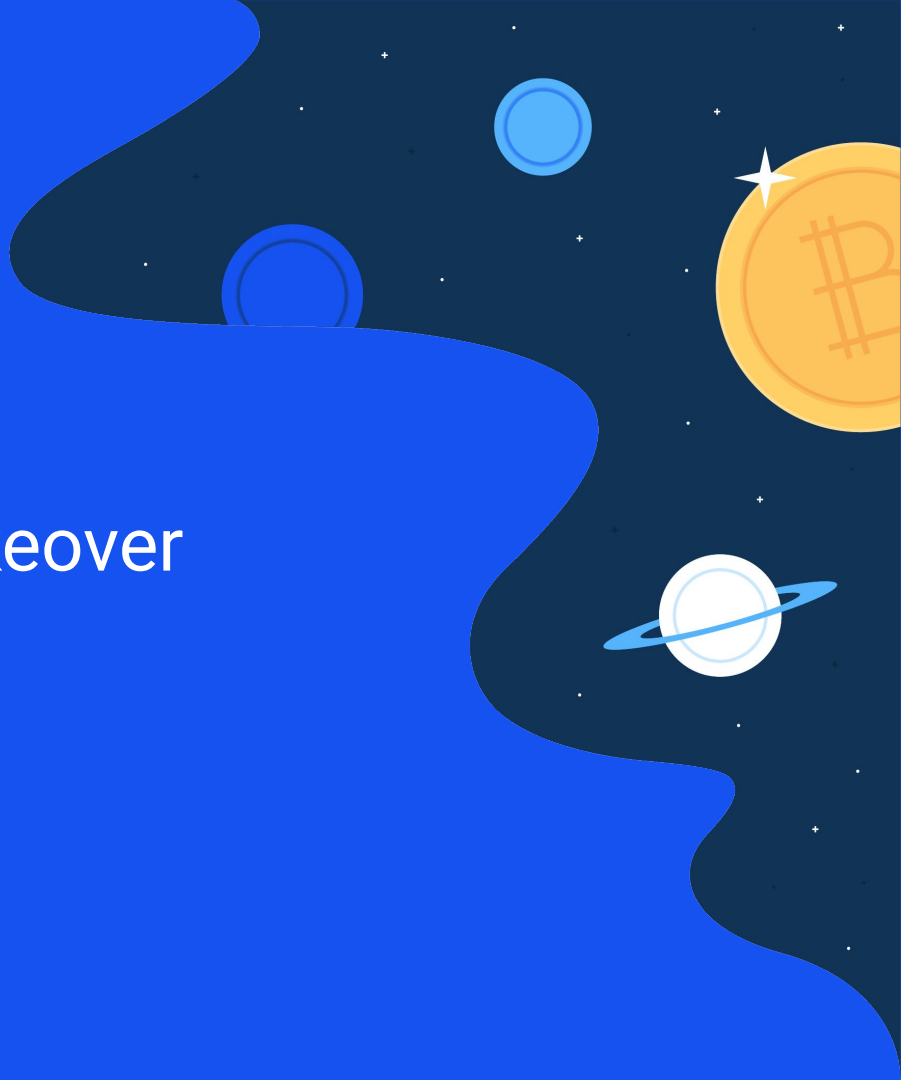
coinbase

The Future of Account Takeover



About Me

I'm Philip Martin, the CISO at Coinbase

Ex-Palantir, Amazon, Sun and US Army

Agenda

00 – Intro

01 – A Bit About ATO

02 – Specific Methods
- SIM Swapping/Porting
- Account Recovery Abuse
- Credential Phishing w/advanced features
- Credential Stuffing
- Social Engineering
- Malware

03 – Emerging Attacker Techniques

04 – Wrap Up & Questions

Who is conducting ATO?

Economically Motivated

- Looking for the shortest path to money, not really fussed with where it comes from.
- Want to show a positive ROI on attacks (although ROI timeline may be long)
- Tend to focus on one thing that works and acquire enough skill/tools to execute that thing repeatedly

Average skill is low (but stddev is high)

- Most ATO is not technically complex, not highly targeted and not expensive. Most actors are playing a numbers game.
- Some ATO is highly detailed, highly targeted and involves significant prep work.
- There is little to no cross-over we've seen between groups in those two camps.

Mostly located in poor countries

- To the extent we are able to track ATO activities back to high-confidence real world identities, they tend to be in places like the Philippines, Nigeria and Eastern Europe.
- (one can argue that only means ATO attackers with poor OPSEC are located in poor countries)
- A $10k payday from ATO may be enough money to keep an attacker in the black for a long time.

How is ATO happening?

Targeted ATO is a Journey

- High end attackers are increasingly targeting victim centers of gravity first
  - email accounts, most commonly, but increasingly things like iCloud.
- By the time an attacker gets to somewhere like Coinbase, they frequently have access to email, file storage, social media, control of a phone number, sometimes even restored backups of target phones.

The Vast Majority of ATO is Not Targeted

- Less than 10% of the ATO or attempted ATO activity we see we rate as 'targeted', and 10% is very, very high compared to most companies.
- By far, the most common types of ATO we see are based on social engineering and are in the vein of the old school tech support scams.

SMS 2FA is effective vs most untargeted ATO, but not always targeted ATO

- Where targeted attackers encounter TOTP 2FA, they pivot to seeking seed backups (frequently in email drafts), cloud-stored mobile device backups, recovery codes, etc.
- This is frequently enabled at some point in the chain by compromise of a lower security account (e.g. academic email used as a recovery email).

SIM Swapping/Phone Porting

Details

- We see SIM swapping more than phone porting these days
- Attacker technique has improved significantly, some SIM swaps last as little as 15 minutes.
- Generally used in highly targeted attacks, focusing on presumed high value targets.
- Attackers are moving from using this to bypass 2FA directly, to using it to hijack account recovery workflows (which are frequently SMS-dependent)

SIM Swapping/Phone Porting

[UPDATED] SIM Swap Fraud: AT&T Sued for $224 Million After Phone Hackers' $24 Million Crypto Hack

16-Aug-2018 ttjack

"law enforcement has even confirmed that AT&T employees profited from working directly with cyber terrorists and thieves in SIM swap frauds"

KrebsonSecurity

In-depth security news and investigation

ADVERTISING/SPEAKING

18 MAY 18 T-Mobile Employee Made Unauthorized 'SIM Swap' to Steal Instagram Account

T-Mobile is investigating a retail store employee who allegedly made unauthorized changes to a subscriber's account in an elaborate scheme to steal the customer's three-letter **Instagram** username. The modifications, which could have let the rogue employee empty bank accounts associated with the targeted T-Mobile subscriber, were made even though the victim customer already had taken steps recommended by the mobile carrier to help minimize the risks of account takeover. Here's what happened, and some tips on how you can protect yourself from a similar fate.

Earlier this month, KrebsOnSecurity heard from **Paul Rosenzweig**, a 27-year-old T-Mobile customer from Boston who had his wireless account briefly hijacked. Rosenzweig had previously adopted T-Mobile's advice to customers about blocking mobile number port-out scams, an increasingly common scheme in which identity thieves armed with a fake ID in the name of a targeted customer show up at a retail store run by a different wireless provider and ask that the number to be transferred to the competing mobile company's network.

Mailing List

Subscribe here

MOTHERBOARD

TECH BY VICE

'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers

California authorities say a 20-year-old college student hijacked more than 40 phone numbers and stole $5 million, including some from cryptocurrency investors at a blockchain conference Consensus.

By Lorenzo Franceschi-Bicchierai

Jul 30 2018, 8:23am Share Tweet

SIM Swapping/Phone Porting

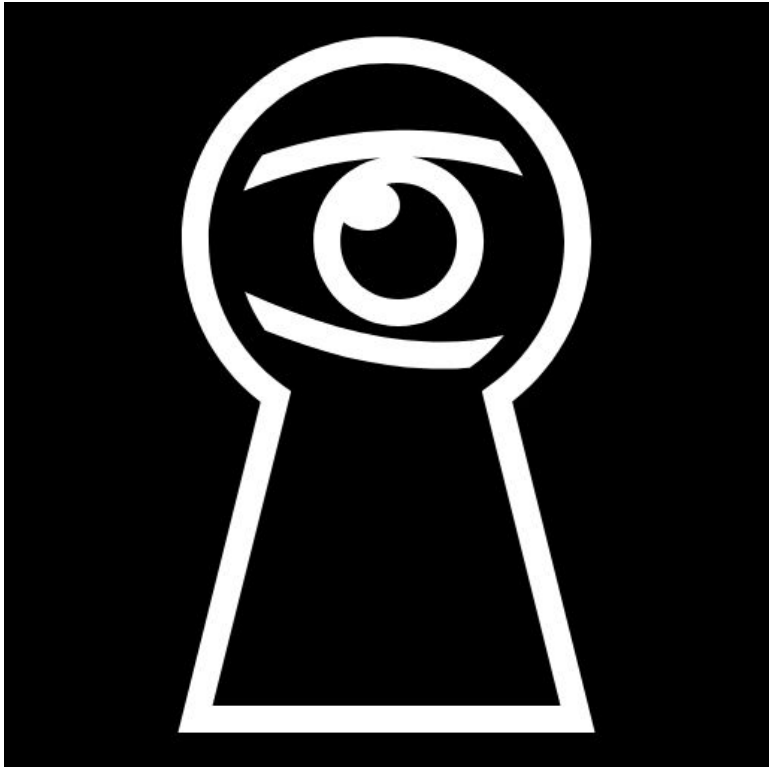
Countermeasures

- Offer non-SMS 2FA options and actively push adoption
- Explore data partnerships with porting and SIM-swapping detection vendors (but this is FAR from 100%)
- I'll go ahead and say it: porting/swapping is NOT in most people's threat models and SMS is still effective 2FA (and certainly better than no 2FA) for the vast majority of people, even in the context of cryptocurrency.

Account Recovery Abuse

Details

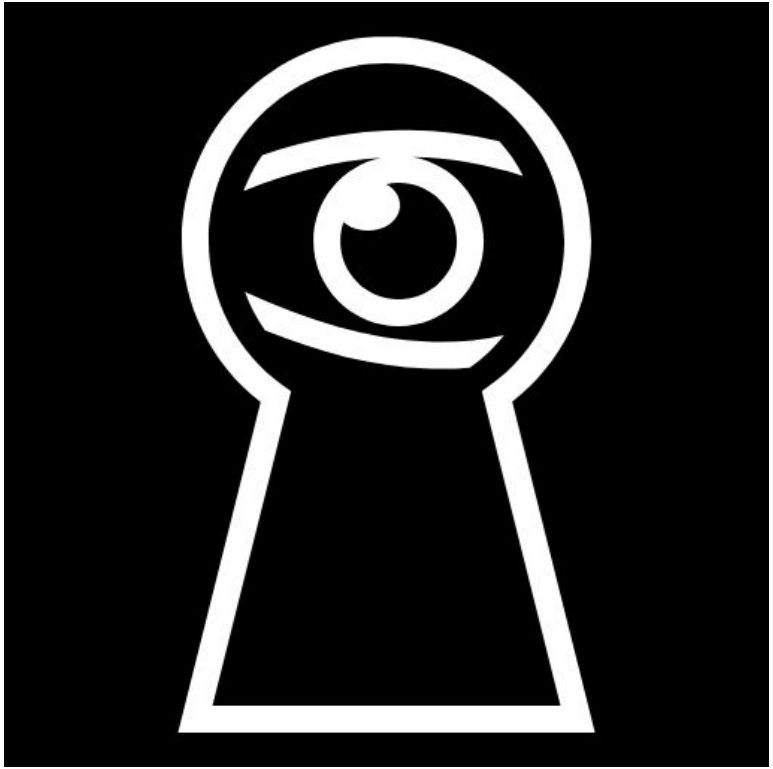
- The abuse of account recovery mechanisms is also a consistent theme when we investigate ATO.
- SMS hijacking is one vector, but even more common is the outdated or poorly secured recovery email.
- Many account recovery schemes result in an account that may have high security depending on the security of a lower-criticality asset (e.g. a core personal email address with U2F and locked down settings depending on an old university email with a reused password and no 2FA)



Account Recovery Abuse

Countermeasures

- We require an ID verification w/ selfie step in our account recovery flow. I think the effectiveness of this is likely to decline in the future as we get better fraud-oriented deepfakes.
- We also enforce a recovery waiting period and aggressive customer contact policy during that waiting period.
    - This is a great control in general, where attackers trigger waiting periods during an ATO (and we have them a number of places) their chances of success go to almost 0.



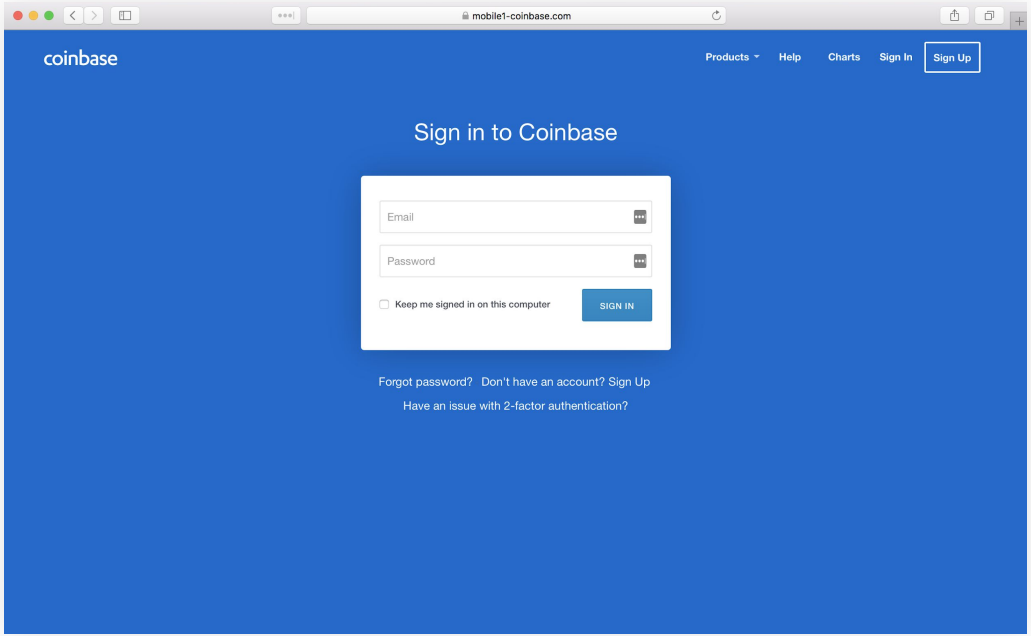
Credential Phishing w/ 2FA Theft

Details

- Credential phishers have upped their game with integrated 2FA theft and real-time account connections.
- We require 2FA codes for several in-app actions (changing 2FA, sending funds, etc) so we see attackers integrating multiple 2FA code collection via fake failures.

Countermeasures

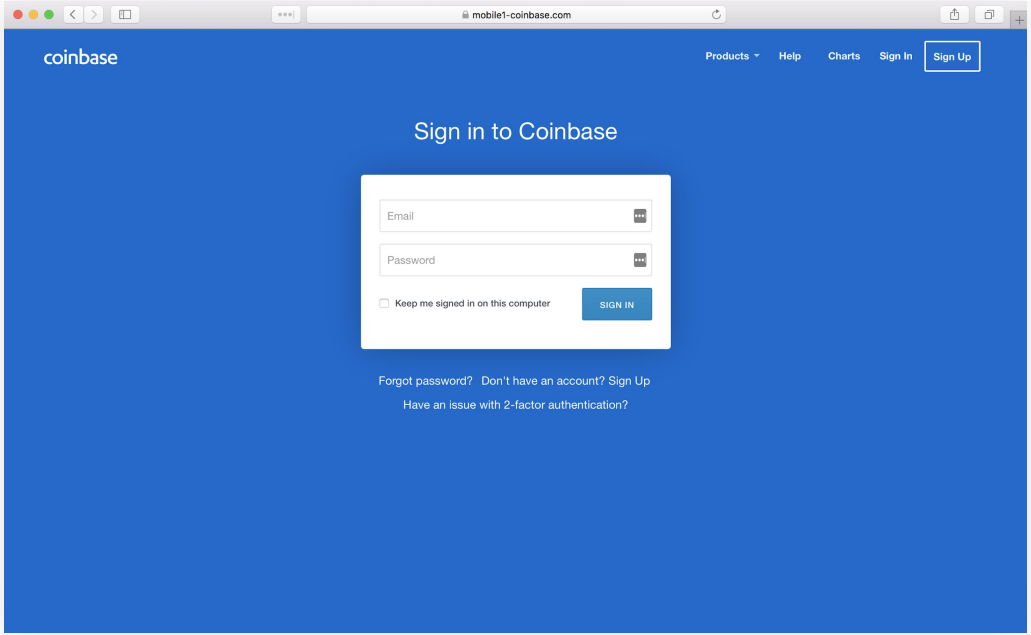
- Device verification is very effective against these attacks, as is rate limiting.



Credential Phishing w/ 2FA Theft

Countermeasures

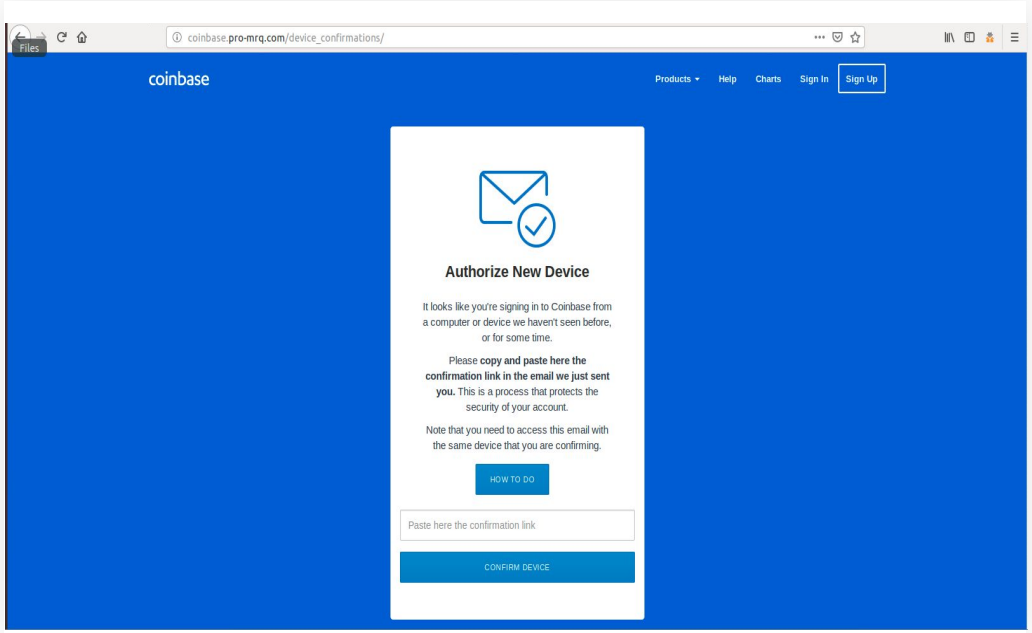
- Device verification is very effective against these attacks
- Rate limiting is also an effective deterrent, especially if you can rate limit on things like browser fingerprint.
- Monitor referrers, as attackers frequently leave references to things like favicons, images, CSS/JS bundles, etc in place.
- Monitor CT logs (although we see a lot of phishing sites these days that doesn't use our brand in the domain



Credential Phishing w/ 2FA Theft

BONUS - Device Verification Bypasses

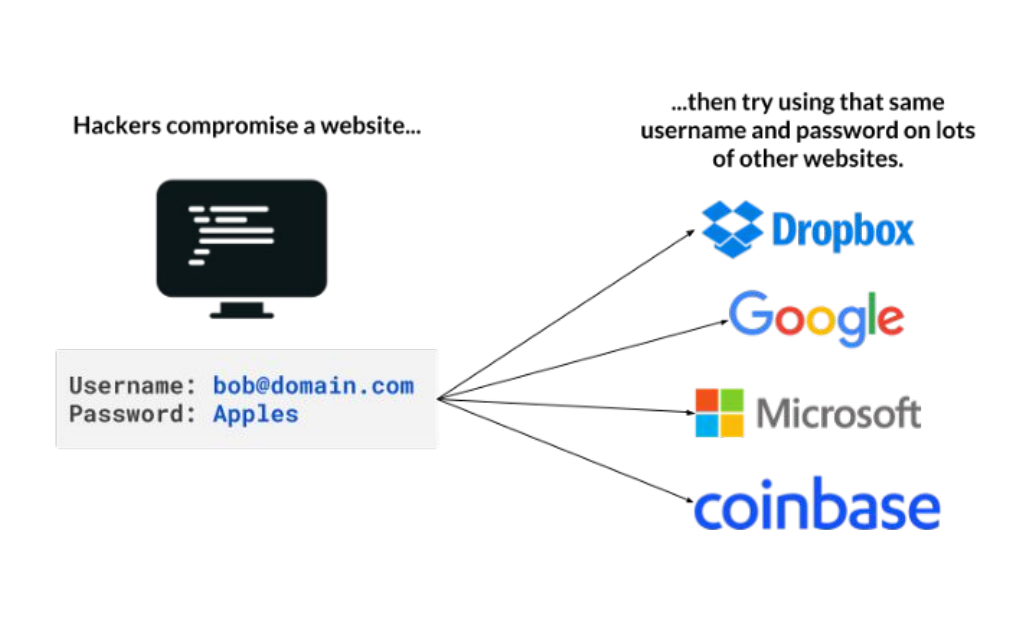
- We do see attackers trying to innovate around DV, but it has a petty low effectiveness rate so far.



Credential Stuffing

Details

- Increasingly seeing this conducted by broad botnets
  - 2-3 requests per IP
  - global footprint



Credential Stuffing

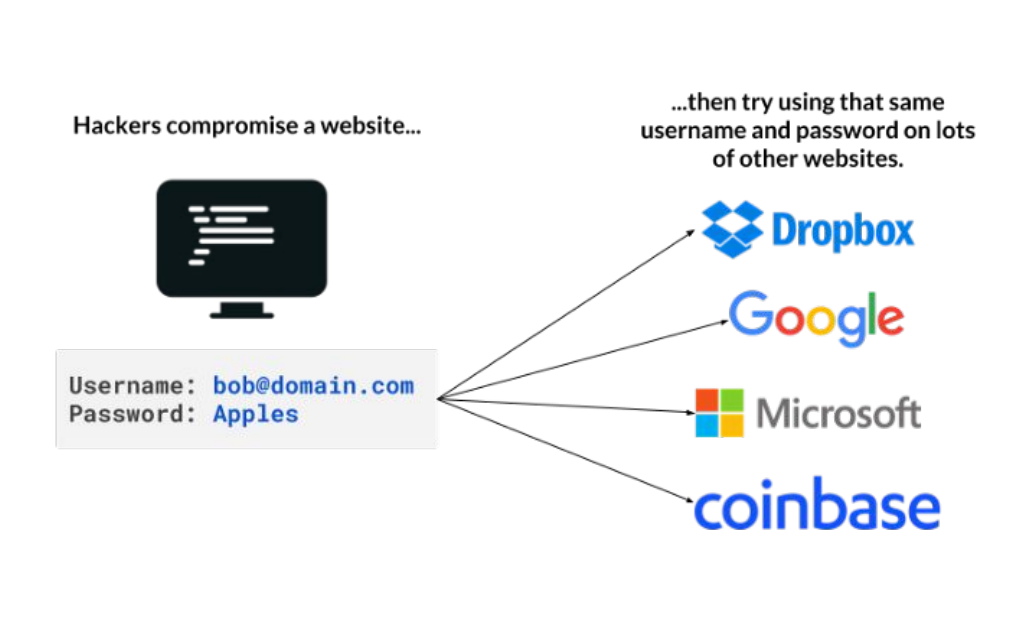
Details

- Increasingly seeing this conducted by broad botnets
  - 2-3 requests per IP
  - global footprint
  - IoT devices (we recently ID'd a toaster trying to login to Coinbase)

Credential Stuffing

Countermeasures

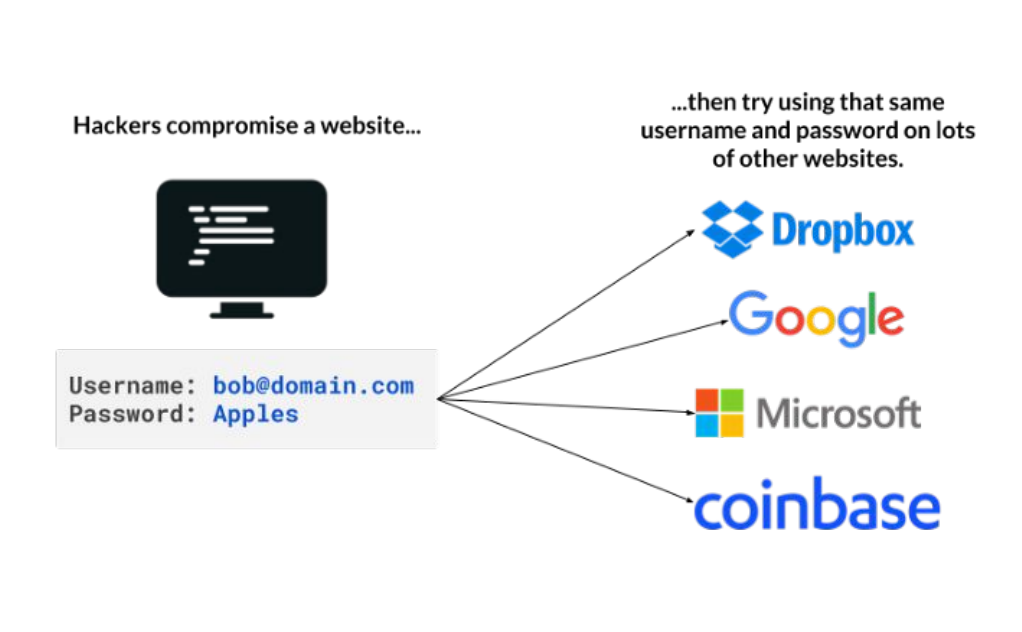
- Rate limiting is effective against some attackers, especially if you can rate limit on specific rare/invalid UAs or other unique behaviors
- 2FA is the ultimate solution. Because we enforce 2FA on all user accounts, our users generally see no impact from credential stuffing.



Credential Stuffing

BONUS - Active Deception

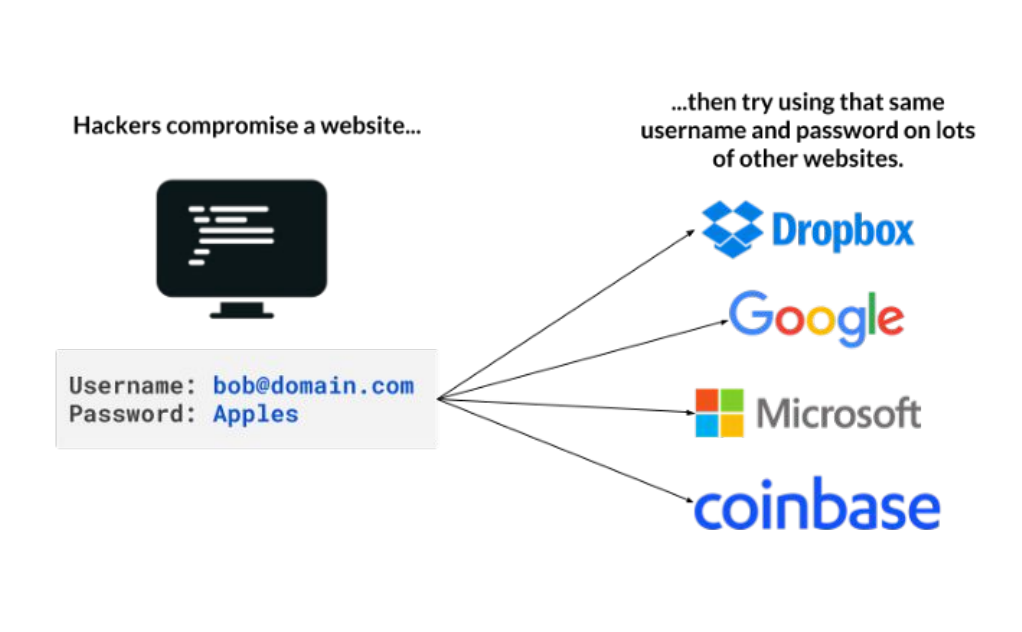
- Since 2016, we've been running a large scale active deception campaign against credential stuffers/list validators.
- We built a system that would identify likely campaigns via a mix of rules and a few heuristics (things like login attempt velocity increases on specific not-latest UAs, header order discrepancies, etc).
- Whenever that system detected a campaign, it feeds it statistically



Credential Stuffing

DOUBLE BONUS - 100% 2FA

- With about 30m global users, we're the largest platform I'm aware of that requires 2FA on all accounts.
- We default to SMS 2FA but also support TOTP and WebauthN.
- Getting folks to move up the 2FA stack is hard, but in-app prompts is key
- 2FA perceptions and approaches vary wildly by region



Social Engineering

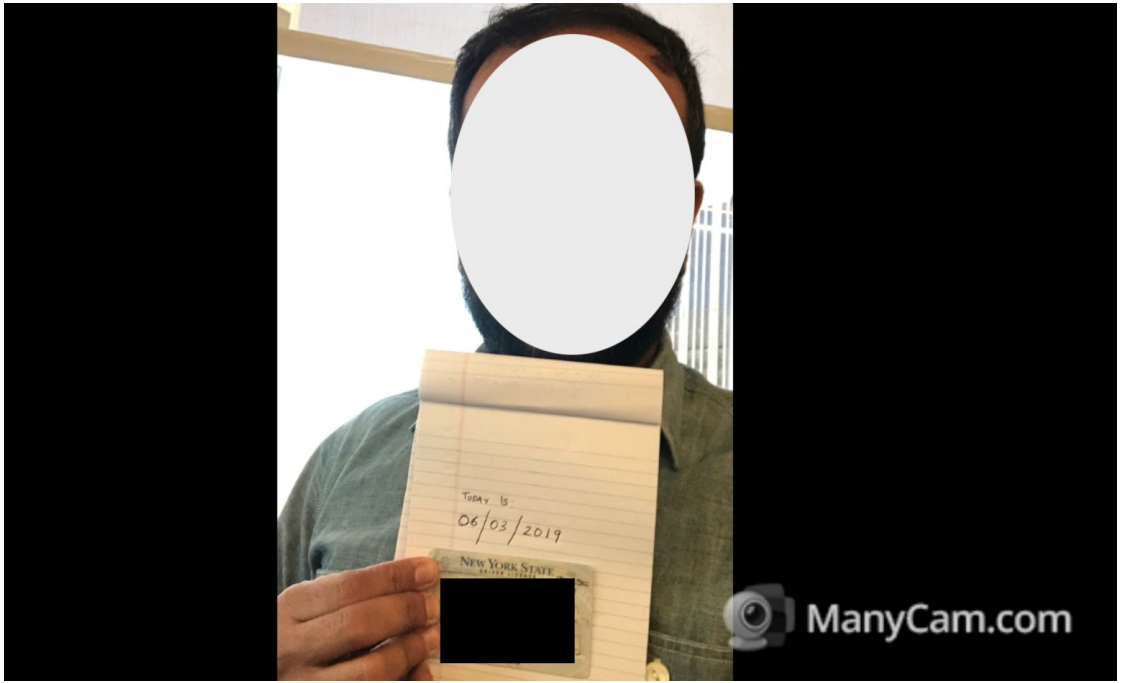
Details

- We see tech support style scams very frequently. The details vary a bit, but it normally comes down to a screen sharing app and tricking the user to transfer screen control while the Coinbase session is logged in.
- Traditionally, we've seen these scams executed as part of a cold calling scheme using call centers in places like India
- Increasingly we're seeing attacks that bring the users to the attackers instead

Social Engineering

Countermeasures

- Screen sharing detection is our main focus. We see fingerprintable differences in things like mouse events, keyboard events, etc.
- We also devote a fair bit of time to detecting and disrupting the channels scammers are using to lure users into their funnel via things like aggressive social media monitoring.



Malware

Details

- Banking Trojans and Malspam (Emotet, LokiBot, TrickBot) being repurposed to target cryptocurrency wallets and exchanges
- This largely shows up as session token theft with connections proxied through the victim system these days, but we've also seen clipboard modifiers, javascript injectors and a few others

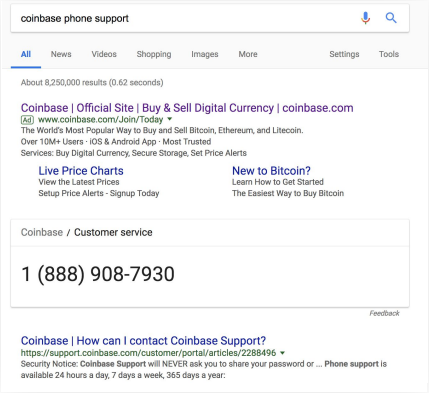
Malware

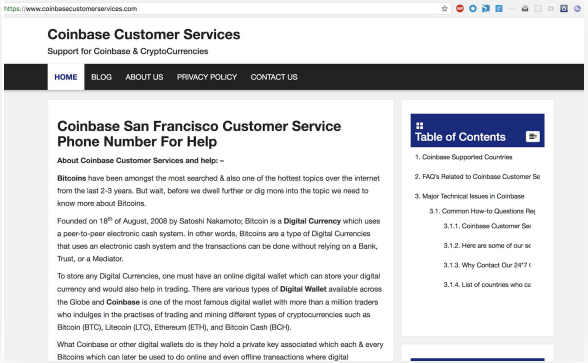
Countermeasures

- For the lower hanging fruit (clipboard modifiers, javascript injectors, etc) there are well-known countermeasures.
- The difficult case is when the malware is proxying connection through the victim computer (or even through the browser). In that case, it's all about flagging behavior changes and injecting friction.
- We dynamically inject 48hr holds on outbound transactions based on a behavior-based risk rating, although not

Emerging Attacker Techniques

Answer Box Pollution





Maps Locations

Wrap Up

The economic incentive to takeover accounts is only increasing

- Cryptocurrency is obviously an incentive, but more and more things are becoming monetizable about our online presence
- Attacks are also getting easier to conduct. Mega-dumps, deepfakes (for ID verification or liveness detection), etc.

Attackers have a fairly broad toolkit and are constantly innovating

- Static defenses are not enough, we need to continue to push the boundary in terms of 2FA normalization and JIT user awareness as well as in technical controls that:
  - Lower the bar for users while raising it for attackers, like WebAuthN; or
  - Change the economics of the situation, like active deception.

ATO Prevention is about incentivising good security behavior

- ATO is sometimes perceived as a user problem, and sometimes it can be, but it's also about enabling users by focusing on Security UI/UX in products and incentivising good security behavior.,
- Broad education is good but not sufficient, the most effective countermeasures we see are just-in-time application features or prompts that directly target attacker

Any Questions?

(BTW, if this sounds like a fun set of challenges then I've probably got an open role that you'd love… https://coinbase.com/careers)