The anatomy of malware attacks

To infect a computer through a web browser, an attacke must accomplish two tasks. First, they must find a way to connect with the victim. Next, the attacker must install malware on the victim's computer. Both of these steps can occur quickly and without the victim's knowledge, depending on the attacker's tactics.

One way for an attacker to make a victim's browser execute their malicious code is to simply ask the victim to visit a web site that is infected with malware. Of course, most victims will not visit a site if told it is infected, so the attacker must mask the nefarious intent of the web site. Sophisticated attackers use the latest delivery mechanisms, and often send malware-infected messages over social networks, such as Facebook, or through instant messaging systems. While these methods have proved successful to a degree, they still rely on tempting a user to visit a particular web site.

Other attackers choose to target web sites that potential victims will visit on their own. To do this, an attacker compromises the targeted web site and inserts a small piece of HTML code that links back to their server. This code can be loaded from any location, including a completely different web site. Each time a user visits a web site compromised in this manner, the attacker's code has the chance to infect their system with malware.

Common types of malware delivery mechanisms:

- **Software updates:** Malware posts invitations inside social media sites, inviting users to view a video. The link tries to trick users into believing they need to update their current software to view the video. The software offered is malicious.
- **Banner ads:** Sometimes called "malvertising," unsuspecting users click on a banner ad that then attempts to install malicious code on the user's computer. Alternatively, the ad directs users to a web site that instructs them to download a PDF with heavily-obscured malicious code, or they are instructed to divulge payment details to download a PDF properly.
- **Downloadable documents:** Users are enticed into opening a recognizable program, such as Microsoft Word or Excel, that contains a preinstalled Trojan horse.
- **Man-in-the-middle:** Users may think they are communicating with a web site they trust. In reality, a cybercriminal is collecting the data users share with the site, such as login and password. Or, a criminal can hijack a session, and keep it open after users think it has been closed. The criminal can then conduct their malicious transactions. If the user was banking, the criminal can transfer funds. If the user was shopping, a criminal can access and steal the credit card number used in the transaction.
- **Keyloggers:** Users are tricked into downloading keylogger software using any of the techniques mentioned above. The keylogger then monitors specific actions, such as mouse operations or keyboard strokes, and takes screenshots in order to capture personal banking or credit card information.

IT'S Simple We Prevent All of This