Se você visitar alguma página e ela solicitar ou exigir o download de um programa (aplicativo) para visualizar algum conteúdo ou uma "atualização" que você precisa, não execute o programa – de preferência, nem faça o download. Avisos de atualização não aparecem dentro da janela do navegador. Esses avisos são normalmente falsos e têm programas maliciosos.

Tomando esses cuidados e usando um antivírus é suficiente para se prevenir, mas não se esqueça de ter um backup atualizado para restaurar seus arquivos caso o pior aconteça.

Fonte: [G1](#), [Tecnundo](#)