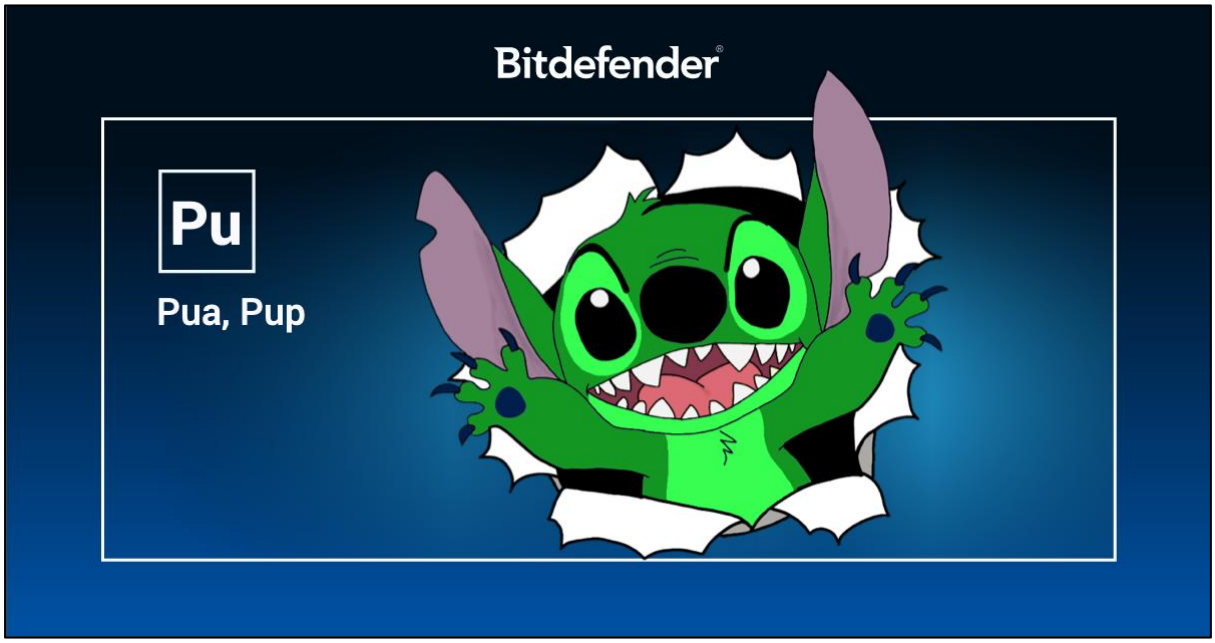
What is a PUA or PUP? Prevention & Removal

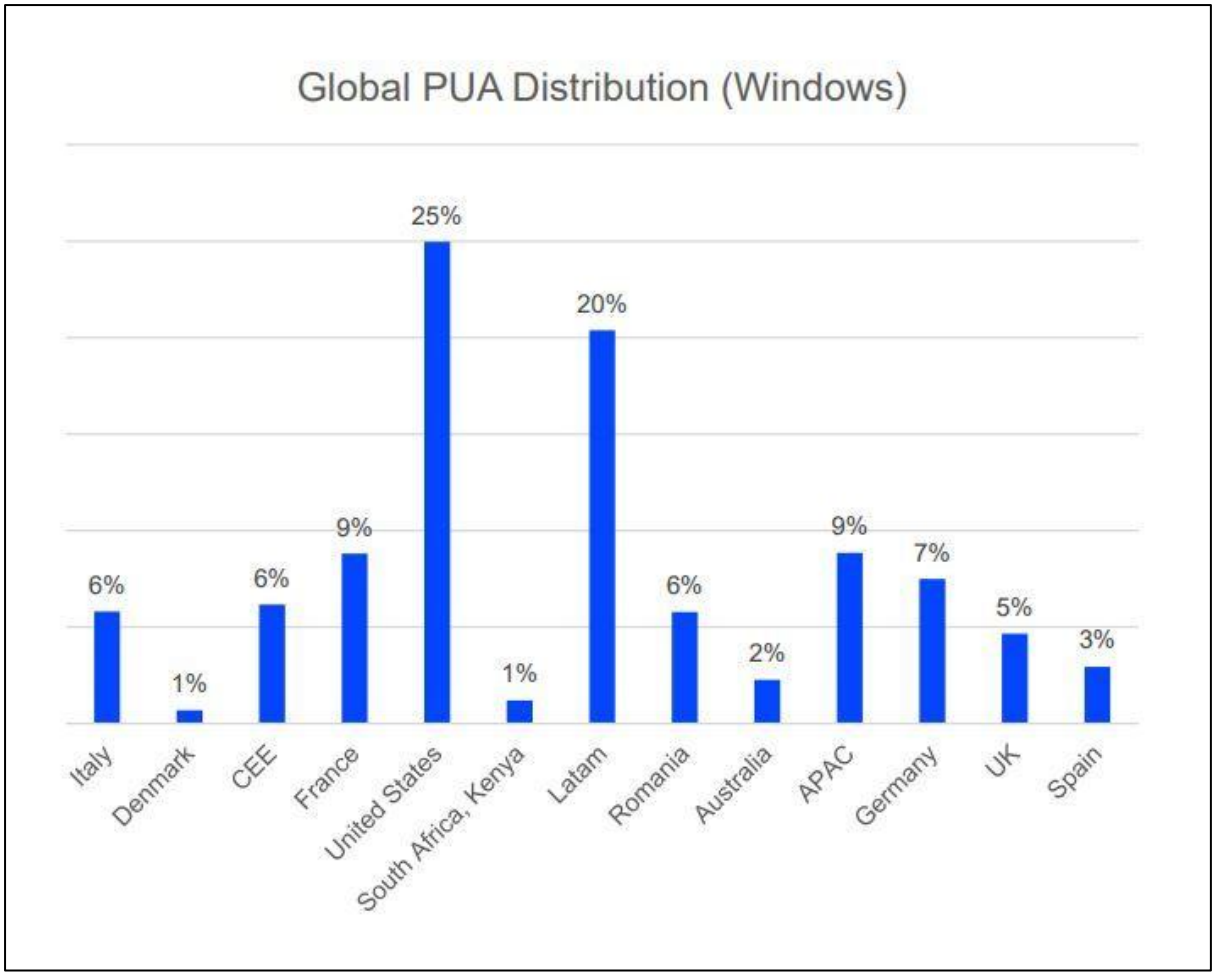
PUA is the acronym for “Potentially Unwanted Application”, while PUP is the acronym for “Potentially Unwanted Program”.

What is a PUA (Potentially Unwanted Application) or PUP (Potentially Unwanted Program)?

Both terms are used to describe a vast category of unnecessary software that collects data it shouldn’t, abuses permissions to generate ad revenue, or tricks users into making large payments, just to name a few. Potentially Unwanted Applications or PUA & Potentially Unwanted Programs or PUP walk the thin line between nuisance and malware. While PUA/PUP mainly just hog system resources, they often also display aggressive ads, collect data without your consent, and may even perform secondary downloads that might hide actual cyber threats.

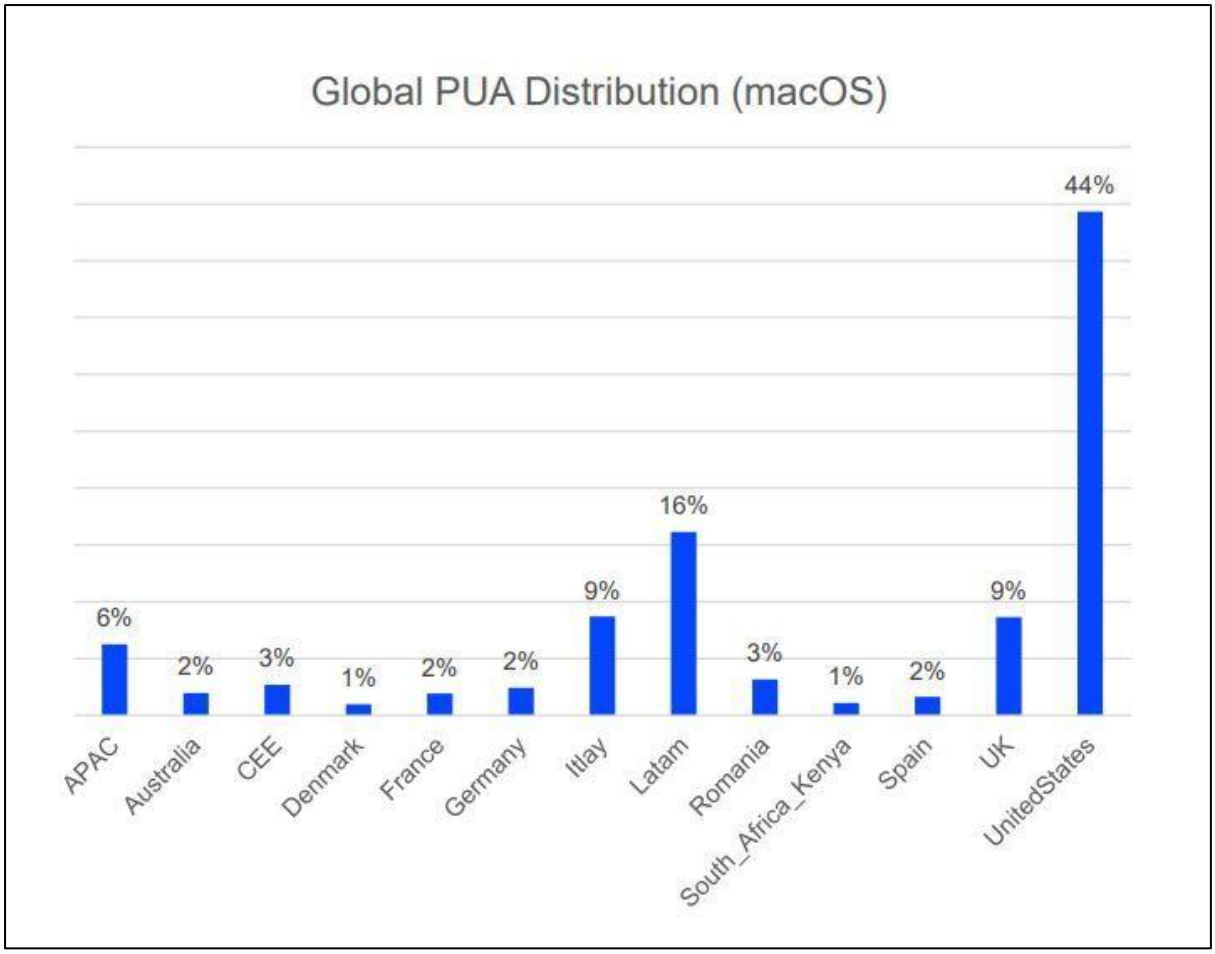


Bitdefender’s telemetry shows that PUAs make up around a third of all threats directed at Windows and macOS systems. PUA operators target large territories with massive PC user bases. The US and Latin America are assailed the most, our data shows.



Global PUA distribution (Windows)

PUAs are most found as freeware, repackaged applications, system cleaners, or other utilities with hidden functionality like data tracking and even coin mining. Others hijack the user's browser, altering its functionality – like changing the default search engine and installing plugins – without consent.



Global PUA Distribution (macOS)

Some of the most aggressive PUAs can modify third-party apps, download additional software behind the scenes, or alter system settings – which can mushroom into actual security and privacy issues.

Equally nefarious are the scareware-type PUAs that display exaggerated or bogus notifications claiming the system is exhibiting problems that require immediate attention. Typically, the software claims to have a solution for the problem – but that solution sits behind a paywall. Beneath the surface, the software lacks the code to perform the alleged fixes. Plus, the problem it claims your computer exhibits likely isn't even real.

Other PUAs display excessive ads, causing a fragmented experience and overall annoyance. These bad-user-experience apps typically permeate the Android ecosystem, but many can also be found in Apple's walled garden, the iOS App Store.

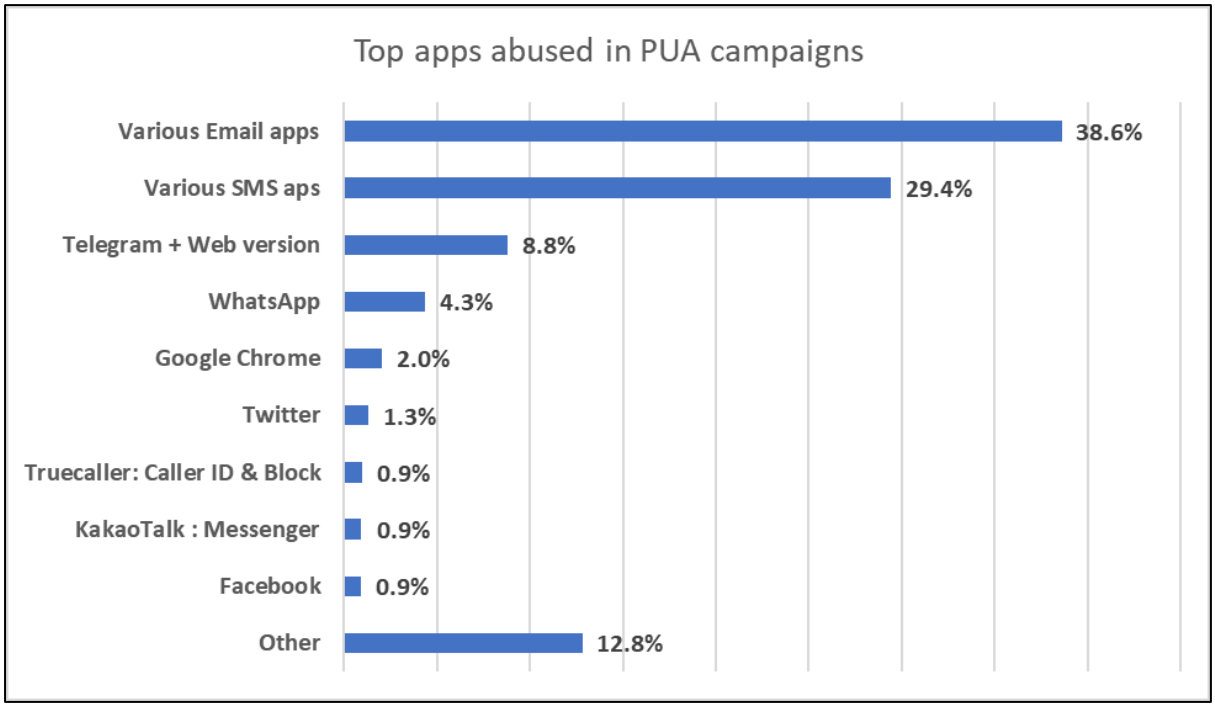
Bundling PUAs are also common. They install other apps and plugins the user may not want. These PUAs are also considered quite dangerous, as they don't disclose their real purpose or behavior upfront, meaning they might also covertly collect data and send it to some unknown server. Another telltale sign that you're dealing with a typical PUA is a lack of conventional means to uninstall the software.

How does a PUA / PUP get into my device?

A potentially unwanted application or potentially unwanted program usually comes bundled with freeware software and will display pop-ups or install a toolbar in the default browser.

Some of them will change the homepage or the search engine, others will run several processes in the background, slowing down the PC or will display numerous ads. These programs can be installed without your consent (also called adware) or will be included by default in the express installation kit (ad-supported).

Most PUA threats spread over emails, but that's not surprising. SMS apps are going strong as an infection vector, even though it's not the first kind of app we think of when it comes to PUA or spam.



Top apps abused in PUA campaigns

How do I avoid a PUA or PUP?

There are a few effective ways to avoid installing potentially unwanted applications:

- Install only legitimate, paid software from the manufacturer's official website.
- When installing freeware, pay attention to the installation wizard and avoid the default installation. Go instead into the advanced/custom options, where you can opt only for the main software, thus avoiding installing bloatware and potentially unwanted bundled programs.
- Use an antivirus that detects PUA and PUP and blocks them before they get installed on your device.

How do I get rid of potentially unwanted applications?

Modern security solutions detect these unwelcome experiences and can help you steer clear of questionable apps. Bitdefender offers the right tool for this job on both desktop and mobile platforms. Simply use the Scan feature to check your device for all malware, including PUA/PUP.

On the other hand, some of these programs are legitimate, but their actions on the system should be stopped if they are performed without the user's explicit consent. For instance, commercial keyloggers are legitimate applications installed by the employer to monitor the activity on the employees' workstations. In such a case, an exclusion has to be made and Bitdefender will automatically skip these files/folders.

If you are not sure whether the software is legitimate, you can submit a scan log. The detection will be studied by our cybersecurity analysts to determine if it is a low-risk application, or if specific actions need to be taken to remove the threat from your PC.