William D. Hyslop
United States Attorney
Eastern District of Washington
James A. Goeke
Assistant United States Attorney
Eastern District of Washington
Scott K. McCulloch
Department of Justice Trial Attorney
National Security Division
Post Office Box 1494
Spokane, Washington 99210 1494
Telephone: (509) 353 2767

FILED IN THE
U.S. DISTRICT COURT
EASTERN DISTRICT OF WASHINGTON

Jul 07, 2020

SEAN F. McAVOY, CLERK

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA,

Plaintiff,

v.

LI XIAOYU (a/k/a "Oro0lxy") and DONG JIAZHI,

Defendants.

4:20-CR-6019-SMJ

INDICTMENT

Vio.: 18 U.S.C. §§ 371, 1030(a)(2)(B), (a)(2)(C), (a)(5)(A)
Conspiracy to Access Without Authorization and Damage Computers (Count 1)

18 U.S.C. § 1832(a)(1-3), 1832(a)(5)
Conspiracy to Commit Theft of Trade Secrets (Count 2)

18 U.S.C. § 1030(a)(2)(B), (a)(2)(C), (b), (c)(2)(B)(i-iii)
Unauthorized Access to Computers (Count 3)

18 U.S.C. §§ 1349, 1343,
Conspiracy to Commit Wire Fraud (Count 4)

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

18 U.S.C. §§ 1028A, 2
Aggravated Identity Theft
(Counts 5-11)

Criminal Forfeiture Allegations
18 U.S.C. §§ 982(a)(2)(B),
1030(i)(1)

The Grand Jury charges:

At all times relevant to this Indictment, unless otherwise stated:

INTRODUCTION

1. Beginning no later than September 2009 and continuing until at least the date of this Indictment, together, Defendants LI XIAOYU (a/k/a "Oro0lxy") (hereinafter "LI" and/or "LI XIAOYU") and DONG JIAZHI (hereinafter "DONG" and/or "DONG JIAZHI") and collectively the "Defendants," each a hacker in the People's Republic of China ("China" or "PRC"), gained unauthorized access to computers around the world and stole terabytes of data.

2. LI and DONG, former classmates at an electrical engineering college in Chengdu, China, used their technical training to hack the computer networks of a wide variety of victims, such as companies engaged in high tech manufacturing; civil, industrial, and medical device engineering; business, educational, and gaming software development; solar energy; and pharmaceuticals. More recently, they researched vulnerabilities in the networks of biotech and other firms publicly known for work on COVID-19 vaccines, treatments, and testing technology. Their victim companies were located all across the world, including among other places the United States, Australia, Belgium, Germany, Japan, Lithuania, the Netherlands, South Korea, Spain, Sweden, and the United Kingdom.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

3. The Defendants stole hundreds of millions of dollars' worth of trade secrets, intellectual property, and other valuable business information. At least once, they returned to a victim from which they had stolen valuable source code to attempt an extortion—threatening to publish on the internet, and thereby destroy the value of, the victim's intellectual property unless a ransom was paid.

4. LI and DONG did not just hack for themselves. While in some instances they were stealing business and other information for their own profit, in others they were stealing information of obvious interest to the PRC Government's Ministry of State Security ("MSS"). LI and DONG worked with, were assisted by, and operated with the acquiescence of the MSS, including MSS Officer 1, known to the Grand Jury, who was assigned to the Guangdong regional division of the MSS (the Guangdong State Security Department, "GSSD").

5. When stealing information of interest to the MSS, LI and DONG in most instances obtained that data through computer fraud against corporations and research institutions. For example, from victims including defense contractors in the U.S. and abroad, LI and DONG stole information regarding military satellite programs; military wireless networks and communications systems; high powered microwave and laser systems; a counter-chemical weapons system; and ship-to-helicopter integration systems.

6. In other instances, the Defendants provided the MSS with personal data, such as the passwords for personal email accounts belonging to individual Chinese dissidents. For example, they provided the MSS with email accounts and passwords belonging to a Hong Kong community organizer, the pastor of a Christian church in Xi'an, and a dissident and former Tiananmen Square protestor. The Defendants also stole email account contents of obvious interest to the PRC Government, such as emails between that same dissident and the office of the Dalai Lama; emails belonging to a Chinese Christian "house" (*i.e.*, not PRC

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Government-approved) pastor in Chengdu, who was later arrested by the PRC government; and emails from a U.S. professor and organizer, and two Canadian residents, who advocated for freedom and democracy in Hong Kong. In some instances the Defendants reacted quickly to the PRC government's perceived desires, targeting the above-mentioned Chengdu house pastor just days after the provincial government banned his church, and conducting reconnaissance on a webmail service and a messaging app when those were used by Hong Kong citizens protesting the PRC government's recent steps to curtail freedoms there.

7. MSS Officer 1 assisted LI and other hackers. For example, when LI encountered difficulty compromising the mail server of a Burmese human rights group, MSS Officer 1 provided him with malware—a computer program designed to compromise a victim computer system—to exploit a popular internet browser. As LI had requested, MSS Officer 1 provided him "0day" malware, *i.e.* malware unknown to the software vendor and to security researchers.

8. MSS Officer 1 and other MSS officers known to the Grand Jury purported to be researchers at the "Guangdong Province International Affairs Research Center." In fact, they were intelligence officers working for the GSSD at Number 5, 6th Crossroad, Upper Nonglin Road, Yuexiu District, in Guangzhou, at the facility depicted in in these images:

//

//

//

//

//

//

//

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.