CHINA AND NORTH KOREA

THE NORTH KOREAN CONNECTION

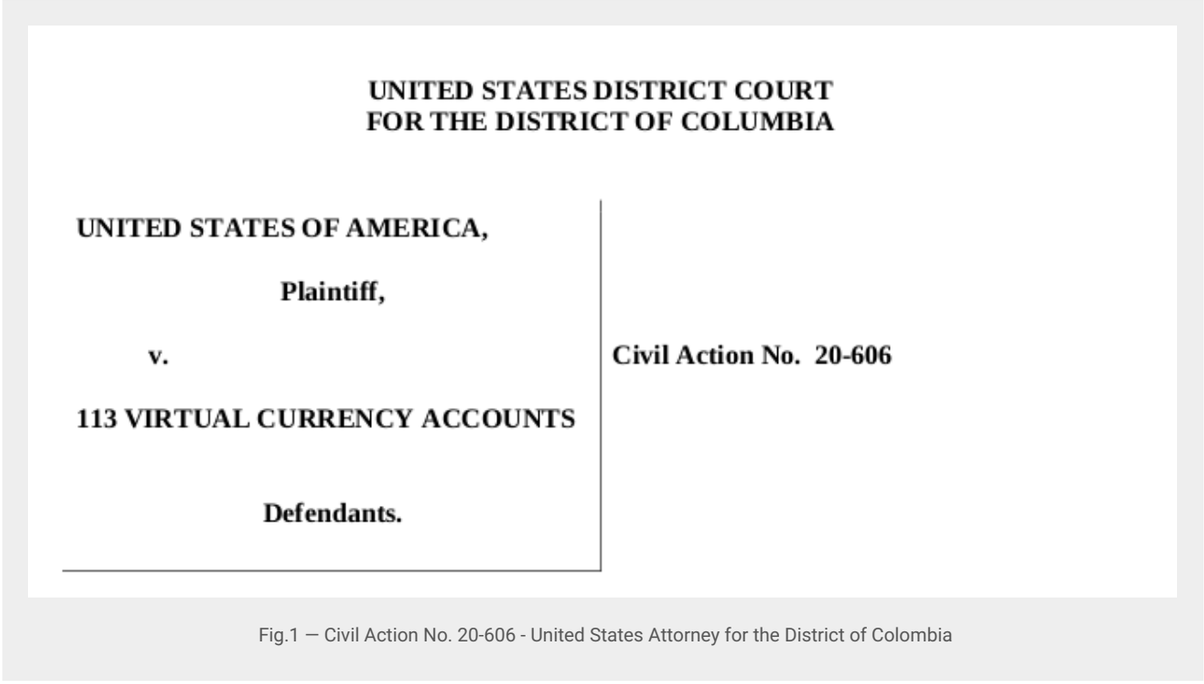
OXT RESEARCH

Introduction

Executive Summary

This report focuses on the complex laundering of thousands of BTC on behalf of the Lazarus Group, the infamous North Korean cybercrime group, by alleged conspirators engaged in money laundering on behalf of the group.

Bitcoin exchanges have been subject to mysterious hacks and breaches throughout bitcoin's history. Hacks and breaches are an inherent risk to custodial services that take control of user's private keys. The hacks are often attributed to exchange insiders, rogue, or even organized hackers.



UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. 113 VIRTUAL CURRENCY ACCOUNTS Defendants.	Civil Action No. 20-606

Fig.1 — Civil Action No. 20-606 - United States Attorney for the District of Colombia

Civil Action No. 20-606 was filed by the United States through the United States Attorney for the District of Colombia against "113 virtual currency accounts". The Complaint seeks to charge two Chinese nationals with aiding the laundering of thousands of stolen BTC on behalf of the Lazarus Group. This report will cover the following information based on the blockchain data provided in Civil Action No. 20-606:

- An overview of the hacks and available information provided in The Complaint
- Commentary on the alleged laundering of funds referenced in The Complaint
- An analysis of the on-going coin laundering alluded to in The Complaint
- Description of postmix spending behavior and destinations of mixed coins

The Complaint

Complaint Overview

On 2 March 2020, The United States Attorney for the District of Columbia filed **Civil Action No. 20-606** based on investigations by the Internal Revenue Service — Criminal Investigations Cyber Crime Unit, Homeland Security, and Federal Bureau of Investigation.

The Complaint seeks asset forfeiture from "113 virtual currency accounts" allegedly controlled by two Chinese Nationals, Tian Yinyin and Li Jiadong (The Conspirators).

The Conspirators are charged with **money laundering** (18 U.S. Code § 1956) and **operation of an unlicensed money service business** (18 U.S. Code § 1960).

The Complaint includes partial documentation of the laundering of stolen funds acquired by hacking several South Korean Bitcoin exchanges.

Fig.2 — KYC Photos of The Conspirators and Associated Usernames

The hackers gained access to exchange hot wallets through social-engineering and email phishing attacks. The Complaint links The Conspirators to North Korean operations based on evidence typical for cybercrimes. We cannot attest to the validity of these claims and expect that additional information has been withheld by law enforcement and security agencies as matters of national security.

While The Complaint does not mention the Lazarus Group, an update to the Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list alleges The Conspirators are "linked to Lazarus Group."

Targeted Exchanges

The Complaint breaks down the laundering of BTC and ETH from four exchange hacks in three phases.

The Complaint uses pseudonyms to refer to the exchanges involved in The Complaint and does not mention the exchange's actual names.

Details surrounding the hacks are generally limited to publicly available information from news reports including timing and volume of cryptocurrency hacked.

We have prepared a summary of the hacked exchanges based on publicly available information and addresses provided in The Complaint.

Table 1 — Exchanges Breached

Phase	Exchange	Amount Stolen	Breach Timeframe
I	**Bithumb** (The Exchange 1)	10,777 BTC + crypto	Mid 2018
I	**Coinrail** (The Exchange 4)	$40 million in crypto	Mid 2018
II	**Youbit** (The Exchange 2)	17% Assets	December 2018
III	**Upbit** (The Exchange 3)	342,000 ETH	November 2019

Defendant properties and entities

The Complaint lists **113** items including exchange IDs, bitcoin addresses, and other altcoin addresses to be forfeited as a part of the Civil Action.

We have documented some of the relevant histories of these accounts including Complaint annotations, volumes sent/received, current balance, and activity dates. This data can be found on Item 1 in the attached Spreadsheet.

On 6 March another 33 addresses were added to the forfeiture list. **The majority of these are Ethereum addresses with a cumulative balance of over 91,000 ETH**.

A list of the exchanges involved, and fund destinations sourced from public data and The Complaint Defendant Properties List are provided in Table 2, below.

Table 2 — Exchange Labels and Defendant Property List

Complaint Pseudonym	Label	Defendant Properties
VCE 1	**HitBTC/Changelly**	63-64
VCE 2	**KuCoin**	112
VCE 3	**Bittrex (Etherscan)**	50-52
VCE 4	**Yobit (ANON-1297295743)**	98-111
VCE 5	**Huobi**	65-70
VCE 6	**ANON-1168556017 (Unlabeled Exchange)**	55-62
VCE 7	**Paxful (ANON-1420439095)**	83-84
VCE 8	**Possibly DarkMarket (ANON-534406706), Related to ANON-1855602832**	71-80
VCE 9	**UpBit (Etherscan)**	113
VCE 10	**Binance (Etherscan)**	44-49
VCE 11	**Unlabeled (Etherscan)**	85-90
VCE 12	**Unknown**	53-54

Updates to OFAC's SDN list

On 2 March 2020, the day of The Complaint filling, the OFAC SDN list was updated to include 20 bitcoin addresses also listed in The Complaint. The addresses are clustered among **Huobi** exchange and VCE 8, a possible Dark Net Market linked to ANON-1855602832.

The Office of Foreign Assets Control is a financial intelligence and enforcement agency of the U.S. Treasury Department. OFAC publishes a list of individuals and companies that U.S. persons are generally prohibited from dealing with.

Shortly after updating the OFAC sanctions list, 13 of the sanctioned addresses received small amounts of BTC, often referred to as "dusting", in a series of two transactions.

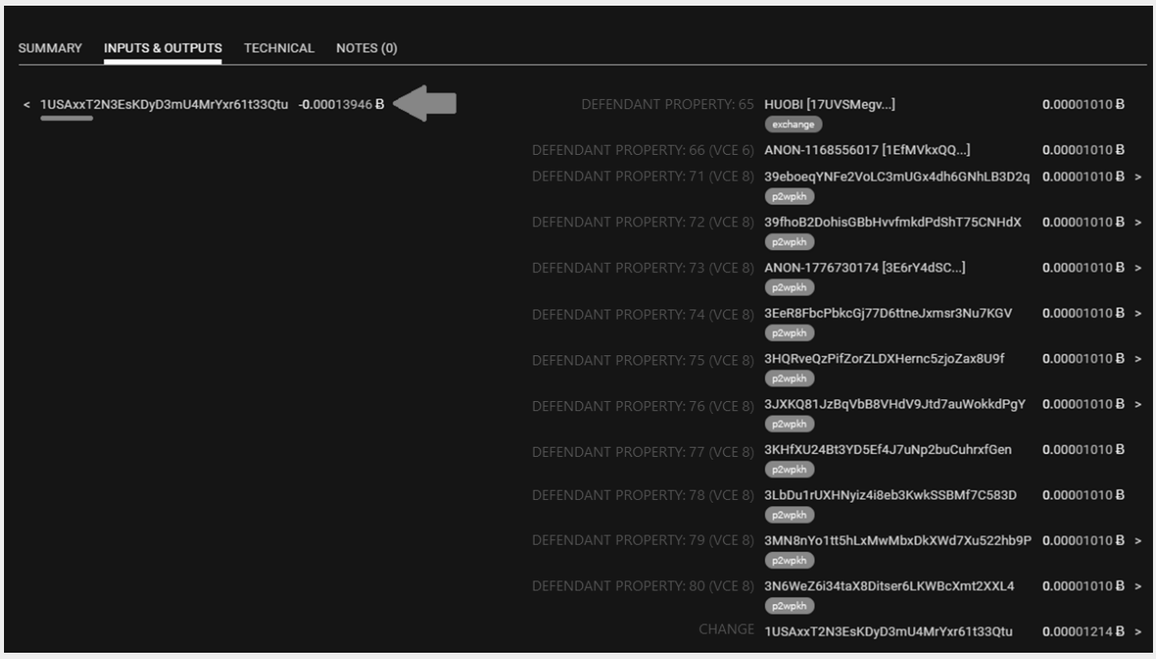


Fig.3 - "Dusting" of Sanctioned Addresses

It's illegal to send fund to entities on OFAC's SDN list, though the possible vanity address may give some hints as to who may be responsible for the "dusting". It's worth noting that "dusting" of addresses on the OFAC sanctions list is common.

A list of the updated OFAC sanctioned addresses is provided in Item 2 of the spreadsheet attached to this report.

The Laundering Process

An Act in Three Parts

The laundering of stolen coins described in The Complaint takes place in three distinct phases.

Phase I
Directly peel stolen funds from hacked or breached exchanges.

Phase II
Use of cryptocurrency exchanges that do not deal with government issued currency and therefore have less strict Know Your Customer (KYC) policies. These exchanges were used as a means of obscuring the origin of the stolen funds.

Phase III
Further peeling from the KYC-lite exchanges to exchanges with established off ramps into national currencies.

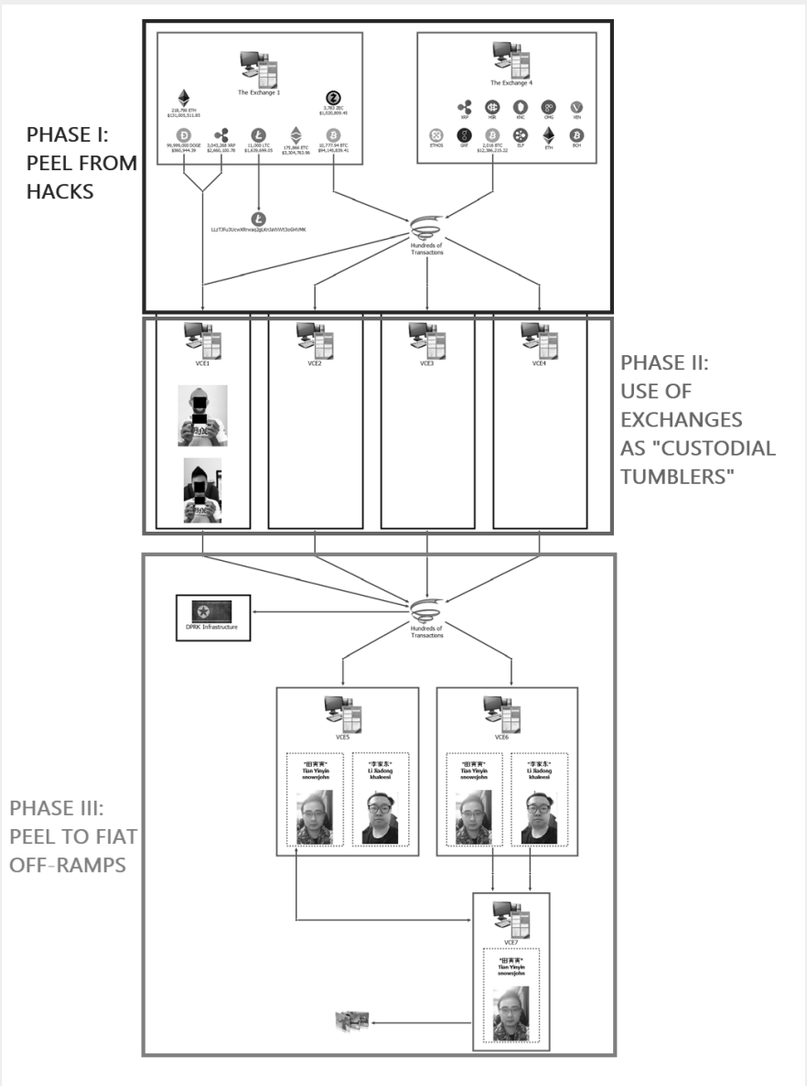


Fig.4 — Laundering Process Schematic

Phase I - Peeling Chains

Peeling chains have been implicated in the obfuscation of bitcoin transactions for some time. A peeling chain consists of a series of transactions with one input and two outputs. One of the transaction outputs (typically the smaller of the two) is interpreted as a payment to a third party. The second transaction output (typically the larger of the two) is interpreted as change back to the transaction sender.

Fig.5 — Example Transaction Graph That Can Be Interpreted as a "Peeling Chain"

Most bitcoin transactions have one input and two outputs and produce peeling chain type transaction graphs. Where the implication of "laundering" enters the transaction graph interpretation is when a peeling chain is used to make multiple payments to the same entity.

Again, these transactions are generally traceable using a transaction graph tool, but peeling chains have the advantage of bypassing compliance software flags. Rather than making a single large value deposit to a service, the total deposit is made in smaller amounts over a series of transactions.

Phase II - Exchanges as Custodial Tumblers

While "peeling chains" are implicated as the predominant method of attempted laundering in The Complaint, the major obfuscation method used by The Conspirators was transfer through KYC-lite or KYC free exchanges as a part of Phase II.

The intent being to use the exchanges as custodial "tumblers". The act of simply operating a shared wallet makes tacking of inflows and outflows of exchange wallets difficult.

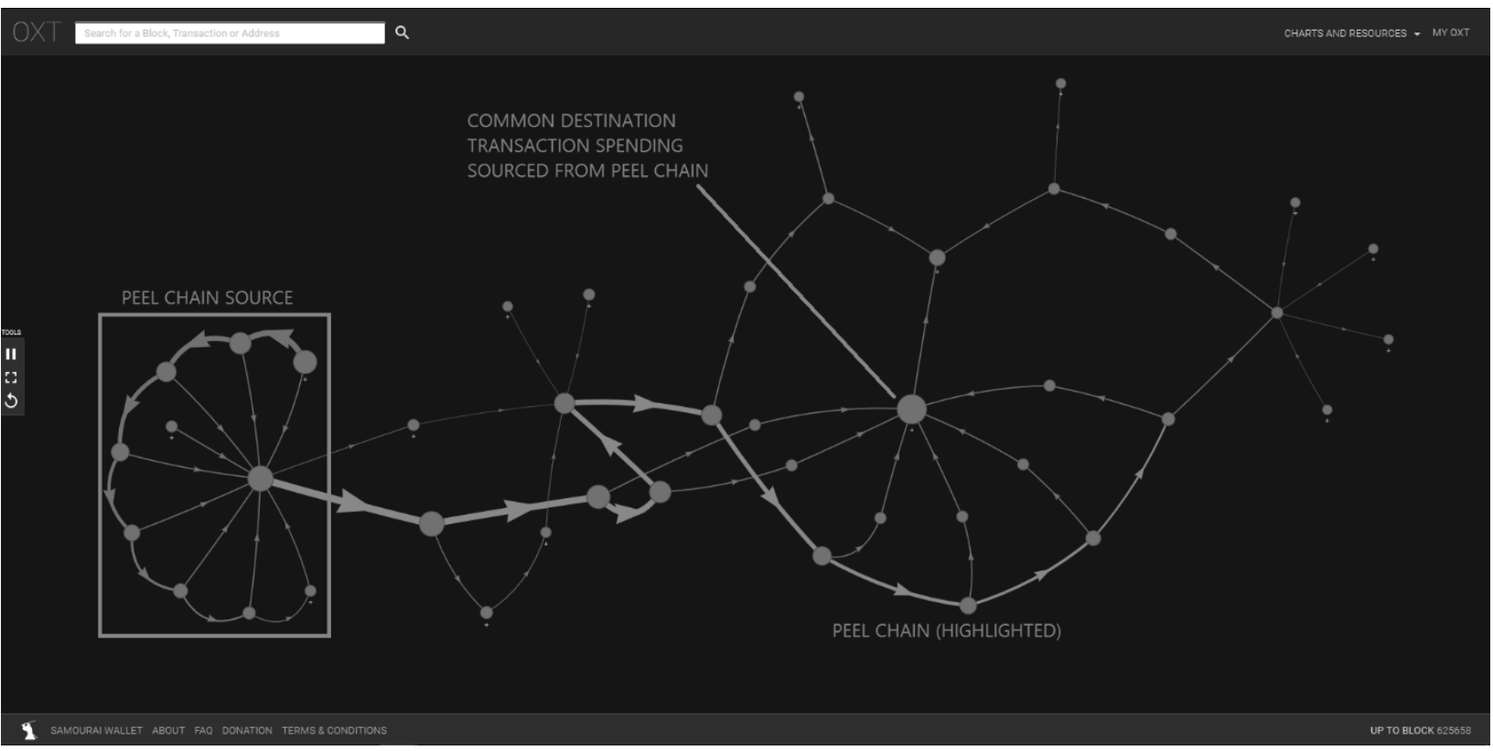


Fig.6 — "True Peeling Chain" Attempting to Obfuscate the Movement of Funds

Phase III - Exit Via Fiat Exchanges with Fiat Off-Ramps

After attempting to break the links between the breached exchanges and the stolen funds using exchanges as custodial tumblers, The Conspirators peeled funds from the first round of exchanges to exchanges with established off-ramps into national currencies.

Exchanges with established off-ramps into national currencies often require KYC (Know Your Customer) information as part of their Anti Money Laundering (AML) polices including government ID that corresponds to a linked bank account and proof of address.

The Conspirators primarily cashed out into national currencies using the services at **Huobi exchange** and ANON-1168556017 (unlabeled exchange).

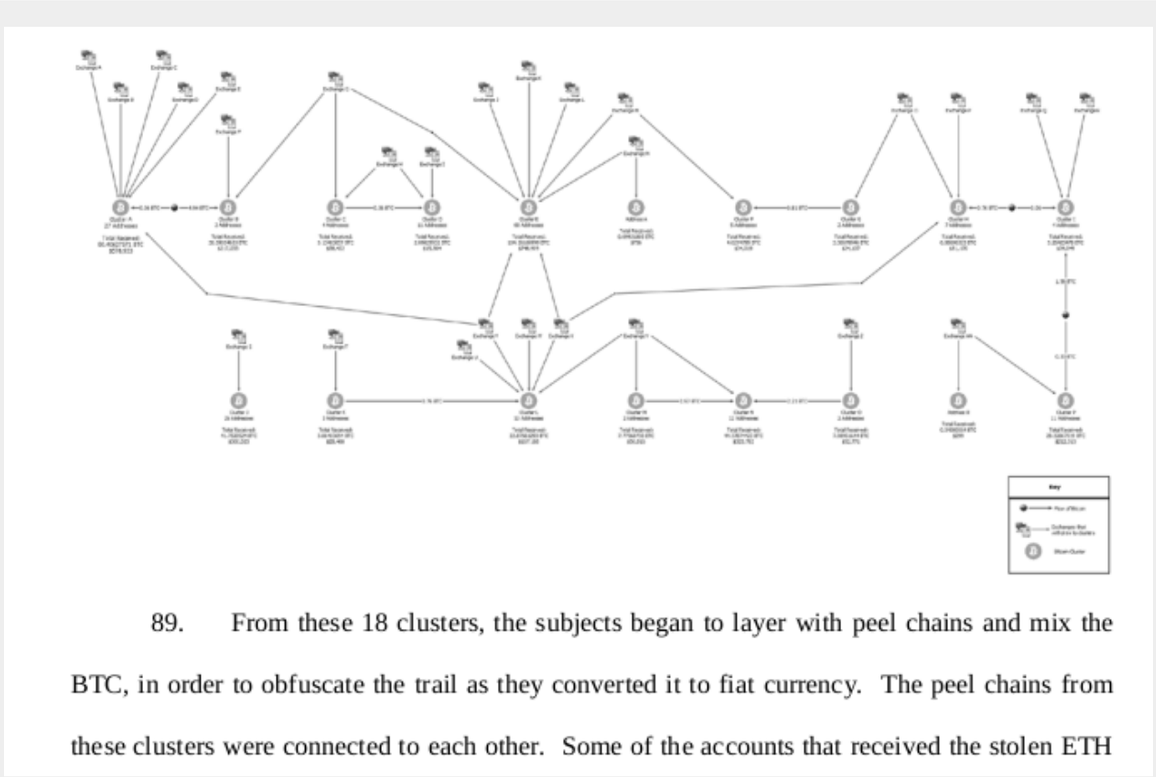
The Complaint alleges a total of 67.3 million USD in withdrawals from the noted exchanges to multiple Chinese banks. In addition, The Conspirators cashed out nearly 1.5 million dollars in iTunes giftcards using the Paxful peer-to-peer exchange.

Mixing of Laundered Funds

Overview

The majority of the addresses in the Defendants Properties list are associated directly with exchanges with the exception of the first 34 addresses which are traceable to the conversion of ETH from the November 2019 Upbit hack. The complaint details the circumstances around these addresses:

> ...approximately 18 different clusters, comprised of approximately 200 different BTC addresses (including Defendant Properties 1 through 34 and Defendant Property 91), that received 383.79970162 BTC ($2,781,754.23) from November 29, 2019 through January 4, 2020. Each of these clusters received BTC that was converted from ETH proceeds traced to the theft of The Exchange 3... From these 18 clusters, the subjects began to layer with peel chains and **mix** [emphasis added] the BTC, in order to obfuscate the trail as they converted it to fiat currency. The peel chains from these clusters were connected to each other.



89. From these 18 clusters, the subjects began to layer with peel chains and mix the BTC, in order to obfuscate the trail as they converted it to fiat currency. The peel chains from these clusters were connected to each other. Some of the accounts that received the stolen ETH

Fig.7 - The Complaint

End of Preview

Going forward updates will be provided through the OXT Research center at research.oxt.me. Given the complexity of this targeted analysis, we are available for consulting to help research teams better understand and evaluate the effects of events like this. Be on the lookout for new features from the OXT Team in the coming months.

OXT research