

	<b>Informação</b>		
	<b>Data</b>	<b>De</b>	<b>Para</b>
		Gabinete de Informática	

<b>Assunto</b>
----------------

Informação sobre Vírus W32/Mydoom A

<b>Desenvolvimento</b>
------------------------

Este vírus propaga-se tipicamente por email e o assunto das mensagens pode ser um dos seguintes:

Test; hi; hello; Mail Delivery System; Mail Transaction Failed; Server Report; Status; Error

Corpo da mensagem pode ser uma das seguintes informações:

Mail Transaction Failed. Partial message is available.  
The message contains Unicode characters and has been sent as a binary attachment.  
The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Os ficheiros em anexo podem ter um dos seguintes nomes:

Document; readme; doc; text; file; data; test; message; body

Com as extensões seguintes:

Scr.; exe; cmd; bat; zip

Depois de infectar um computador, procura pela aplicação de partilha de ficheiros KaZaA. Se esta for detectada, é copiado um ficheiro para a directoria de partilha desta aplicação. O nome do ficheiro poderá ser um dos seguintes:

winamp5 ; icq2004-final ; activation\_crack; strip-girl-2.0bdcom\_patches; rootkitXP;  
office\_crack; nuke2004

Se receber mensagens com as características mencionadas acima apague-as de imediato sem as abrir.

Informa-mos que o nosso servidor de email está configurado de modo a desinfetar as mensagens antes de chegarem aos postos de trabalho. Deste modo as mensagens infectadas que chegam ao Outlook Express por meio do servidor do ipt já foram não contêm o vírus.

Avisamos no entanto que quem recebe email por webmail caso do hotmail.com, sapo.pt portugalmail.pt, e outros do género, pode estar desprotegido em relação a este vírus e deve proceder com cuidados redobrados sendo aconselhado a usar somente a conta de email do ipt.

Pode encontrar mais informações sobre este virus em:

[http://www.pcseguro.pt/pcseguro.dll/noticias\\_fv?codigo=760](http://www.pcseguro.pt/pcseguro.dll/noticias_fv?codigo=760)

Se suspeitar que o seu computador está infectado aceda a este link para descarregar o utilitário pqremove.com que poderá limpar o seu computador deste vírus.

<http://193.137.5.210/apoioadm/mydomm/pqremove.com>, qualquer dúvida não existe em contactar o Gabinete de Informática.