I

ILOVEYOU Worm: How the Love Letter Attack Spread

The ILOVEYOU worm used a deceptive love-letter attachment and automated address-book propagation to spread rapidly in May 2000. Learn how it worked and why its security lessons still matter.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 6, 2026

READ TIME
4 min

CONTENTS

In this guide

ILOVEYOU, also called the **Love Letter** or **Love Bug** worm, was a destructive email-borne outbreak that began spreading widely on May 4, 2000. It combined a personal-looking message with automated propagation. People commonly call it the ILOVEYOU

virus, but **worm** is the more precise term because the script copied and distributed itself.

01 What the ILOVEYOU email looked like

The message used the subject **ILOVEYOU**, a short invitation to read an attached love letter, and a file named **LOVE-LETTER-FOR-YOU.TXT.vbs**. The final `.vbs` extension meant it was a Visual Basic Script, not a text document. Windows configurations that hid known file extensions could make the attachment appear to end in `.TXT`, helping the disguise.

Opening the attachment executed the script. Merely reading this historical filename in an article is harmless; the danger came from running the attached script on a vulnerable Windows configuration.

02 How the ILOVEYOU worm worked

1. **Social engineering:** the emotional subject encouraged recipients to open an unexpected attachment quickly.
2. **Script execution:** Windows Script Host ran the malicious VBScript after the user opened it.
3. **Local changes:** the worm copied itself, changed registry settings, and altered or overwrote several kinds of files.
4. **Email propagation:** it used Microsoft Outlook and the victim’s address book to send copies to other people.
5. **Trusted appearance:** new recipients often recognized the sender, even though that person had not intentionally sent the message.

This feedback loop allowed the outbreak to expand quickly through organizations and personal contact lists. Mail systems were overwhelmed, while infected computers also suffered file damage.

03 Why it spread so successfully

- The message appeared to come from a known contact.
- The subject exploited curiosity and emotion rather than a technical vulnerability alone.
- The double extension disguised executable script content as a text letter.
- Script execution and access to the email client were permissive on many systems.
- Automated address-book distribution reached many recipients from every infected account.
- Many organizations had limited attachment filtering and incident-response automation in 2000.

04 Virus or worm?

Term	Typical behavior	How it applies
Computer virus	Replicates by attaching to or modifying a host file or boot area	“ILOVEYOU virus” is the popular name, but it is less precise
Computer worm	Self-propagates between systems or users	ILOVEYOU sent copies of itself through email contacts
Trojan	Disguises malicious behavior as something desirable	The love-letter lure had a Trojan-like social-engineering element

Malware categories can overlap in delivery technique, but self-propagation is the defining reason ILOVEYOU is described as a worm.

05 What to do with a suspected historical sample

1. Do not open or forward the attachment, even in a virtual machine unless you are an authorized malware analyst.
2. Disconnect an affected legacy computer from networks and shared storage.

3. Use an updated security scanner appropriate for the system and preserve important evidence.
4. Restore altered files from a verified backup; some overwritten data may not be repairable.
5. Check mailboxes and gateways for other copies and notify recipients who may have opened them.

Modern supported systems and email services block many original ILOVEYOU techniques, but unsafe legacy systems can still execute old scripts. The name is also reused in hoaxes and unrelated detections, so verify the exact attachment and security alert.

06 Lessons that still apply

Show full file extensions, block unnecessary script attachments, and do not trust a file solely because it came from someone you know. Confirm unexpected attachments through a separate channel. Keep email clients and operating systems supported, restrict scripting where it is not needed, and maintain offline or protected backups. Organizations should provide a fast way to report suspicious messages and remove matching copies from other inboxes.

07 Frequently asked questions

Who sent an ILOVEYOU message from a friend’s account?

The infected script could send itself automatically using the victim’s address book. The apparent sender may not have intentionally written the message.

Can ILOVEYOU infect a modern phone?

The original VBScript targeted Windows and Outlook-era behavior. A message using the same words today may instead be phishing, a hoax, or different malware and should be evaluated on its actual link or attachment.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com