# Malware Found in Arch Linux AUR Package Repository

By Catalin Cimpanu

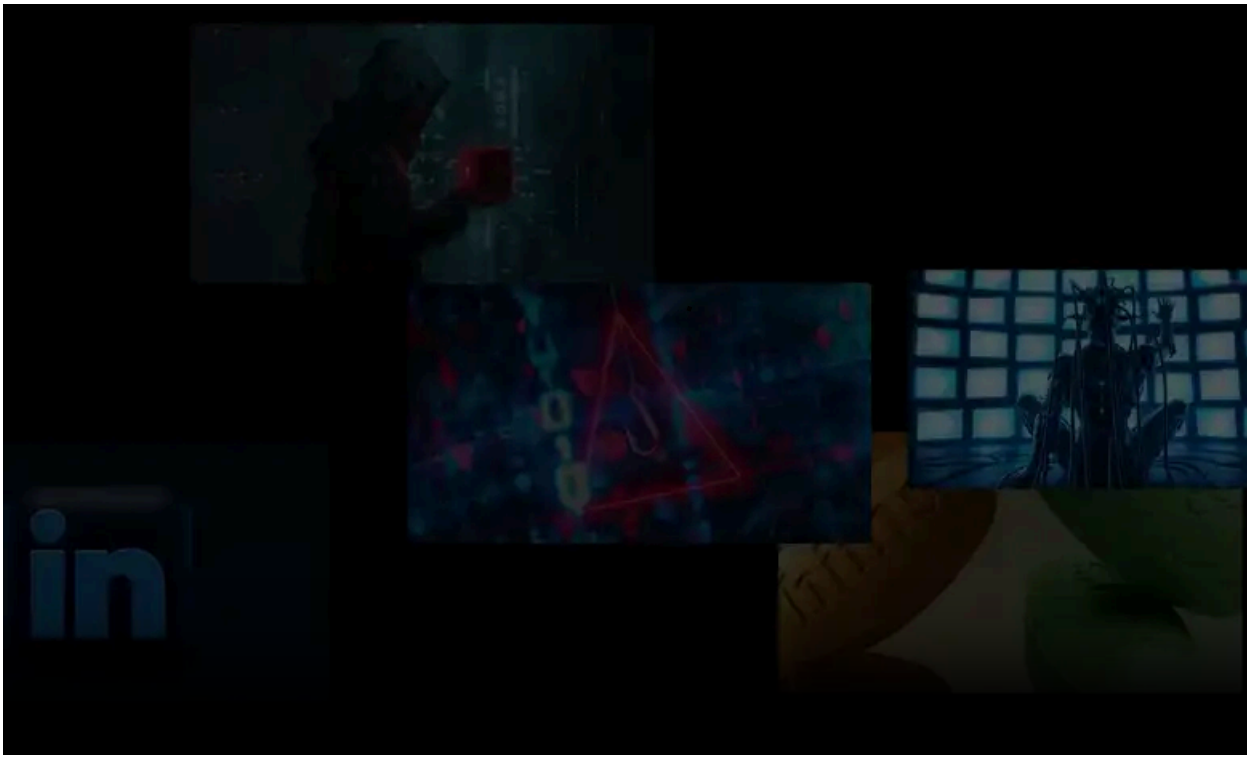
Published: 2018-07-10 · Archived: 2026-04-05 16:12:56 UTC


Malware has been discovered in at least three Arch Linux packages available on AUR (Arch User Repository), the official Arch Linux repository of user-submitted packages.

The malicious code has been removed thanks to the quick intervention of the AUR team.

## Info-stealer found in "acroread" Arch Linux package

The incident happened because AUR allows anyone to take over "orphaned" repositories that have been abandoned by their original authors.



On Saturday, a user going by the pseudonym of "xeactor" took over one such orphaned package named "acroread" that allows Arch Linux users to view PDF files.

According to a Git commit to the package's source code, xeactor added malicious code that would download a file named "~x" from ptpb.pw, a lightweight site mimicking Pastebin that allows users to share small pieces of texts.

When the user would install the xeactor package, the user's PC would download and execute the ~x file [VirusTotal, source code], which would later download and run another file named "~u" [VirusTotal, source code].

Besides downloading ~u, the main purpose of the first file (~x) was also to modify systemd and add a timer to run the ~u file at every 360 seconds.

## Malware didn't do much

The purpose of the second file (~u) was to collect data about each infected system and post these details inside a new Pastebin file, using the attacker's custom Pastebin API key.

Collected data includes details such as the date and time, machine's ID, CPU information, Pacman (package manager) details, and the outputs of the "uname -a" and "systemctl list-units" commands.

No other malicious actions were observed, meaning the acroread package wasn't harming users' systems, but merely collecting data in preparation for... something else.

There isn't a self-update mechanism included, meaning xeactor would have needed a second acroread package update to deploy more intrusive code, or potentially another malware strain.

## Two other yet-to-be-named packages also found infected

The AUR team also said it found similar code in two other packages that the xeactor user had recently taken over. The following packages and versions were known to be affected:

acroread 9.5.5-8
balz 1.20-3
minergate 8.1-2

All malicious changes to all three packages have now been reversed, and xeactor's account has been suspended. The AUR repository should not be confused with official pacakges in the Arch Build System (ABS). AUR packages are user generated and submitted to the repository, while ABS packages are official packages from trusted sources. The Arch Linux team has warned users for years about verifying each AUR package before installing it.

The Arch Linux team is the second Linux distro that has found malware on its user-submitted package repository this year. In May, the Ubuntu Store team found a cryptocurrency miner hidden in an Ubuntu package named 2048buntu.

---