SECURITY OF COMPUTER SYSTEMS

Introduction to Malware

The contraction of **mal**icious soft**ware** known as **malware**.

Malware is any piece of software that is designed with the intent to damage, disrupt or gain unauthorised access to your device and inflict harm to data and/or people in multiple ways.

It is one of the biggest threats on the internet

and it comes in a bewildering variety of forms, each with its own method of delivery

Malware Attacks Examined

Malware discussion typically encompasses three main aspects:

- Objective: What the malware is designed to achieve
- Delivery: How the malware is delivered to the target
- Concealment: How the malware avoids detection (this item is beyond the scope of this discussion)

Objectives

- Malware is created with an objective in mind. While it could be said that the objective is "limited only to the imagination of its creator," this will focus on some of the most common objectives observed in malware.

Exfiltrate Information

- Stealing data, credentials, payment information, etc. is a recurring theme in the realm of cybercrime. Malware focused on this type of theft can be extremely costly to a person, company, or government target that falls victim.

Disrupt Operations

- Actively working to “cause problems” for a target’s operation is another objective seen in malware. From a virus on a single computer corrupting critical OS files (making that one system unusable) to an orchestrated, physical self-destruction of many systems in an installation, the level of “disruption” can vary. And there’s also the scenario where infected systems are directed to carry out large-scale distributed denial of service attacks.

- Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.

Examples of Malware:

- Trojan Horse
- Backdoor
- Rootkit
- Ransomware
- Adware
- Virus
- Worms
- Spyware
- Botnet
- Crypter

Different Ways a Malware can Get into a System

- Instant Messenger applications
- IRC (Internet Relay Chat)
- Removable devices
- Attachments
- Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- Browser and email software bugs
- NetBIOS (FileSharing)
- Fake programs
- Untrusted sites and freeware software
- Downloading files, games, and screensavers from Internet sites

Common Techniques Attackers Use to Distribute Malware on the Web

- **Blackhat Search Engine Optimization (SEO):** Ranking malware pages highly in search results.
- **Malvertising:** Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites.
- **Compromised Legitimate Websites:** Hosting embedded malware that spreads to unsuspecting visitors.

- **Social Engineered Click-jacking:** Tricking users into clicking on innocent-looking web pages.

- **Spear phishing Sites:** Mimicking legitimate institutions is an attempt to steal login credentials.

- **Drive-by Downloads:** Exploiting flaws in browser software to install malware just by visiting a web page.

Types of attacks

1. Worms

- Worms are spread via software vulnerabilities or phishing attacks. Once a worm has installed itself into your computer's memory, it starts to infect the whole machine and in some cases… your whole network.
- Depending on the type of worm and your security measures, they can do serious damage. These parasitic nasties can…
- **Modify and delete files**
- **Inject malicious software onto computers**
- **Replicate themselves over and over to deplete system resources**
- **Steal your data**
- **Install a convenient backdoor for hackers**
- They can infect large numbers of computers fast, consuming bandwidth and overloading your web server as they go.

2. Viruses

- Unlike worms, viruses need an already-infected active operating system or program to work. Viruses are typically attached to an executable file or a word document.

- Most people are probably aware that a .exe file extension could lead to issues if it's not from a trusted source. But there are hundreds of other file extensions that denote an executable file.

- Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus is able to replicate itself and spread through your systems.

- For computer viruses, your contact list is the equivalent of a packed train for the common cold. It hijacks your applications and uses your own apps to sneeze all over everyone… sending out infected files to your colleagues, friends and clients. Because it looks like it's coming from a trustworthy source (you!), it has a much higher chance of spreading.

3. Bots & Botnets

- A bot is a computer that's been infected with malware so it can be controlled remotely by a hacker.
- That bot (aka a zombie computer), can then be used to launch more attacks or to become part of a collection of bots (aka a botnet).
- Botnets are popular with hacker show-offs (the more bots you collect, the mightier a hacker you are) and cyber criminals spreading ransomware. Botnets can include millions of devices as they spread undetected.

Botnets help hackers with all manner of malicious activities, including:

- **DDOS Attacks**
- **Keylogging, screenshots and webcam access**
- **Spreading other types of malware**
- **Sending spam and phishing messages**

4. Trojan Horses

- Just as it sounds, a Trojan Horse is a malicious program that disguises itself as a legitimate file. Because it looks trustworthy, users download it and… hey presto, in storms the enemy.
- Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once you've got the Trojan on your device, hackers can use it to…
- **Delete, modify and capture data**
- **Harvest your device as part of a botnet**
- **Spy on your device**
- **Gain access to your network**

5. Ransomware

- Ransomware denies or restricts access to your own files. Then it demands payment (usually with crypto-currencies) in return for letting you back in.
- In May 2017, a ransomware attack spread across 150 countries and compromised over 200k computers within just one day. Aptly named WannaCry, the attack caused damage estimated in the hundreds of millions to billions of dollars.
- WannaCry affected MS Operating systems that did not have the latest patch installed for a known vulnerability. To reduce the risk of ransomware attacks…
- **Always keep your Operating System up to date**
- **Keep your Anti-Virus software up to date**
- **Back-up your most important files**
- **Don't open attachments from unknown sources (WannaCry was spread via a .js attachment)**

6. Adware & Scams

- Adware is one of the better-known types of malware. It serves pop-ups and display ads that often have no relevance to you.

- Some users will put up with certain types of adware in return for free software (games for example). But not all adware is equal. At best, it's annoying and slows down your machine.

- At worst, the ads link to sites where malicious downloads await unsuspecting users. Adware can also deliver Spyware and is often easily hacked, making devices that have it installed a soft target for hackers, phishers and scammers.

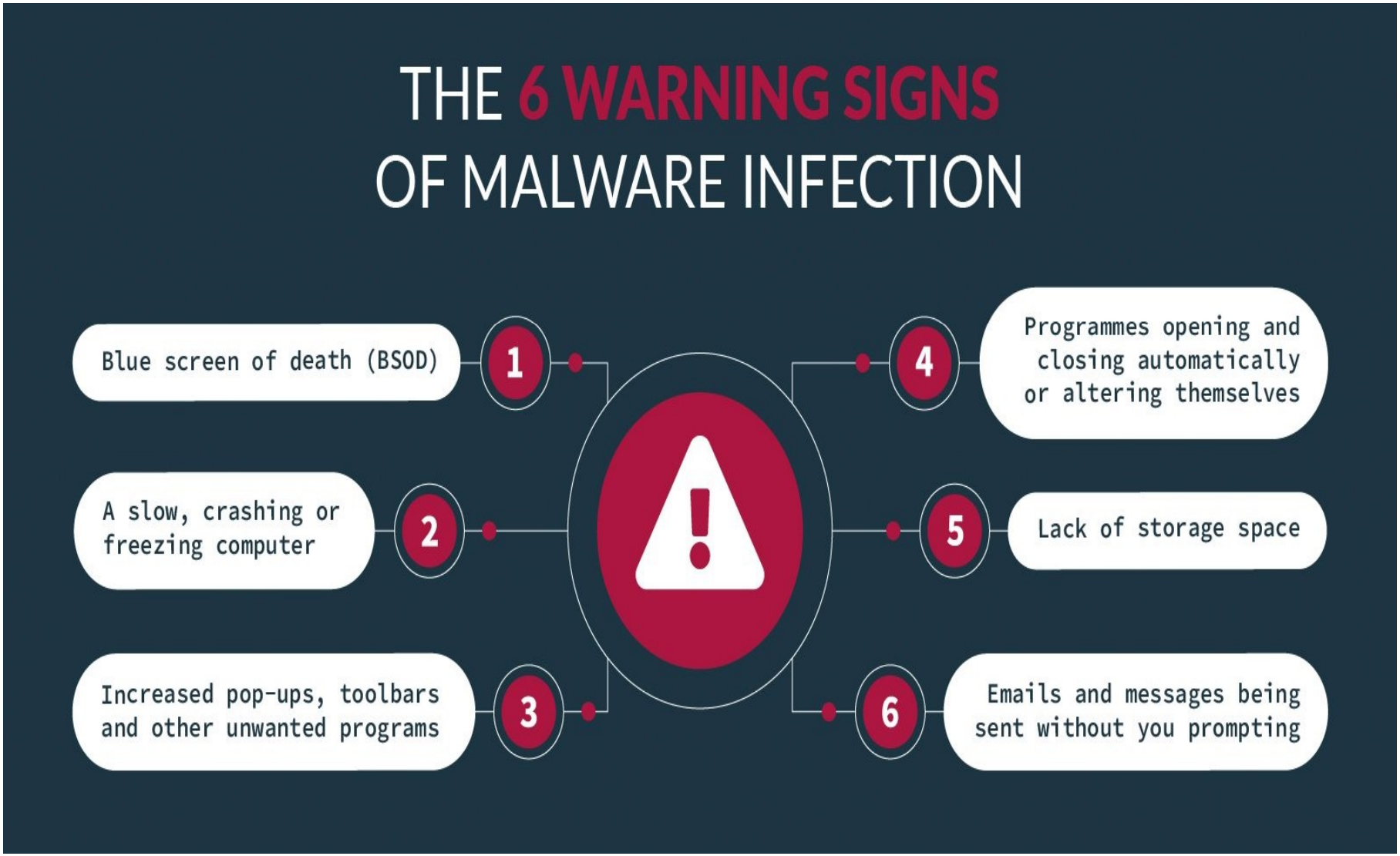
7. Spyware

- Spyware secretly records your online activity, harvesting your data and collecting personal information such as usernames, passwords and surfing habits.
- Spyware is a common threat, usually distributed as freeware or shareware that has an appealing function on the front end with a covert mission running in the background that you might never notice. It's often used to carry out identity theft and credit card fraud.
- Once on your computer, spyware relays your data to advertisers or cyber criminals. Some spyware installs additional malware that make changes to your settings.

8. Spam & Phishing

- Phishing is a type of social engineering attack, rather than a type of malware. But is a common method of cyber attack . Phishing is successful since the emails sent, text messages and web links created look like they’re from trusted sources. They’re sent by criminals to fraudulently acquire personal and financial information.
- Some are highly sophisticated and can fool even your most savvy users. Especially in cases where a known contact’s email account has been compromised and it appears you’re getting an instruction from your boss or IT colleagues. Others are less sophisticated and simply spam as many emails as they can with a message about ‘checking your bank account details’.

Warning signs of malware infection



If you've noticed any of the following, you may have malware on your device:

- A slow, crashing or freezing computer
- Blue screen of death (BSOD)
- Programmes opening and closing automatically or altering themselves
- Lack of storage space
- Increased pop-ups, toolbars and other unwanted programs
- Emails and messages being sent without you prompting them

Password Attacks

Most widely used types of attacks are

- Password Guessing
  The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always as difficult as you'd expect.
- Password Resetting
  Attackers often find it much easier to reset passwords than to guess them. Many password cracking programs are actually password resetters.
- Password sniffing

  Some password crackers can sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process.

- Password Capturing
  Many attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the Internet. Symantec reports that 82 percent of the most commonly used malware programs steal confidential information.
- password cracking
- It is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password. The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or to act as a preventive measure whereby system administrators check for easily crackable passwords.

Password Attack Methods

1. Brute Force Attack

- One of the most common forms of password attack methods, and the easiest for hackers to perform. In fact, inexperienced hackers favor this method precisely because of this.
- In a brute force attack, a hacker uses a computer program to login to a user's account with all possible password combinations. Moreover, brute force accounts don't start at random; instead, they start with the easiest-to-guess passwords.

2. Dictionary Attack

- Conversely, a dictionary attack allows hackers to employ a program which cycles through common words. A brute force attack goes letter by letter, whereas a dictionary attack only tries possibilities most likely to succeed.
- Also, dictionary attacks rely on a few key factors of users' psychology. For example, users tend to pick short passwords and base their passwords off common words. So a dictionary attack starts with those words and variations (adding numbers at the end, replacing letters with numbers, etc.).

3. Phishing

- Usually, hackers disguise their phishing attacks as unsuspecting emails posing as legitimate and known services. From these emails, hackers take users to fake login pages disguised as the legitimate service. Often, the hackers add a subtle, threatening dimension to their emails like the prospect of service cancellation. This forces the users to hand over their credentials before giving it careful consideration.
- Also, a variation of phishing attack is the social engineering attack. These identity attacks use the social conventions of the workplace to fool users. Hackers could pose as the IT team and directly ask users for their passwords without risking detection.
- Finally, phishing facilitates password guessing, but of course, hackers can always just guess with the information they find online. Distressingly, they often turn out to be right in the end.

4. Rainbow Table Attack

- Wisely, enterprises often hash their users' passwords; hashing entails mathematically converting caches of passwords into cryptographic, random-looking strings of characters to prevent them from being misused. If hackers can't read the passwords, they can't abuse them.
- A rainbow table compiles a list of pre-computed hashes. It already has the mathematical answers for all possible password combinations for common hash algorithms. Like many identity management threats, this one uses time to its advantage.

5. Credential Stuffing

- In a credential stuffing attack, hackers use lists of stolen usernames and passwords in combination on various accounts, automatically trying over and over until they hit a match.
- Credential stuffing relies on users' tendency to reuse their passwords for multiple accounts, often to great success. Further, hackers share stolen passwords on the Dark Web or sell them, so this information proliferates among threat actors.
- Technically, credential stuffing falls under the umbrella of brute force password attack methods. Yet it proves incredibly effective because it uses known passwords.

6. Password Spraying

- password spraying expands the potential targets exponentially. Thus, it helps hackers avoid account lockout policies which would trigger on repeat login failures. At the very least, it mitigates their effectiveness.
- Surprisingly, these password attack methods tend to move slowly. Hackers prefer to attack methodically from account to account, trying different passwords. This allows the timers on account lockout detection tools to revert before moving back with a different password. Password spraying can be particularly dangerous for single sign-on or cloud-based authentication portals.

7. Keylogger Attack

- keylogger attacks install a program on users' endpoints to track all of a users' keystrokes.
- So as the user types in their usernames and passwords, the hackers record them for use later. This technically falls under the category of malware or a digital virus, so it must first infect the users' endpoints.

Denial-of-Service

What is a Denial-of-Service Attack?

- Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.
- In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources.
- DoS attack leads to unavailability of a particular website and show network performance.

Basic Categories of DoS/DDoS Attack Vectors

- **Volumetric Attacks:** Consumes the bandwidth of target network or service.
- **Fragmentation Attacks:** Overwhelms target's ability of re-assembling the fragmented packets.
- **TCP State-Exhaustion Attacks:** Consumes the connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers.
- **Application Layer Attacks:** Consumes the application resources or service thereby making it unavailable to other legitimate users.

DoS/DDoS Attack Techniques

- Bandwidth Attacks and Service Request Floods
- SYN Flooding Attack
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Application-Level Flood Attacks
- Permanent Denial-of-Service Attack
- Distributed Reflection Denial of Service (DrDoS)

Unauthorized Access

- Unauthorized access refers to individuals gaining access to an organization's data, networks, endpoints, applications or devices, without permission. It is closely related to authentication – a process that verifies a user's identity when they access a system. Broken, or misconfigured authentication mechanisms are a main cause of access by unauthorized parties.

common causes of unauthorized access

- Weak passwords selected by users, or passwords shared across services
- Social engineering attacks, primarily phishing, in which attackers send messages impersonating legitimate parties, often with the aim of stealing user credentials
- Compromised accounts – attackers often seek out a vulnerable system, compromise it, and use it to gain access to other, more secure systems

- Insider threats – a malicious insider can leverage their position to gain unauthorized access to company systems
- Zeus malware – uses botnets to gain unauthorized access to financial systems by stealing credentials, banking information and financial data
- Cobalt strike – a commercial penetration testing tool used to conduct spear-phishing and gain unauthorized access to systems

Immediate security risks posed by unauthorized access

By gaining unauthorized access to organizational systems or user accounts, attackers can:

- Steal or destroy private data
- Steal money or goods by carrying out fraud
- Steal user identities
- Compromise systems and use them for illegitimate or criminal activity
- Sabotage organizational systems or deface websites
- Cause physical damages – by gaining access to connected devices

Types of Unauthorized Access

1. Tailgating

- One of the most common types of unauthorized access is tailgating, which occurs when one or more people follow an authorized user through a door. Often the user will hold the door for an unauthorized individual out of common courtesy, unwittingly exposing the building to risk. One way to decrease the likelihood of tailgating is by giving training to all credentialed users on security and awareness. An even more effective reduction technique is to implement turnstiles, mantraps or another solution that restricts entry to one individual at a time and generates an alarm if someone tries to circumvent it.

2. Door Propping

- Similar to tailgating, propping doors open, most often for convenience, is another common way unauthorized individuals gain access to a location and potentially create a dangerous situation for the people and assets within. Some access control systems include the capability to detect when doors are propped and alert security personnel, who can respond and investigate the situation as needed.

3. Levering Doors

- You might be surprised to know how easily many doors can be levered open using something as small as a screwdriver or as large as a crowbar. Advanced access control systems include forced-door monitoring and will generate alarms if a door is forced. The effectiveness of these systems varies, with many systems prone to a high rate of false positives, poor database configuration or lack of active intrusion monitoring. With these tools and tactics in place, however, they are highly effective at detecting door levering.

4. Keys

- Whether stolen, lost or loaned out, keys pose a major problem. They are often impossible to track when lost, forgotten, stolen or loaned to someone else, and if an individual tends to tailgate to enter the building, he or she may not notice missing keys for several days. During that time, there is huge risk, and the only way to ensure the continued security of a building is to re-core locks on multiple doors, which can be very expensive. Electronic key management solutions can be deployed to track keys, with the added benefit that many of these systems can be integrated with access control for an added layer of security.

5. Access Cards

- With the added advantage of identifying authorized users who swipe in with an access control reader, electronic key cards are a more high-tech alternative to traditional keys. However, they are prone to the same risks associated with keys, namely the potential to be lost, stolen or shared with an authorized or unauthorized person.

Best Practices to Prevent Unauthorized Access

1. Strong Password Policy
2. Two Factor Authentication (2FA) and Multifactor Authentication
3. Physical Security Practices
4. Monitoring User Activity
5. Endpoint Security

Privilege escalation

- Privilege escalation is a common way for attackers to gain unauthorized access to systems within a security perimeter.
- Attackers start by finding weak points in an organization's defenses and gaining access to a system. In many cases that first point of penetration will not grant attackers with the level of access or data they need. They will then attempt privilege escalation to gain more permissions or obtain access to additional, more sensitive systems.

Horizontal vs. Vertical Privilege Escalation

There are two types of privilege escalation:

- Horizontal privilege escalation—an attacker expands their privileges by taking over another account and misusing the legitimate privileges granted to the other user.
- Vertical privilege escalation—an attacker attempts to gain more permissions or access with an existing account they have compromised. For example, an attacker takes over a regular user account on a network and attempts to gain administrative permissions. This requires more sophistication and may take the shape of an Advanced Persistent Threat.

- There are many privilege escalation methods in Windows operating systems. Here is a brief review of three common methods and how you can prevent them.

Access Token Manipulation

- **Attack description**
  Windows uses access tokens to determine the owners of running processes. When a process tries to perform a task that requires privileges, the system checks who owns the process and to see if they have sufficient permissions. Access token manipulation involves fooling the system into believing that the running process belongs to someone other than the user who started the process, granting the process the permissions of the other user.
- **Techniques**
  There are three ways to achieve access token manipulation:
- **Duplicating an access token** using the Windows DuplicateToken(Ex) and then using ImpersonateLoggedOnUserfunction or SetThreadToken function to assign the impersonated token to a thread.

- **Creating a new process with an impersonated token** using the DuplicateToken(Ex) function together with the CreateProcessWithTokenW function.
- **Leveraging username and password to create a token** using the LogonUser function. The attacker possesses a username and password, and without logging on, they create a logon session, obtain the new token and use SetThreadToken to assign it to a thread. In this method, an adversary has a username and password, but the user is not logged
- **Mitigation**
  There is no way to disable access tokens in Windows. However, to perform this technique an attacker must already have administrative-level access. The best way to prevent the attack is to assign administrative rights in line with the least-privilege principle, regularly review administrative accounts and revoke them if access is no longer needed. Also, monitor privileged accounts for any sign of anomalous behavior.

Bypass User Account Control

- **Attack description**
  The Windows user account control (UAC) mechanism creates a distinction between regular users and administrators. It limits all applications to standard user permissions unless specifically authorized by an administrator, to prevent malware from compromising the operating system. However, if UAC protection is not at the highest level, some Windows programs can escalate privileges, or execute COM objects with administrative privileges.
- **Mitigation**
  Review IT systems and ensure UAC protection is set to the highest level, or if this is not possible, apply other security measures. Regularly review which accounts are a local administrator group on sensitive systems and remove regular users who should not have administrative rights.

BACKDOOR ATTACKS

- The backdoor attack is a type of malware that is used to get unauthorized access to a website by the cybercriminals. The cybercriminals spread the malware in the system through unsecured points of entry, such as outdated plug-ins or input fields.

Web server backdoors are used for a number of malicious activities, including:

- Data theft
- Website defacing
- Server hijacking
- The launching of distributed denial of service (DDoS) attacks
- Infecting website visitors (watering hole attacks)
- Advanced persistent threat (APT) assaults

How to protect

- Good news bad news. The bad news is that it's difficult to identify and protect yourself against built-in backdoors. More often than not, the manufacturers don't even know the backdoor is there. The good news is that there are things you can do to protect yourself from the other kinds of backdoors.

1. Change your default passwords
2. Monitor network activity
3. Choose applications and plug-ins carefully
4. Use a good cyber security solutions