Devolutions

Spyware: What It Is, What It Does & What to Do About It

SPYWARE IS A STRAND OF MALWARE THAT IS DESIGNED TO SECRETLY INFILTRATE A VICTIM'S COMPUTER

In the James Bond franchise, spies are elegant and sophisticated subversives who can climb treacherous mountains, outswim killer sharks, and even defeat enemies with a handy bagpipe flamethrower. But in the cybercrime world, spies aren't in the same class as 007 — in fact, sometimes they aren't even human at all. They're spyware.

What Is Spyware?

Spyware is a strand of malware that is designed to secretly infiltrate a victim's computer, harvest data, and submit it to third parties. It runs continuously in the background and can persist for years. While the hackers behind spyware are capable of exploiting just about anything they can get their hands on — including stuff many victims think is harmless like internet usage information — they are especially interested in confidential and private data such as credit card and bank account details, and of course the motherlode: login credentials.

Since spyware has been around for so long (the term was introduced all the way back in 1995) it tends to not get the same attention — or trigger the same amount of anxiety — as other cyberthreats such as ransomware, phishing, or supply chain attacks. However, spyware is a serious, pervasive, and imminent threat — and not just for users with desktops and laptops: mobile users are also at risk.

Indeed, mobile spyware is designed to hide in a device's background and steal data such as SMS messages, call logs, contact lists, emails, photos, browser histories, and so on. Some types of mobile spyware can even secretly take pictures, track locations, and control devices through commands sent by remote servers or SMS. In July 2021, a group of newspaper and media organizations, assisted by Amnesty International's Security Lab and the research group Citizen Lab, disclosed that one of the world's most sophisticated and invasive spyware tools — called Pegasus — had been used to hack (and attempt to hack) dozens of mobile phones owned by human rights activists, journalists, political dissidents, and business executives.

How Spyware Spreads

For **PCs and laptops**, there are four common spyware access points:

- Masquerading as software that victims think is useful, such as a download manager, drive cleaner, web search engine, Internet accelerator, etc.
- Hidden as an add-on, extension, or plug-in within a larger software package.
- Passive downloads that infect victims who click on web, email, or SMS links — or in some cases, you can become a target merely by visiting a malicious website or viewing a malicious banner ad (a.k.a. drive-by download).
- Through backdoors, worms, and trojans.

For **mobile devices**, some of the most common spyware access points include:

- Free unsecured Wi-Fi available in coffee shops, airports, etc.
- Operating system defects, which cause vulnerabilities that hackers can exploit.
- Malicious programs that are hidden inside apps that seem safe and legitimate.

Types of Spyware

There are many different types of spyware, and each has its own characteristics. Here is a look at some of the most common:

- **Adware:** Monitors activity and sells data to advertisers and malicious actors, or serves up malicious ads.
- **Infostealer:** Collects information and scans it for specific data and instant messaging conversations.
- **Keyloggers (a.k.a. Keystroke Loggers):** Records keystrokes, then saves data — such as usernames, passwords, text messages, emails, and everything else — into an encrypted log file.
- **Rootkits:** Enables hackers to deeply infiltrate devices by exploiting security vulnerabilities, or by logging into machines as an Administrator. Rootkits are very difficult — and in some cases impossible — to detect.
- **Red Shell:** Infiltrates a device while victims are installing compromised PC games, then tracks their online activity (generally used by developers to enhance games and improve marketing campaigns).
- **System Monitors:** Tracks activity such as emails sent, social media and other sites visited, and keystrokes.
- **Tracking Cookies:** Dropped onto a device by a website and used to follow online activity.
- **Trojan:** Infiltrates a device through a Trojan, which ultimately delivers the spyware.

Symptoms of Spyware

If you complain to your doctor about your legs being red, swollen, and incredibly itchy after a stroll through a wooded area, then she will probably say that you have the symptoms of a poison ivy rash (sorry to hear that).

Well, there are some common symptoms that suggest your computer or mobile device has been infiltrated by spyware, too. Here is what to look out for:

- Your computer/device is running slower than usual.
- Your computer/device is freezing and/or crashing frequently.

- Pop-up ads are repeatedly appearing in your browser(s).
- You see unusual error messages.
- You see unexpected browser changes.
- New icons suddenly start appearing in your taskbar.
- Your browser's favorites folder has been modified.
- You cannot modify your browser settings.
- After you conduct a search using one browser, another browser completes it for you.

And if you're using a mobile device, here are some additional symptoms that may suggest that Spyware is the culprit:

- You are using much more data for some inexplicable reason.
- Your battery is draining quickly and you do not know why (remember that spyware runs in the background without interruption).
- Your device is overheating (again, because spyware uses a significant amount of battery/data).
- You hear strange sounds during calls — which could be an app recording what you say and hear.
- You discover odd apps that you do not recall downloading.
- You see surprise billings in your App Store or Google Play accounts.
- Your device shows signs of activity in stand-by mode (e.g., camera opens, messages being sent, etc.).
- It takes an unusually long time to shut down your device.

Before looking at how to get rid of spyware, it is important to add two important things: one good and one bad. We will start with the former.

The good news is that the above indications are only symptoms of a potential spyware infection. They are not rock-solid evidence that spyware absolutely exists. For example, a computer or phone may start to get sluggish for a variety of reasons unrelated to spyware (e.g., reaching its end of life, not enough memory, etc.).

The bad news is that other types of malware share many of these symptoms — so while you may not have spyware (phew!), you may in fact have something even more insidious and threatening (ack!).

How to Get Rid of Spyware

Below, we highlight some basic steps to get rid of malware from a desktop/laptop PC running Windows, which are the most targeted types of machines. But what if you use a Mac, an iPhone, or an Android phone? Don't worry: after these steps, we will also share links that provide instructions for removing spyware from your machine or device as well.

Steps to Remove Spyware from Windows-Based Desktops and Laptops:

1. Disconnect from the Internet.
2. Use the Add/Remove Programs option to try and uninstall the unwanted or questionable program(s).
3. Always reboot after uninstalling the program(s), even if you are not prompted to do so.
4. Perform a full system scan with an up-to-date antivirus program. Ideally, this will highlight any other suspicious programs that you can clean, quarantine, or delete as necessary. There are many good antivirus programs available, and some of them are free such as Norton Power Eraser.
5. If the spyware (or spyware symptoms) persists, then access your system's hard drive in safe mode — so that the spyware does not load. Then, manually access the spyware folders and delete them. If you are not skilled in this area, then get help from an expert.

Hopefully, this will eliminate all spyware from your life. But how do you keep spyware from coming back to haunt your machine? Here is some practical advice:

- Do not open emails from unknown senders.
- Do not download files from untrustworthy sources.
- Do not click on pop-up advertisements.
- Only use reputable antivirus software, and keep it updated.
- Do your research before downloading/installing programs — especially if they are free.

Instructions for Mac/iOS/Android

As promised, if you are concerned that your Mac machine, iPhone, or Android phone is infected with spyware, then click the links below for step-by-step instructions that will hopefully solve the problem quickly and permanently:

- For Mac: https://macpaw.com/how-to/remove-spyware-from-mac
- For iPhone: https://clario.co/blog/how-to-remove-spyware-iphone-mac
- For Android: https://www.certosoftware.com/how-to-remove-spyware-from-an-android-phone/

The Bottom Line

Spyware is not making headlines these days like ransomware, but it is certainly the type of threat that must be taken seriously. Remember that 80% of data breaches start with compromised credentials, and spyware can open the backdoor for hackers to steal highly confidential data. By staying vigilant, scanning regularly, and exercising caution as you journey across the interwebs, you can stay a step ahead of the bad guys!