

French cybercriminal pleads guilty to fraud and aggravated identity theft for hacking private information

Published: 2023-09-27 · Archived: 2026-04-02 11:57:37 UTC

Seattle – A 22-year-old French citizen from Epinal, France, pleaded guilty to conspiracy to commit wire fraud and aggravated identity theft in U.S. District Court in Seattle, announced Acting U.S. Attorney Tessa M. Gorman. Sebastien Raoult, aka Sezyo Kaizen, was arrested last year in Morocco and was extradited to the U.S. in January 2023. Raoult and two co-conspirators were indicted by a grand jury sitting in the Western District of Washington in June 2021.

“People often think their actions from behind a screen won’t have consequences for them. Raoult and his co-conspirators used deceptive tactics to trick people into sharing personal login information and breached confidential data from numerous companies,” said Acting U.S. Attorney Tessa M. Gorman. “The FBI Seattle Cyber Task Force and our office’s cyber unit work tirelessly to ensure victims of fraud and hacking like this get justice.”

According to the plea agreement, Raoult and his co-conspirators hacked into protected computers of corporate entities for the theft of confidential information and customer records, including personally identifiable information and financial information. They hacked numerous companies, including companies in Washington State, elsewhere in the United States, and around the world. After Raoult and his co-conspirators hacked companies, a user going by the name ShinyHunters posted hacked data from many of those companies for sale on dark web forums, including RaidForums, EmpireMarket, and Exploit. Between April 2020 and July 2021, ShinyHunters posted sales of hacked data from more than 60 companies. Sometimes ShinyHunters threatened to leak or sell stolen sensitive files if the victim did not pay a ransom.

According to the records filed in the case, Raoult helped create websites that pretended to be login pages belonging to legitimate businesses. The conspirators sent phishing emails to company employees that were designed to look like they came from legitimate businesses and contained links to those login pages. Victims provided their account sign-on credentials on those fake login pages, and the conspirators obtained the victims’ credentials. Raoult and his co-conspirators used the login information to breach victims’ accounts, steal the data stored there, and search the stolen data for credentials to access additional data on companies’ networks and third-party service providers, such as cloud storage services. In total, the conspirators stole hundreds of millions of customer records and caused loss to victim companies that is estimated to exceed \$6 million.

The conspiracy to commit wire fraud is punishable by a maximum of 27 years in prison. Aggravated identity theft is punishable by a mandatory minimum two-year prison term to follow any other prison sentence imposed in the case.

The case is being investigated by the FBI Seattle Cyber Task Force. The case is being prosecuted by Assistant United States Attorney Miriam R. Hinman. DOJ’s Office of International Affairs is providing substantial

assistance. The Department of Justice also appreciates the significant cooperation and assistance provided by Moroccan and French authorities.

Source: <https://www.justice.gov/usao-wdwa/pr/french-cybercriminal-pleads-guilty-fraud-and-aggravated-identity-theft-hacking-private>