Cybercrime websites selling hacking tools to transnational organized crime groups seized

justice.gov/usao-sdtx/pr/cybercrime-websites-selling-hacking-tools-transnational-organized-crime-groups-seized

January 30, 2025

Press Release

HOUSTON – A total of 39 domains and their associated servers have been seized in a coordinated effort involving an international disruption of a Pakistan-based network of online marketplaces selling hacking and fraud-enabling tools a group known as Saim Raza (aka HeartSender) operated, announced U.S. Attorney Nicholas J. Ganjei along with Supervisory Official Antoinette T. Bacon of the Justice Department's Criminal Division and Special Agent in Charge Douglas Williams of the FBI.

The seizures occurred Jan. 29 and were conducted in coordination with the Dutch National Police.

According to the affidavit filed in support of these seizures, Saim Raza has used these cybercrime websites since at least 2020 to sell phishing toolkits and other fraud-enabling tools to transnational organized crime groups who used them to target numerous victims in the United States, resulting in over $3 million in victim losses.

> "Almost everyone has a friend or loved one that has been affected by these types of computer hacks," said Ganjei. "These scams not only target businesses but individuals as well and cause significant hardship to the victims. Even though these people reside abroad, the use of these websites made it easy for them to spread their malicious hacking tools for a fee. However, today we have significantly disrupted their ability to harm others."

The Saim Raza-run websites operated as marketplaces that advertised and facilitated the sale of tools such as phishing kits, scam pages and email extractors often used to build and maintain fraud operations. Not only did Saim Raza make these tools widely available on the open internet, it also trained end users on how to use the tools against victims by linking to instructional YouTube videos on how to execute schemes using these malicious programs, making them accessible to criminal actors that lacked this technical criminal expertise. The group also advertised its tools as "fully undetectable" by antispam software.

The transnational organized crime groups and other cybercrime actors who purchased these tools primarily used them to facilitate business email compromise schemes wherein the cybercrime actors tricked victim companies into making payments to a third party. Those payments would instead be redirected to a financial account the perpetrators controlled, resulting in significant losses to victims. These tools were also used to acquire victim user credentials and utilize those credentials to further these fraudulent schemes. The seizure of these domains is intended to disrupt the ongoing activity of these groups and stop the proliferation of these tools within the cybercriminal community.

The FBI Houston Field Office is conducting the investigation. The Justice Department appreciates the cooperation and significant assistance law enforcement partners in the Netherlands have provided.

Assistant U.S. Attorney Rodolfo Ramirez and Trial Attorney Gaelin Bernstein of the Criminal Division's Computer Crime and Intellectual Property Section are prosecuting the case.

Updated January 30, 2025

Topic

Cybercrime

Component

USAO - Texas, Southern

Related Content

Press Release

Previously extradited Nigerian national sent to prison for role in multimillion-dollar business email compromise scheme
A 45-year-old dual citizen of Nigeria and the United Kingdom has been ordered to federal prison following his conviction in a wire fraud conspiracy involving two districts

October 1, 2024

Press Release

Previously extradited Nigerian national pleads guilty for his role in multimillion dollar business email compromise scheme
A 45-year-old Nigerian national previously extradited from the United Kingdom has pleaded guilty to wire fraud conspiracy

April 8, 2024

Press Release

U.S. government disrupts botnet People's Republic of China used to conceal hacking of critical infrastructure

A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-sponsored hackers

January 31, 2024