black hat USA 2022

Smishsmash

Text Based 2fa Spoofing Using OSINT, Phishing Techniques and a Burner Phone

About us

Thomas Olofsson

- Digital Nomad (many homes)
- Founder sec-t.org
- Co-founder FYEO Inc
- Winner Defcon CTF ages ago
- Secure coding and development
- Climbs and dives

thomas@gofyeo.com

Twitter: @skjortan

Mikael Byström

- Hardware and software hacker
- Collector of intel and fun HW
- Runs LP village @sec-t.org
- Player of CTFs and other games
- Co-founder FYEO Inc
- Breaks stuff for fun and profit

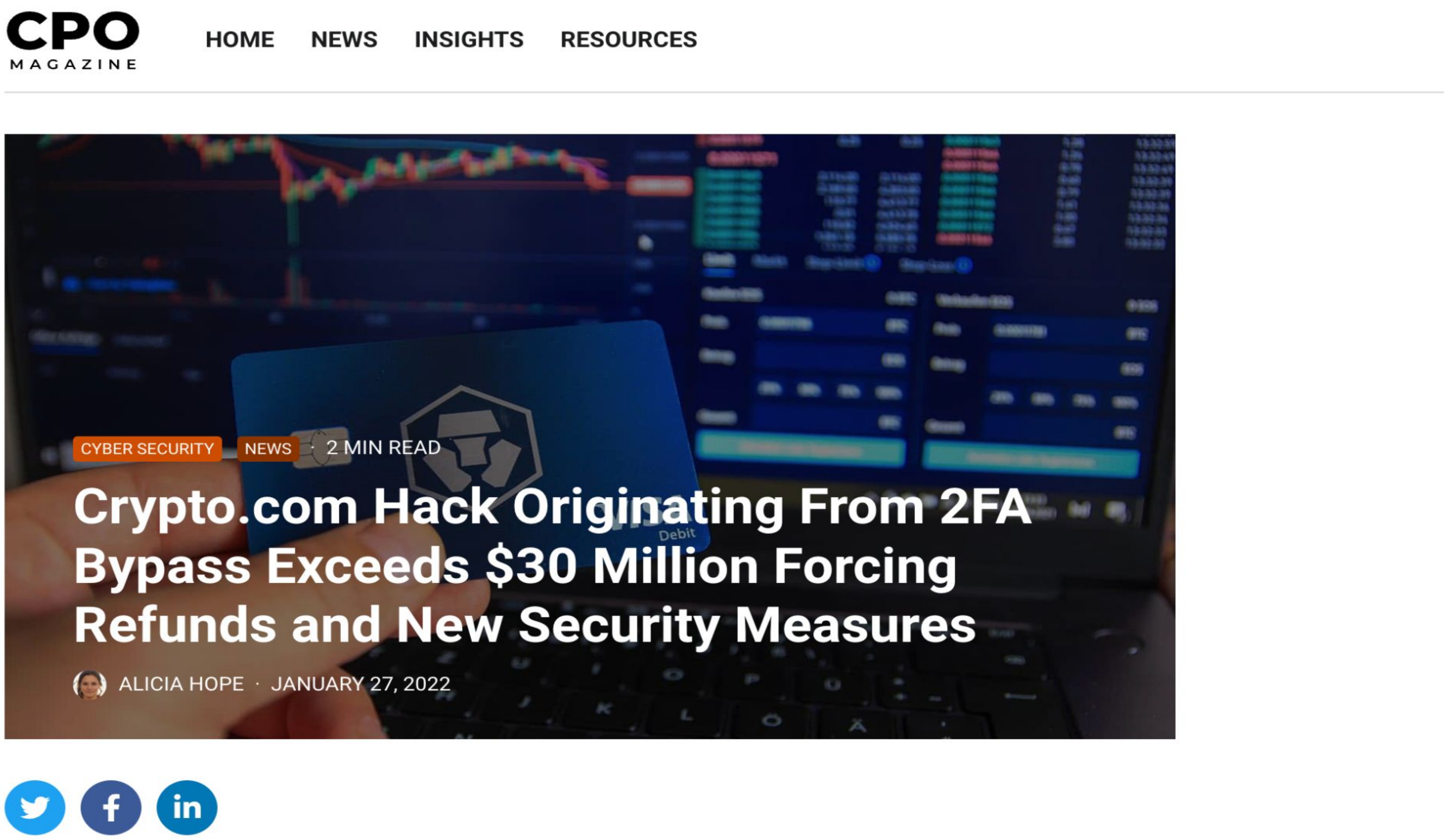
mikael.bystrom@gofyeo.com

Twitter @gsocgsoc

Tl; dr (So basically)

Text Messages (SMS) for two factor authentication

is broken!



Crypto.com Hack Originating From 2FA Bypass Exceeds $30 Million Forcing Refunds and New Security Measures

ALICIA HOPE · JANUARY 27, 2022

Smishing (SMS phishing)

We are seeing more and more text-based phishing attacks by the day.

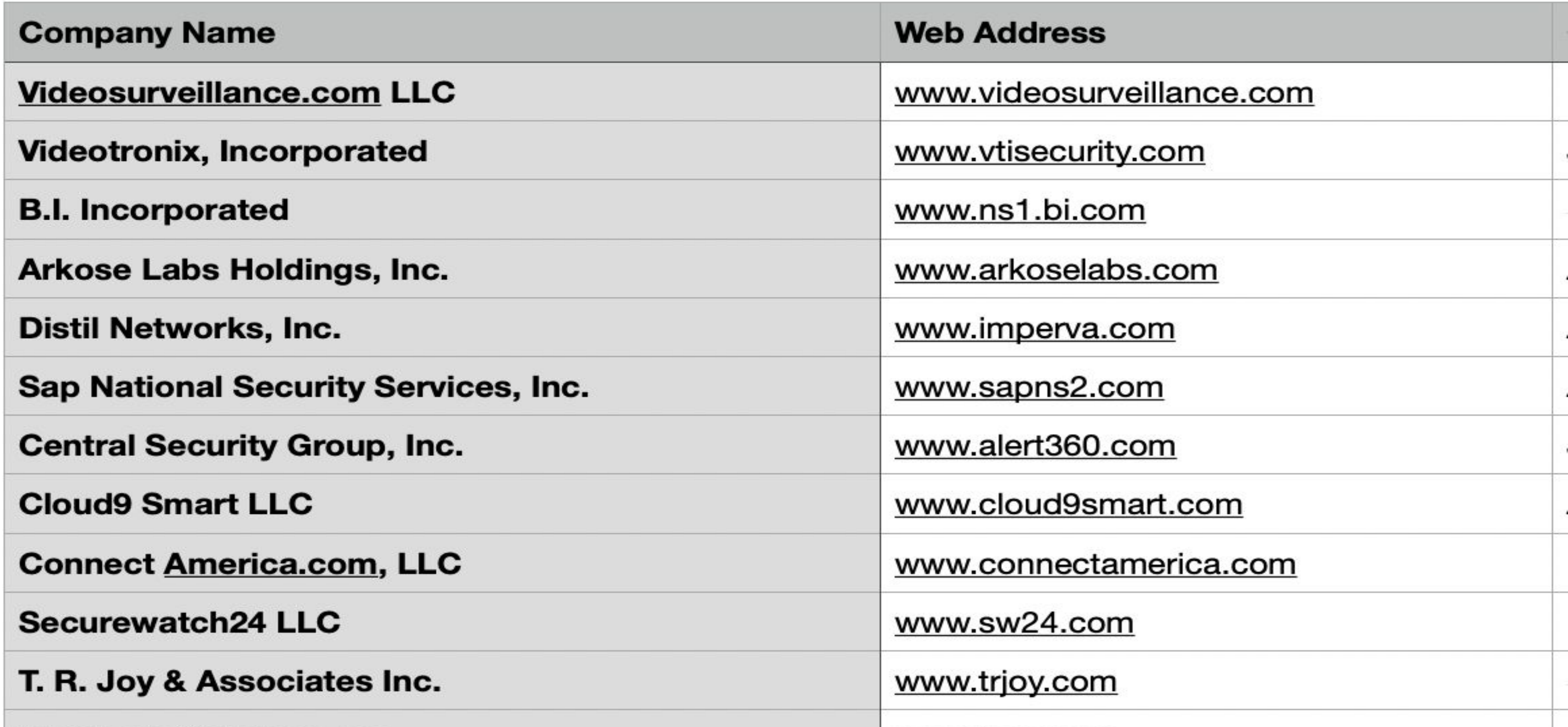
- Most of the phishing protection mechanisms are not designed to protect against this as they are still mostly for email.
- Smishing attacks have expanded by over 7x in the first two quarters of 2021 compared to 2020.*
- Hard to verify integrity of sender or the messages
- **Less than 35% of The People Actually Know when They're Becoming the Target of Smishing Attacks**

* https://earthweb.com/smishing-statistics/

Why this sudden increase in smishing?

- Higher implicit trust than emails!
- Still fewer SMS than email spam
- Much higher success rate than email due to less implemented counter measures
- Mobile browser functionality (We will get to that later)
- **Oh,** and the eternal source of leaked user data that just keeps giving ...

Digital dumpster diving



Company Name	Web Address
Videosurveillance.com LLC	www.videosurveillance.com
Videotronix, Incorporated	www.vtisecurity.com
B.I. Incorporated	www.ns1.bi.com
Arkose Labs Holdings, Inc.	www.arkoselabs.com
Distil Networks, Inc.	www.imperva.com
Sap National Security Services, Inc.	www.sapns2.com
Central Security Group, Inc.	www.alert360.com
Cloud9 Smart LLC	www.cloud9smart.com
Connect America.com, LLC	www.connectamerica.com
Securewatch24 LLC	www.sw24.com
T. R. Joy & Associates Inc.	www.trjoy.com

Getting the ducks in a row

Once you have the dump files its all about making sense of the data

Breach	**Total Credentials**	**phone numbers**
Facebook.com	509M	123M
us-extended-cellphone-feeds	91M	90M
Verifications.io	763M	67.8M
Peopledatalabs.com	622M	49M
Linkedin.com	400M	45.8M
…		
Blackhat 2022	16k	16k

All your Numbers are belong to us!

Demo!

CATS: ALL YOUR NUMBERS ARE BELONG
TO US.

[CREDENTIALS]

USERNAME:PASSWORD/HASH

[CREDENTIALS]

USERNAME:PASSWORD:TELEPHONE

Telephone rainbow tables anyone?

- Together with our 22 Billion password hashes and email pairs this is a great start for simulating attacks.
- We are currently able to tie one in 10 email addresses on the internet to a valid telephone number.*
- We have so far indexed in excess of 500M (Million) phone numbers and email pairs (We are still indexing and think we will soon double this number) taking us to 1 in 5 emails.

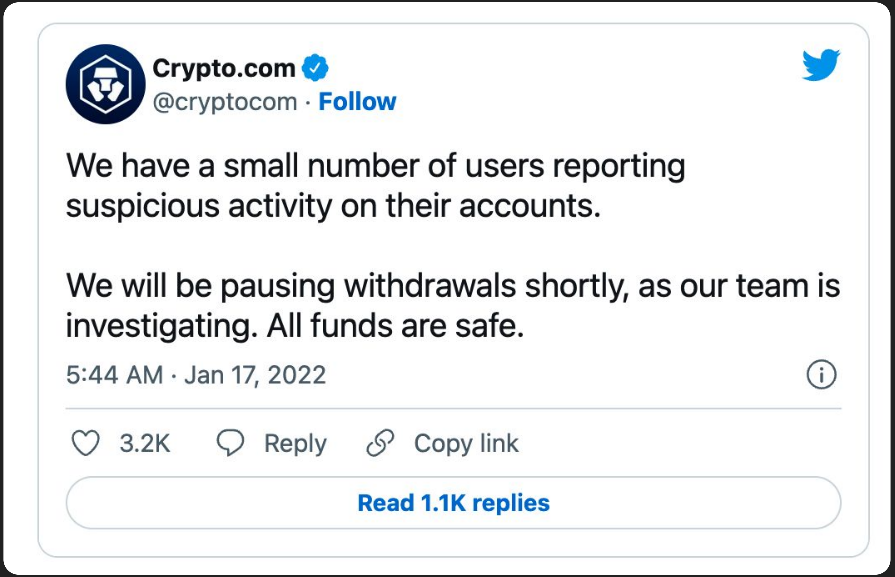
* 4.8B unique email: passwords / ~524M phone numbers

If we can do this, so can the bad guys

Examining the postmortem of the attacks

Crypto.com attack

- $34.6M lost from 436 accounts
- 2fa bypass via smishing password reset

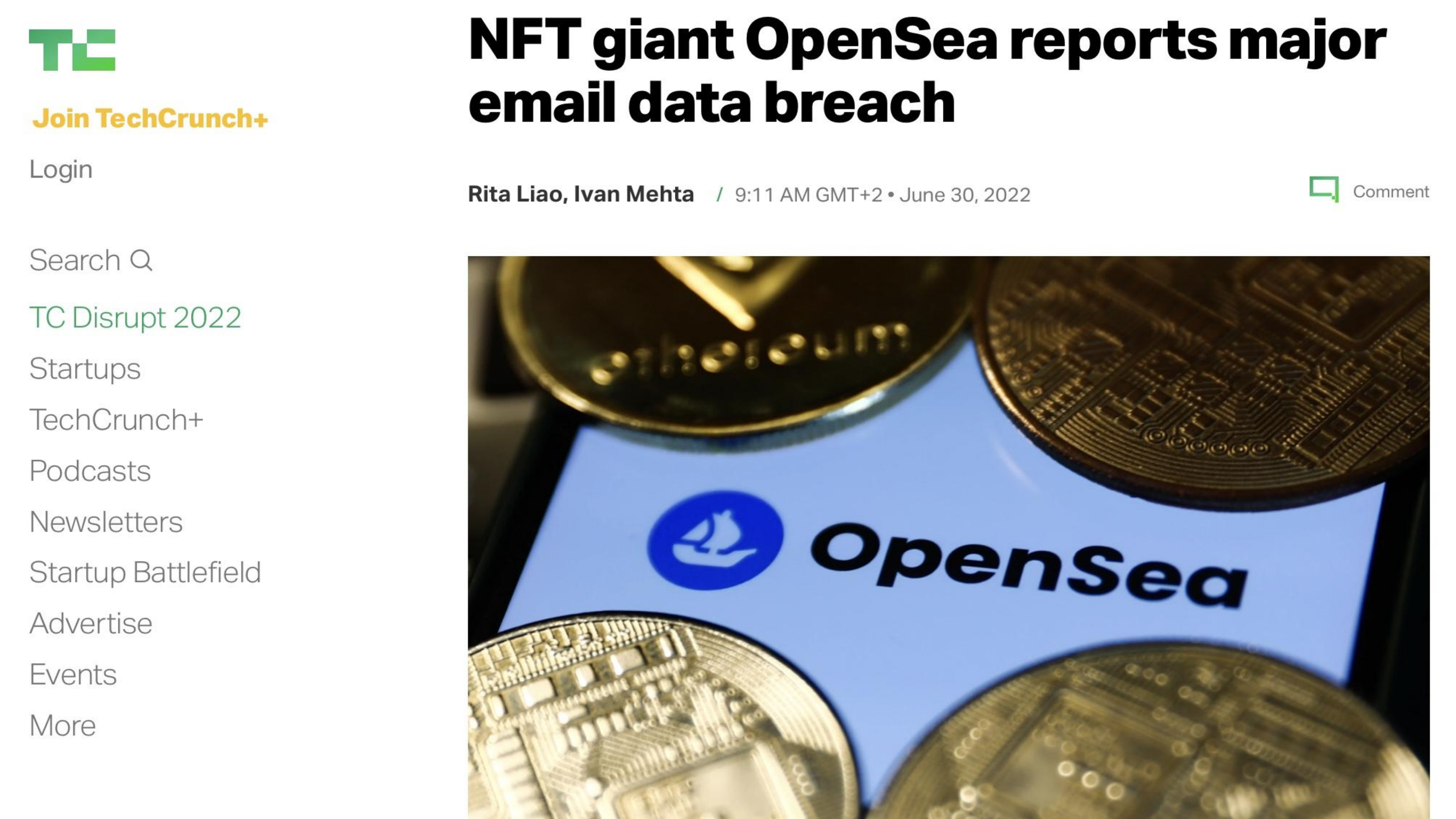


Crypto.com
@cryptocom · Follow

We have a small number of users reporting suspicious activity on their accounts.

We will be pausing withdrawals shortly, as our team is investigating. All funds are safe.

5:44 AM · Jan 17, 2022



NFT giant OpenSea reports major email data breach

Rita Liao, Ivan Mehta / 9:11 AM GMT+2 • June 30, 2022

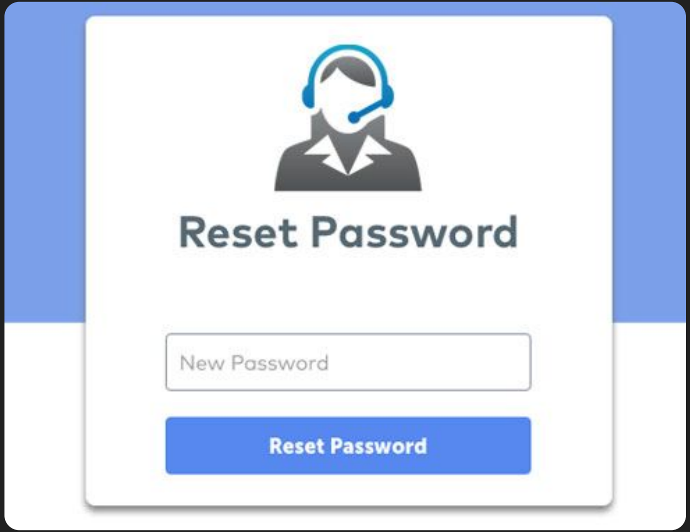
Coinbase attack

“In order to access your Coinbase account, these third parties first needed prior knowledge of the email address, password, and phone number associated with your Coinbase account“

“However, in this incident, … the third party took advantage of a flaw in Coinbase’s SMS Account Recovery process in order to receive an SMS two-factor authentication token and gain access to your account”

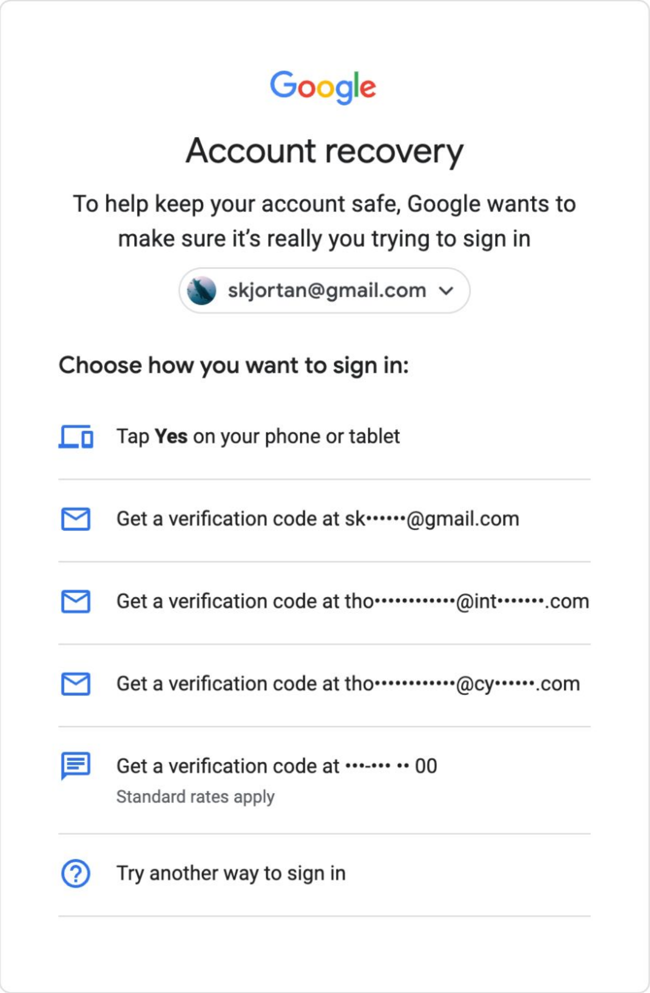
The most popular 2fa bypass via Smishing/phishing

1. Account recovery and password resets to change phone number
2. SMS injection into initiated login with 2fa enabled
3. Smishing / phishing proxies against the real sites, saving the session cookies
4. Sim jacking / sim cloning /porting



Account recovery

- In general the account recovery options are quite open
- Helps with verifying other linked accounts and telephone numbers
- Helpdesk is still a popular way to change telephone numbers for 2fa



Google

Account recovery

To help keep your account safe, Google wants to make sure it's really you trying to sign in

skjortan@gmail.com

Choose how you want to sign in:

Tap **Yes** on your phone or tablet

Get a verification code at sk••••••@gmail.com

Get a verification code at tho••••••••••••@int•••••••.com

Get a verification code at tho••••••••••••@cy••••••.com

Get a verification code at •••-•••• •• 00
Standard rates apply

Try another way to sign in

Let’s talk about SMS (text messages)

SMS aka Short Message Service was basically a way to use an unused space in the packet format that GSM used in 1985!!!

- The SMS was first developed in 1984 by Friedhelm Hillebrand and Bernard Ghillebaert.
- The first text message was sent Dec 3rd, 1992 from Neil Papworth, Sema Group Telecoms.
- Papworth’s text — “Merry Christmas” — was successfully sent to Richard Jarvis at Vodafone.

SMS as a security (bearer) token.

- SMS protocol has NO SENDER VERIFICATION whatsoever.
- There is no check from who or what the from_number field includes except alpa-num.
- ANY 7 bit ASCII is valid... as long as you can log in to a SMSC you can send whatever you want.
- So getting a text from "your number" is as legit as from "SANTA CLAUS". *

*some us-based carriers have started to block non numeric sender ids in late 2020

Demo (Smishing) Teaching old phones new trix

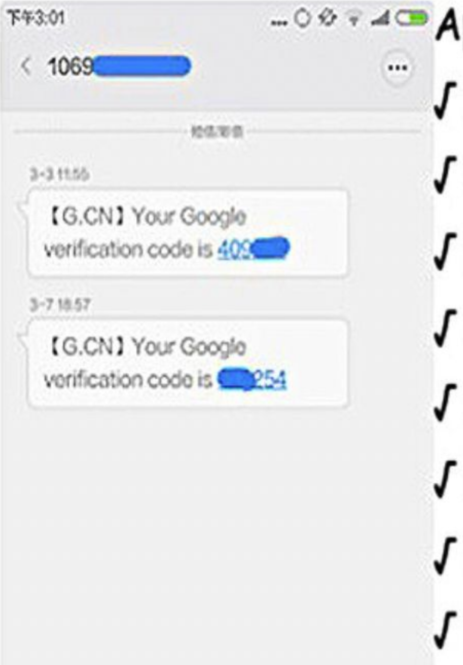
There is a couple of ways to send SMS (Texts):

- Manually via your phone...
  - Duh
- Sending sms through modem / old phone
  - DEMO
- Sending sms through API service
  - Spoofing demo

Going professional Adversary

Application

///



下午3:01

1069[redacted]

3-3 11:55

【G.CN】Your Google verification code is 409[redacted]

3-7 18:57

【G.CN】Your Google verification code is [redacted]254

Application

√ Ideal for telecom distributors, resellers ,service providers,

√ SMS Verfication & ONE time passwords

√ Marketing campaigns (Promotion, sale,...)

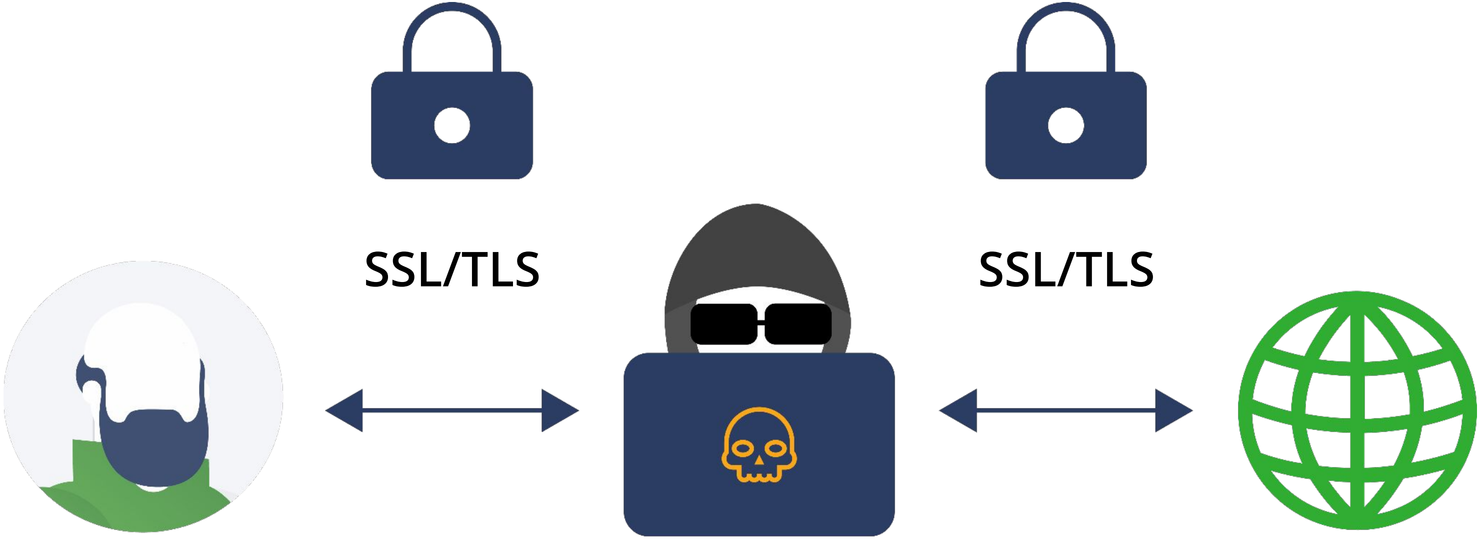
√ Bulk SMS Compagin

√ Information services

√ SMS-Newsletters

√ Notification-SMS (Appointments, birthdays,...)

√ Surveys & Feedback request



SSL/TLS

SSL/TLS

Phished user

Adversary in the middle

Website server

Smishash attack (all together now)

DEMOS Anyone?

How to integrate this into red teaming

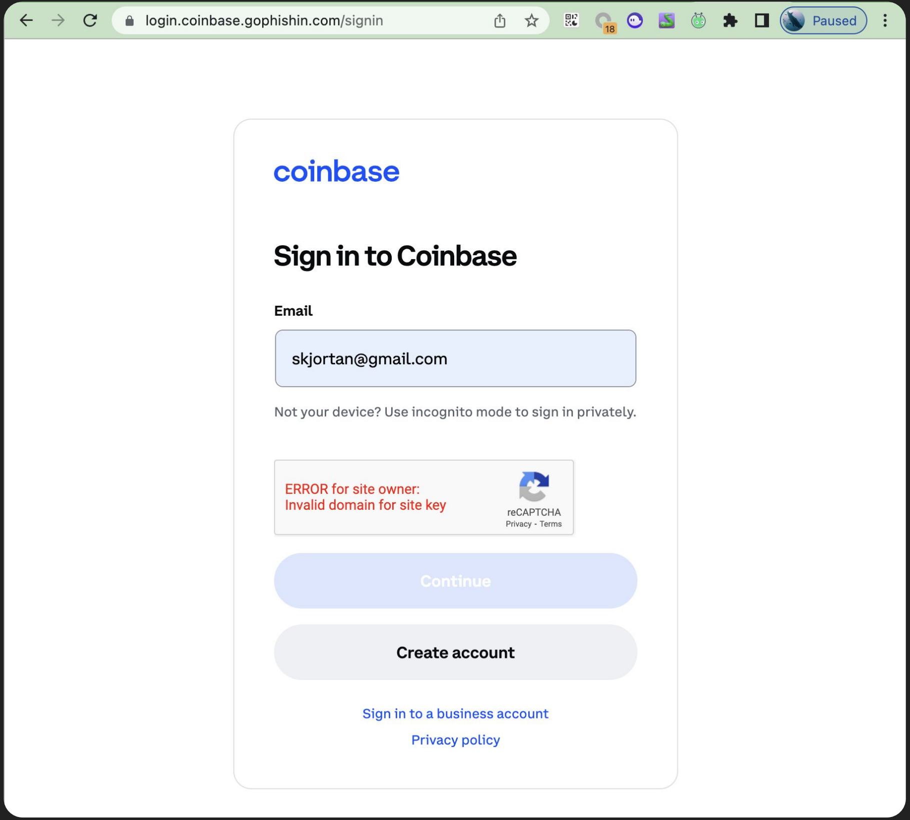
- Start with OSINT collection
  - Indexing some of the large dumps will go a far way
- Smishing
  - Api providers are plentiful (We got blocked by Twillio)
  - Our sample scripts are being open sources
- Mitm proxies
  - We recommend evilginx as a good easy start
  - https://github.com/kgretzky/evilginx2

Lets go smishing! :)

Protection against nitm 2fa bypass

Protect against man in the middle

- Recaptcha (Hidden)
  - Employed by most current crypto exchanges
- Cloudfront cookies (hidden)
  - Easy quick mitigation but possible to bypass
- Cors headers and cors settings
  - could protect



login.coinbase.gophishin.com/signin

coinbase

Sign in to Coinbase

Email: skjortan@gmail.com

Not your device? Use incognito mode to sign in privately.

ERROR for site owner:
Invalid domain for site key

Release of research data

- Full release of hashed data available at

  https://s3.us-west-1.amazonaws.com/phonesearch.api.gofyeo.com/files/full_export.zip

- Full unhashed made data available at request for accredited security researchers (or at least trusted and well known)
- Search available on https://phonesearch.gofyeo.com

Key takeaways

- 1 in 5 email and login accounts can be tied to a valid phone number
- SMS has no security built in and can easily be spoofed even by you
- It’s hard(er) to spot fake sites on mobile
- The mobile will auto fill the 2fa tokens when received

Questions?

F Y E O

Visit us at booth IC50!
gofyeo.com