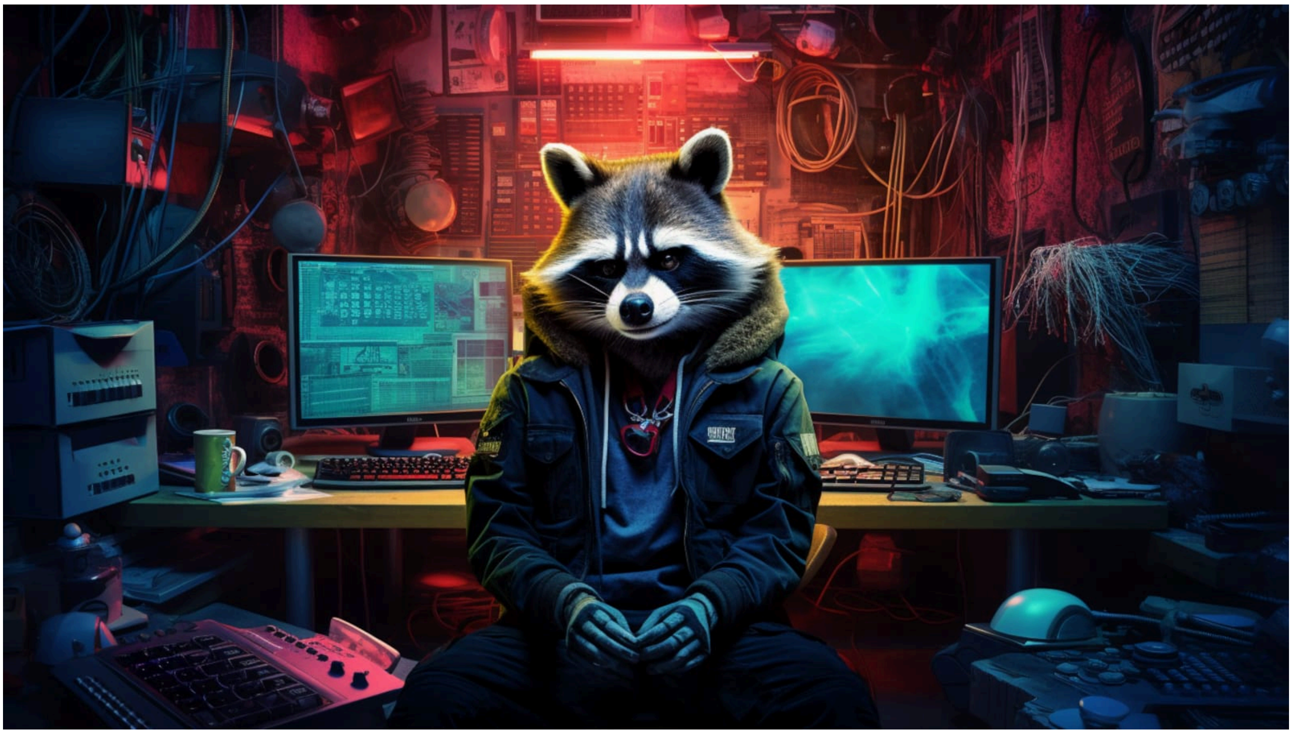
Raccoon Stealer malware operator gets 5 years in prison after guilty plea

By Sergiu Gatlan

Published: 2024-12-18 · Archived: 2026-04-05 14:37:12 UTC



Ukrainian national Mark Sokolovsky was sentenced today to five years in prison for his involvement in the Raccoon Stealer malware cybercrime operation.

According to unsealed court documents, Sokolovsky (also known as raccoon-stealer, Photix, and black21jack77777) and his conspirators rented the malware to other threat actors under a MaaS (malware-as-a-service) model for $75 per week or $200 monthly.

After infecting a device, Raccoon Stealer collects and steals a wide range of data, including credentials, cryptocurrency wallets, credit card data, email data, and other sensitive information from dozens of applications.

In March 2022, police arrested Sokolovsky in the Netherlands. The FBI also took the malware offline by dismantling its infrastructure in a joint action with law enforcement authorities in the Netherlands and Italy.

The Raccoon Stealer cybercrime gang also suspended operations around the time of Sokolovsky's arrest, saying that one of their lead developers had been killed during Russia's invasion of Ukraine. Since then, the malware operation has been revived several times, with newer versions adding more data theft capabilities.

Sokolovsky was extradited to the United States in February 2024 after being indicted for fraud, money laundering, and aggravated identity theft in October 2022. One year later, he pleaded guilty and agreed to pay at least $910,844.61 in restitution.

"Mark Sokolovsky was a key player in an international criminal conspiracy that victimized countless individuals by administering malware which made it cheaper and easier for even amateurs to commit complex cybercrimes," said U.S. Attorney Jaime Esparza today.

"Sokolovsky's infostealer was responsible for compromising more than 52 million user credentials, which were then used in furtherance of fraud, identity theft, and ransomware attacks on millions of victims worldwide," FBI Special Agent in Charge Aaron Tapp added.

After dismantling Raccoon Stealer's infrastructure in March 2022, the FBI also created a website to help victims check whether their information was included in the stolen data using this malware.

If your data has been compromised, you will receive an email containing additional information and resources at the address provided when searching the FBI's Raccoon Infostealer Disclosure portal.

Source: https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-operator-gets-5-years-in-prison-after-guilty-plea/amp/