Why aren't encrypted Microsoft Word documents flagged by Sophos Anti−Virus?

Document ID: 118244

Contributed by Stephan Fiebrandt and Chris Haag, Cisco TAC Engineers.
Aug 12, 2014

Contents

Introduction

This document describes the scanning behavior of sophos antivirus on Cisco Email Security Appliance (ESA).

Background Information

Sophos Anti−Virus can be configured to treat encrypted messages differently from unencrypted messages. In most cases, Microsoft Word documents encrypted using the built−in encryption methods are not flagged as encrypted by Sophos. As per Sophos:

"The Office95 format uses a simple encryption that can be decrypted on the fly so we can scan the encrypted macros.

The Office97 format uses a strong encryption which we cannot decrypt, but the macros are not in the encrypted part so we can scan them anyway. (It is the macros we need to get at)."

To encrypt Microsoft Word documents in Word 2003, go to Tools −> Options. Click the "Security" tab and set a password to open the file.