The 4 most common ways to spread malware today

If there's one thing that poses a threat to all users of technology, it's malware. This malware can be extremely dangerous, harmful, and comes in many different forms.

But how did malware become so common? What are the main tactics and tools used by cybercriminals to infect devices?

1. Malicious Downloads

Today, there are countless types of software that you can download from the Internet. But the wide availability of programs on so many different websites has created a great opportunity for cybercriminals to find a way to infect devices with malware as easily as possible.

If you are not using a completely legitimate website to download software, such as a developer, you always run the risk of downloading a malicious program. This could be something as potentially less harmful as adware, but it could also be as serious as ransomware or a harmful virus.

Because people often don't check if a file is safe before downloading or don't even know what signs they should look for, this infection route is extremely popular among criminals. network. So, what can you do to avoid downloading malicious stuff?

First, you should make sure that you only download files from trusted websites. It can sometimes be difficult to find the right file to download for your particular operating system or OS version, but don't let this inconvenience lead you to a suspicious website. Of course, it can sometimes be difficult to determine if a website is legit, but you can use a link checker site to get around this hurdle.

Also, if the software you're looking for is usually paid and you see a "free" version to download, this is extremely suspicious. While it may seem tempting to try the free version of an expensive program, it can put you in a much worse situation if there's malware lurking in the file.

You can also use any anti-virus software you have installed to scan files before downloading, or use scanning sites like VirusTotal to quickly check any file for free.

2. Email phishing

Phishing is one of the most commonly used forms of cybercrime today. This is mainly because most people can be contacted via email, text message, or direct message. On top of that, cybercriminals can easily deceive victims through a phishing message using convincing or professional language, as well as the right type of format and images.

In an online scam, an attacker sends their target a message claiming to be some official, trusted party. For example, an individual may receive an email from the post office informing them that their package has been diverted and that they need to provide certain information in order for it to be safely delivered. This type of emergency communication works effectively in forcing the receiver to comply with the sender's request.

In this phishing email there will be a link that the target is asked to click on to enter their details, verify an action or do something similar. However, in reality, this link is completely malicious. In most cases, the website will be designed to steal any data you enter, such as your contact details or payment information. But phishing can also be used to spread malware through supposedly "safe" or "official" links that attackers send you. In this case, you may have put yourself in danger right after clicking the link.

Again, a link checker site is very helpful for your safety, especially when it comes to phishing, as it allows you to instantly determine how safe any given URL is.

Above all, it's important to check emails for typos, unusual sender addresses, and suspicious attachments. For example, if you received an email from FedEx, but the email address says something slightly different, such as "f3dex", you may be dealing with a phishing attack. Running such a quick test can help you avoid unnecessary risks.

3. Remote Desktop Protocol

Remote Desktop Protocol (RDP) is a technology that allows a user's computer to connect directly to another computer over a network. Although this protocol was developed by Microsoft, it can now be used on a wide range of different operating systems, making it accessible to almost anyone. As usual, however, cybercriminals have developed a way to exploit this popular tool.

Sometimes, RDP can be poorly protected or left open on an old system, which gives an attacker a perfect attack chance. Fraudsters find these insecure systems using popular scanning tools. When an attacker finds a vulnerable connection and is able to access a remote computer via the protocol, they can infect that computer with malware and even get data from the device. infected without the owner's permission.

Ransomware has become a common problem among RDP users. In fact, Paloalto's 2020 Unit 42 Incident Response and Data Breach Report shows that, of the 1,000 recorded ransomware attacks, 50% used RDP as the initial means of infection. This is a type of malware that encrypts the victim's files and holds them hostage until the attacker's (usually financial) demands are met. The attacker will then provide the victim with the decryption key, although there is no guarantee that they will do this.

To protect your device when using RDP, it's important to use strong passwords, use two-factor authentication, and update servers whenever possible to make sure you're using the software. most secure.

4. USB

While it is easy to infect a device with malware remotely, that doesn't mean it still can't be done physically. If an attacker happens to have direct access to a victim's device, using a USB can be a quick and easy way to get malware to install.

Malicious USB drives are often equipped with malicious code that can collect data available on the victim's device. For example, a drive could infect a device with a keylogger, which can track everything a victim enters, including logins, payment details, and sensitive contact information.

Using USB, an attacker can basically download any type of malware to the device, including ransomware, spyware, viruses, and worms. This is why it's important to password protect all your devices and power off or lock them whenever you're not around.

You can also disable your USB ports if you have to turn on your computer while away.

In addition, you should avoid using any USB that you do not know its contents or scanning any drive with anti-virus software before.

Cybercriminals continue to develop new ways to spread malware and attack victims. It's important that you protect your device in every way possible and double-check any software, files, and links before downloading or accessing them. Simple little steps like these can keep you safe from malicious entities.