

Ukrainian National Extradited to U.S. for Alleged Cybercrimes

[justice.gov/usao-wdtx/pr/ukrainian-national-extradited-us-alleged-cybercrimes](https://www.justice.gov/usao-wdtx/pr/ukrainian-national-extradited-us-alleged-cybercrimes)



Press Release

Thursday, February 15, 2024

For Immediate Release

U.S. Attorney's Office, Western District of Texas

AUSTIN, Texas – A Ukrainian national was extradited to the United States from the Netherlands after being indicted for crimes related to fraud, money laundering and aggravated identity theft.

According to court documents, Mark Sokolovsky, 28, conspired to operate the Raccoon Infostealer as a malware-as-a-service or “MaaS.” Individuals who deployed Raccoon Infostealer to steal data from victims leased access to the malware for approximately \$200 per month, paid for by cryptocurrency. These individuals used various ruses, such as email phishing, to install the malware onto the computers of unsuspecting victims. Raccoon Infostealer then stole personal data from victim computers, including log-in credentials, financial information, and other personal records. Stolen information was used to commit financial crimes or was sold to others on cybercrime forums.

In March 2022, concurrent with Sokolovsky’s arrest by Dutch authorities, the FBI and law enforcement partners in Italy and the Netherlands dismantled the digital infrastructure supporting the Raccoon Infostealer, taking its then existing version offline.

Sokolovsky is charged with one count of conspiracy to commit fraud and related activity in connection with computers; one count of conspiracy to commit wire fraud; one count of conspiracy to commit money laundering; and one count of aggravated identity theft. He made his initial court appearance Feb. 9, and is being held in custody pending trial.

Through various investigative steps, the FBI has collected data stolen from many computers that cyber criminals infected with Raccoon Infostealer, including more than 50 million unique credentials and forms of identification. The United States does not believe it is in possession of all the data stolen by Raccoon Infostealer and continues to investigate. The FBI has created a website where anyone can input their email address to determine whether it is contained within the U.S. government's repository of Raccoon Infostealer stolen data: <https://raccoon.ic3.gov/home>. Victims of the Raccoon Infostealer can find more information at www.justice.gov/usao-wdtx/victim-assistance-raccoon-infostealer.

U.S. Attorney Jaime Esparza for the Western District of Texas, Special Agent in Charge Aaron Tapp for the FBI San Antonio Division, and Special Agent in Charge Paul DelleDonne for The Department of the Army Criminal Investigation Division would also like to thank the Justice Department's Office of International Affairs and the FBI Legal Attachés in Rome; The Hague, Kyiv, and Warsaw for their critical assistance; and the following foreign partners: Ministry of Justice of Italy; Special Unit for the Protection of Privacy and Technological Fraud of the Italian Guardia di Finanza; Procura della Repubblica di Brescia; the Netherlands Ministry of Justice and Security; Dutch National Police; and Netherlands Public Prosecution Service.

An indictment is merely an allegation and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

###

Contact

USATXW.MedialInquiry@usdoj.gov

Updated February 16, 2024
