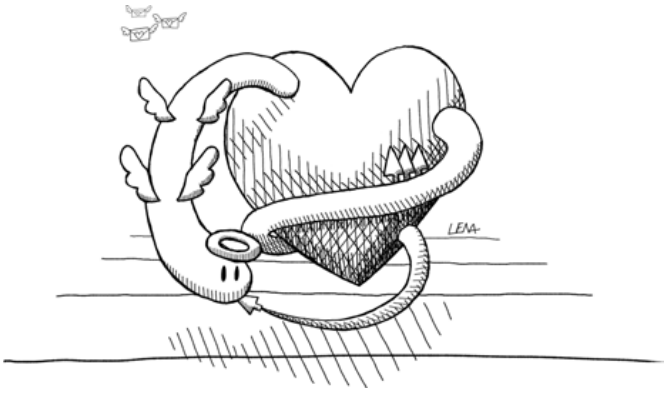
Chapter I
ILOVEYOU



ILOVEYOU, commonly known as the "Love Bug," represents a defining moment in the evolution of socially driven malware. It first appeared in 2000 and wound explosively through global email systems by persuading users to infect themselves. Disguised as a personal message of affection, the worm persuaded recipients to open a seemingly harmless attachment, then replicated itself through address books and shared files. Its success demonstrated that emotional persuasion could rival technical exploitation as a mechanism of large-scale digital infection.

Lenaean Taxonomy

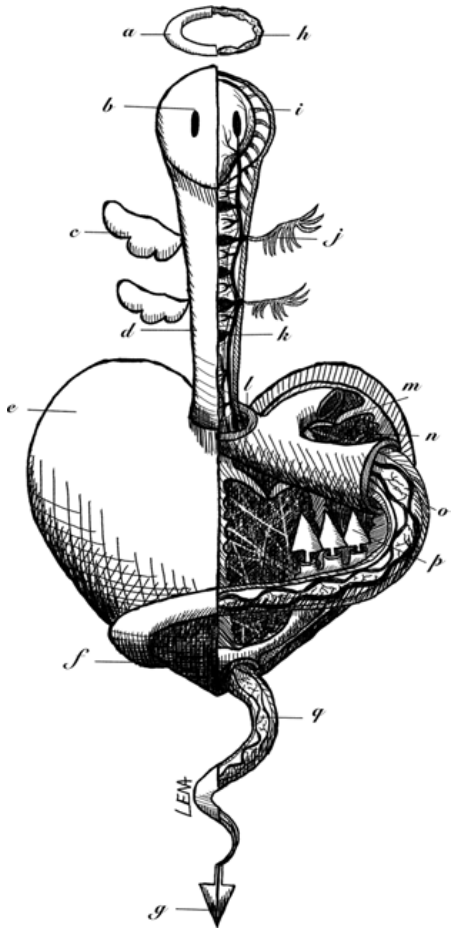
ILOVEYOU is formally classified within the Lenaean system as:

Winwormia Infector Loveletterius (Global 2000)

Lenaean Taxonomy	
Rank	**Description**
Kingdom: *Winwormia*	A Windows-dwelling worm, favored by permissive scripting and hidden extensions
Function: *Infector*	Its chief act is conversion, overwriting files into vessels of replication
Trait: *Loveletterius*	The sentimental lure of a love letter that invited voluntary execution
Region: *Global*	Its reach crossed continents within hours
Year: *2000*	The era of email's innocence, before defensive hardening became widespread

Anatomy

The anatomical structure of **ILOVEYOU** reveals a creature evolved for deception, social propulsion, and viral reproduction through misplaced trust.



ILOVEYOU
Winwormia Infector Loveletterius (Global 2000)

a. Halo — A glowing golden halo of innocence. The halo mirrors the email wrapper: a message of affection accompanied by, to all appearances, a harmless text attachment. Beneath lies executable script.

b. Eyes — Minimal, primitive eyes. The worm is not aware of the network itself. It perceives the world through the host's email client, inheriting the user's social connections.

c. Wings — A dual pair of wings. The lightweight script allows the organism to replicate easily across systems. Unlike compiled malware, its body consists entirely of plaintext instructions that can be copied and redistributed freely.

d. Torso — A slender tubular body, representing the worm's execution pipeline. Its internal logic follows a straightforward sequence of actions: replication, persistence, propagation, and travel through filesystems. The structure is simple, pipelined, and highly automated.

e. Heart — A heart beating with tenacity. Once executed, the worm embeds itself within the host system so that it may awaken again whenever the machine restarts. Each reboot restarts the organism's circulation.

f. Tail — A prehensile tail, tipped with deception. The visible filename suggests an innocent text document, but the hidden extension reveals its true executable nature.

g. Cursor Arrow — Gripped tightly, like Cupid's arrow. The click of a cursor is the spark of life. Each user who opens the attachment unknowingly launches a new instance into circulation.

h. Halo Innards — Beneath the halo's glow lies the internal machinery. The script contains instructions for interacting with files, system settings, and the host's email environment. Its code is transparent and unencrypted, yet capable of widespread disruption.

i. Brain — A primitive brain composed of simple instructions. Despite its modest size, this script directs the organism's full life cycle of persistent replication and infection of external resources.

j. Veins — Channels through which information flows. The worm maintains records of which contacts have already received copies, allowing it to regulate its own circulation and avoid redundant transmission.

k. Organs — A metabolism adapted to the filesystem. Certain types of files are consumed, replaced, or disguised, turning trusted documents and media into extensions of the worm's own body.

l. Arteries — Arteries carry its message outward through existing communication channels. Every contact in the host's address book becomes a potential new host.

m. Heart Valves — Valves ensuring the flow moves forward. Once files are overwritten or replaced, recovery is difficult without an external backup. The worm's circulation is largely irreversible.

n. Heart Strings — Strings pulled to stir emotion. An affectionate message is a powerful vector.

o. Digestive Tract — A tract feeding on the filesystem. The worm traverses directories methodically, converting familiar files into new vectors of infection.

p. Quiver of Cursors — A quiver of arrows poised to fire toward new hosts. Additional communication channels beyond email can also distribute the worm, extending its reach across multiple digital communities.

q. Excretory System — The residue left behind. Modified files, altered system settings, and staged script

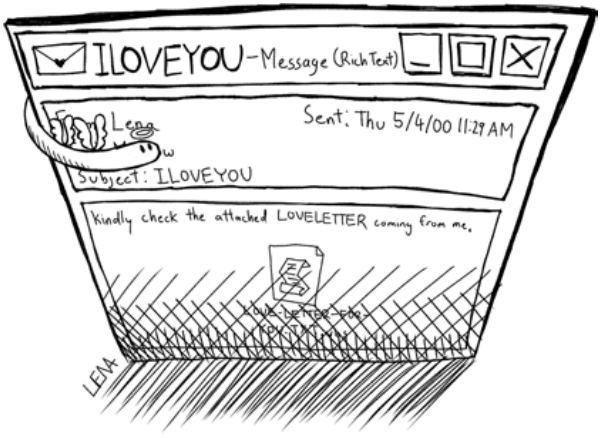
copies litter the organism's passage through the host environment.

Behavior

ILOVEYOU behaves less like a predator and more like a parasite, surviving by exploiting social instincts rather than overpowering its host.

Delivered with Love

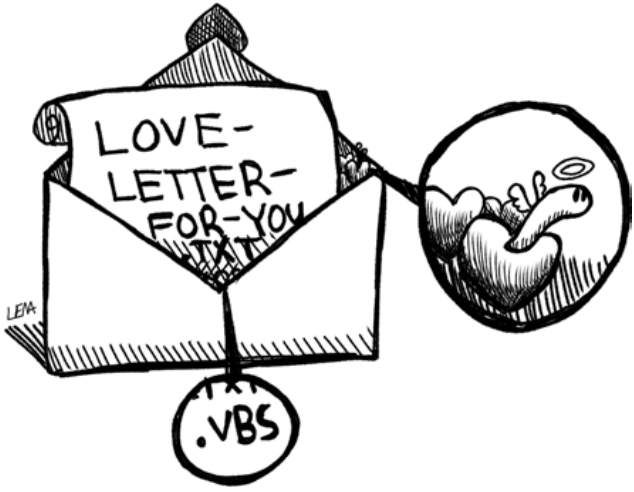
The infection vector of **ILOVEYOU** was simple. Recipients received an email from a "familiar contact" bearing the subject line `ILOVEYOU`. The message read, "Kindly check the attached LOVELETTER coming from me" and included an attachment named *LOVE-LETTER-FOR-YOU.TXT.vbs*.



*The **ILOVEYOU** email*

When a recipient double-clicked the attachment disguised as a love letter, the embedded VBScript executed immediately. Windows' default behavior of hiding known file extensions obfuscated the script's true nature, causing the attachment to appear as a harmless text file. What users believed to be a confession of affection was actually the moment of infection.

Once executed, **ILOVEYOU** initiated its life cycle autonomously, transitioning from dormant payload to active organism in an instant.



*The hidden extension of the **ILOVEYOU** attachment*

From Me to You

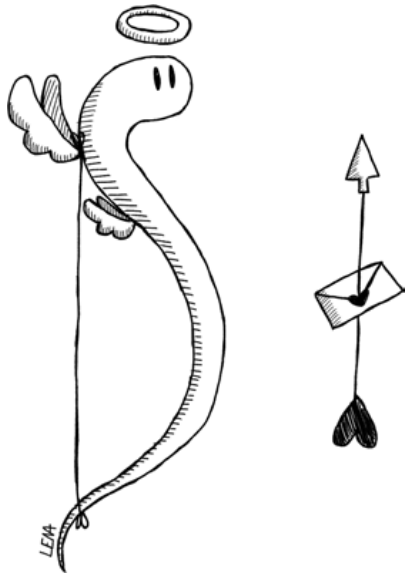
Unbeknownst to the recipient, the "familiar contact" who appeared to have sent the message had already been hijacked by **ILOVEYOU**. Once the attachment was

executed, the new victim inherited that same role, becoming the next "familiar contact" in the chain.

Upon activation, **ILOVEYOU** invoked Microsoft Outlook through its scripting interface, accessing MAPI address lists and enumerating every available address book. For each list, it iterated through every stored entry and constructed a new outbound message bearing the subject line `ILOVEYOU` and the original attachment, *LOVE-LETTER-FOR-YOU.TXT.vbs*.

To regulate its spread, the worm created registry values under `HKEY_CURRENT_USER\Software\Microsoft\WAB\`*`listname`* and `HKEY_CURRENT_USER\Software\Microsoft\WAB\`*`addressentry`* for each address list and each individual address. These keys recorded which contacts had already received the worm, preventing duplicate mailings during subsequent executions. The worm also installed itself to run at system startup, so any newly added addresses were automatically sent a love letter upon the next reboot.

Propagation did not require confirmation, throttling, or even user awareness. The infected system functioned as an unwitting mail server, dispatching copies of the worm across preexisting online communities at network speed. Within hours, tens of millions of infected emails flooded global networks, saturating corporate mail servers and overwhelming national and enterprise infrastructure. The worm spread faster than advisories or warnings could be disseminated, like biological outbreaks in immunologically naive populations.



The worm bow and the cursor-tipped arrow

Appetite for Files

In parallel with mass mailing, **ILOVEYOU** initiated its destructive feeding cycle. It traversed both fixed and remote drives, recursively enumerating directories in search of specific file types. Files with extensions including *.vbs*, *.vbe*, *.js*, *.jse*, *.css*, *.wsh*, *.sct*, *.hta*, *.jpg*, *.jpeg*, *.mp2*, and *.mp3* were targeted for conversion.

For script-based files such as *.vbs* and *.vbe*, the worm overwrote the original contents directly with its own source code. For JavaScript and related scripting formats, **ILOVEYOU** deleted the original file and replaced it with a new file of the same base name but with a *.vbs* extension.

Image files such as *.jpg* and *.jpeg* were deleted and replaced with copies of the worm bearing an appended *.vbs* extension (for example, *photo.jpg.vbs*).

Audio files received slightly different treatment. Rather than deleting *.mp2* and *.mp3* files outright, the worm modified their file attributes to hide them and created a malicious *.vbs* counterpart with the same base name. When users later double-clicked what appeared to be their original media file, the worm executed instead.

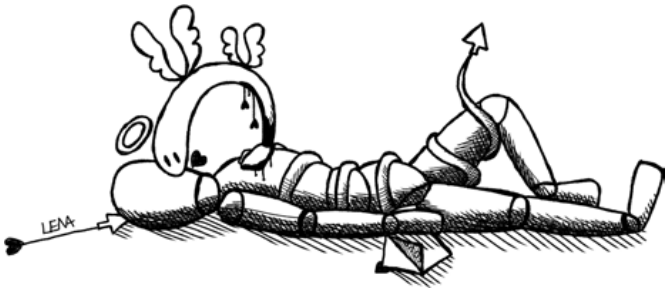
This behavior simultaneously destroyed user data and transformed trusted local files into secondary launch vectors. Each overwritten or disguised file became both a consumed resource and a reproductive organ.

A Sticky Situation

To ensure its own endurance, **ILOVEYOU** copied itself into multiple files, including copies masquerading as *MSKernel32.vbs* and *Win32DLL.vbs*, and it modified Windows Registry values under both `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` and `HKEY_LOCAL_MACHINE\Software\Microsoft Windows\CurrentVersion\RunServices` to guarantee execution at system startup.

It also manipulated Internet Explorer's start page settings to retrieve a secondary payload, *WIN-BUGSFIX.exe*, a trojan designed to harvest cached internet access credentials and transmit them to an external email address, commonly reported as *mailme@super.net.ph*.

It survived through replication at scale, without need of polymorphism, encryption, or stealth concealment.



Lovestruck

The (Un)Natural History

The history of **ILOVEYOU** is remarkable for its simplicity and the offline conditions that allowed it to flourish. It showed that curiosity and affection can propagate faster than caution.

This section follows the outbreak after its execution. **ILOVEYOU** was a social event as much as a technical one: a chain reaction moving through trust relationships, institutional dependencies, and legal systems that were not yet built to absorb software behaving like a self-propagating organism.

Patient Zero

The earliest traceable instances of **ILOVEYOU** emerged on May 4, 2000, traced to internet service accounts in Manila, Philippines. Within hours, investigators correlated infected messages and network logs, narrowing the source to a residential internet account in the Philippine capital.

Investigative attention soon focused on Onel de Guzman, a computer science student at AMA Computer College in Manila, whose undergraduate thesis proposal had explored password acquisition and unrestricted internet access. The proposal was rejected on grounds of illegality: A faculty member annotated the submission with the remark "We do not produce burglars." Yet its methods for harvesting credentials to bypass internet access controls closely anticipated the worm's secondary payload.

Patient zero opening the attachment

Although investigators linked de Guzman to the worm's creation and charges were filed under existing statutes, the Department of Justice subsequently dropped them. The relevant access-device law was ruled

inapplicable to computer intrusion, and the accompanying theft charge lacked sufficient evidence.

In later interviews, de Guzman acknowledged authorship, describing the worm as an experiment intended to obtain internet passwords rather than to cause global disruption. Whether framed as experiment, protest, or miscalculation, the episode marked one of the first instances in which a single individual, operating from a modest domestic setting, triggered a worldwide digital epidemic.

From the Philippines with Love

To watch **ILOVEYOU** spread on May 4, 2000, was to watch an organism outrun every institution built to contain it. It moved west with the working day, and the defensive systems of each time zone woke to find it already inside them. By 6:40 AM EDT, the US Department of Defense Joint Task Force–Computer Network Defense had registered the worm inside military systems. By 11:00 AM EDT, the US National Infrastructure Protection Center (NIPC) had posted a public advisory, describing a spread it could no longer get ahead of. By 6:00 PM EDT, more than 420,000 internet hosts had been reported infected. By the time most people understood what they were looking at, the organism had already wound its way around the world.

The outbreak exposed just how unprepared the host environment was. Investigators identified the likely author within days, but Philippine law at the time did not criminalize the creation or release of malicious code. The legal system, like the email clients the worm fed on, had

simply never evolved a defense against this kind of organism, because nothing like it had needed defending against before. Prosecutors had a suspect, but had no framework under which to charge them.

The environment adapted the way some ecosystems do after a novel predator arrives: not in time to stop the first wave, but quickly enough to meet the next. The Philippine Congress enacted the Electronic Commerce Act of 2000 (Republic Act No. 8792). Section 33 criminalized hacking, the introduction of computer viruses, and other unauthorized interference, prescribing six months to three years' imprisonment and a minimum fine of one hundred thousand pesos, with the maximum scaled to the damage done.

*Patient zero unknowingly firing out **ILOVEYOU***

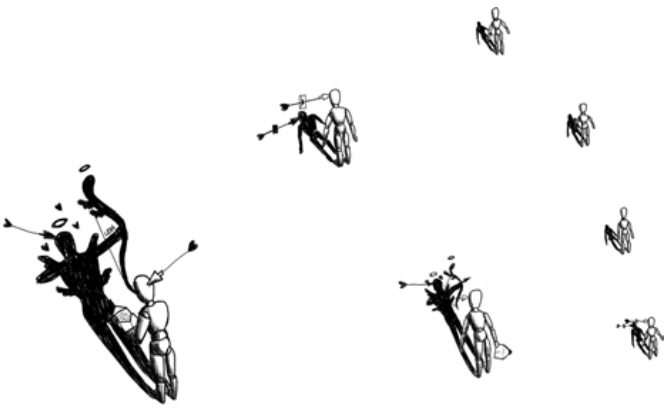
ILOVEYOU had revealed two vulnerabilities at once, one in software and one in law. Both had been built for a world in which malicious code stayed local and discreet. A

self-propagating organism forced each of them to evolve at the speed of the infrastructure it had learned to inhabit.

An Expensive Letter

The appetite of **ILOVEYOU** is best measured by what it consumed. It struck during peak business hours across Asia and Europe, reaching North America before the morning was out, and it did so with none of the restraint of its ancestors. Where the 1999 Melissa virus had mailed itself to only the first fifty contacts in an address book, **ILOVEYOU** took every entry in every available Outlook address list. It was an insatiable feeder.

Inside the US federal government, the organism found a near-uniform habitat. Of the twenty agencies later surveyed by the US General Accountability Office (GAO), only seven escaped widespread infection, most of them spared only because they did not run Microsoft Outlook, and so were not on the worm's menu. Eight reported email outages lasting more than a day. The US Department of Health and Human Services took in roughly three million infected messages, with some systems down for six days. The US Veterans Health Administration (VHA) absorbed close to seven million. The National Aeronautics and Space Administration (NASA) lost at least a thousand files. The US Department of Labor spent over sixteen hundred employee hours and twelve hundred contractor hours digging itself back out.



The exponential propagation of ***ILOVEYOU***

The organism did not respect borders between sectors any more than it respected borders between nations. AT&T, Ford Motor Company, Dow Jones, ABC News, the International Monetary Fund, and the British Parliament all went dark in its passage.

Contemporary estimates of the global damage ranged from $100 million to over $10 billion, a span so wide it reveals less about the worm than about how poorly anyone could yet measure a thing like it. The GAO itself cautioned that the indirect costs, lost productivity, and emergency-response labor could not be counted with any precision. But the lesson held regardless of where in that range the true figure fell: An organism could saturate the world's infrastructure and inflict systemic economic shock in a day, then be gone by the next.

Love Goes Viral

The outbreak revealed one last weakness, this time in the nervous system meant to sense such things coming. The GAO later concluded that federal agencies had not been effectively warned before the infection reached them, even though the machinery for centralized coordination already existed.

By the time the worm's spread exhausted itself, it was estimated to have infected between forty-five and fifty million computers, a population large enough to mark a turning point not just in security but in public awareness. For most people alive in 2000, **ILOVEYOU** was the first piece of malware they ever knew by name.

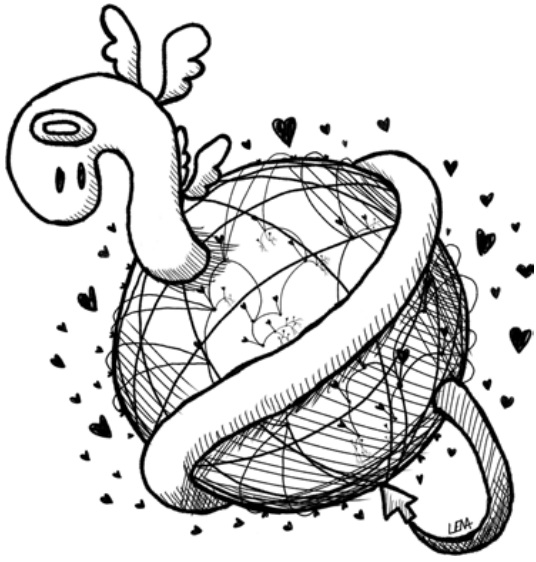
The "Love Bug" settled into collective memory as a parable about digital intimacy and the cost of misplaced trust. It taught a generation of users to be suspicious of unexpected attachments, pushed organizations to invest in antivirus infrastructure, and permanently changed how the world saw the humble email: no longer just a message, but a possible point of entry.

Ancestor of Worms

Self-propagating programs long predated **ILOVEYOU**. In 1988, the Morris worm demonstrated that code could replicate autonomously across connected UNIX systems, exploiting software vulnerabilities in sendmail, finger, and trust relationships between hosts. Though unintended in scale, the Morris worm temporarily disabled an estimated ten percent of the internet's nodes at the time and became the first major internet worm to result in

criminal prosecution under the US Computer Fraud and Abuse Act, which had became law in 1986. These early worms remained largely confined to technical communities and spread within research networks and institutional systems by exploiting configuration weaknesses.

ILOVEYOU marked a transition from experimental contagion to cultural phenomenon. It proved that mass replication did not require low-level exploitation techniques or deep system knowledge. By aligning itself with existing social networks and everyday communication habits, the worm achieved planetary reach using ordinary email infrastructure. This architecture established a reproducible template. Future worms would differ in technical implementation, but the ecological lesson endured: Connectivity amplifies replication, and trust accelerates it. In malware phylogeny, **ILOVEYOU** is pivotal. It stands between the academic worm of 1988 and the era of globally disruptive, multivector outbreaks that followed. It demonstrated that a single actor, operating with commodity tools and social insight, could trigger cascading systemic effects across governments, corporations, and households. After **ILOVEYOU**, worms rose above the limits of networked research environments and became recognized as instruments of global consequence.



***ILOVEYOU** takes over the world*