

Re: Employees & their family / friends in collusion to bypass email fi

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2006-11/msg02795.html>

- *From:* "Leif Pedersen [MVP]" <Leif.pedersenNO-SPAM@xxxxxxxxxxx>
 - *Date:* Sun, 26 Nov 2006 10:37:25 +0100
-

Hi,

Microsoft Forefront security for Exchange server (formerly Antigen) will do this for you.

Leif

"DefenderD90" <DefenderD90@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:405E82E0-226E-46DE-A6F6-E1D635021E1B@xxxxxxxxxxxxxxxxxxxx>

Currently, we have a barracuda that has about 40 manually typed extensions in the barracuda interface to filter movie formats by extension.

However, it seems individuals are getting their friends on the outside to rename :

blah.mpeg to blah.qrx – meaning it is a fake extension.

This bypasses the filters.

I asked barracuda networks if its possible to do any kind of mime filtering, that analyzes the data, and not just the extension, through header/footer analysis of the attachment(s), and they said it is not possible.

can any 3rd party mail clients take this task, and deliver with an answer?

That is our outside to inside filter.

However, it also seems once employees get this, they are circulating and cc'ing everyone for example: a 7meg movie attachment, and sending it to 19 other employees....truely a waste of of the business email database space.

Re: Employees & their family / friends in collusion to bypass email fi

Is there a way for exchange '03 enterprise, or any 3rd party addons, to monitor internal to internal deliverance of multimedia files, and if they do extension renaming or embedding in archived attachments, or a renamed archived zip file to blah.jmz , true data analysis of content.

If it continues, it'll become an HR issue leading to termination, but I need professional opinions on this.