Viruses, Spyware, Malware, etc. Explained: Understanding Online Threats

By Bryan Clark

Read the original article here: http://www.makeuseof.com/tag/viruses-spyware-malware-etc-explained-understanding-online-threats/

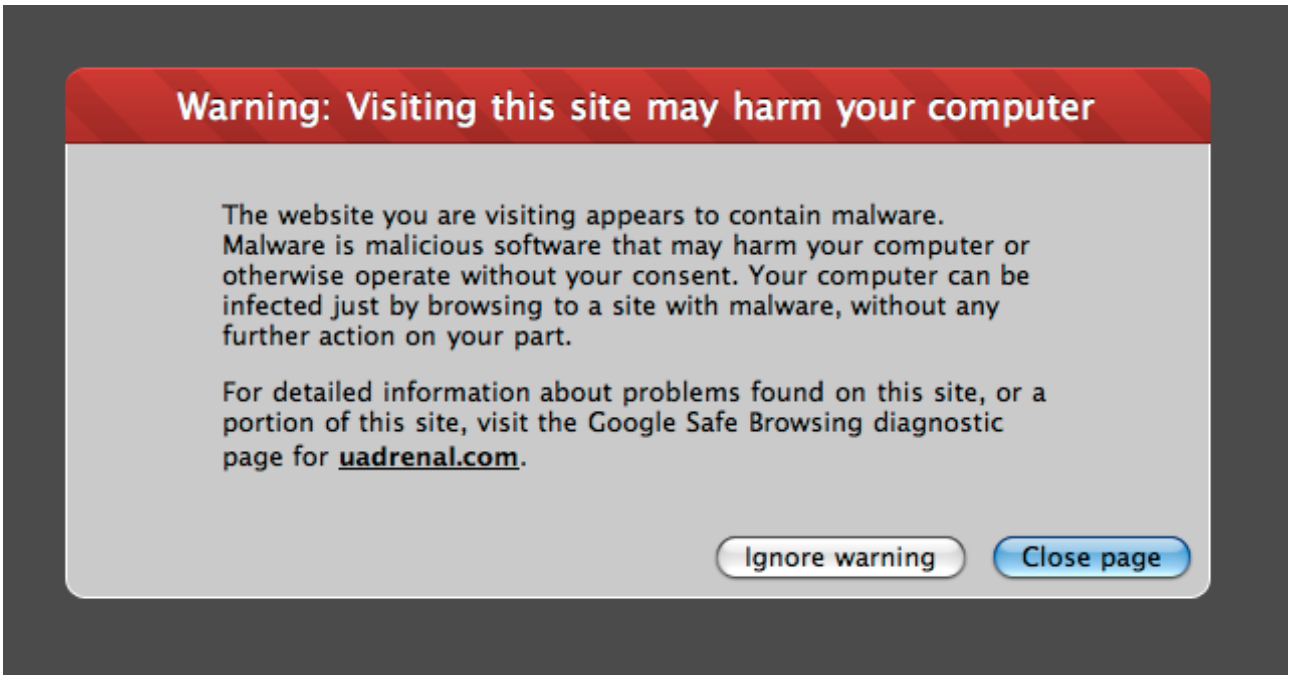
When you start to think about all the things that could go wrong when browsing the Internet, the web starts to look like a pretty scary place. Luckily, Internet users as a whole are getting far more savvy, and better at recognizing risky online behavior.

While pages with a dozen download buttons – or auto-checked boxes that tricked us into downloading things we didn't want – are no longer quite as effective as they once were, that doesn't mean there aren't hackers out there right now trying to come up with new methods of deception. In order to protect ourselves from these threats it's important to understand just what they are, and how they differ.

Let's dive in.

Understanding Online Security Threats and How They Differ

Malware



Malware is short for malicious software. This means that while most of us refer to these threats as viruses, the correct catch-all term should indeed be malware. Malicious software comes in many forms, but malware itself is a general term that could be used to describe any number of things, such as viruses, worms, trojans, spyware, and others. In short, it's a program or file with bad intentions, the nature of which could encompass just about anything.

Luckily, malware is exactly what all of the most popular antivirus programs are looking for. Getting affected by malware happens, and it doesn't have to be catastrophic. Learn the right protocol for dealing with malware, and how to avoid it in the first place for the safest browsing experience.

Viruses

Viruses consist of malicious code that infects a device after you install a software. Typically this infection happens through USB drives, Internet downloads, or email attachments, but it can happen in numerous other ways as well. It's important to note that the infection doesn't actually occur just from having the infected files on your computer. The infection happens once the program runs for the first time, whether through Autorun, a manual install, or an executable file that the user opens.

Once opened – or run – the infection happens. From that point, it can be very difficult to find and rid yourself of the virus due to the nature in which it works. While actual details are virus-specific, they tend to replicate themselves and infect the file system of the device they reside in by spreading from file to file before they are inevitably – and usually unknowingly – passed on to another machine.

Unlike other threats, viruses have no other purpose than attempting to render your computer inoperable. Some of them have been particularly good at it. Most others are quite weak and easy to detect.

Oh, and it should be pointed out – due to popular opinion – that Macs aren't immune to viruses.

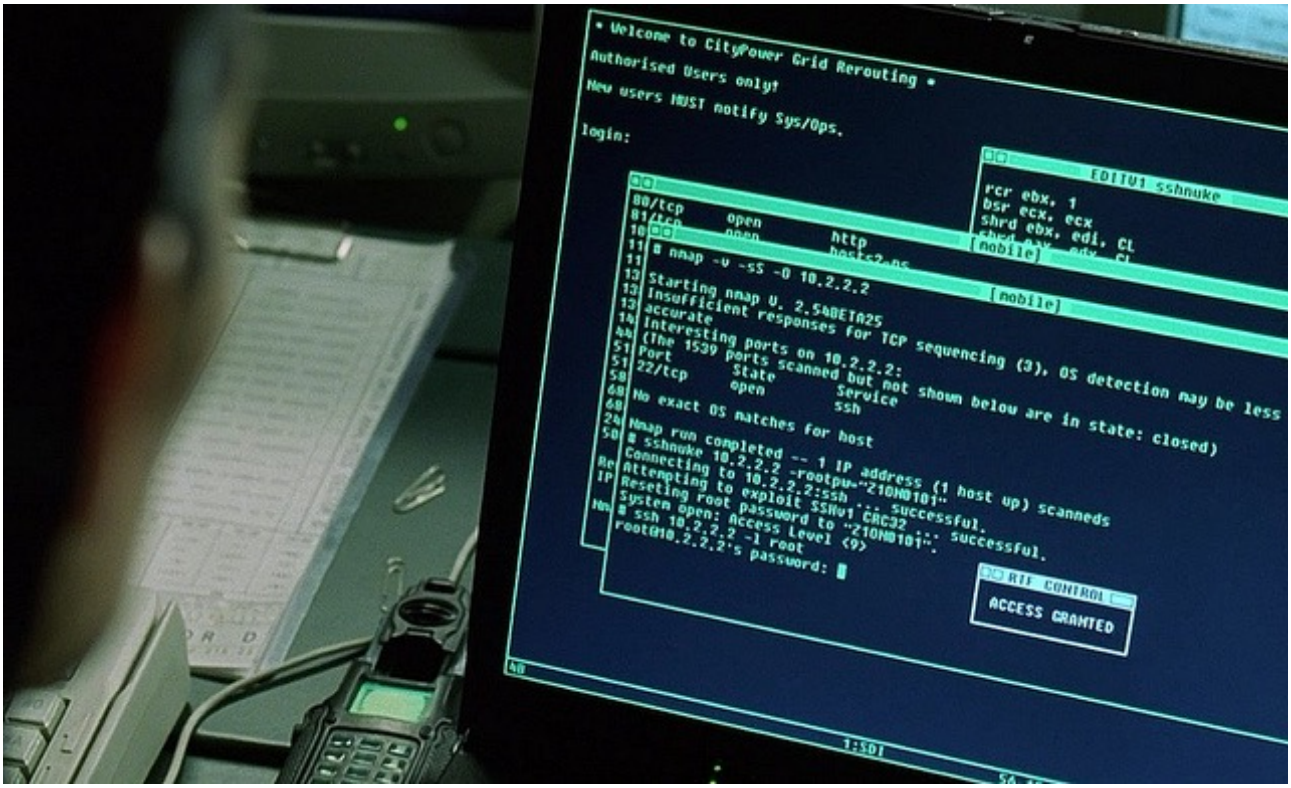
Adware

While relatively benign in most cases, adware might be the most annoying of the threats we'll talk about today.

Adware is bundled with otherwise legitimate apps or software, which makes initial detection somewhat difficult. A common example is the checkbox at the bottom of a download link (often pre-checked) that asks if we want to "Include X for free" – well, "X" is often the program containing the adware. This isn't a hard and fast rule, but it's not uncommon. If you aren't sure what these additional programs are, or how they function, don't download them.

Adware infections are also possible through no fault of our own. Recent stories detail at least one major manufacturer including adware – or an adware-like browser hijack – in their computers by default. While Lenovo, and Superfish are the exception, rather than the rule, it's important to note that these threats happen and often times there isn't much we can do about it.

Trojans and Backdoors

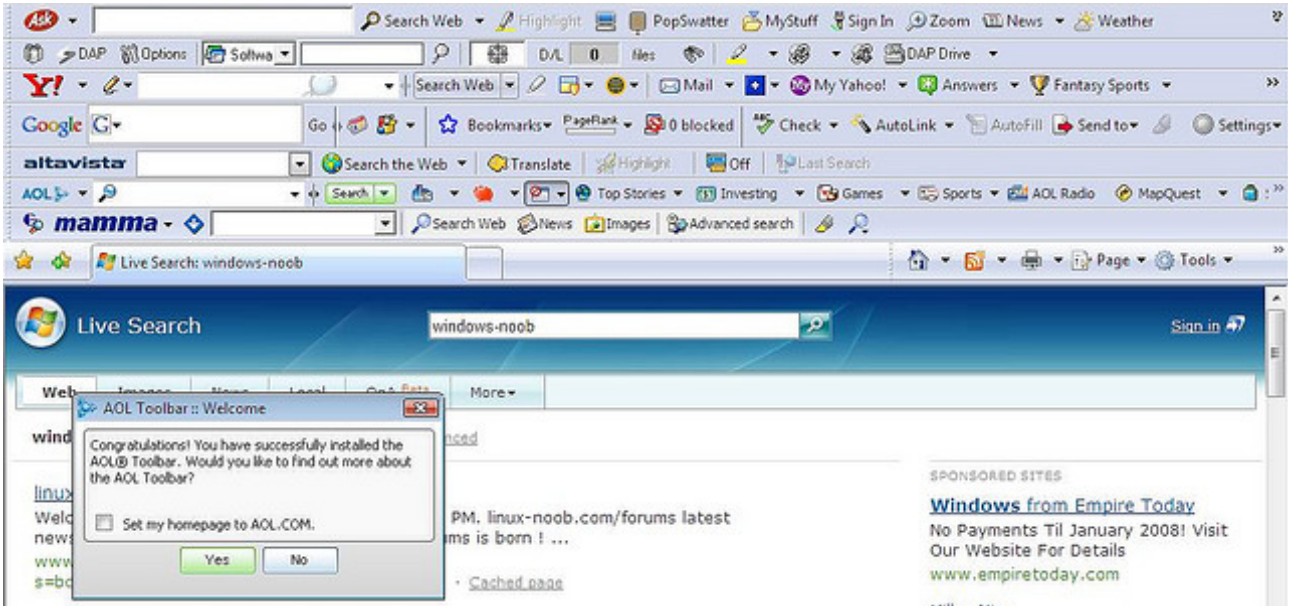


Trojans were named after the Trojan Horse, which was a giant wooden horse used to conceal Greek soldiers as they entered Troy during the Trojan War. History lesson aside, this is the same way that a trojan damages your computer. It hides malicious code inside a seemingly innocuous program or file in order to gain access to your machine. Once inside, the program installs itself on your device, and communicates with a server in the background without your knowledge. This gives an outside party access to your computer through what's commonly referred to as a backdoor.

While giving an outside party access to your computer is scary in and of itself, the implications of what they could be doing with this access is even scarier. What complicates matters is the small footprint that these backdoors leave, which keeps the user completely in the dark that any privacy breech is even occurring.

One benefit of a backdoor is the nature in which they operate. Since the hacker must connect to your machine remotely, they won't be able to do this if you disable the Internet connection while you attempt to locate and remove the malicious code.

Spyware

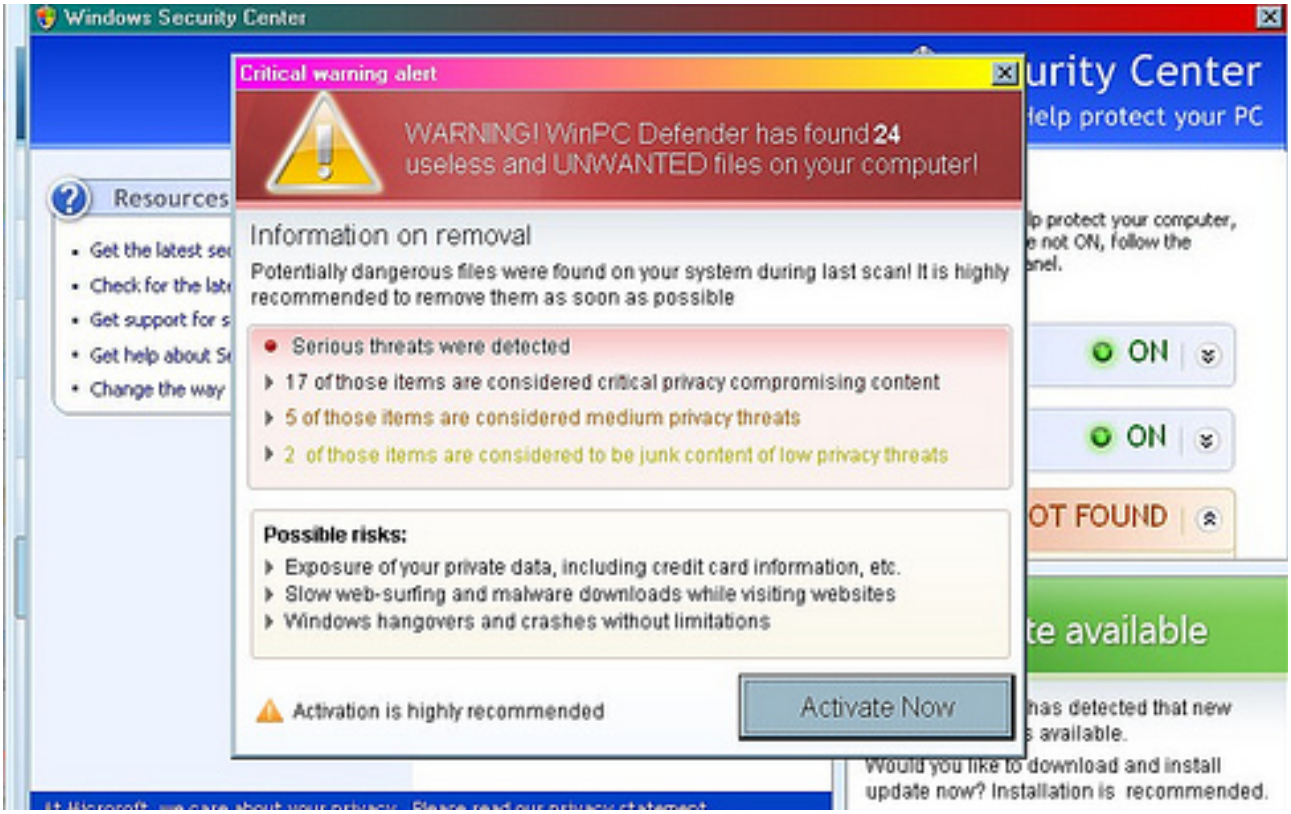


Spyware is the most common piece of badware on the Internet. While it's quite deceptive in nature and a major annoyance, most spyware is relatively harmless. Typically, spyware is used to monitor browsing behavior in order to better serve relevant ads. What makes it bad is how these companies go about collecting your data. Rather than relying on tracking pixels – or cookies – like most major companies, spyware acts like more of a trojan in that you install it and it communicates data from your computer back to a server, all while most of us are completely oblivious to its presence in the first place.

Other, more malicious forms of spyware, are far more dangerous. While typical spyware is mostly used for ad-serving purposes, malicious spyware communicates sensitive data back to another user, or a server. This data can include emails, photos, log files, credit card numbers, banking information, and/or online passwords.

Spyware is most often downloaded by the user as part of an add-on to a legitimate download (such as a toolbar) or included as part of a freeware or shareware program.

Scareware and Ransomware

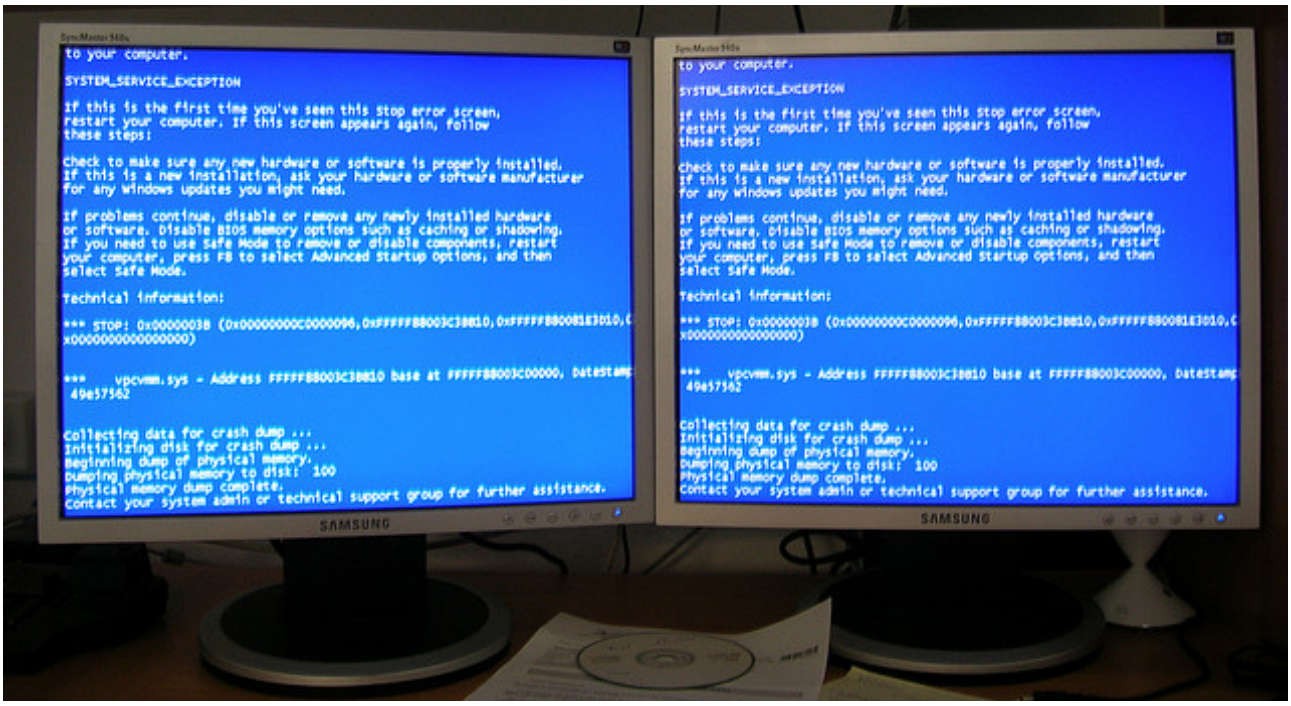


Scareware and ransomware differ in their approach, but the end goal for both is to collect money by manipulating the user into believing something that's often untrue.

Scareware most often takes the form of programs that pop up and tell you that your computer is infected with some sort of malware. When you click to remove the (often) multiple instances of malware, you are forced to pay to purchase the full version before the program can clean your system and rid it of the infections or threats.

Ransomware operates a bit differently in the sense that after the malicious software is installed, it'll often lock down your system outside of a window that allows you to pay the ransom in order to regain use of it. While ransomware is generally among the easiest threats to remove, it can be quite scary for a non-savvy computer user. As such, many believe that they must give in and pay the ransom in order to regain control of the machine.

Worms



Worms are by far the most damaging form of malware. While a virus attacks one computer and relies on a user to share infected files in order for it to spread, a worm exploits security loopholes in a network and can potentially bring the whole thing to its knees in a matter of minutes.

Networks with security vulnerabilities are targeted by introducing the worm into the network and allowing it to pass (often unnoticed) from computer to computer. As it passes from one device to another, the infection spreads until each machine is infected – or – the worm is isolated by removing the infected machines from the network.

Unnamed Exploits, Security Flaws and Vulnerabilities

No matter how competent the developer, every program has security flaws and vulnerabilities. These security flaws allow hackers to exploit them in order to gain access to the program, alter it in some way, or inject their own code (often malware) within it.

If you were ever wondering why programs had so many security updates, it's because of the constant cat and mouse being played between developers and hackers. The developer attempts to find, and patch, these holes before they're exploited, while the hacker attempts to exploit security flaws before they're discovered and patched by a developer.

The only way to stay even remotely safe from these exploits is to keep your operating system and each of your programs up-to-date by installing updates as they become available.

Staying Safe Online

If you're using the web, there's no foolproof method to avoid all online threats, but there are certainly things you can do to make yourself safer.

Some of these are:

- Keep your operating system and each of your programs up-to-date by downloading updates as they become available.
- Install a good antivirus program and keep the virus definitions up-to-date.
- Utilize a firewall that monitors both inbound and outbound traffic. Keep an eye on the flow of this traffic to help to detect the presence of threats that may be communicating with outside servers.
- Avoid unsafe downloads from unknown and untrusted sources.
- Use your antivirus program, or a malware detection program to scan suspicious links before opening them.
- Avoid pirated software.

Again, if you spend any portion of your time on the web, it's unlikely that you can completely protect yourself from all the badware out there. While infections and exploits can – and do – happen to anyone, I don't think any of us would argue that we could stay a little safer with subtle changes in our browsing or computer use habits.

Photo credit: Warning! by Paul Downey via Flickr, Virus by Yuri Samoilov via Flickr, Annoying pop up via Shutterstock, Hackers – Seguridad by TecnoDroidVe via Flickr, Toolbars by mdornseif via Flickr, Malware by mdaniels7 via Flickr, Dual Crash by Dr. Gianluigi "Zane" Zanet via Flickr, Caps Lock by DeclanTM via Flickr