Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks

Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is designating **Zhou Shuai,** a Shanghai-based malicious cyber actor and data broker, and his company, **Shanghai Heiying Information Technology Company, Limited** (Shanghai Heiying). In collaboration with another malicious cyber actor, U.S.-sanctioned Yin Kecheng, Zhou Shuai illegally acquired, brokered, and sold data from highly sensitive U.S. critical infrastructure networks.

ZHOU SHUAI: CHINESE HACKER AND DATA BROKER

Since at least 2018, **Zhou Shuai** has acted as a data broker, selling illegally exfiltrated data and access to compromised computer networks. At least some of this data was acquired by known China-backed malicious cyber actor and former Shanghai Heiying employee Yin Kecheng. Yin Kecheng, who was sanctioned by OFAC on January 17, 2025, was involved in the 2024 compromise of the Department of the Treasury's network. Notable U.S. victims of Yin Kecheng and Zhou Shuai's partnership include technology companies, a defense industrial base contractor, a communications service provider, an academic health system affiliated with a university, and a government county municipality.

In 2020, Zhou Shuai appeared to be working from a set of intelligence requirements that included targets within the United States, Russia, and Western Europe. Data types of interest included telecommunications data, border crossing data, data on personnel in religious research, data on media industry personnel, and data on public servants. These requirements almost certainly originated from the CCP's intelligence services. In early 2021, Zhou Shuai brokered the sale of documents stolen from a U.S. cleared defense contractor.

SHANGHAI HEIYING: A HAVEN FOR HACKERS

Zhou Shuai established **Shanghai Heiying Information Technology Company, Limited** (Shanghai Heiying) in 2010 and is still its majority owner. Shanghai Heiying is a Shanghai-based cybersecurity company that has employed numerous known China-backed malicious cyber actors, including Yin Kecheng.

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked.

Dated 5 March, 2025