Newly Unsealed Indictment Charges Ukrainian National with International Cybercrime Operation

Published: 2022-10-25 · Archived: 2026-04-10 02:36:01 UTC

AUSTIN – A newly unsealed federal grand jury indictment charges Mark Sokolovsky, 26, a Ukrainian national, for his alleged role in an international cybercrime operation known as Raccoon Infostealer, which infected millions of computers around the world with malware.

According to court documents, Sokolovsky, who is currently being held in the Netherlands pursuant to an extradition request by the United States, 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.

Through various investigative steps, the FBI has collected data stolen from many computers that cyber criminals infected with Raccoon Infostealer. While an exact number has yet to be verified, FBI agents have identified more than 50 million unique credentials and forms of identification (email addresses, bank accounts, cryptocurrency addresses, credit card numbers, etc.) in the stolen data from what appears to be millions of potential victims around the world. The credentials appear to include over four million email addresses. 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. The website is raccoon.ic3.gov. If the email address is within the data, the FBI will send an email to that address notifying the user. Potential victims are encouraged to fill out a detailed complaint and share any financial or other harm experienced from their information being stolen at FBI's Internet Crime Complaint Center (IC3) at ic3.gov/Home/FileComplaint.

"This case highlights the importance of the international cooperation that the Department of Justice and our partners use to dismantle modern cyber threats," said Deputy Attorney General Lisa O. Monaco. "As reflected in the number of potential victims and global breadth of this attack, cyber threats do not respect borders, which makes international cooperation all the more critical. I urge anyone who thinks they could be a victim to follow the FBI's guidance on how to report your potential exposure."

"I applaud the hard work of the agents and prosecutors involved in this case as well as our international partners for their efforts to disrupt the Raccoon Infostealer and gather the evidence necessary for indictment and

notification to potential victims," U.S. Attorney Ashley C. Hoff said. "This type of malware feeds the cybercrime ecosystem, harvesting valuable information and allowing cyber criminals to steal from innocent Americans and citizens around the world. I urge the public to visit the FBI's Raccoon Infostealer website, find out if their email is within the stolen data, and file a victim complaint through the FBI's IC3 website."

"Today's case is a further reminder the FBI will relentlessly pursue and bring to justice cyber criminals who seek to steal from the American public," said FBI Deputy Director Paul Abbate. "We have once again leveraged our unique authorities, world-class capabilities, and enduring international partnerships to maximize impact against cyber threats. We will continue to use all available resources to disrupt these attacks and protect American citizens. If you believe you're a victim of this cybercrime, we urge you to visit raccoon.ic3.gov."

"This case highlights the FBI's unwavering commitment to work closely with our law enforcement and private sector partners around the world to hold cybercriminals accountable for their actions and protect the American people from cybercrime," said FBI Special Agent in Charge Oliver E. Rich Jr. "This case also serves as a reminder to public and private sector organizations of the importance to report internet crime and cyber threats to law enforcement as soon as possible. Working together is the only way we're going to stay ahead of rapidly changing cyber threats."

"This indictment demonstrates the resolve and close cooperation of the Army Criminal Investigation Division and the FBI working jointly to protect and defend the United States," stated Special Agent in Charge Marc Martin, Army CID's Cyber Field Office. "Army CID would also like to thank our law enforcement partners in Italy and the Netherlands."

Sokolovsky is charged with one count of conspiracy to commit computer 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. The Amsterdam District Court issued a decision on September 13, 2022, granting the defendant's extradition to the United States. Sokolovsky has appealed that decision.

If convicted, Sokolovsky faces a maximum penalty of 20 years in prison for the wire fraud and money laundering offenses, five years for the conspiracy to commit computer fraud charge, and a mandatory consecutive two-year term for the aggravated identity theft offense. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI's Austin Cyber Task Force, with the assistance of the Department of the Army Criminal Investigation Division (Army CID), is investigating the case. The FBI Austin Cyber Task Force is supported by Army CID, Austin Police Department, the Naval Criminal Investigative Service, the Round Rock Police Department and the Texas Department of Public Safety.

Victims of the Raccoon Infostealer can find more information at www.justice.gov/usao-wdtx/victim-assistance-raccoon-infostealer. Assistant U.S. Attorneys Michael C. Galdo and G. Karthik Srinivasan are prosecuting the case. The Department of Justice's Office of International Affairs is assisting with foreign evidence requests and the extradition request.

U.S. Attorney Hoff and Special Agent in Charge Rich would also like to thank the FBI Legal Attachés in Rome, The Hague, and Warsaw for their assistance in the investigation and disruption of the Raccoon Infostealer, along with 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; Netherlands Police; and Netherlands Public Prosecution Service.

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

###
