Sensitive information on millions of convicted felons just leaked online.

This Wednesday, cybersecurity researchers from Malwarebytes published a blog post detailing that a group of cybercriminals leaked a database containing criminal records of millions of Americans. The database is said to contain 70 million rows of data.

Given how Malwarebytes worded the announcement, we can assume its researchers did not have direct access to this database. Still, it was said that it contained people’s full names, dates of birth, known aliases, postal addresses, dates of arrest, dates of conviction, sentences, and more.

## Building a new leaks site

The database is quite fresh, holding data generated between 2020 and 2024. Each row represents a single felony, not a record of all the crimes a person may have committed, Malwarebytes's Pieter Arntz confirmed to Tom’s Guide.

The data was leaked by two known cybercriminals – EquationCorp and USDoD.

The latter, according to the researchers, is a “high-profile player” in the field of data leaks, allegedly closely associated with Connor Fitzpatrick, AKA Pompompurin.

For those who haven’t been paying attention, Pompompurin was the owner and master administrator of BreachForums, the world’s most popular underground forum for sharing stolen and leaked data, malware, and other warez. The forum was recently dismantled, and Fitzpatrick arrested.

## Are you a pro? Subscribe to our newsletter

Sign up to the TechRadar Pro newsletter to get all the top news, opinion, features and guidance your business needs to succeed!

Malwarebytes claims USDoD is planning on building a new leak forum similar to BreachForums, and that pushing this data out there could be a PR stunt to draw attention and raise interest in the new site.

At this time, it is unknown from whom the hackers stole this data, when, or how.

In any case, our American readers with a criminal history should pay attention to the emails

Все права защищены

save pdf date >>> 06.12.2025

they’re getting, especially if they mention criminal convictions, carry attachments and links, or demand urgent action. Hackers are likely to exploit the database in phishing and social engineering attacks.

Все права защищены