جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني
DEPARTMENT OF CYBER SECURITY

SUBJECT:

MALICIOUS CODES

CLASS:

THIRD

LECTURER:

DR. SUHA ALHUSSIENY

LECTURE: (1)

MALICIOUS SOFTWARE, TYPES OF MALICIOUS SOFTWARE

Definition- :

Malware – short for malicious software – is software used or programmed by attackers to disrupt computer operation, gather sensitive information or gain unauthorized access to computers.

Malicious software or Malware is a software that designed for harm, exploit, or compromise the functionality, security of computer system, networks or devices some examples of malware are backdoor, trojan horse, worms , e - mail viruses, spyware,

TYPES OF MALICIOUS SOFTWARE

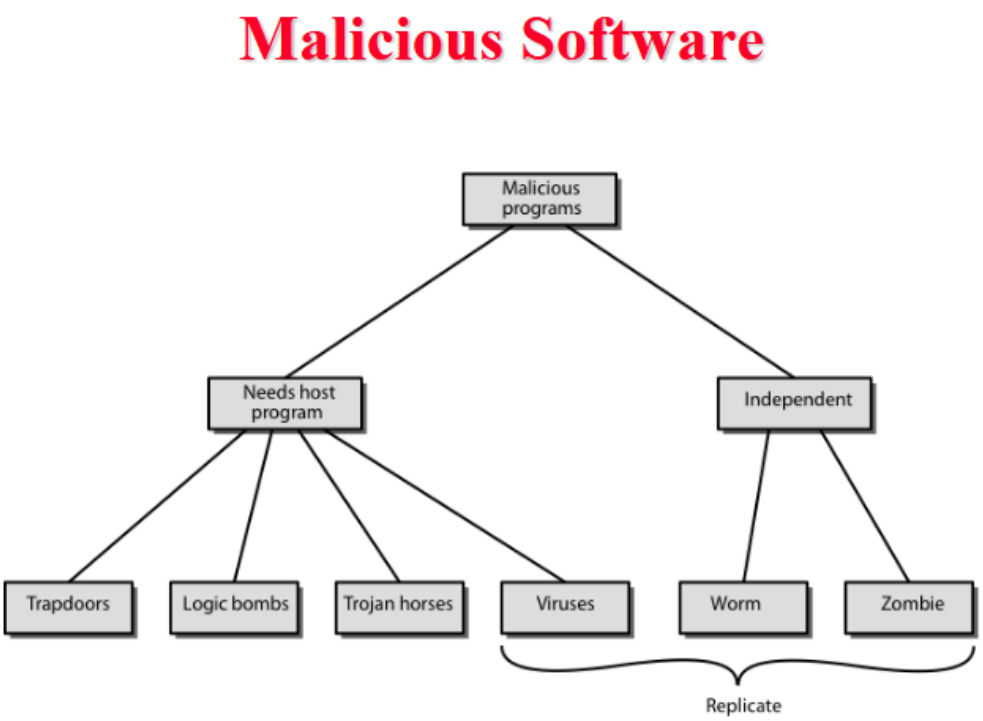
Malicious software can be divided into two categories: those that need a host program, and those that are independent. The former, referred to as parasitic, are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. Viruses, logic bombs, and backdoors are examples. Independent malware is a self-contained program that can be scheduled and run by the operating system .Worms and bot programs are examples.

We can also differentiate between those software threats that do not replicate and those that do. The former are programs or fragments of programs that are activated by a trigger.

Examples are logic bombs, backdoors, and bot programs. The latter consist of either a program fragment or an independent program that, when executed, may produce one or more copies of itself to be activated later on the same system or some other system .Viruses and worms are examples.

The main difference between a virus and a worm is that a worm does not need a host document. In other words, a worm does not need to attach itself to another program. In that sense, a worm is self-contained

On its own, a worm is able to send copies of itself to other machines over a network.



Virus: Malware which spreads from one computer to another by embedding copies of itself into files, which by some means or another are transported to the target. The medium of transport is often known as the vector of the virus. The transport may be initiated by the virus itself (for example, it may send the infected file as an e-mail attachment) or rely on an unsuspecting human user (who for example transports a CD-ROM containing the infected file.

Worm: Malware which spreads from one computer to another by transmitting copies of itself via a network which connects the computers, without the use of infected files.

Trojan horse: Malware which is embedded in a piece of software which has an apparently useful effect. The useful effect is often known as the overt effect, as it is made apparent to the receiver, while the effect of the malware, known as the covert effect، is kept hidden from the receiver.

Logic bomb: Malware which is triggered by some external event, such as the arrival of a specific date or time, or the creation or deletion of a specific data item such as a file or a database entry.

Backdoor: Malware which, once it reaches the target, allows the initiator to gain access to the target without going through any of the normal login and authentication procedures.

Zombie: Malware can turn a computer in to a zombie, which is a machine that is controlled externally to perform malicious attacks , usually as a part of a botnet.

Malicious code - reasons for increase

•Growing number and connectivity of computers

– Everybody is connected and dependant on computers

– the number of attacks increases

–attacks can be launched easily (automated attacks(

•Growing system complexity

– unsafe programming languages

–heterogeneity

–hiding code is easy

–verification and validation is impossible (let alone proofs(

•Systems are easily extensible

–mobile code, dynamically loadable modules

– incremental evolution of systems

Backdoor

A backdoor, also known as a trapdoor, is a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures. Programmers have used backdoors legitimately for many years to debug and test programs; such a backdoor is called a maintenance hook. This usually is done when the programmer is developing an application that has an authentication procedure, or a long setup, requiring the user to enter many different values to run the application. To debug the program, the developer may wish to gain special privileges or to avoid all the necessary setup and authentication. The programmer may also want to ensure that there is a method of activating the program should something be wrong with the authentication procedure that is being built into the application. The backdoor is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.

✓**A backdoor** is a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms. Web server backdoors are used for a number of malicious activities, **including:**

- Data theft
- Website defacing
- Server hijacking
- Infecting website visitors

How does a backdoor work?

Backdoors are used by hackers to gain access to a device by circumventing security mechanisms. Often time's developers install backdoors as a means of troubleshooting their program, but this also leaves a gap for hackers to exploit. The term is often used to describe vulnerabilities put in place on purpose, for example, to allow government surveillance groups to access citizens' smart phones and computers.

step by step

1. **Initial access / foothold.**
    - The attacker first gets into the environment by exploiting a vulnerability, phishing, stolen credentials, or supply-chain compromise.
2. **Install the backdoor.**
    - The attacker places code or config changes that allow future access without normal login: e.g., a hidden user account, a web shell on a web server, a modified service that listens on a secret port, or a persistent agent.
3. **Ensure persistence.**
    - The backdoor is made to survive reboots and updates: it may add startup scripts, scheduled tasks, service units, or modify boot components.
4. **Hide and evade.**
    - Techniques include changing file metadata, process hiding, hooking system calls, using encryption, polymorphism, or placing code in obscure locations.
5. **Command & control (C2) or direct access.**

- The backdoor may open a remote channel (reverse shell, encrypted C2 traffic) or give an attacker an always-on admin account to log in.

6. **Use & expand.**
   - Attacker uses the backdoor to exfiltrate data, move laterally, drop more tools, or recruit the host into a botnet.
7. **Self-clean / stealth.**
   - Some backdoors remove traces of installation or modify logs to hide activity.

Common types of backdoors

- **Hidden user accounts / credentials**
  A new user account or SSH key that looks legitimate but is only known to the attacker.
- **Web shells / webserver backdoors**
  Small server-side scripts (PHP/ASP/Python) uploaded to a website that allow file upload, command execution, or database access.
- **Rootkits / kernel backdoors**
  Deeper implants that hook kernel APIs to hide processes, files, or network connections.
- **Firmware or BIOS backdoors**
  Backdoors embedded in device firmware, persisting across OS reinstallations.

How attackers communicate with a backdoor

- **Reverse connection:** host connects out to attacker (evades inbound firewall rules).

- **Beaconing:** periodic small, encrypted requests to a C2 server to retrieve commands.
- **Outbound channels via common protocols:** HTTP(S), DNS, or legitimate cloud services (abuse of Slack, GitHub, Blob storage).
- **Direct login:** attacker logs in using backdoor account or key.

Detection methods & tools (defensive)

- **Network monitoring:** Netflow, IDS/IPS, EDR network sensors, anomaly detection for beaconing.
- **Host monitoring:** Endpoint Detection & Response (EDR), process whitelisting, integrity checking (file hashes).
- **Log analysis:** Centralized logging (SIEM) with alerts for new users, new services, or scheduled task changes.
- **Baseline & integrity:** Maintain a known-good baseline (file checksums) and watch for deviations.
- **Honeypots / canaries:** Plant decoy accounts or files to catch attackers using backdoors.
- **YARA / signatures:** Use YARA rules or signatures to detect known web shell strings or suspicious patterns (rules for detection — *not* for exploitation).

How to prevent backdoors — practical hardening steps

- Strong password policies and multi-factor authentication (MFA).
- Least privilege: users and services only get the permissions they need.
- Code review and change-control processes (reduce insider backdoors).

- Patch management (OS, apps, firmware) — many backdoors start from known vulnerabilities.
- Disable unused services/ports and harden exposed services (rate limit, IP allowlists).
- Network segmentation and egress filtering (limit where hosts can connect).
- Monitor for unusual account creation, scheduled tasks, or startup changes.
- Maintain offsite backups and test recovery (in case attacker tries to destroy backups).
- Rotate and audit keys and certificates periodically.

Real-world examples

- **Web shells** uploaded to compromised web servers, used as persistent access points.
- **RATs (Remote Access Trojans)** that create long-lived access channels.

Supply-chain incidents where legitimate software releases include hidden backdoors (e.g., tainted updates).

H.W

1. Malware is short for:

2. Which malware type requires a host program?

3. Which malware type is self

contained and runs independently?

4. A worm spreads mainly through:

5. A Trojan horse hides its malicious action as:

6. Malware activated by specific time or event is:

7. A backdoor allows attackers to bypass:

8. A zombie computer is mainly used in:

9. Which malware replicates itself inside files?

10. Which malware does NOT need to attach to files?

11. The main transport of

12. Which malware is triggered by deletion of a file?

13. A hidden account created by attacker is a type of:

14. Malware embedded in firmware is called:

15. Which malware spreads via e

16. Which malware effect is hidden from the user?

17. Which is a method attackers use for backdoor communication?

18. A system turned into a zombie is controlled:

19. Which factor increases malicious code

20. Which defensive technique detects web shells?

21 . A backdoor is also

22 . Which is an example of a webserver

23 . A backdoor hidden in hardware is known as:

24 . Which is NOT a backdoor type?

25 . One way attackers communicate with