STATE SUPPORTED CYBER CRIME:
THE U.S. CRIMINAL JUSTICE RESPONSE

Sean Newell
Deputy Chief - Cyber
Counterintelligence and
Export Control Section
November 18, 2021

What is the "Hybrid Threat"?

- Intelligence services tolerating criminal activity in exchange for criminal actors assisting in intelligence operations;
- Intelligence service officers engaging in cybercrime (potential "moonlighting"); and
- Intelligence services engaging in activities traditionally in the exclusive realm of criminal actors.

JULY 2020 – *UNITED STATES V. DING, ET AL.*

Ministry of State Security's (MSS) Guangdong State Security Department (GSSD)

Alleged Motivations:

- Intrusions for their own monetary benefit.
- Intrusions seeking data of obvious interest to the Ministry of State Security.

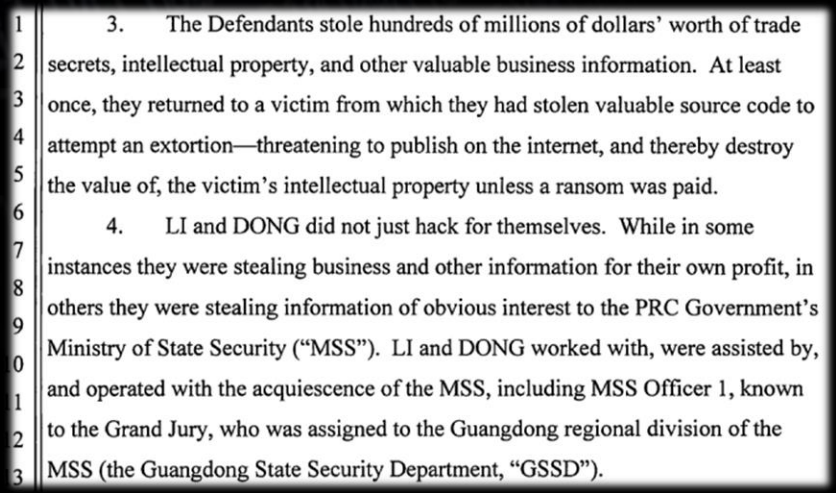
Targeted countries:

- United States
- Australia
- Belgium
- Germany
- Japan
- Lithuania
- The Netherlands
- South Korea
- Spain
- Sweden
- United Kingdom

WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft



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").

SEPT. 2020 – *UNITED STATES V. JIANG, ET AL*

"APT 41"

Alleged Motivations:

- Intrusions for their own monetary benefit:
  - Ransomware;
  - Crypto-Jacking; and
  - Supplying stolen "digital goods" to Malaysian gaming company.

- Intrusions seeking data of obvious interest to the PRC government.

- More than 100 victims worldwide.

An"), the PRC Ministry of Public Security. JIANG advised his associate not to "touch domestic stuff anymore." JIANG's associate agreed, explaining that, if he were to commit such "a crime, [he] couldn't even get out of Sichuan [Province in the PRC]." JIANG boasted that he was "the classic example of maintaining low key," and claimed that he was "very close" with the "GA", meaning the PRC Ministry of State Security. JIANG and his associate agreed that JIANG's working relationship with the Ministry of State Security provided JIANG protection, because that type of association with the Ministry of State Security provided such protection, including from the Ministry of Public Security, "unless something very big happens."

FEB. 2021 – *UNITED STATES V. PARK, ET AL.*

Reconnaissance General Bureau
(a/k/a/ “Lazarus Group” and “APT 38”)

Range of criminal activities:

- Bank heists;
- ATM cash-outs;
- Ransomware/Extortion;
- Theft of cryptocurrency; and
- Malicious cryptocurrency apps.

Attempted theft of more than $1.3 billion.

Victims in more than 150 countries worldwide.

ARRESTS

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Wednesday, September 8, 2021

International Money Launderer Sentenced to More Than 11 Years in Prison for Laundering Millions of Dollars in Cyber Crime Schemes

Defendant Ordered to Pay Victims in U.S. and Elsewhere More Than $30 Million in Restitution

FOR IMMEDIATE RELEASE — Wednesday, September 16, 2020

Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China

"Chasing the Money"

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | TOPICS | NEWS | RESOURCES | CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

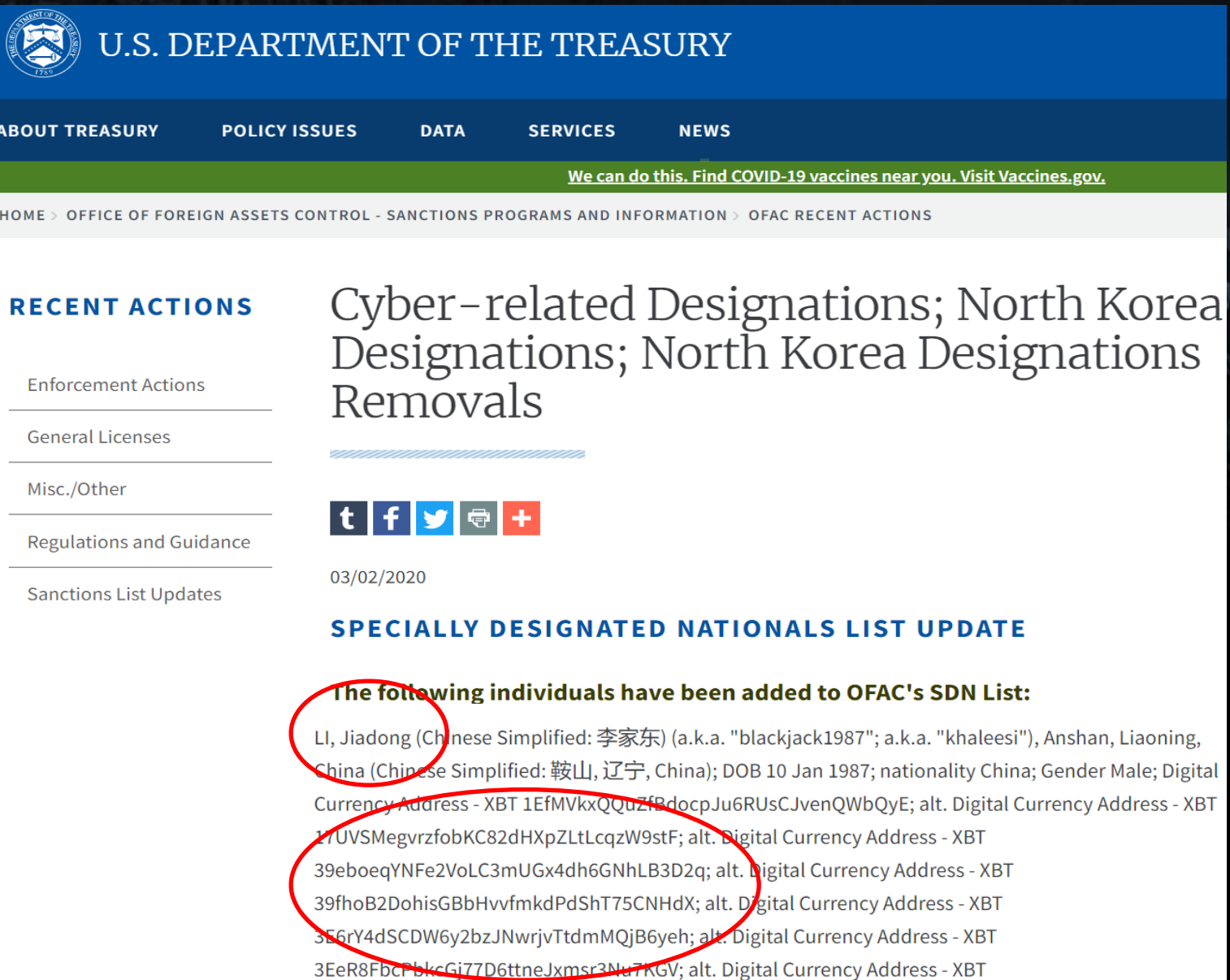
FOR IMMEDIATE RELEASE — Wednesday, February 17, 2021

Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe

Indictment Expands 2018 Case that Detailed Attack on Sony Pictures and Creation of WannaCry Ransomware by Adding Two New Defendants and Recent Global Schemes to Steal Money and Cryptocurrency from Banks and Businesses while Operating in North Korea, China

The U.S. Attorney's Office and FBI also obtained seizure warrants authorizing the FBI to seize cryptocurrency stolen by the North Korean hackers from a victim in the indictment – a financial services company in New York – held at two cryptocurrency exchanges. The seizures include sums of multiple cryptocurrencies totaling approximately $1.9 million, which will ultimately be returned to the victim.

"CHASING THE MONEY"



U.S. DEPARTMENT OF THE TREASURY

ABOUT TREASURY | POLICY ISSUES | DATA | SERVICES | NEWS

We can do this. Find COVID-19 vaccines near you. Visit Vaccines.gov.

HOME > OFFICE OF FOREIGN ASSETS CONTROL - SANCTIONS PROGRAMS AND INFORMATION > OFAC RECENT ACTIONS

RECENT ACTIONS

- Enforcement Actions
- General Licenses
- Misc./Other
- Regulations and Guidance
- Sanctions List Updates

Cyber-related Designations; North Korea Designations; North Korea Designations Removals

03/02/2020

SPECIALLY DESIGNATED NATIONALS LIST UPDATE

The following individuals have been added to OFAC's SDN List:

LI, Jiadong (Chinese Simplified: 李家东) (a.k.a. "blackjack1987"; a.k.a. "khaleesi"), Anshan, Liaoning, China (Chinese Simplified: 鞍山, 辽宁, China); DOB 10 Jan 1987; nationality China; Gender Male; Digital Currency Address - XBT 1EfMVkxQQuZfBdocpJu6RUsCJvenQWbQyE; alt. Digital Currency Address - XBT 17UVSMegvrzfobKC82dHXpZLtLcqzW9stF; alt. Digital Currency Address - XBT 39eboeqYNFe2VoLC3mUGx4dh6GNhLB3D2q; alt. Digital Currency Address - XBT 39fhoB2DohisGBbHvvfmkdPdShT75CNHdX; alt. Digital Currency Address - XBT 3E6rY4dSCDW6y2bzJNwrjvTtdmMQjB6yeh; alt. Digital Currency Address - XBT 3EeR8FbcPbkcGj77D6ttneJxmsr3Nu7KGV; alt. Digital Currency Address - XBT

Private Sector Partners

APT 41 Disruption

EMPOWERING NETWORK DEFENDERS

TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

16 Sept 2020

Alert Number
AC-000133-TT

WE NEED YOUR HELP!

If you identify any suspicious activity within your

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Indictment of China-Based Cyber Actors Associated with APT 41 for Intrusion Activities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips | Resources | Industrial Control Systems

National Cyber Awareness System > Alerts > AppleJeus: Analysis of North Korea's Cryptocurrency Malware

Alert (AA21-048A)

AppleJeus: Analysis of North Korea's Cryptocurrency Malware

Original release date: February 17, 2021 | Last revised: March 02, 2021

International Partnerships