

# 12 de maio de 2017, algum computador na Europa...



## Ooops, your files have been encrypted!

English

### What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

**Payment will be raised on**  
5/16/2017 00:47:55

Time Left  
02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55

Time Left  
06:23:57:37

**Em 12 de maio de 2017 começaram relatos de ataques de ransomware em computadores do NHS (UK)**

**Em poucas horas sistemas Windows foram atacados em vários países da Europa.**

**Em pouco tempo a praga cruza o oceano fazendo vítimas nas Américas, inclusive no Brasil.**

**Observa-se um número incomum de "probes" na porta 445/tcp tanto em IPv4 quanto em IPv6.**

**Nesse mesmo dia, Marcus Hutchins, aka MalwareTech, do UK, descobriu que o wannacry tenta resolver o curioso nome [iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com](http://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com)**

**Hutchins registrou o domínio e notou que ele funciona como uma chave de desligamento do wannacry.**

**Por que um malware teria uma chave de desligamento?**

**1. para ser parado por controle remoto?**

**2. (mais provável) para evitar que fosse analisado em ambiente controlado.**

**Pouco tempo depois, Adrien Guinet, francês, descobriu que o wannacry deixava intactos na memória dados suficientes para quebrar-lhe a criptografia e publicou um destravador para o velho Windows-XP.**

**O susto maior passou, mas fica a pergunta:**

**O QUE FIZEMOS DE TÃO ERRADO?**

## **O QUE FIZEMOS DE TÃO ERRADO?**

- 1. não manter software atualizado. A Microsoft havia lançado remendos contra as vulnerabilidades exploradas pelo wannacry, mas poucos sistemas foram atualizados;**
- 2. não configurar firewalls adequadamente. CIFS/SMB são serviços que só fazem sentido em redes internas, não há porque disponibilizá-los para a Internet!**
- 3. backup, backup, backup!  
prevenção e canja de galinha só fazem mal à galinha!**

**No final, tivemos muita sorte, se a chave de desligamento não tivesse sido encontrada e não se descobrisse como decifrá-lo, o mundo ainda estaria em pânico como na manhã do dia 12.**