



Smishsmash

Blackhat 2022

Thomas Olofsson

- Digital Nomad (many homes)
- Founder sec-t.org
- Co-founder FYEO Inc
- Winner defcon CTFs ages ago
- Secure coding and development
- Likes threat actor research and incident investigations

thomas@gofyeo.com

Twitter: @skjortan

Mikael Bystrom

- Hardware and software hacker
- Collector of hardware and intel
- Picks locks and breaks stuff
- Player of CTFs and chess
- Co-founder FYEO Inc
- Some other fun fact

mikael.bystrom@gofyeo.com

Twitter @gsocgsoc



CYBER SECURITY

NEWS

2 MIN READ

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 compare to 2020. *
- Hard to verify integrity or 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 trust than emails!
- Still fewer SMS than email spam
- Much higher success rate than email spam due to less implemented counter measures

Digital dumpster diving

How did we find these phone numbers and “Dump files”

- There is a whole online community dedicated to trading in stolen / leaked data
- Both on clear-net sites and on the darknet
- Go where the bad guys hang out.



Getting the ducks in a row

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

- Listing some of the most popular leaked files and how many telephone numbers they contained. (Logo garden)
 - a. **Facebook.com - 123 million phone numbers and 180 million emails**
 - b. **Jd.com - 96M**
 - c. **Vk.com - 78M**
 - d. ...

All your Numbers are belong to us!



CATS : ALL YOUR **NUMBERS** ARE BELONG
TO US.

[CREDENTIALS]

USERNAME:PASSWORD/HASH

[CREDENTIALS]

USERNAME:PASSWORD:TELEPHONE

Telephone rainbow tables anyone?

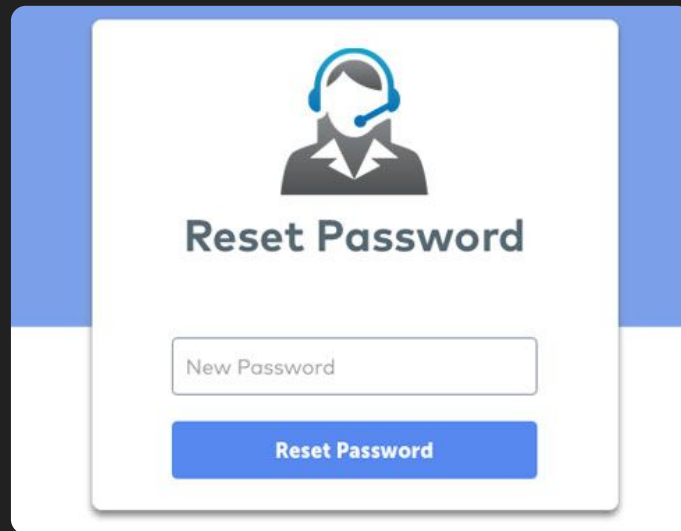
- We are currently able to tie one in 10 email addresses on the internet to a valid telephone number.
- We have so far indexed in excess of 500M (Million) phone numbers and email pairs (We are still indexing and think we will soon double this number)
- Together with password hashes this is a great start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

If we can do this, so can the bad guys

The examples being:

- Human rights watch attack (2018)
- Crypto.com (2021)
- Opensea (2022)

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




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

Crypto.com attack

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



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”

Opensea.com attack

Oh oh er... after we did this research this happened.

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 token.

- SMS messages have 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 this now in late 2020

Demo time let's send some SMS messages (Smishing)

- Sending sms through API service
- Sending sms through modem / old phone

Demo Teaching old phones new tricks

Application

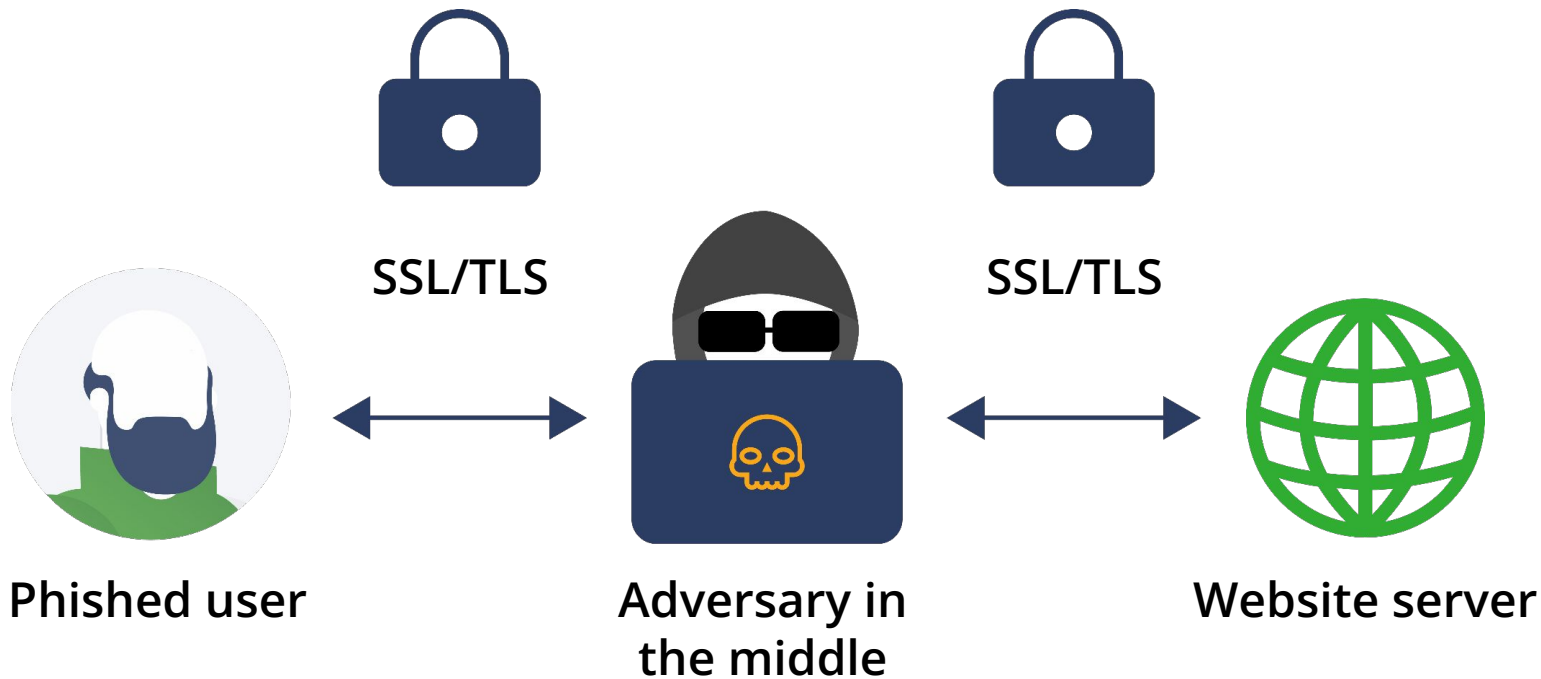


Application

- ✓ Ideal for telecom distributors, resellers ,service providers,
- ✓ SMS Verification & ONE time passwords
- ✓ Marketing campaigns (Promotion, sale,...)
- ✓ Bulk SMS Compagin
- ✓ Information services
- ✓ SMS-Newsletters
- ✓ Notification-SMS (Appointments, birthdays,...)
- ✓ Surveys & Feedback request

Smishash attack (all together now)

DEMOS Anyone?



How to integrate this into red teaming

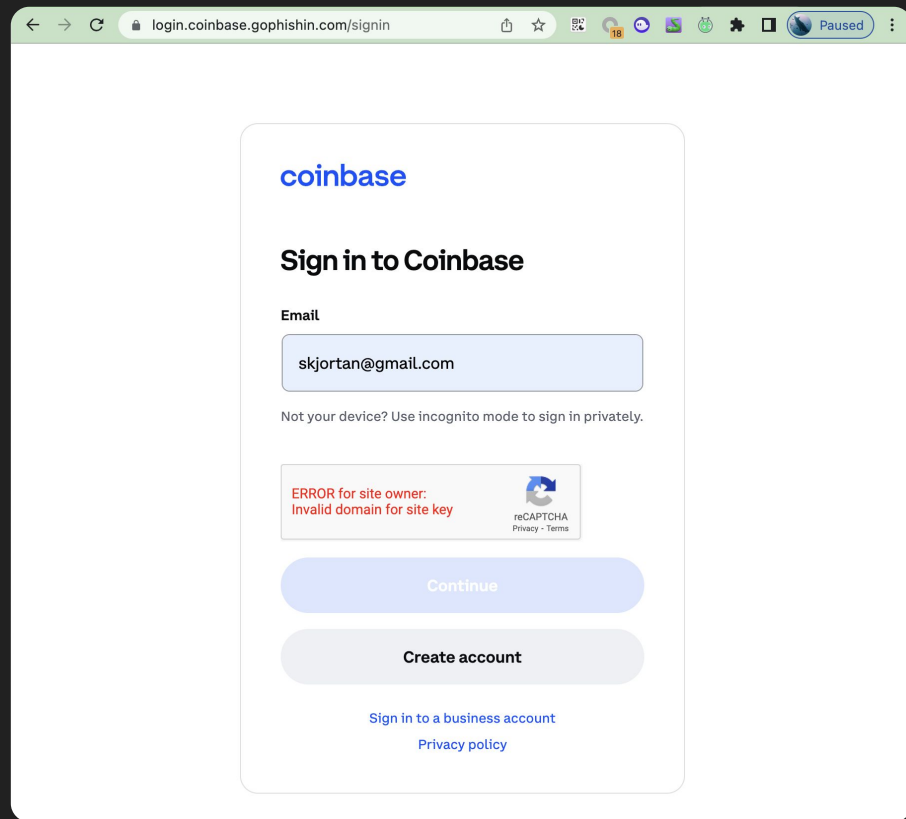
- Start with OSint collection
 - Indexing some of the large dumps will go a fat way
- Smishing
 - Api providers are plentiful
 - Our sample scripts are being open sources
- Mitm proxies
 - We recommend evilginx as a good easy start
 - <https://github.com/kgretzky/evilginx2>

Lets go phishing! :)

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



Release of research data

Full release of hashed data available at gitlab://xyz-smishsmasish-db

Full data available at request for accredited security researchers

Questions?

F Y E O
gofyeo.com