INTERPOL

Criminal Proceed

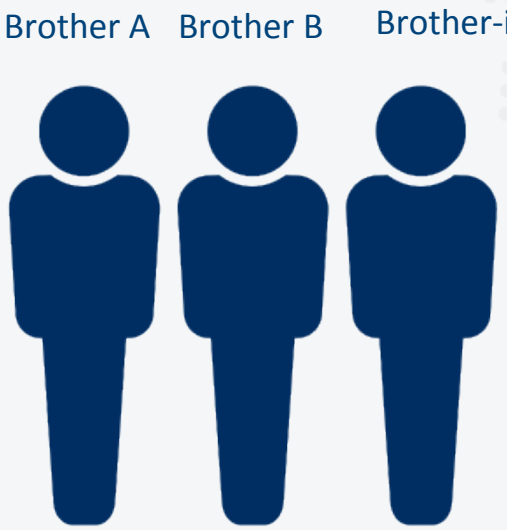
Sungjin HONG
Digital Crime Officer
Cyber Directorate

Contents

- **Cases**
  - Garlic Field Case
  - Nayana Web Hosting firm case
- **Silver Notice**
- **Solution**
  - Money tracking(Egmont Group)
  - Bitcoin tracking

- **Garlic field case**
  - The Biggest cybercrime proceed in Korea
  - Police seizure 10 million USD

- **Garlic field case**
  - Jan 2008 to Nov 2009, Subjects managed an illegal online gambling site and earned about 15 million USD from the business.



- **Garlic field case**
  - Brothers are arrested by the police and sent to a prison. the brother-in-law was to manage those criminal proceed

Brother A

Brother B
1.5 years in prison

- **Garlic field case**
  - The brother-in-law got an idea how to hide the money. He bought a garlic field and bury 10 million dollars

- **Garlic field case**
  - Later, these money is found by another police investigation and all the criminal proceed, worth 10 million USD, was confiscated. The brother-in-law was sentenced to one year in prison

- **Nayana Web Hosting Firm case**
  - On 12 June 2017, a Korean web hosting company, Nayana, experienced malware infection encrypting its 150 servers. About 3,000 clients were hosted on them

Your files have been encrypted…

Warning!!

Your documents, photos, databases, important files have been encrypted!

If you modify any file, it may cause make you cannot decrypt!!!

To decrypt your files please visit the following website:

http://7lv4vg4n26cxleel.onion.to/purchase?mid=B088433450D732AD2F5B103580842288
http://7lv4vg4n26cxleel.onion.nu/purchase?mid=B088433450D732AD2F5B103580842288
http://7lv4vg4n26cxleel.hiddenservice.net/purchase?mid=B088433450D732AD2F5B103580842288
http://7lv4vg4n26cxleel.gbe0.top/purchase?mid=B088433450D732AD2F5B103580842288
http://qzjordhlw5mqhcn7.onion.to/purchase?mid=B088433450D732AD2F5B103580842288
http://qzjordhlw5mqhcn7.onion.nu/purchase?mid=B088433450D732AD2F5B103580842288
http://qzjordhlw5mqhcn7.hiddenservice.net/purchase?mid=B088433450D732AD2F5B103580842288
http://qzjordhlw5mqhcn7.gbe0.top/purchase?mid=B088433450D732AD2F5B103580842288

If the above address will be unable to open or very slow, follow these steps:

1. Download and install the tor browser. Download Tor
2. After successful installation, run the browser, waiting to initialize.
3. In the address bar enter:

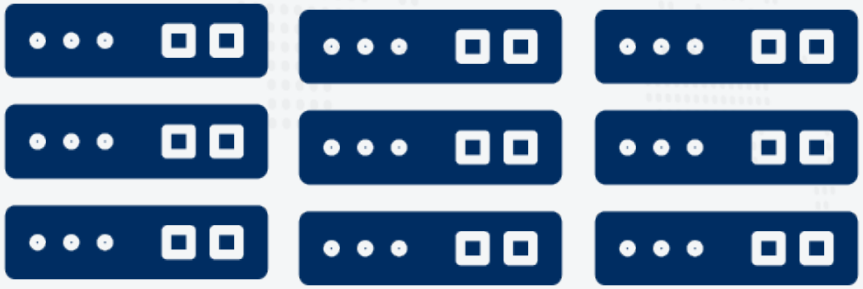
- **Nayana Web Hosting Firm case**
  - The subject asked to pay ransom, 4.4 million USD, but the CEO of the company negotiated to 1.1 million USD

- **Nayana Web Hosting Firm case**
  - The hacker used 147 Bitcoin wallets

Bitcoin Address	Amount	Date
1FYHTHCUN5ZnVTmAMTZjfqNJTvQEop6cd8	Paid(2.6685bit)	2017-06-14
1GQJ9Jcf5g1u763cxvXB5x7xkA6j2YQjoN	Paid(2.6685bit)	2017-06-14
1LtPHnpfoU7MkTbun1qEs1ef9LagZpb8Ej	Paid(2.6685bit)	2017-06-14
1CgrwWXtqqEKqTH985NoJcYXSWSChNa1ve	Paid(2.6685bit)	2017-06-14
13eSqT8mNRKiVGZ1m1e2zaPJd23f7o8YpX	Paid(2.6685bit)	2017-06-14
1GRXy69FtUUFhmByVfVoCA6A9j94XfZeG1	Paid(2.6685bit)	2017-06-14
19dmaPw6j8zvDw6zk55LCXWNr5wgm32fsX	Paid(2.6685bit)	2017-06-14
163cUdd8Tif7u6QArfSHy8CUGfAd1SjLtb	Paid(2.6685bit)	2017-06-14
1MJVgPoyRFnckjtEVtn1j3dYCBtUSpN3Vx	Paid(2.6685bit)	2017-06-14
12FtmjoSYoaFe4NYSZ3kL55m2zBnVY8r8j	Paid(2.6685bit)	2017-06-14
13rBEzGteVMzYWCyhnYQ7TrR8ShDvPgaKV	Paid(2.6685bit)	2017-06-14
1LCDbcZWUjvN8tBGCPtjsgtcRK2Nt4cTtF	Paid(2.6685bit)	2017-06-14
1G117QEJrtRDfZzEHQRbMEwiTVYNb2VExZ	Paid(2.6685bit)	2017-06-14
177EEqv4zCZ3zRbek27Q1N1hdnQDqjw9nj	Paid(2.6685bit)	2017-06-14
1CWTGScU7WVTDoZsyC5hq72G8jqT1QKSnF	Paid(2.6685bit)	2017-06-14
15nHs63Z8HDr9sjyTJJdoFHGzPTVwUPbsW	Paid(2.6685bit)	2017-06-14
1P7dHBHqxbauNkAP6M81U7tKqrToBnxtyD	Paid(2.6685bit)	2017-06-14
1JA32oGeg4QjPiW8KS64KFF2fVCyh12gha	Paid(2.6685bit)	2017-06-14
12GovuyZXCzn1EyjpM33wCVdY93WvL8qN8	Paid(2.6685bit)	2017-06-14

- **Nayana Web Hosting Firm case**
  - The victim decrypted the whole system after paying the ransom by Bitcoin
  - What vulnerabilities they had?
    - Linux kernel in 2008
    - Apache and PHP server version in 2006

No update…



- **Silver Notice**
  - Over the past few years, only 3 to 5 percent of global illicit financial flows have been seized and confiscated
  - Increasing the need for improved international cooperation mechanisms on asset tracing and recovery through better information sharing and the creation of new legal and operational tools

- **Silver Notice**
  - Interpol implemented numerous initiatives and network specialized in the field such as the Global Focal Point Initiative on Asset Recovery

- The Global Focal Point Network on Asset Recovery provides a secure information exchange platform for criminal asset recovery.
- Authorized law enforcement officers designated as “Focal Points” to respond to the immediate needs for assistance in asset recovery.

- The immediate strategic objective of this initiative is to respond to concerns of asset freezing, seizing, confiscating and recovering stolen assets.
- A continuing objective is to facilitate secure exchange of sensitive information among the Focal Points who are from anti-corruption and asset recovery agencies.

- Through INTERPOL secure channels, registered Focal Points can access:
  - Information and contact details of Focal Points from other jurisdictions;
  - Legislative, administrative, investigative and judicial frameworks for member countries;
  - A knowledge library;
  - All valid INTERPOL Notices published for corruption-related offences;
  - INTERPOL Notices to freeze assets;
  - A 24-Hour Initial Action Checklist for an asset recovery investigation.

- **Silver Notice**
  - Pilot project concerning a new category of notice specifically devoted to the tracing and recovery of assets

Red Notice
To seek the location and arrest of wanted persons with a view to extradition or similar lawful action.

Yellow Notice
To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.

Blue Notice
To collect additional information about a person's identity, location or activities in relation to a crime.

Black Notice
To seek information on unidentified bodies.

- **Silver Notice**
  - Pilot project concerning a new category of notice specifically devoted to the tracing and recovery of assets

Green Notice
To provide warnings and intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.

Orange Notice
To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety.

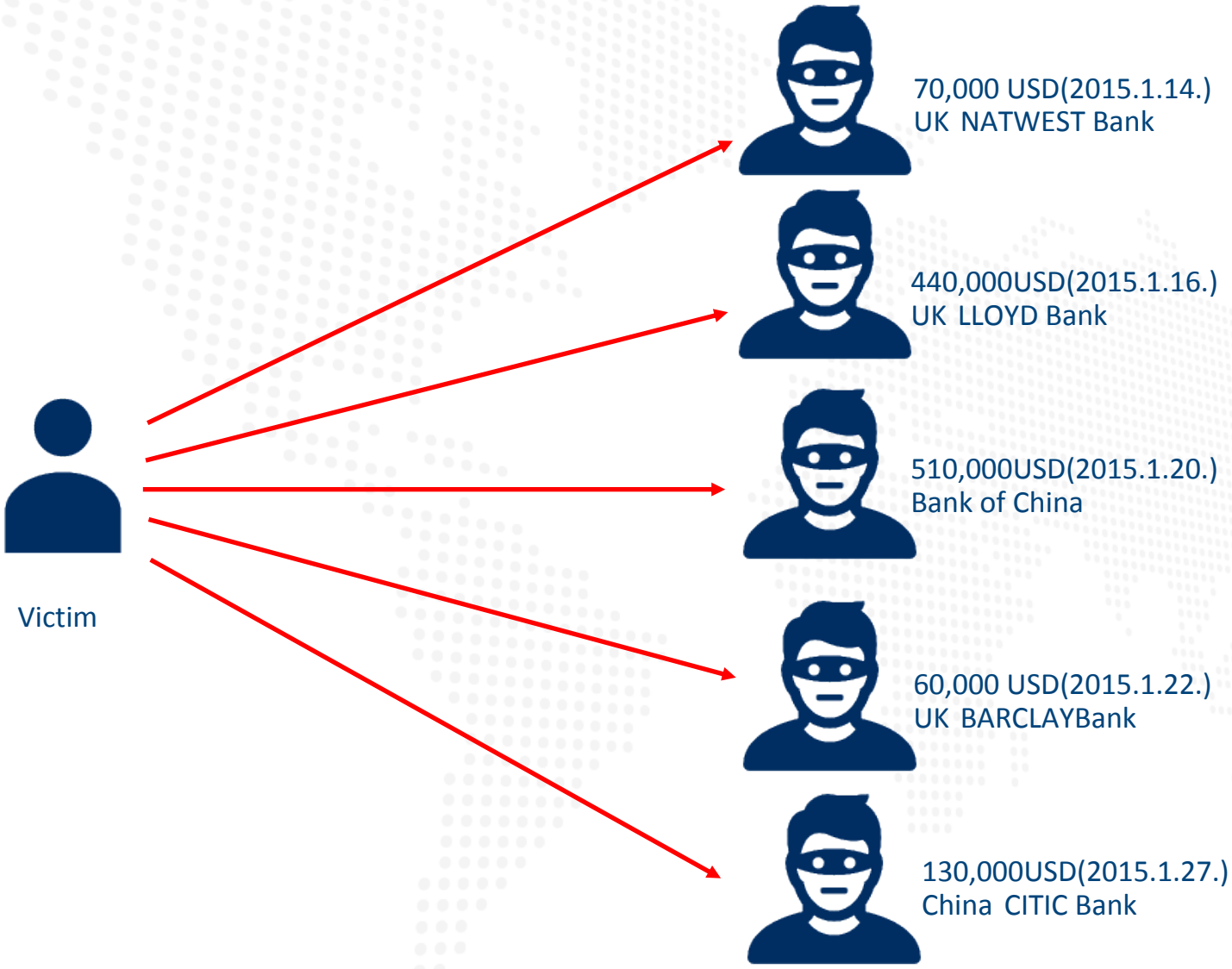
INTERPOL–United Nations Security Council Special Notice
Issued for groups and individuals who are the targets of UN Security Council Sanctions Committees.

Purple Notice
To seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.

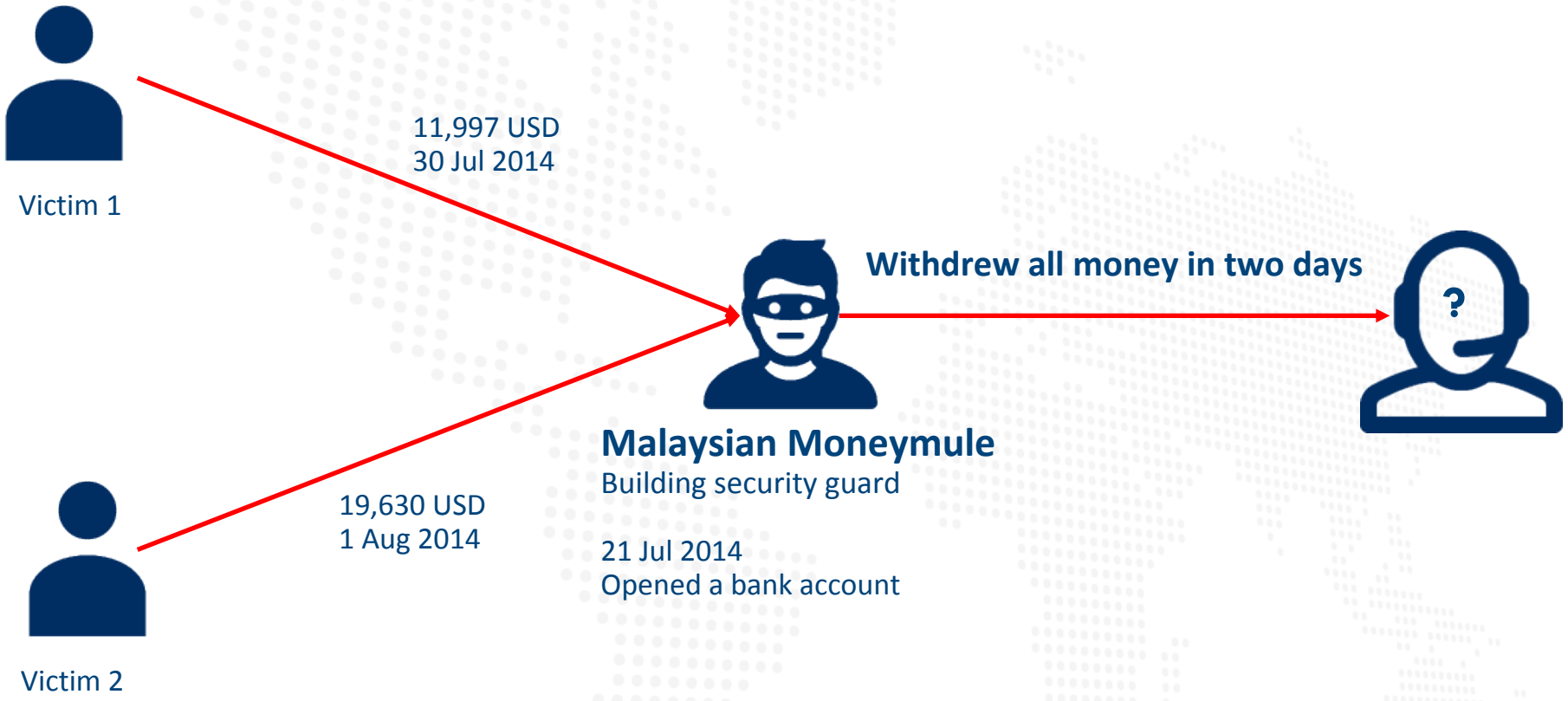
Solution 1 – Read money flow

- **Egmont Group**
  - The Egmont Group is a united body of **154 Financial Intelligence Units (FIUs)**. The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing

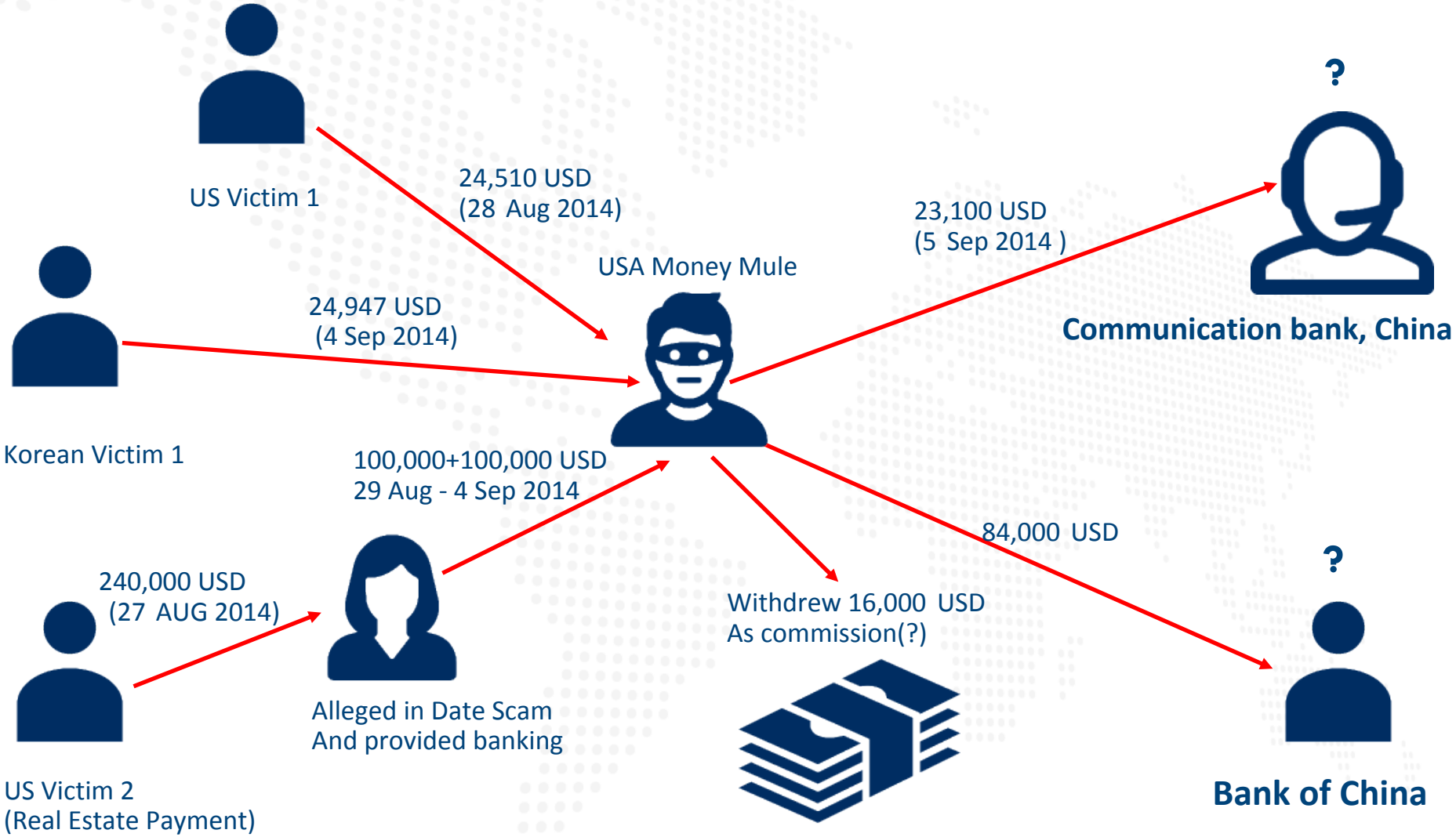
- Business email compromise case



- Business email compromise case



- Business email compromise case

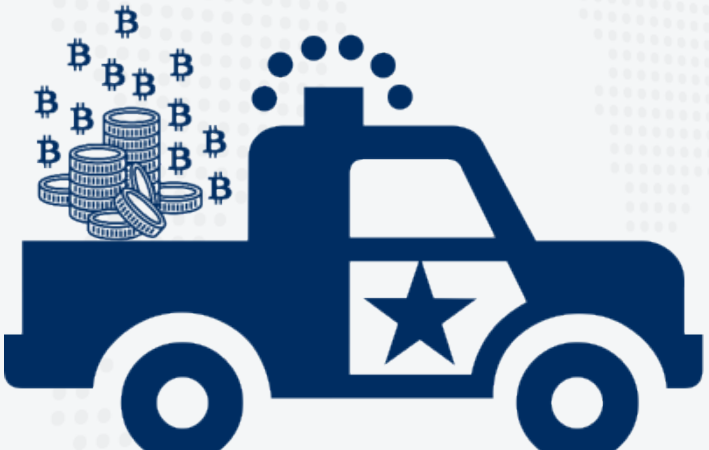


Solution 1 – Egmont Group

- **Expedite alternative to MLAT**
  - Usually takes 2-3 months to get a reply
  - Broad and collective access to alleged bank accounts
  - Well organized analysis report

Solution 2 – Read cryptocurrency flow

- **Bitcoin tracking and seizure**
  - FBI seized 144,000 Bitcoin, worth 28.5 million USD, from Ross Ulbricht, Alleged Owner Of Silk Road in Oct 2013
  - In 2017, Korean Police seized 216 Bitcoin, worth 400 thousands USD, from an owner of an obscene website.
    - During the criminal procedure, the value of Bitcoin doubled..



Solution 2 – Read cryptocurrency flow

- **Research on Bitcoin tracking tools**
  - Interpol is developing a software with private sectors

Solution 2 – Read cryptocurrency flow

- **Sharing of Bitcoin exchange's contact point**
  - Only chance to link cryptocurrency and criminal (Case of DD4BC)
  - Member countries contribution requested

INTERPOL

نشكركم جزيل الشكر على انتباهكم

Thank You-Merci-Gracias

s.hong@interpol.int