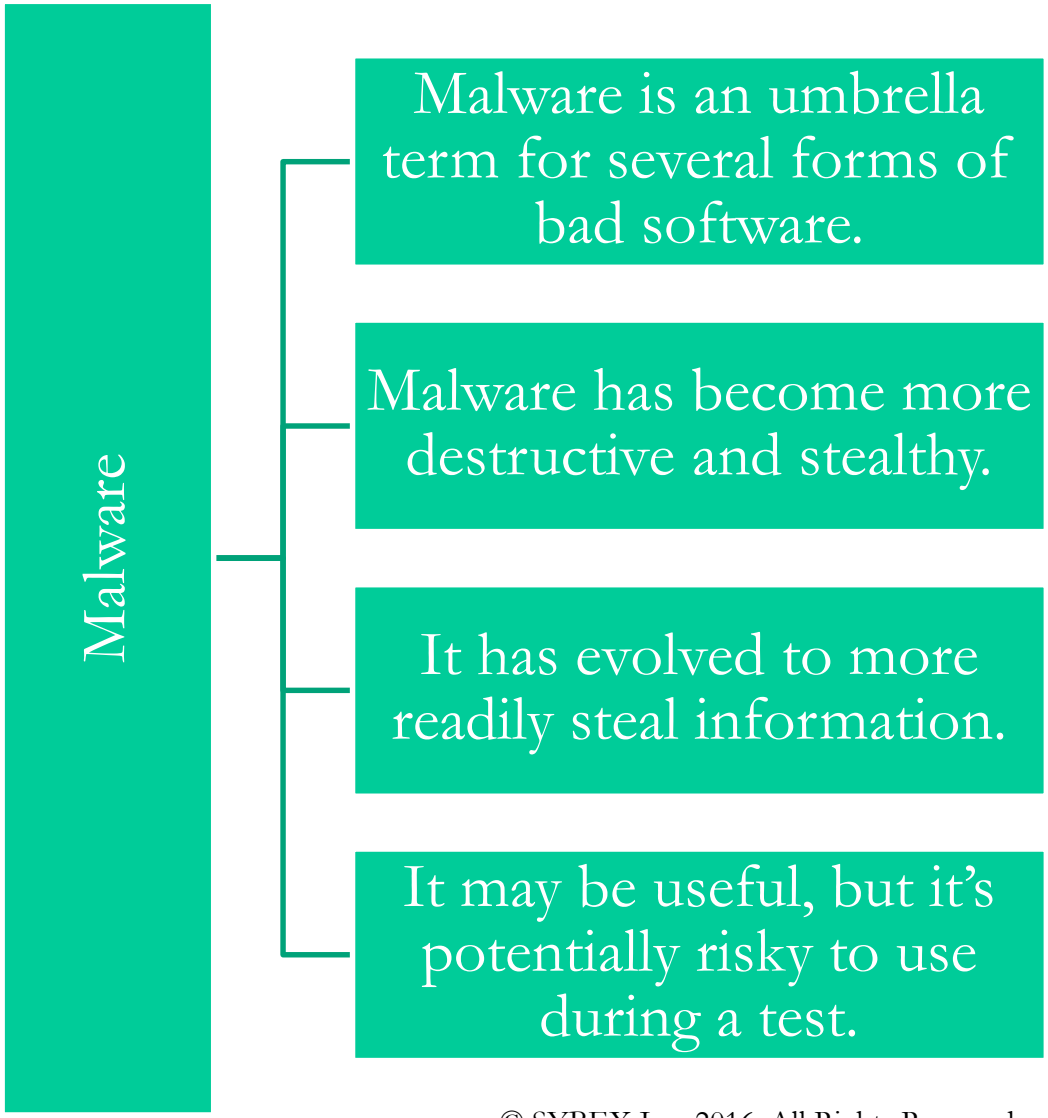
Malware

Chapter 8

SYBEX

An Overview of Malware

Malware has quickly become one of the leading problems plaguing modern technology, with several million new forms of malware created every year (by some estimates around 1,200 new pieces are created each hour).



SYBEX

Forms of Malware

Malware is anything that consumes resources and time while providing nothing in return and uses those resources to perform some operation that is counter to the system owner's best interests.

- Viruses
- Worms
- Trojan horses
- Rootkits
- Spyware
- Adware
- Ransomware

SYBEX

Authors of Malware

- Criminals
- Skilled programmers
- Casual users
- Students

SYBEX

A Closer Look at the Creators

Students and newbies

Younger computer users

Professional and experienced programmers

Researchers and testers

SYBEX

Virus Family Tree

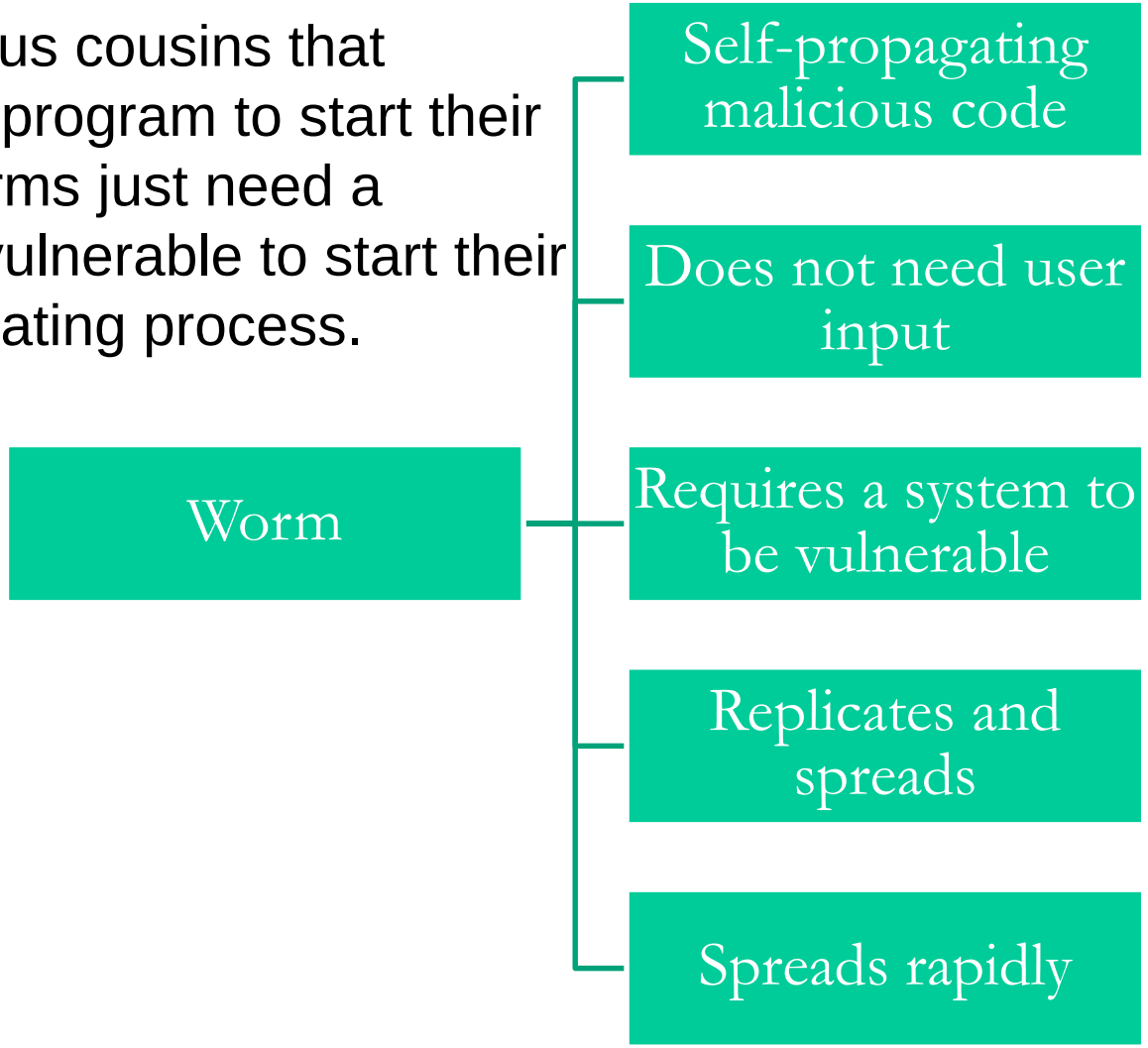
When talking about viruses, it is important that you have an understanding that not all viruses are created equal, and in fact there is a whole family of virii.

- MBR virus
- File infector virus
- Macro virus
- Service injection viruses
- Multipartite
- Polymorphic
- Encrypted

SYBEX

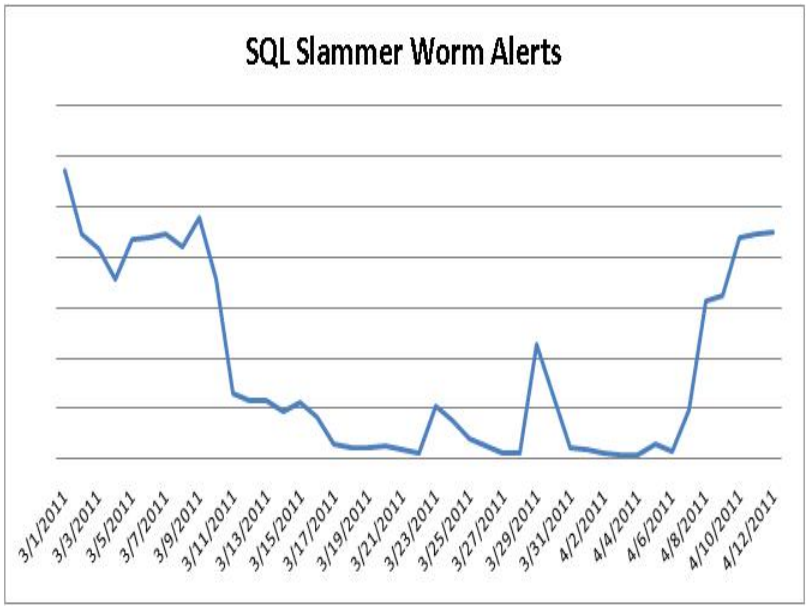
What Is a Worm?

Unlike their virus cousins that require a host program to start their dirty work, worms just need a system to be vulnerable to start their own self-replicating process.



SYBEX

Worm Example: Slammer

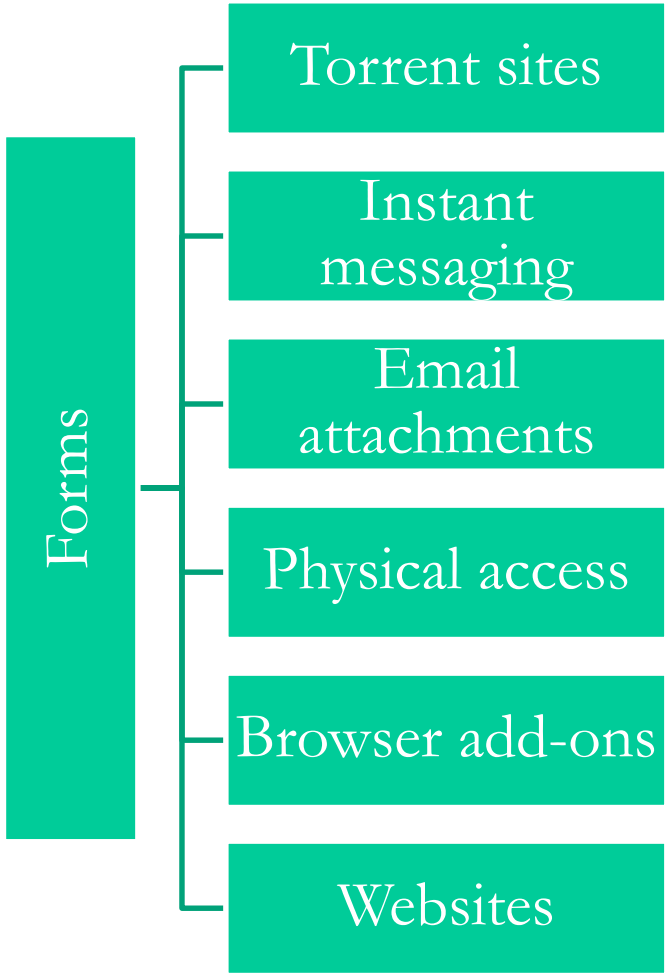


- Doubled every 8.5 seconds for first 3 minutes of life
- Ran 55 million scans at peak
- 75,000 infections in ten minutes
- Smaller in size than previous worms
- Generated random IP addresses
- Preyed on SQL Server systems

SYBEX

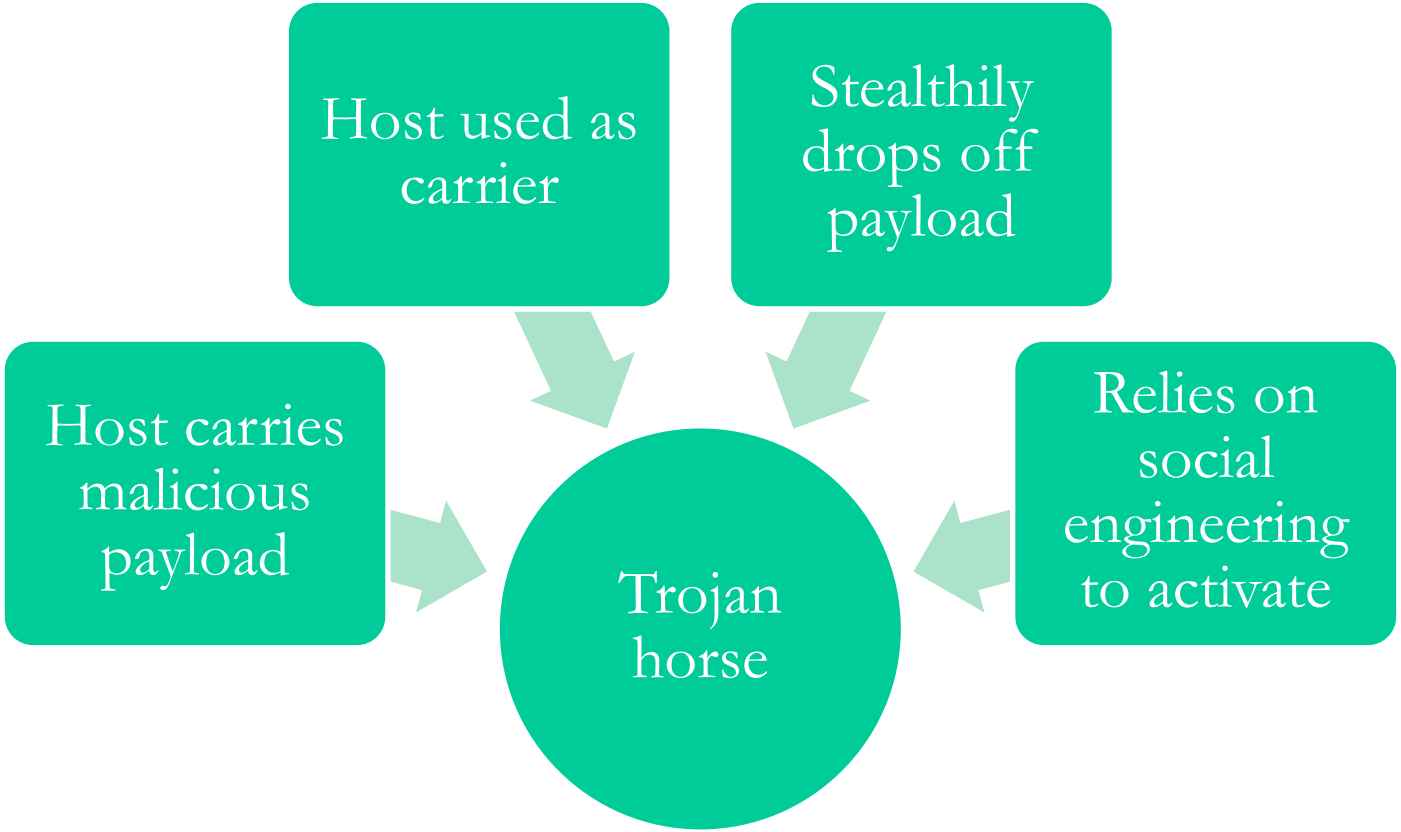
Spyware

This type of software operates in the background and out of a user's sight quietly collecting information and transmitting it to its creator.



SYBEX

Trojan Horses



By using another program as its carrier, it relies on what is known as social engineering, or taking advantage of human behavior, to carry out its actual infection.

What Do Trojans Do?

Because Trojans are so versatile and can go unnoticed, their popularity has exploded, and they've become the malware of choice for many online criminals.

- Create backdoors
- Spy
- Steal passwords
- Use your computer as a zombie
- Send SMS messages

SYBEX

Summary

- Types of backdoors
- Type of Trojans
- Categories of malware
- Malware creation kits
- Importance of keyloggers

SYBEX