

Life cycle of a Computer Deep: from Infection to Kill

You may have heard many warnings now that you did not open the email attachment unless you fully trust the sender and you are waiting for the attachment. Open unrelated attachments of fish



You may have heard many warnings now that you did not open the email attachment unless you fully trust the sender and you are waiting for the attachment. Opening unidentified attachments is the most common way you can catch and spread dangerous software called worms.

But how do computer worms really spread?The answer to this question will help you understand the steps you can take to protect yourself and others.

A virus is a computer program that attempts to spread from computer to computer by attaching itself to a computer file. A virus often requires human action, such as sharing a file or opening an email, to spread. A computer worm, like a virus, is designed to copy itself from one computer to another, but it does it automatically by taking control of the features in the computer, but these features can transmit files or information. When you

have deep in your system it can move on its own. A major danger of worms is that it is capable of replicating in large quantities.

How Your Computer Can Be Infected

Hackers have become experts in disguising computer worms as e-mail attachments. When an unsuspecting user opens the attachment, the worm is activated, and, depending on the purpose of the hacker, the worm will automatically send it as an attachment of email to everyone in the address book. email of that user.

Mydoom worm, which began appearing in February 2004, uses a particularly sophisticated technique to convince users to click on the attached file. Its creator carefully writes out some legitimate email error messages, using several different titles such as "Mail Delivery System," "Test," or "Mail Transaction Failed." Sometimes you can often receive these types of emails. These are the official messages that tell us that one of the e-mails sent does not reach the recipient. They often contain technical language that most of us don't understand. The creator of Mydoom mimics this language in a way that he can trick millions of people to open the attachment.

Later versions of Mydoom use terrifying techniques, including sending emails that appear to be sent from an Internet Service Provider (ISP) to warn you that you have a worm and how to keep it unique. The most to kill it is to open the attachment. As you can already guess, the attachments contain worms.

How Worms Spread from A Computer to Multiple Computers

One of the most sophisticated reproduction techniques of a worm is sending many e-mails containing attachments that are dangerous to everyone in the user's address book. In this way it disguised itself as an e-mail from a trusted friend. Therefore, it is very important to be careful before opening an attachment of email.

Attack

In addition to self-dispersion, worms can program themselves to perform other operations. For example, Mydoom is designed so that infected computers (also known as "zombie computers") will attack specific targets at a specific time. These attacks, known as "Distributed Service Denial" (DDoS) attacks, are designed to flood their targets with network traffic and make them error-free.

Prevent and Kill

The best way to prevent worm infection is to be careful when opening attachments of email messages. If you receive an email attachment from a friend, the safest way is to contact them and ask them if they intend to send the attachment. If you receive an email attachment from someone you don't know, the safest way is to delete it.

If you need an effective antivirus software, please refer to the following article: **10 top antivirus software**

You finished reading the article "**Life cycle of a Computer Deep: from Infection to Kill**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.