Stefan Ćertić

University of Belgrade

Internet Topology Security Issues

June, 21, 2017

2 factor authentication (2FA) vulnerabilities

Introduction

Most of the major players in the industry today double secure the accounts of their users so that they can be able to regain access just in case they forget or lose the password. The move is perfect as it allows the user to recover his or her credentials. However, the study herein shows that double securing an account can be one of the most dangerous security and privacy threats. Both private users and enterprises trust the major players in the internet such as Google, Facebook, LinkedIN and Twitter by giving them their privacy and allows them to process their sensitive data.

However, as many people concentrate more on the large enterprises that are trusted, very few people take into consideration the impact of the background players who sell two-factor authentication security to those enterprise players. The latter can result to a perfect opportunity for a business to position on the right spot, and generate huge profits by selling the accounts access.

Considering the following assumptions;

- A certain company A specializes in PIN code deliveries through Phone Calls or SMS.
- Assuming that Company A grows big through the mergers and the acquisitions so it also starts providing services to Facebook, Google, LinkedIN, Twitter and Banks.

- Assume that every time one decides to change his password through phone by SMS or Call, or login to the banking profile, the particular service provider would initiate an API call towards Company A asking them to send you the code.

The attack Pattern;

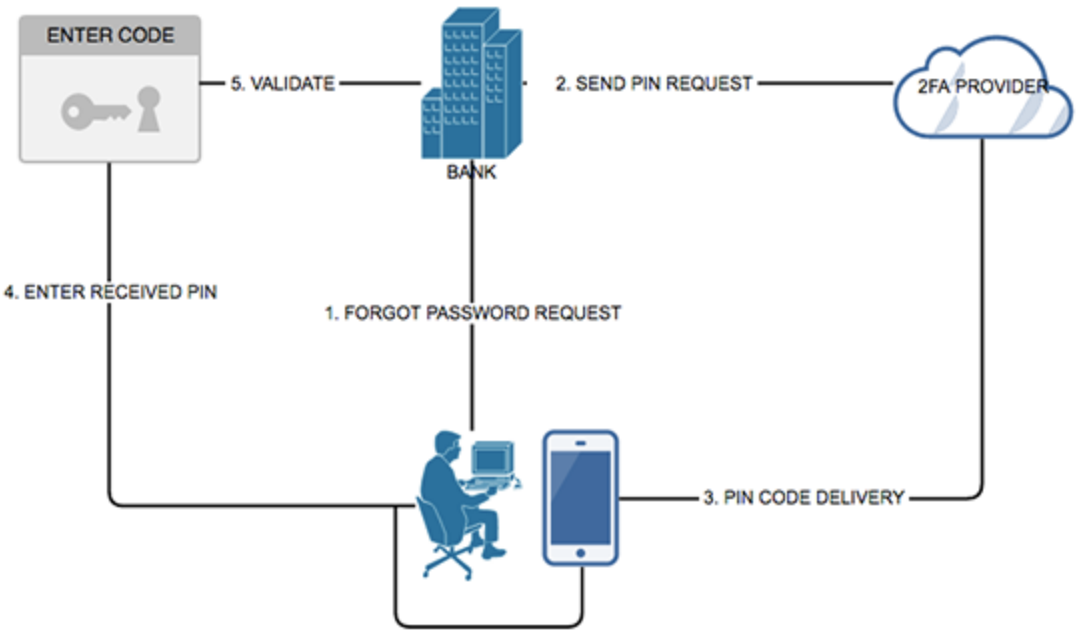
A person in company Y has the capability to virtually access any part of the digital life of the users of the companies to which it provides services. The person can view everything from life, social profiles, chats, contacts, messages, places you visit, as well as your bank account.

The Flow:

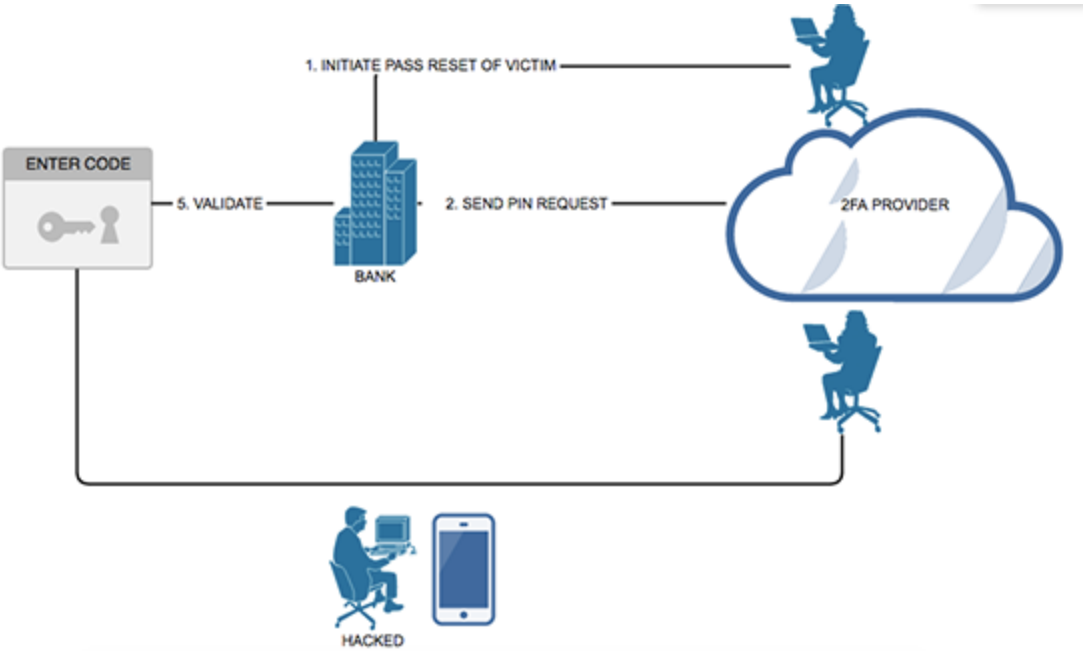
The attack can start when person X working at Company Y intentionally starts a password reset with a specific target victim in mind. Person X then intercepts the password reset message and performs a direct login to the account without the owner noticing. The implementation of double securing accounts opens a new discussion as far as Internet security is concerned and as information technology gets centralized in the current world. Looking at it in this context, instead of securing the account of the user, it makes it even more vulnerable than the initial approaches. The latter could open up an opportunity for a black market that targets online users using the techniques suggested in this study.

The following diagrams can be used to represent the regular flow and the attack flow paths.

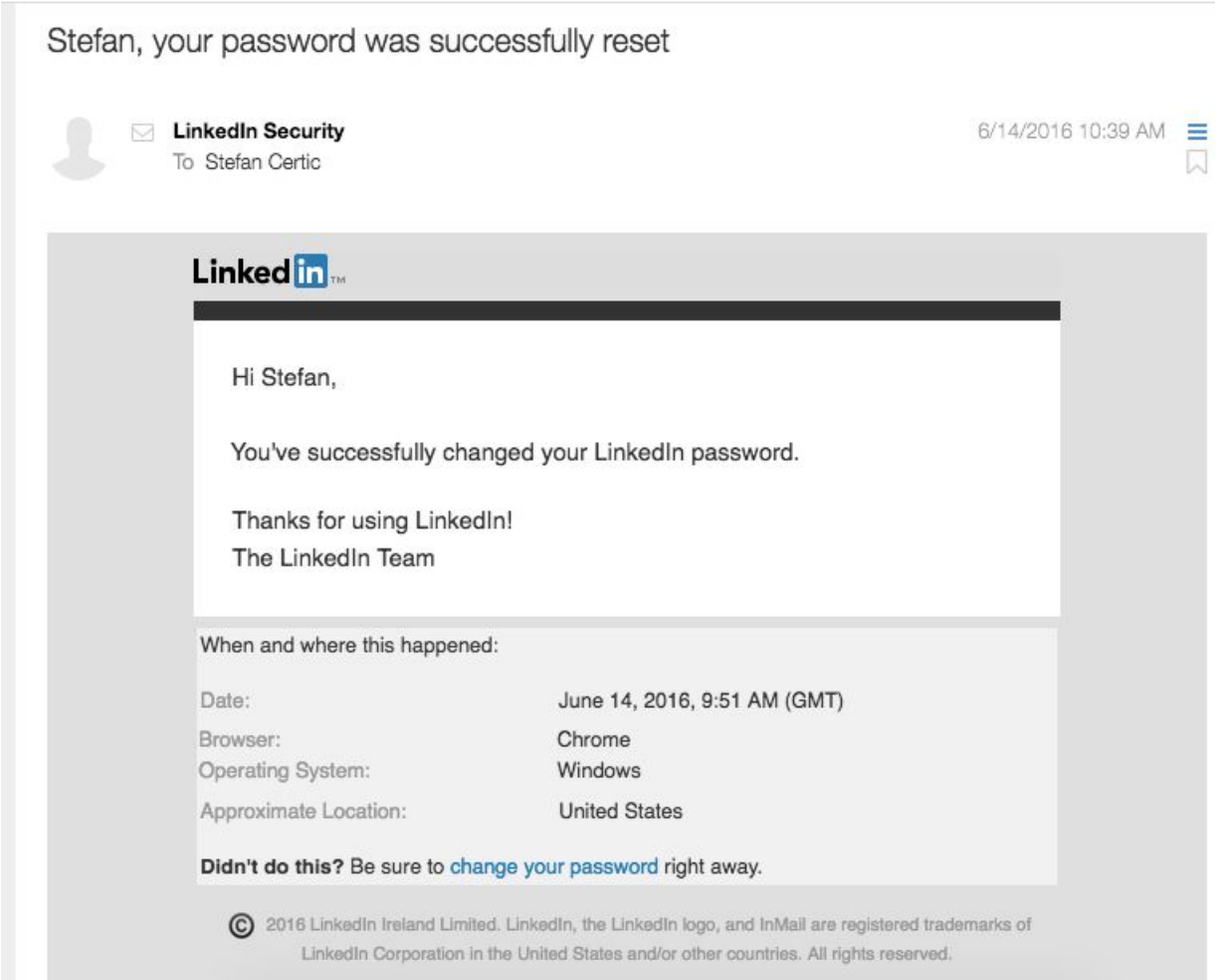
Regular request flow



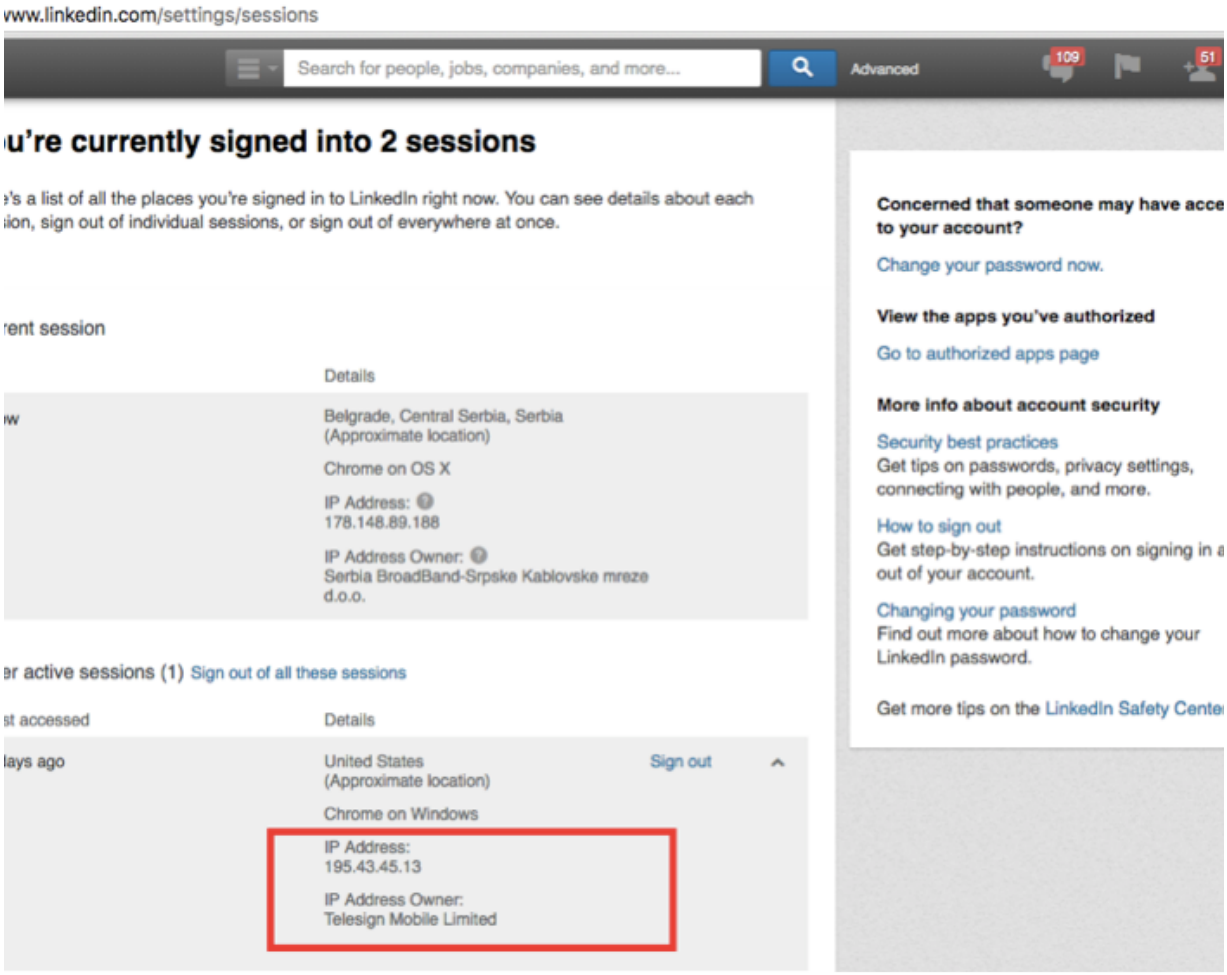
Attack flow



The above scenario has been confirmed and many people have reported that their LinkedIN and Facebook accounts had been hacked. A forensic investigation of the systems revealed that the following scenario was being used to successfully hack accounts.

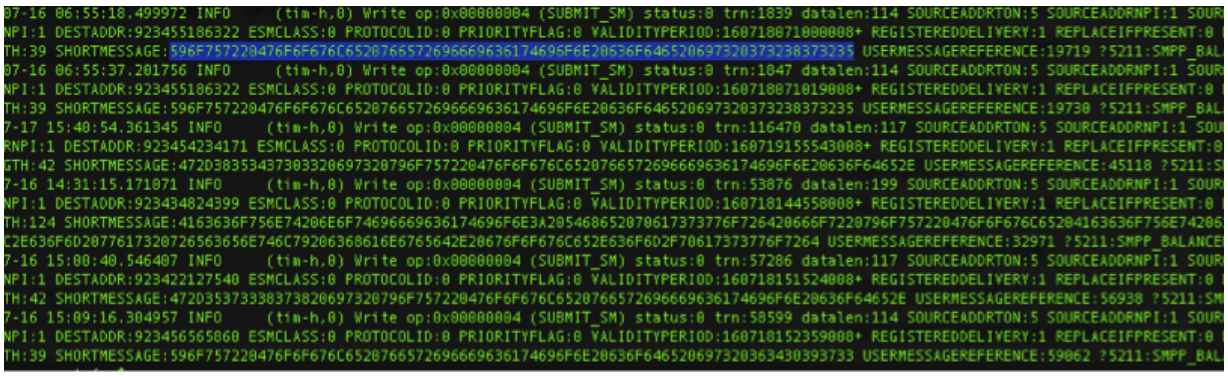


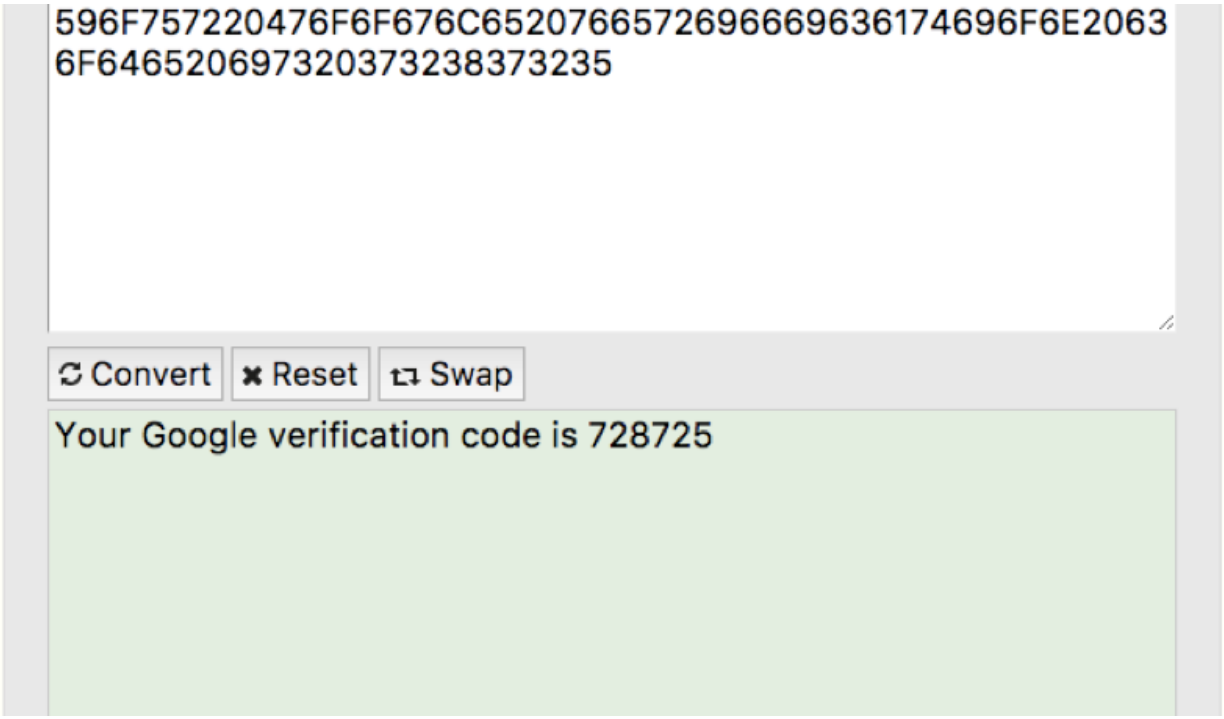
From the above image, it is clear that the email shows that a password reset had been done using Chrome on a windows device located in the United States. The login sessions can also be used to detect cases of successful account hacking as can be seen in the screenshot below.



The image shows two active logins using Chrome, from Windows, and the location is in the United States, and more important from the block that has been assigned to one of the Biggest 2FA providers on the world that process Google, Facebook, Instagram, Twitter and many other Services.

Traffic is not delivered in any form of encryption. Due to a fact that SMS/Voice MSU market function just like a stock market, after the code gets submitted from Social Network for upward delivery, it's up to their partner to choose the "least cost route". There is no Encryption In 2FA transmission:



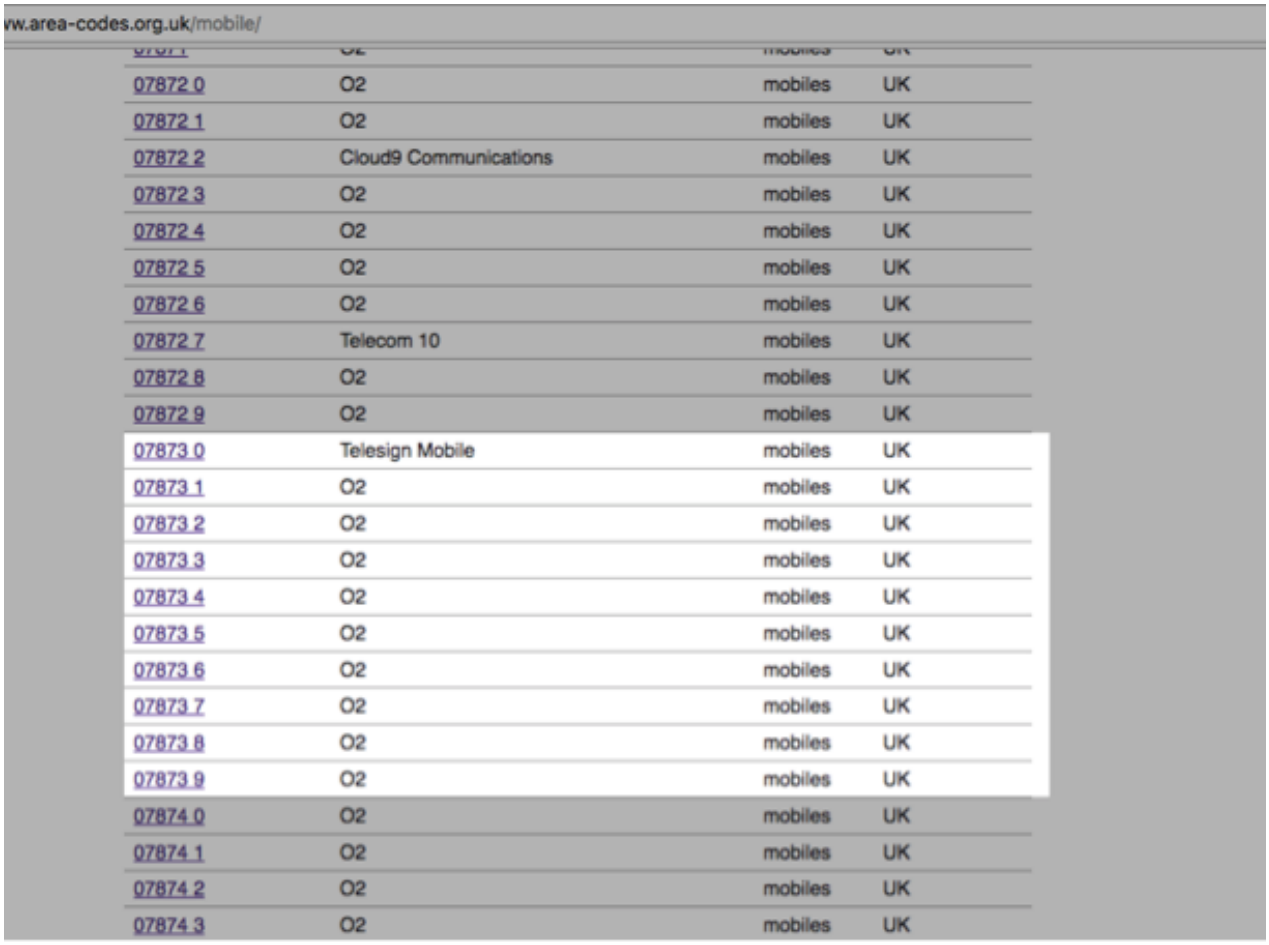


Methods to achieve targeted attack

The targeted attack can be achieved by dropping the SMS/Voice call price on the global market for specific Country and the operator of the Victim, as a result of least cost routing, it's a matter of minutes when the traffic is going to get re-routed towards the attacker platform. In

order to be able to do so, without being suspicious, it could employ very serious tricks.

This is the UK numbering plan of prefixes issued by Ofcom.



07872 0	O2	mobiles	UK
07872 1	O2	mobiles	UK
07872 2	Cloud9 Communications	mobiles	UK
07872 3	O2	mobiles	UK
07872 4	O2	mobiles	UK
07872 5	O2	mobiles	UK
07872 6	O2	mobiles	UK
07872 7	Telecom 10	mobiles	UK
07872 8	O2	mobiles	UK
07872 9	O2	mobiles	UK
07873 0	Telesign Mobile	mobiles	UK
07873 1	O2	mobiles	UK
07873 2	O2	mobiles	UK
07873 3	O2	mobiles	UK
07873 4	O2	mobiles	UK
07873 5	O2	mobiles	UK
07873 6	O2	mobiles	UK
07873 7	O2	mobiles	UK
07873 8	O2	mobiles	UK
07873 9	O2	mobiles	UK
07874 0	O2	mobiles	UK
07874 1	O2	mobiles	UK
07874 2	O2	mobiles	UK
07874 3	O2	mobiles	UK

How below market cost is achieved to "get Social Networks verifications" at any time without even being suspicious:

- 078730 allocated by Ofcom to company X
- 078731 078732 078733 ... 078739 allocated to O2

Operators worldwide will try to short-down the lists of Global Titles (similar to iptables rules), and most of them have only 07873 = O2

Result:

• Traffic accepted even there is no Roaming Agreement with X (based on O2), Invoice goes to O2 - not X.

• Even if O2 has no agreement, it's in small operators interest to accept messages from a giant. The test by setting a number from the example pool using a voip white channel resulted in China Telecom thinks my operator is O2. This is the one and only case of such allocation in the UK or anywhere in the world.

Conclusion

This looks like a very sophisticated scheme aiming to control whole market with the idea of being able to get access to any account at any time. The company might even make a loss on their business, and sell the access to any targeted account on any service to government or private sector via third parity companies to make enormous amount of profit. This study presents forensic evidences that scenario is already happening, affecting the whole Internet community.