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.

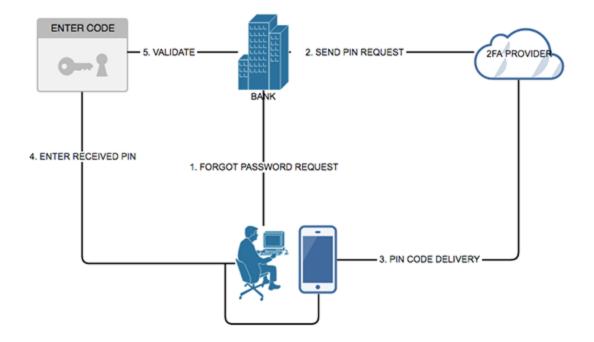
• Assume that every time one decides to change his password through phone by SMS or Call, or login to the banking profile, the particular service provider would initiate an API call towards Company A asking them to send you the code.

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:*

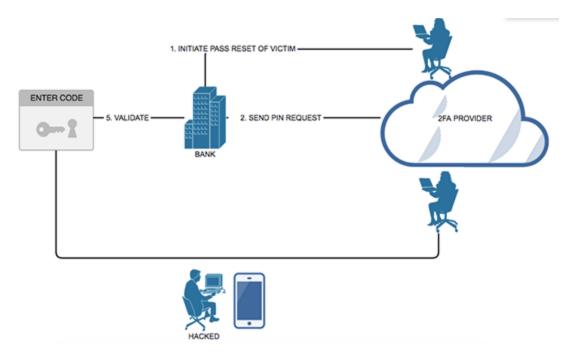
The attack can start when person X working at Company Y intentionally starts a password reset with a specific target victim in mind. Person X then intercepts the password reset message and performs a direct login to the account without the owner noticing. The implementation of double securing accounts 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





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.

Stefan, your password was succes	ssfully reset		
To Stefan Certic		6/14/2016 10:39 AM	
Linked in			
Hi Stefan,			
You've successfully change	ed your LinkedIn password.		
Thanks for using LinkedIn! The LinkedIn Team			
When and where this happened:			
Date:	June 14, 2016, 9:51 AM (GMT)		
Browser:	Chrome		
Operating System:	Windows		
Approximate Location:	United States		
Didn't do this? Be sure to change your password right away.			
~	inkedIn, the LinkedIn logo, and InMail are registered tradem United States and/or other countries. All rights reserved.	narks of	

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.

vww.linkedin.com/settings/ses	sions				
	Search for people, jobs, companies, and more	٩	Advanced	- 109	51
u're currently sign	ed into 2 sessions				
, , ,	ned in to LinkedIn right now. You can see details about ea s, or sign out of everywhere at once.	ch	to your acce		y have acce
			Change you	r password now.	
rent session			View the ap	ps you've authori	zed
	Details		Go to author	ized apps page	
	Belgrade, Central Serbia, Serbia		More info al	bout account secu	urity
w	(Approximate location) Chrome on OS X IP Address: @			t practices basswords, privacy with people, and mo	
	178.148.89.188 IP Address Owner: @ Serbia BroadBand-Srpske Kablovske mreze		How to sign Get step-by- out of your a	n out y-step instructions on signing in	n signing in a
er active sessions (1) Sign out of	d.o.o. all these sessions		Changing yo Find out mor LinkedIn pas	e about how to cha	inge your
st accessed	Details		Get more tip	s on the LinkedIn S	afety Cente
lays ago	United States Sign out (Approximate location)	^			
	Chrome on Windows				
	IP Address: 195.43.45.13				
	IP Address Owner: Telesign Mobile Limited				

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:

07-16 NP1:1 97-16 NP1:1 TH:39 97-16 NP1:1 TH:3 STH:4 S	2 SHORTMESSAGE:4720383534373033286 (4:31:15.171071 INFO (tim-h,0) DESTADDR:923434824399 ESMCLASS:8 4 SHORTMESSAGE:4163636F756E74206E6 5F602077617320726563656E746C792063 5:60240.546407 INFO (tim-h,0) DESTADDR:923422127540 ESMCLASS:8 SHORTMESSAGE:47203537333837382609 (5:80:16.304957 INFO (tim-h,0) DESTADDR:92345655680 ESMCLASS:8	PROTOCOLID:0 PRIORITYFLAG:0 VA 652076657269666963617469666226 Write op:0x00000004 (SUBMIT_S PROTOCOLID:0 PRIORITYFLAG:0 V 97320796F757220476F5F675C65207 Write op:0x0000004 (SUBMIT_S PROTOCOLID:0 PRIORITYFLAG:0 VA F74696669636174696F6E3A2054686 68616E6765642220676F6F676C65207 Write op:0x00000004 (SUBMIT_S PROTOCOLID:0 PRIORITYFLAG:0 VA 7320796F757220476F6F676C65207 Write op:0x00000004 (SUBMIT_S PROTOCOLID:0 PRIORITYFLAG:0 VA	ALIDITYPERIOD:160719155543008+ /6572696669536174696F6220636F6 M) status:0 trn:53076 datalen: /LDITYPERIOD:160718144558008+ /52070617373776F726420666F72207 /636F602F70617373776F7264 USERMI M) status:0 trn:57206 datalen: /LDITYPERIOD:160718151524008+ /6572696669636174696F6220636F64	REGISTEREDDELIVERY:1 REPLACEIFPRES 4532 USERMESSAGEREFERENCE:45118 ? 19 SOURCEADDORTM:5 SOURCEADDRNF1: REGISTEREDDELIVERY:1 REPLACEIFPRESE 967757220476F6675C65204163636F7566 ESSAGEREFERENCE:32971 ?5211:SMPP_B4 117 SOURCEADDORTM:5 SOURCEADDRNF1: REGISTEREDDELIVERY:1 REPLACEIFPRESE 6526 USERMESSAGEREFERENCE:56938 ?5 144 SOURCEADDORTM:5 SOURCEADORNF1: REGISTEREDDELIVERY:1 REPLACEIFPRESE	L SOUR ENT:0 P BALL SOUR P BALL 1 SOUR PP BALL 1 SOUR ENT:0 211:5M ENT:0 211:5M ENT:0 211:5M ENT:0 211:5M ENT:0 215 200 211:5M ENT:0 215 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 211:5M 200 200 200 200 200 200 200 200 200 20
	596F757220476F 6F646520697320			6174696F6E2063	
	Convert Rese	et 🗗 Swap			
	Your Google verif	ication code is 7	28725		

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.

STULT OZ Incomes OK 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 07872.8 O2 mobiles UK 07872.9 O2 mobiles UK 07873.0 Telesign Mobile mobiles UK 07873.1 O2 mobiles UK 07873.3 O2 mobiles UK 07873.4 O2 mobiles UK 07873.5 O2 mobiles UK 07873.6 O2 mobiles UK 07873.9 O2 mobiles UK 07873.9 O2 mobiles UK 07873.9 O2 <th>codes.org.uk/mobile/</th> <th></th> <th></th> <th></th>	codes.org.uk/mobile/			
Q7872.1Q2mobilesUKQ7872.2Cloud9 CommunicationsmobilesUKQ7872.3Q2mobilesUKQ7872.4Q2mobilesUKQ7872.5Q2mobilesUKQ7872.6Q2mobilesUKQ7872.7Telecom 10mobilesUKQ7872.8Q2mobilesUKQ7872.9Q2mobilesUKQ7873.1Q2mobilesUKQ7873.2Q2mobilesUKQ7873.3Q2mobilesUKQ7873.4Q2mobilesUKQ7873.5Q2mobilesUKQ7873.6Q2mobilesUKQ7873.7Q2mobilesUKQ7873.8Q2mobilesUKQ7873.9Q2mobilesUKQ7873.1Q2mobilesUKQ7873.2Q2mobilesUKQ7873.4Q2mobilesUKQ7873.6Q2mobilesUKQ7873.7Q2mobilesUKQ7873.8Q2mobilesUKQ7873.9Q2mobilesUKQ7874.0Q2mobilesUKQ7874.1Q2mobilesUKQ7874.2Q2mobilesUK	0/0/1	UL .	moonea o	ix
Q7872.2Cloud9 CommunicationsmobilesUKQ7872.3O2mobilesUKQ7872.4O2mobilesUKQ7872.5O2mobilesUKQ7872.6O2mobilesUKQ7872.7Telecom 10mobilesUKQ7872.8O2mobilesUKQ7872.9O2mobilesUKQ7873.1O2mobilesUKQ7873.2O2mobilesUKQ7873.3O2mobilesUKQ7873.4O2mobilesUKQ7873.5O2mobilesUKQ7873.6O2mobilesUKQ7873.7O2mobilesUKQ7873.8O2mobilesUKQ7873.9O2mobilesUKQ7873.1O2mobilesUKQ7873.4O2mobilesUKQ7873.6O2mobilesUKQ7873.7O2mobilesUKQ7873.8O2mobilesUKQ7873.9O2mobilesUKQ7874.0O2mobilesUKQ7874.1O2mobilesUKQ7874.2O2mobilesUK	07872.0	02	mobiles U	к
Diff Diff Diff Diff 078723 O2 mobiles UK 078724 O2 mobiles UK 078725 O2 mobiles UK 078726 O2 mobiles UK 078727 Telecom 10 mobiles UK 078728 O2 mobiles UK 078729 O2 mobiles UK 078731 O2 mobiles UK 078732 O2 mobiles UK 078733 O2 mobiles UK 078734 O2 mobiles UK 078735 O2 mobiles UK 078736 O2 mobiles UK 078737 O2 mobiles UK 078738 O2 mobiles UK 078739 O2 mobiles UK 078739 O2 mobiles UK 078740 O2 mobiles UK<	07872 1	02	mobiles U	к
Difference Difference Difference 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 07873.0 Telesign Mobile mobiles UK 07873.1 O2 mobiles UK 07873.3 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 07873.9 O2 mobiles UK 07873.9 O2 mobiles UK 07874.0 O2 m	07872.2	Cloud9 Communications	mobiles U	к
O7872 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 07873 9 O2 mobiles UK 07873 9 O2 mobiles UK 07874 0 O2 mobiles UK 07874 1 O2	07872.3	02	mobiles U	к
O7872 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	07872 4	02	mobiles U	к
D7872.7 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 07873.3 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 07873.9 O2 mobiles UK 07873.9 O2 mobiles UK 07874.0 O2 mobiles UK 07874.1 O2 mobiles UK 07874.2 O2	07872 5	02	mobiles U	к
OT872.8 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 07873.4 O2 mobiles UK 07873.6 O2 mobiles UK 07873.9 O2 mobiles UK 07873.9 O2 mobiles UK 07874.0 O2 mobiles UK 07874.1 O2 mobiles UK 07874.2 O2 mob	07872.6	02	mobiles U	к
07872 9 02 mobiles UK 07873 0 Telesign Mobile mobiles UK 07873 1 02 mobiles UK 07873 2 02 mobiles UK 07873 3 02 mobiles UK 07873 4 02 mobiles UK 07873 5 02 mobiles UK 07873 6 02 mobiles UK 07873 7 02 mobiles UK 07873 8 02 mobiles UK 07873 9 02 mobiles UK 07873 9 02 mobiles UK 07873 9 02 mobiles UK 07874 0 02 mobiles UK 07874 1 02 mobiles UK 07874 2 02 mobiles UK	07872 7	Telecom 10	mobiles U	к
Q7873.0 Telesign Mobile mobiles UK Q7873.1 O2 mobiles UK Q7873.2 O2 mobiles UK Q7873.3 O2 mobiles UK Q7873.3 O2 mobiles UK Q7873.4 O2 mobiles UK Q7873.5 O2 mobiles UK Q7873.6 O2 mobiles UK Q7873.7 O2 mobiles UK Q7873.8 O2 mobiles UK Q7873.9 O2 mobiles UK Q7873.4 O2 mobiles UK Q7873.6 O2 mobiles UK Q7873.7 O2 mobiles UK Q7873.9 O2 mobiles UK Q7874.0 O2 mobiles UK Q7874.1 O2 mobiles UK Q7874.2 O2 mobiles UK	07872 8	02	mobiles U	к
07873 1 02 mobiles UK 07873 2 02 mobiles UK 07873 3 02 mobiles UK 07873 4 02 mobiles UK 07873 5 02 mobiles UK 07873 6 02 mobiles UK 07873 6 02 mobiles UK 07873 7 02 mobiles UK 07873 8 02 mobiles UK 07873 9 02 mobiles UK 07873 9 02 mobiles UK 07874 0 02 mobiles UK 07874 1 02 mobiles UK 07874 2 02 mobiles UK	07872 9	O2	mobiles U	к
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	07873.0	Telesign Mobile	mobiles U	к
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	07873 1	02	mobiles U	к
Q7873.4 Q2 mobiles UK Q7873.5 Q2 mobiles UK Q7873.6 Q2 mobiles UK Q7873.7 Q2 mobiles UK Q7873.8 Q2 mobiles UK Q7873.9 Q2 mobiles UK Q7873.9 Q2 mobiles UK Q7874.0 Q2 mobiles UK Q7874.1 Q2 mobiles UK Q7874.2 Q2 mobiles UK	07873.2	02	mobiles U	к
07873 5 02 mobiles UK 07873 6 02 mobiles UK 07873 7 02 mobiles UK 07873 8 02 mobiles UK 07873 9 02 mobiles UK 07873 9 02 mobiles UK 07874 0 02 mobiles UK 07874 1 02 mobiles UK 07874 2 02 mobiles UK	07873.3	02	mobiles U	к
07873 6 02 mobiles UK 07873 7 02 mobiles UK 07873 8 02 mobiles UK 07873 9 02 mobiles UK 07874 0 02 mobiles UK 07874 1 02 mobiles UK 07874 2 02 mobiles UK	07873.4	02	mobiles U	к
Q7873 7 Q2 mobiles UK Q7873 8 Q2 mobiles UK Q7873 9 Q2 mobiles UK Q7874 0 Q2 mobiles UK Q7874 1 Q2 mobiles UK Q7874 2 Q2 mobiles UK	07873.5	02	mobiles U	к
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	07873.6	02	mobiles U	к
07873 9 O2 mobiles UK 07874 0 O2 mobiles UK 07874 1 O2 mobiles UK 07874 2 O2 mobiles UK	07873 7	02	mobiles U	к
07874.0 O2 mobiles UK 07874.1 O2 mobiles UK 07874.2 O2 mobiles UK	07873.8	02	mobiles U	к
07874 1 O2 mobiles UK 07874 2 O2 mobiles UK	07873.9	02	mobiles U	к
07874.2 O2 mobiles UK	07874.0	02	mobiles U	к
	07874 1	O2	mobiles U	к
07074.0 00 mehiles UK	07874.2	02	mobiles U	к
07674-3 02 mobiles UK	07874.3	02	mobiles U	к

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

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.