

Alleged French cybercriminal to appear in Seattle on indictment for conspiracy, computer intrusion, wire fraud and aggravated identity theft

 justice.gov/usao-wdwa/pr/alleged-french-cybercriminal-appear-seattle-indictment-conspiracy-computer-intrusion

January 26, 2023



Press Release

A member of the so-called “ShinyHunters Group,” the defendant was arrested in Morocco and extradited to the U.S.

Seattle – A 21-year-old French citizen from Epinal, France, will appear tomorrow January 27, 2023, in U.S. District Court in Seattle on a nine-count indictment alleging conspiracy to commit computer fraud and abuse, conspiracy to commit wire fraud, four counts of wire fraud and three counts of aggravated identity theft, announced U.S. Attorney Nick Brown.

Sebastien Raoult aka Sezyo Kaizen, was arrested last year in Morocco and was extradited to the U.S. this week. Raoult and two co-conspirators were indicted by a grand jury sitting in the Western District of Washington on June 23, 2021. Raoult’s initial appearance will be at 2:00 PM in front of Magistrate Judge Michelle L. Peterson

“Too many bad actors believe they can illegally access proprietary information and personal financial information by hiding behind a keyboard,” said U.S. Attorney Nick Brown. “FBI Seattle Cyber Task Force and our experienced cyber unit is working diligently to identify, arrest, and prosecute those who seek to victimize people, businesses, and industries in the Western District of Washington and around the world.”

According to the indictment, Raoult was a participant in a hacking group that dubbed itself the “ShinyHunters.” The conspirators allegedly hacked into protected computers of corporate entities for the theft of proprietary and corporate information. The group advertised sensitive stolen data for sale and sometimes threatened to leak or sell stolen sensitive files if

the victim did not pay a ransom. Since early 2020, ShinyHunters Group has marketed and promoted data stolen from more than 60 companies in Washington State and elsewhere around the world.

According to the indictment, the conspirators created websites that appeared to be login pages belonging to legitimate businesses. The conspirators allegedly sent phishing emails to company employees that were designed to look like they came from legitimate businesses and contained links to those login pages. When victims provided their account sign-on credentials on those login pages, the conspirators obtained the victims' credentials. Using the stolen credentials, the conspirators allegedly accessed protected computers with companies' data.

The ShinyHunters maintained accounts on various dark web sites where they advertised stolen data for sale, including customer databases with personal and financial information. The conspirators also used social media accounts to direct potential buyers to the dark web marketplaces to purchase stolen data. Sometimes the conspirators alerted the media to their hacking or posted images on a victim website claiming credit for hacking the company.

Some of the victims of the ShinyHunters hacking were located in the Western District of Washington but others were located around the world. The victims range from tech companies, to an international stock trading company, to an apparel company, and a nutrition and fitness company. Millions of customer records were included in the stolen data.

In addition to the conspiracy counts, the wire fraud counts correspond to particular malicious emails to entities in the State of Washington and other transmissions involving the State of Washington. The three identity theft counts are for the use of other people's log-in credentials to access victim company data.

In addition to Raoult, the indictment charges 23-year-old Gabriel Kimiaie-Asadi Bildstein aka "Kuroi" and "Gnostic Players," of Tarbes, France, and 22-year-old Abdel-Hakim El Ahmadi aka "Zac" and "Jordan Keso" of Lyon, France.

The conspiracy to commit computer fraud and abuse charge is punishable by a maximum of ten years in prison. The conspiracy to commit wire fraud count is punishable by a maximum of 27 years in prison. Wire fraud is punishable by a maximum of 20 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 charges contained in the indictment are only allegations. A person is presumed innocent unless and until he or she is proven guilty beyond a reasonable doubt in a court of law.

The case is being investigated by the FBI Seattle Cyber Task Force. The case is being prosecuted by Assistant United States Attorney Miriam 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.

[raoult_et_al_indictment_flat.pdf](#) (3.53 MB)

Contact

Press contact for the U.S. Attorney's Office is Communications Director Emily Langlie at (206) 553-4110 or Emily.Langlie@usdoj.gov.

Updated January 26, 2023

Topics

Cybercrime

Identity Theft

Component

[USAO - Washington, Western](#)

Press Release Number: 5