An official website of the United States government Here's how you know

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, June 10, 2021

Slilpp Marketplace Disrupted in International Cyber Operation

Slilpp was a Marketplace for Allegedly Stolen Online Account Login Credentials, Offering Over 80 Million Stolen Credentials for Over 1,400 Victim Providers Worldwide

The Justice Department today announced its participation in a multinational operation involving actions in the United States, Germany, the Netherlands, and Romania to disrupt and take down the infrastructure of the online marketplace known as Slilpp.

According to a seizure warrant affidavit that was unsealed today, since 2012, the Slilpp marketplace has been selling stolen login credentials, including usernames and passwords for bank accounts, online payment accounts, mobile phone accounts, retailer accounts, and other online accounts. According to the affidavit, the Slilpp marketplace allowed vendors to sell, and customers to buy, stolen login credentials by providing the forum and payment mechanism for such transactions; Slilpp buyers subsequently used those login credentials to conduct unauthorized transactions (such as wire transfers) from the related accounts. To date, over a dozen individuals have been charged or arrested by U.S. law enforcement in connection with the Slilpp marketplace.

According to the affidavit, the FBI, working in coordination with foreign law enforcement partners, identified a series of servers that hosted the Slilpp marketplace infrastructure and its various domain names. Those servers and domain names were seized pursuant to domestic and international legal process.

"The Slilpp marketplace allegedly caused hundreds of millions of dollars in losses to victims worldwide, including by enabling buyers to steal the identities of American victims," said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department's Criminal Division. "The department will not tolerate an underground economy for stolen identities, and we will continue to collaborate with our law enforcement partners worldwide to disrupt criminal marketplaces wherever they are located."

"With today's coordinated disruption of the Slilpp marketplace, the FBI and our international partners sent a clear message to those who, as alleged, would steal and traffic in stolen identities: we will not allow cyber threats to go unchecked," said Acting U.S. Attorney Channing D. Phillips of the District of Columbia. "We applaud the efforts of the FBI and our international partners who contributed to the effort to mitigate this global threat."

"American identities are not for sale," said Assistant Director in Charge Steven M. D'Antuono of the FBI Washington Field Office. "The FBI remains committed to working with our international partners to dismantle global cyber threats."

At the time of the disruption, the affidavit alleges that stolen account login credentials for over 1,400 account providers were available for sale on the Slilpp marketplace. According to the affidavit, a fraction of the victimized account providers have calculated losses so far; based on limited existing victim reports, the stolen login credentials sold over Slilpp have been used to cause over $200 million in losses in the United States. The full impact of Slilpp is not yet known.

The U.S. Attorney's Office for the District of Columbia, the FBI Washington Field Office, and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) conducted the operation in close cooperation with investigators and prosecutors from several jurisdictions, including Germany's Bundeskriminalamt, the Netherlands' National High Tech Crime Unit, and Romania's Directorate for the Investigation of Organized Crime and Terrorism. The Justice Department's Office of International Affairs also provided significant assistance.

CCIPS Senior Counsel Laura-Kate Bernstein and Assistant U.S. Attorney Demian Ahn of the District of Columbia led the U.S. efforts.

In September 2020, FBI Director Christopher Wray announced the FBI's new strategy for countering cyber threats. The strategy focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. Victims are encouraged to report the incident online with the Internet Crime Complaint Center (IC3) at https://www.ic3.gov/. For more information on ransomware prevention, visit: https://www.ic3.gov/media/2016/160915.aspx.

Topic(s):
Cyber Crime

Press Release Number:
21-542

Component(s):
Criminal Division
Criminal - Computer Crime and Intellectual Property Section
Criminal - Office of International Affairs
Federal Bureau of Investigation (FBI)
USAO - District of Columbia

Updated June 10, 2021