Alleged SmokeLoader malware operator facing federal charges in Vermont

By Jonathan Greig

Published: 2025-04-18 · Archived: 2026-04-05 23:11:39 UTC

An alleged operator of the SmokeLoader malware is now facing federal hacking charges in Vermont after accusations that he stole personal information on more than 65,000 people.

Nicholas Moses initially had charges filed in North Carolina this week, but the case was transferred to federal prosecutors in Vermont on Wednesday.

Court documents accuse Moses, operating under the alias “scrublord,” of operating “a computer malware program known as SmokeLoader.”

“Moses deployed the malware as a means to harvest personal information and passwords from victims without the knowledge of the owners of the victim computers," prosecutors said.

"Thousands of computers around the world have been infected with the SmokeLoader malware by Moses and over 65,000 victims have had their personal information and passwords stolen by Moses.”

At least one of the victims named in the initial filing is a Charlotte-based FDIC-insured financial institution. Moses is being charged with one count of conspiracy to commit fraud and related activity in connection with computers.

From at least January 2022 to May 2023, Moses allegedly maintained a command and control server located in the Netherlands to deploy the SmokeLoader malware and receive stolen data from victim computers.

In one November 30, 2022 incident, Moses allegedly participated in a chat where he "provided the usernames and passwords for victim accounts with multiple video on-demand streaming services which were acquired through the SmokeLoader infostealer.”

Moses claimed he had acquired "over half a million stealer logs" and that he sold stolen victim credentials and passwords for about $1 to $5 each, prosecutors said.

Moses also shared a screenshot of the SmokeLoader interface which showed a database of 619,763 files containing stolen victim data.

The Justice Department did not respond to requests for comment, and it’s unclear why the case was transferred to Vermont. One of the documents attached to the charges appears to show that Moses pleaded guilty to the charge in Vermont.

SmokeLoader is a complex malware strain primarily functioning as a loader, which downloads stealthier or more effective malicious software into the system. However, because of its modular design, SmokeLoader can perform

a wide range of functions, including stealing credentials, executing distributed denial-of-service (DDoS) attacks and intercepting keystrokes.

The price for this malicious toolkit varies, with options ranging from $400 for the basic bot to $1,650 for the complete package, featuring all available plugins and functions. According to previous reports, the malware has been advertised on underground forums since 2011.

The tool has been used widely among Russian cybercriminals and state actors, particularly in attacks targeting Ukraine.

Europol 'Endgame' raids

Last week, officials from Europol announced follow-up actions to a massive botnet takedown codenamed Operation Endgame in May 2024, which shut down the biggest malware droppers, including IcedID, SystemBC, Pikabot, Bumblebee and SmokeLoader.

Europol said that in early 2025, a coordinated series of arrests, house searches and so-called 'knock and talks' were conducted involving customers of the SmokeLoader pay-per-install botnet, operated by the actor known as 'Superstar.'

At least five unnamed people were arrested or detained as part of the operation. Multiple law enforcement agencies in Canada, Denmark, the Czech Republic, France, Germany, the Netherlands and the U.S. followed the leads uncovered in Operation Endgame to link online personas and their usernames to real-life individuals.

"When called in for questioning, several suspects chose to cooperate with the authorities by facilitating the examination of digital evidence stored on their personal devices," Europol explained.

"Several suspects resold the services purchased from SmokeLoader at a markup, thus adding an additional layer of interest to the investigation. Some of the suspects had assumed they were no longer on law enforcement's radar, only to come to the harsh realisation that they were still being targeted."

They noted that Operation Endgame is not over and more actions will eventually be announced.

Additional Reporting by James Reddick.

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
