Justice Department Seizes Domains Behind Major Information-Stealing Malware Operation

Published: 2025-05-21 · Archived: 2026-04-05 21:51:26 UTC

The Justice Department announced today the unsealing of two warrants authorizing the seizure of five internet domains used by malicious cyber actors to operate the LummaC2 information-stealing malware service.

“The Department will continue to use its unique tools, authorities, and partnerships to disrupt malicious cyber operations and criminal networks,” said Sue J. Bai, head of the Justice Department’s National Security Division. “Today’s disruption is another instance where our prosecutors, agents, and private sector partners came together to protect us from the persistent cybersecurity threats targeting our country. We are grateful for their work and dedication.”

“Malware like LummaC2 is deployed to steal sensitive information such as user login credentials from millions of victims in order to facilitate a host of crimes, including fraudulent bank transfers and cryptocurrency theft,” said Matthew R. Galeotti, head of the Justice Department’s Criminal Division. “Today’s announcement demonstrates that the Justice Department is resolved to use court-ordered disruptions like this one to protect the public from the theft of their personal information and their assets. The Department is also committed to working with and appreciates the efforts of the private sector to safeguard the public from cybercrime.”

“The FBI is committed to disrupting the key services that cyber criminals rely on,” said Assistant Director Bryan Vorndran of FBI’s Cyber Division. “That’s why, with our partners, we took action against the most popular infostealer service available in online criminal markets, which is responsible for millions of attacks against victims. Thanks to partnerships with the private sector, we were able to disrupt the LummaC2 infrastructure and seize user panels. Together, we are making it harder, and more painful, for cyber criminals to operate.”

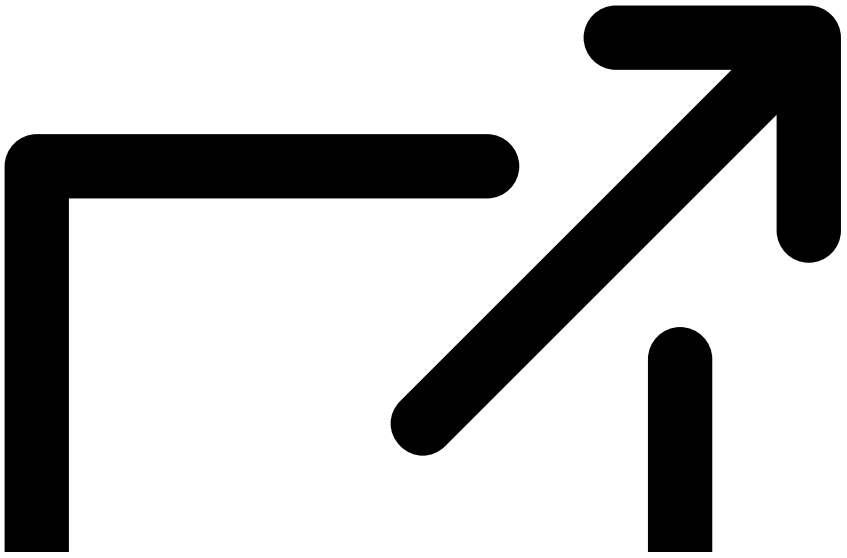
As alleged in the affidavits filed in support of the government’s seizure warrants, the administrators of LummaC2 used the seized websites to distribute LummaC2, an information-stealing malware, to their affiliates and other cyber criminals. According to court documents, common targets for cybercriminals using malware like LummaC2 include browser data, autofill information, login credentials for accessing email and banking services, as well as cryptocurrency seed phrases, which permit access to virtual currency wallets. As alleged in the affidavits, the FBI has identified at least 1.7 million instances where LummaC2 was used to steal this type of information.

The government’s affidavit further alleges that the seized domains, also referred to as user panels, served as login pages for the LummaC2 malware, allowing credentialed users and administrators to access and deploy LummaC2. On May 19, 2025, the government seized two domains. On May 20, 2025, as detailed in court documents, the LummaC2 administrators informed their users of three new domains that they had set up to host the user panel. The next day, the government then seized those three domains.

The seizure of these domains by the government will prevent the owners and cybercriminals from using the websites to access LummaC2 to compromise computers and steal victim information. Individuals who now visit

the websites will see a message indicating that the site has been seized by the Justice Department, including the FBI.

Concurrent with today's actions and consistent with the Department's approach to public-private operational coordination, Microsoft announced an independent civil action

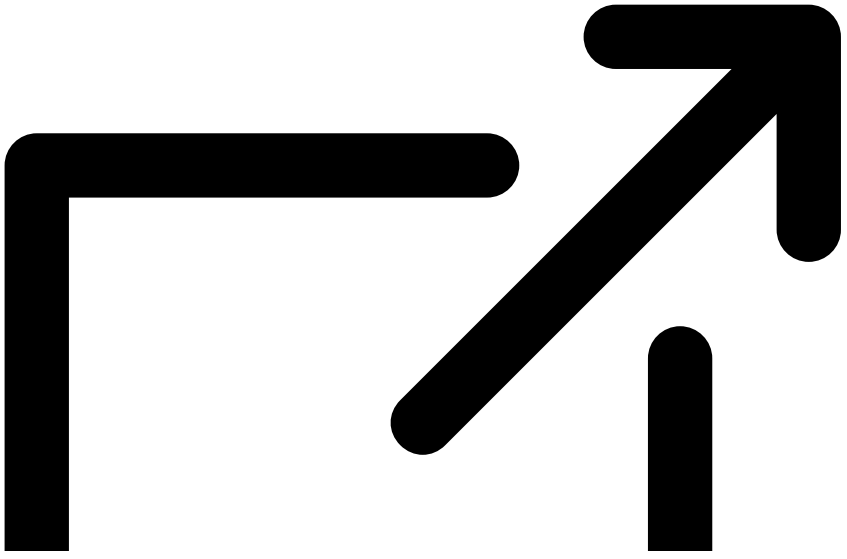


to take down 2,300 internet domains also claimed to be used by the LummaC2 actors or their proxies.

FBI's Dallas Field Office is investigating the case.

The U.S. Attorney's Office for the Northern District of Texas, the National Security Division's National Security Cyber Section, and the Criminal Division's Computer Crime and Intellectual Property Section are handling the case.

The U.S. Department of State's Rewards for Justice (RFJ) program



, which is administered by the Diplomatic Security Service, offers a reward of up to $10 million for information on foreign government-linked individuals participating in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act.

Anyone with information on any other foreign government-linked malicious cyber actors or activity targeting U.S. critical infrastructure should contact Rewards for Justice via the RFJ Tor-based tip line at: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required). Learn more about Rewards for Justice and their reward offers at RewardsforJustice.net.

If you believe you have a compromised computer or device, please visit the FBI's Internet Crime Complaint Center (IC3). You may also contact your local FBI field office directly.
