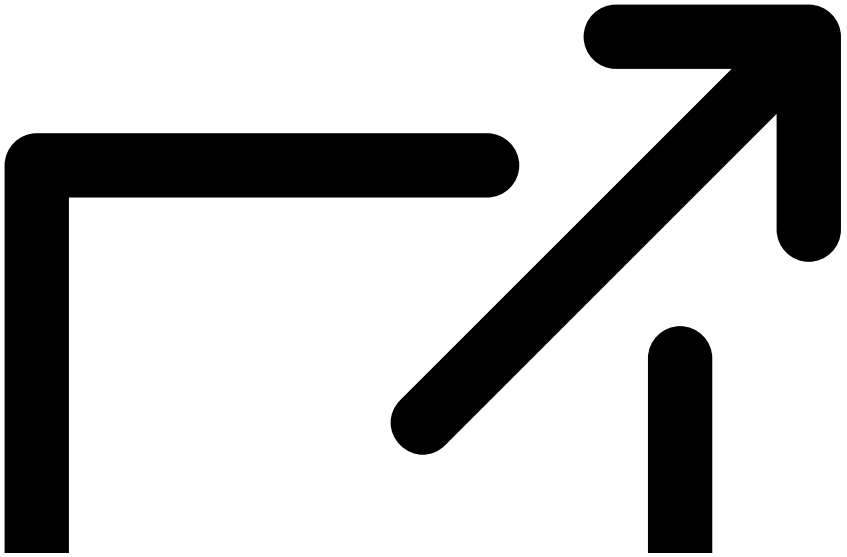
U.S. Joins International Action Against RedLine and META Infostealers

Published: 2024-10-28 · Archived: 2026-04-07 02:02:16 UTC

AUSTIN, Texas – The Department of Justice joined the Netherlands, Belgium, Eurojust and other partners in announcing an international disruption effort against the current version of RedLine Infostealer, one of the most prevalent infostealers in the world that has targeted millions of victim computers, and the closely-related META Infostealer.

The Justice Department, FBI, Naval Criminal Investigative Service, IRS Criminal Investigation, Defense Criminal Investigative Service, and Army Criminal Investigation Division joined international partners in the Joint Cybercrime Action Taskforce ("JCAT") Operation Magnus (supported by Europol) to seize domains, servers, and Telegram accounts used by the RedLine and META administrators to disrupt the operations of the infostealers.

International authorities have created a website at www.operation-magnus.com



with additional resources for the public and potential victims.

Infostealers are a prevalent form of malware used to steal sensitive information from victim's computers including usernames and passwords, financial information, system information, cookies, and cryptocurrency accounts. The stolen information—referred to as "logs"—is sold on cybercrime forums and used for further fraudulent activity and other hacks. RedLine has been used to conduct intrusions against major corporations. RedLine and META infostealers can also enable cyber criminals to bypass multi-factor authentication (MFA) through the theft of authentication cookies and other system information.

RedLine and META are sold through a decentralized Malware as a Service ("MaaS") model where affiliates purchase a license to use the malware, and then launch their own campaigns to infect their intended victims. The

malware is distributed to victims using malvertising, e-mail phishing, fraudulent software downloads, and malicious software sideloading. Various schemes, including COVID-19 and Windows update related ruses have been used to trick victims into downloading the malware. The malware is advertised for sale on cybercrime forums and through Telegram channels that offer customer support and software updates. RedLine and META have infected millions of computers worldwide and, by some estimates, RedLine is one of the top malware variants in the world.

Through various investigative steps, law enforcement has collected victim log data stolen from computers infected with RedLine and META. While an exact number has not been finalized, agents have identified millions of unique credentials (usernames and passwords), email addresses, bank accounts, cryptocurrency addresses, credit card numbers, etc. The United States does not believe it is in possession of all the stolen data and continues to investigate.

The Department has unsealed a warrant issued in the Western District of Texas that authorized law enforcement to seize two domains used by RedLine and META for command and control.

In conjunction with the disruption effort, the Justice Department unsealed charges against Maxim Rudometov, one of the developers and administrators of RedLine Infostealer. According to the complaint, Rudometov regularly accessed and managed the infrastructure of RedLine Infostealer, was associated with various cryptocurrency accounts used to receive and launder payments and was in possession of RedLine malware. For his actions, he has been charged with access device fraud, in violation of 18 U.S.C. § 1029, conspiracy to commit computer intrusion, in violation of 18 U.S.C. §§ 1030 and 371, and money laundering, in violation of 18 U.S.C. § 1956.

If convicted, Rudometov faces a maximum penalty of 10 years in prison for access device fraud, five years in prison for conspiracy to commit computer intrusion, and 20 years in prison for money laundering. The complaint is merely an allegation, and the defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The FBI Austin Cyber Task Force is investigating the case. The Task Force participants include the Naval Criminal Investigative Service, IRS Criminal Investigation, Defense Criminal Investigative Service, and Army Criminal Investigation Division, among other agencies.

Assistant U.S. Attorney G. Karthik Srinivasan is prosecuting the case. The Justice Department’s Cybercrime Liaison Prosecutor to Eurojust and Office of International Affairs also provided significant assistance.

The disruption effort announced today was in conjunction with Operation Magnus, a JCAT law enforcement operation to investigate RedLine and META Infostealers. The participating agencies included the Dutch National Police, Belgian Federal Police, Belgian Federal Prosecutor’s Office, United Kingdom National Crime Agency, Australian Federal Police, Portuguese Federal Police, and Eurojust.

###

Attachment:

Attachment: