EXHIBIT 2

LCX AG
Security Incident

Funds Tracing Report

Vaduz, Liechtenstein

January 17, 2022

STRICTLY CONFIDENTIAL

About LCX

LCX AG is the operator of the Internet platform LCX.com, which among other things enables trading in crypto currencies on LCX Exchange (exchange.LCX.com). LCX AG is registered as a TT service provider according to TVTG. LCX follows strict security requirements and has implemented corporate governance structures including an internal policy called "Information Security, Blockchain Operations and Business Continuity Policy".

LCX implemented strict security measures and policies on operation security. Our current process includes: Periodically reinitialize a hot wallet, Use secret sharing schemes, Follow Do not store more than 5% of all deposits in hot wallets, Store crypto in several hot wallets for each cryptocurrency platform.

In 2021 LCX conducted a 7 month cyber security audit and penetration test by an external audit firm and received a score of 9 out of 10 possible points. https://www.lcx.com/lcx-top-for-safety-and-security/

Summary: Theft of Crypto Assets Worth approx. $7.94 Million USD

At roughly 11:23 PM CET on January 9th, LCX's Technology team detected unauthorized access of one crypto wallet at the LCX platform. A total of approx. 7.94M USD of crypto assets were stolen. 0.70M USD has been frozen. All other LCX wallets are not impacted.

LCX announced in public that no users and clients will be harmed and that the user balance will not be affected. LCX will reimburse the full amount stolen and pay the reimbursement from its own funds.

The hacker wallet address is

0x165402279f2c081c54b00f0e08812f3fd4560a05.

https://etherscan.io/address/0x165402279f2c081c54b00f0e08812f3fd4560a05

Investigating Team and Investigating Agency

LCX started collaborating with BLIN Agency (Blockchain Investigative Agency) based in Geneva, Switzerland. Blin Agency provides investigation and tracking services in the blockchain. The expert team can trace the money to the endpoints (exchanges) and provide proof of a connection between the withdrawals from the mixer and the deposits (the funds/money, directly connected to the hack).

This report includes the initial results and research by the external agency.

Where are the funds now?

Based on the investigation the investigating agency assumes the funds are held in the following wallets.

- **1500 ETH** (approx. $4.9 million USD) of stolen funds are held in this wallet
  0x29875bd49350ac3f2ca5ceeb1c1701708c795ff3
  https://etherscan.io/address/0x29875bd49350ac3f2ca5ceeb1c1701708c795ff3
- 4.1 Million LCX Token (approx. $590'000k USD) of stolen funds are held in this wallet
  0x5C41b35DD45E951222C5e61a34FDF0A3Bd53Ed72
  https://etherscan.io/address/0x5C41b35DD45E951222C5e61a34FDF0A3Bd53Ed72

How could we identify the hacker?

The investigating agency believes that 5.97 ETH of the stolen assets withdrawn from Tornado through the two addresses went to Bithumb.

- 0x475cb73f11BC9B37E975DA6ecB0124D1A1040ba4
  https://etherscan.io/address/0x475cb73f11BC9B37E975DA6ecB0124D1A1040ba4
- 0xCD0BC31eaa9Ff54f47ff1ed6089BB47214b54c49
  https://etherscan.io/address/0xCD0BC31eaa9Ff54f47ff1ed6089BB47214b54c49

Bithumb is a regulated exchange based in South Korea. https://bithumbcorp.com/en/
Their general contact email is info@bithumbcorp.com

As Bithumb claims to be regulated in South Korea we assume that the platform might have Know-Your-Customer (KYC) information of their user and this could identify the hacker / person involved in this hack.

The two transactions above will be enough for Bithumb to identify the involved parties and users, as they can trace back the incoming deposit and link it to a verified user account.

LCX

Tracing Funds at Tornado Cash Mixer

Here is what the investigating team traced so far having the information from the open sources.

The hackers use the Tornado Cash mixer. Tornado Cash is a fully decentralized protocol for private transactions on Ethereum. https://tornado.cash/

On January 10th 2022 the stolen assets went in 16 transactions to tornado-100:

- 0xf9943460adc510685033431badfdcaacc4ea2dc3a2c354a951bb55075533b155
- 0xeb70c13fb5112450c95219b24f8a10c25ac8881b4461c9aeebe9515f51431111
- 0x8a1537a8b6cb73b925cac975e89a1fa4e17f5680ecaf5db48f3a6a6f48c8796a
- 0x8662df454aac5f16000bbfaac06006847df50926c354f3472f2ab3d033ff0869
- 0xac9cc9e61de8c721c0cf042c92c92170dbcf116eafafba34bc613c765ee067c4
- 0x3be546315700bc036edbf8bc76729be702335b3891ed7354b32ffd9ea200d17d
- 0xb6e641840b0aacefa99ffa382080e8e9092b055603ee4604d887c6879e843e1e
- 0x48a289c3b24a8e80afb4b2001fa7fa5570da15bf8d156fd0e38449db350d629d
- 0xf4c951fea743be0d459cd972140599a4c593882b24eb0a927050eff80f55a300
- 0x1951ee55a4fb341385f20414d3c83332a373eb6c1a29a99d8339006fbc75d31d
- 0x77c151cdf1d5919ac50bfa3ff988ffed97d715b75d49f54769cc245e55ff1a37
- 0x397d2ec1c3ae6f113d011a014e2720bbcc6219ad0230a680640e60e043a3f00c
- 0xbe4ccd4a8ddfe66f1a3b76fa82809f610753c2aeddd8cc3a9af562e5173ffd17
- 0xdf06b46cd939d170ef78c0c4ad6e535da6e2ee5e23567cf37523dbe885bf8fb4
- 0x6dd348d98a48d8457a1c31783db0c1392553319adfbc5a613edb49c6ea788856
- 0x42ea0512ebf4a7bdf079fc212f9a67fac6a8519e276fe8dae03171d4830045e2

Also, 29 went to tornado-10 and 1 to tornado-1

The investigating agency currently suspect this withdrawal address

0x475cb73f11BC9B37E975DA6ecB0124D1A1040ba4

It received 15 transactions from tornado 100 and one from tornado 10 as belonging to the hackers.

After from that address there were two transactions:

1500 ETH went to 0x29875bd49350aC3f2Ca5ceEB1c1701708c795FF3

5.97 ETH went to 0xCD0BC31eaa9Ff54f47ff1ed6089BB47214b54c49

Tracing Funds Exchanged at 1inch Decentralized Exchange

The investigating agency believes that hackers changed some altcoins (most probably LCX token) to ETH and got withdrawal from 1inch for approx. 82.7 ETH (approx. $270'000 USD)
Transaction ID: 0x27923917b4f706d2388a491b30f6630a030ce826af925341f741ed6cc4285c7e)

With the next transactions

- 0x03eea0d70cffb03d31f87f72cdddb377c1fd3bfd45f1cc02ec4b3a06f82aa910
- 0x8b3a21b411f1e1e528082fd29fe82a0eb7fc78e7ebce439debc3cc9c7918d4d7
- 0xc5d6e61d9f46696b42c51ac1a4f5d82c3090291da02416da031c3871ac1e8bf6

The hackers filled an address 0x5C41b35DD45E951222C5e61a34FDF0A3Bd53Ed72 for about 89 ETH

Then it was transferred to 0x2D0699A972fd4cB1FA78B31574Bd73eB53B615b3

and after - to Tornado Cash 10 in these transactions

- 0xba04ff3556326330e7ab9a14062f2f70d60dc7e6d50080444dad0b7a72c6d157
- 0xd4480d82f6919c92c20948301b67823f4e86e8af1e827cf851d95c4b5016c4ec
- 0xc70e1346e66e91714efb17e8d575b272bc66c4c66b4b40c7f8c88353483187cd
- 0xb2298650a7d85cce739973e3a3c0964fc42b6e5853c46ef76a0f2c0aae59459f
- 0x577baef028524d8188a010fcecd47c301296ca11f5d88086a051921c1ffcc0ae
- 0xbc8017e0ee96f5d9d54c677ddedd03790ac9dd056b0247b43c758511c158ad7c
- 0x86774c7fef2df558a3e3ae586006e135b07f48544a73b08b7b942b7fe9e45c26
- 0xa0e5cff00cedbf50978b455a98dddb7ff3f9120a5e79eb7ad721a7f0c76fdc1e

Summary and Next Steps

LCX has not made these wallets public and have not informed blockchain analytics company Elliptic at this point in time. The reason is that we do not want to warn the hacker and inform the hacker that we might have exposed the funds. Thus we are treating the information provided strictly confidential.

Suggested next steps by the Police and FIU:

> Contact Bithumb by the police or FIU to request identification of the transacting user and request Bithumb to disclose the information for this investigation.

Suggested next step in collaboration by LCX and authorities:

> Trace and monitor the two key hacker wallets (1500 ETH wallet and 4.1M LCX Token wallet) in case there are future transactions to another regulated exchange the hacker could be identified.