CryptoChameleon: New Phishing Tactics Exhibited in FCC-Targeted Attack

By Lookout

Published: 2024-02-29 · Archived: 2026-04-05 14:05:09 UTC

Summary:

Lookout recently discovered an advanced phishing kit exhibiting novel tactics to target cryptocurrency platforms as well as the Federal Communications Commission (FCC) via mobile devices. Following the tactics of groups like Scattered Spider, this kit enables attackers to build carbon copies of single sign-on (SSO) pages, then use a combination of email, SMS, and voice phishing to trick the target into sharing usernames, passwords, password reset URLs and even photo IDs from hundreds of victims, mostly in the United States.

Employees targeted at

- Federal Communications Commission (FCC)
- Binance
- Coinbase

Cryptocurrency users at

- Binance
- Coinbase
- Gemini
- Kraken
- ShakePay
- Caleb & Brown
- Trezor

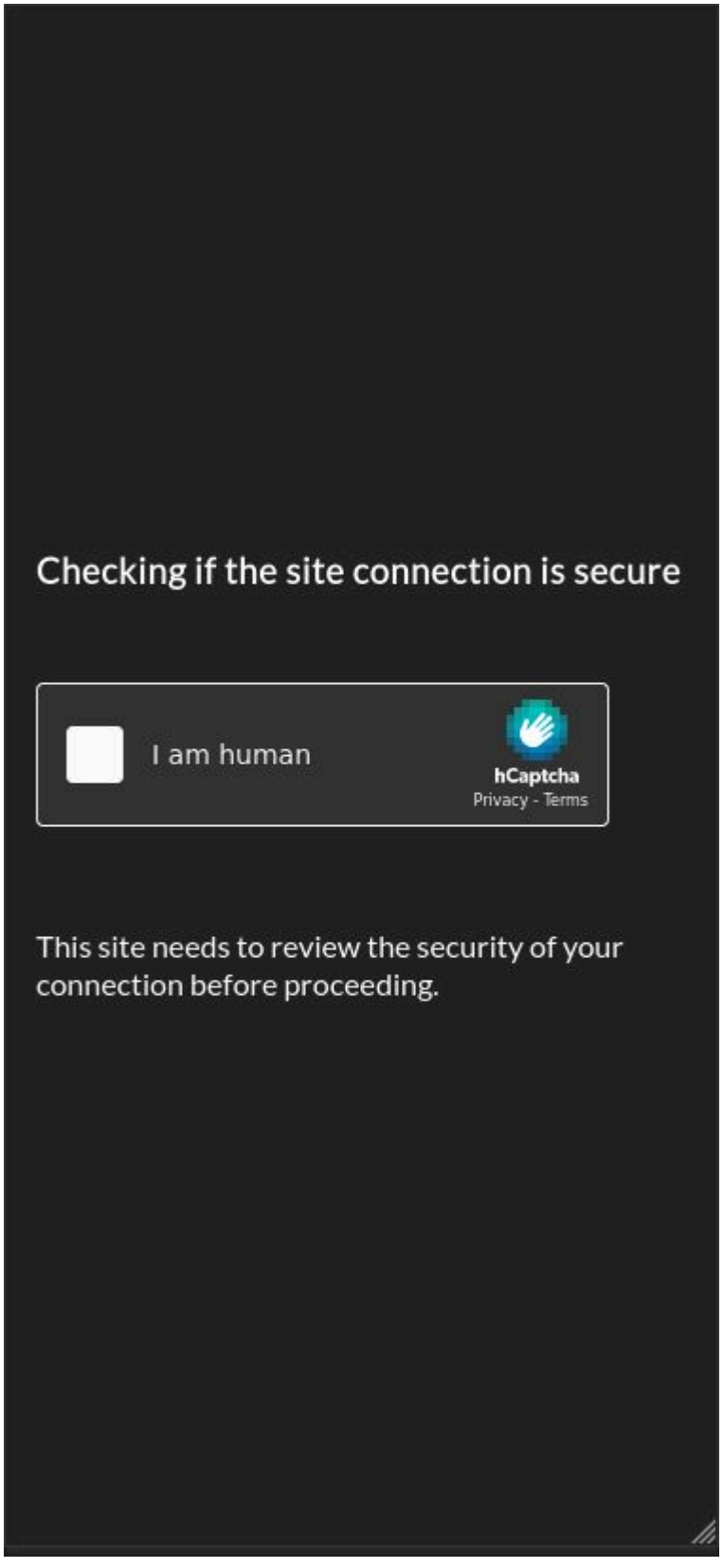
Email, Password management, and Single sign-on services

- LastPass
- AOL
- Gmail
- iCloud
- Okta
- Outlook
- Twitter
- Yahoo

Tactics and Flow of the FCC Phishing Site

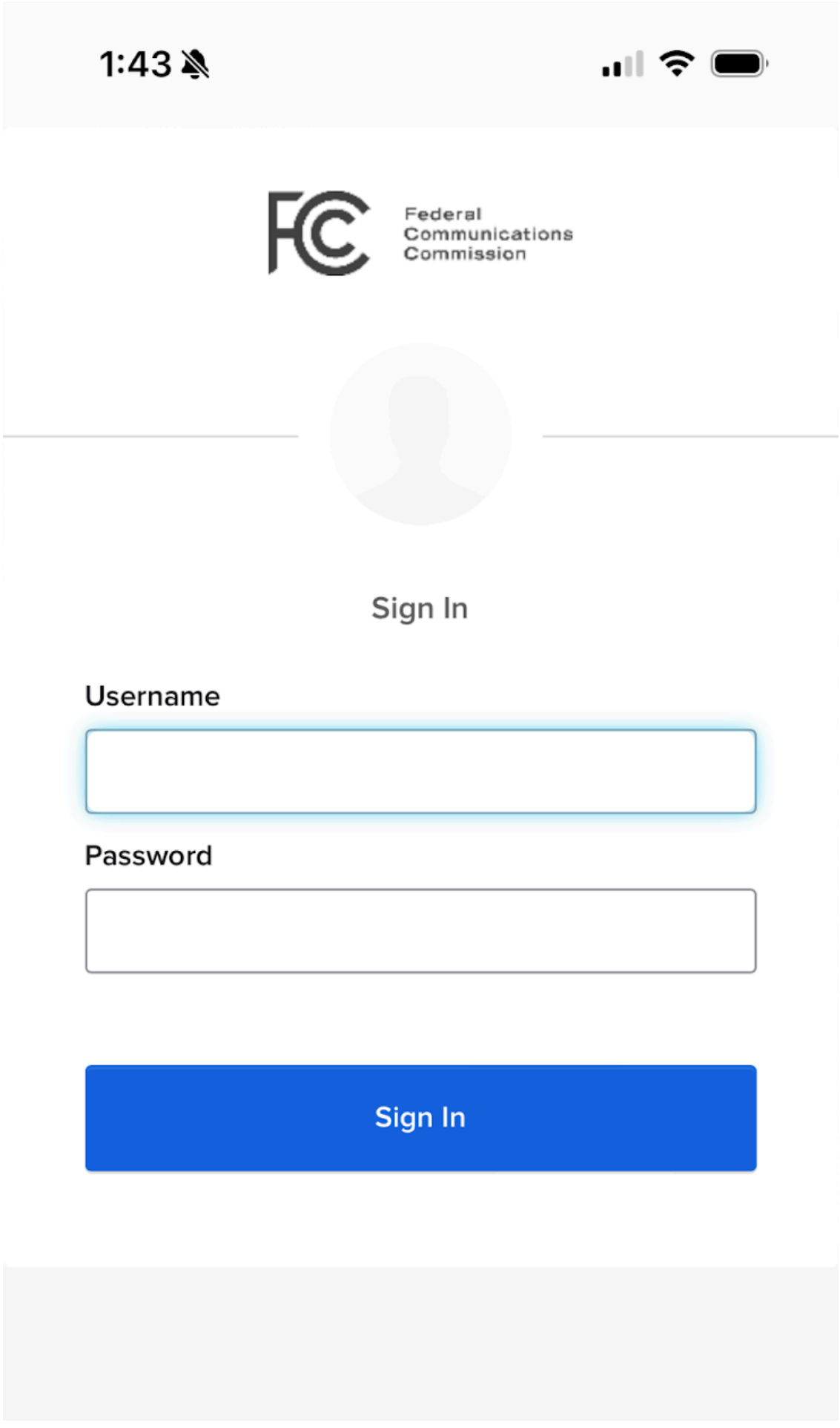
Lookout first flagged this phishing kit when our automated analysis discovered a suspicious new domain registration that matched a common format used by Scattered Spider, as mentioned in a recent warning by CISA. The domain in question was fcc-okta[.]com, which is only a single character different from the legitimate FCC Okta Single Sign On (SSO) page.

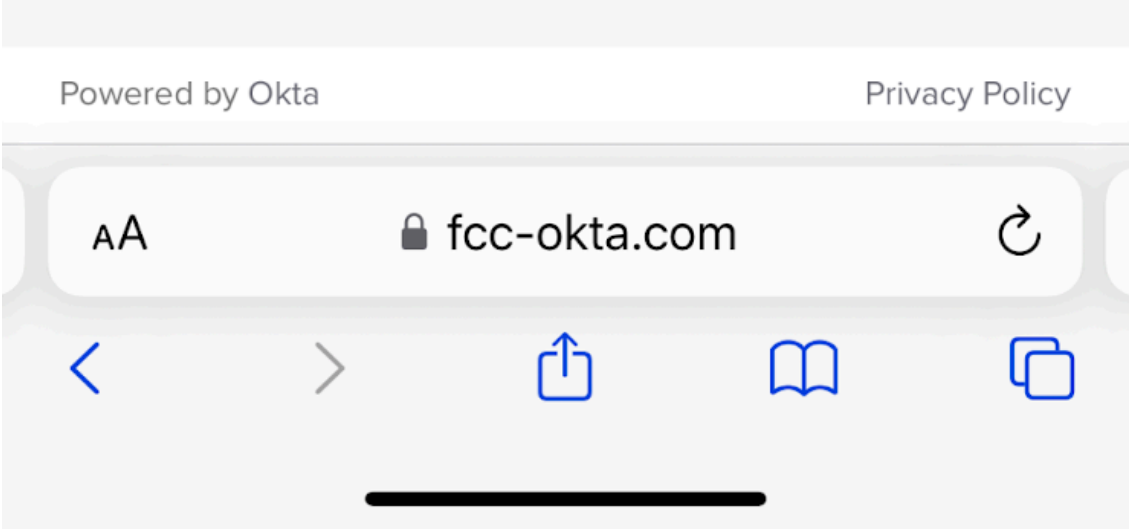
This phishing kit first asks the victim to complete a captcha using hCaptcha. This is a novel tactic that prevents automated analysis tools from crawling and identifying the phishing site. It may also give the illusion of credibility to the victim, as typically only legitimate sites use captcha.



Upon visiting the site, the user is asked to confirm they are human.

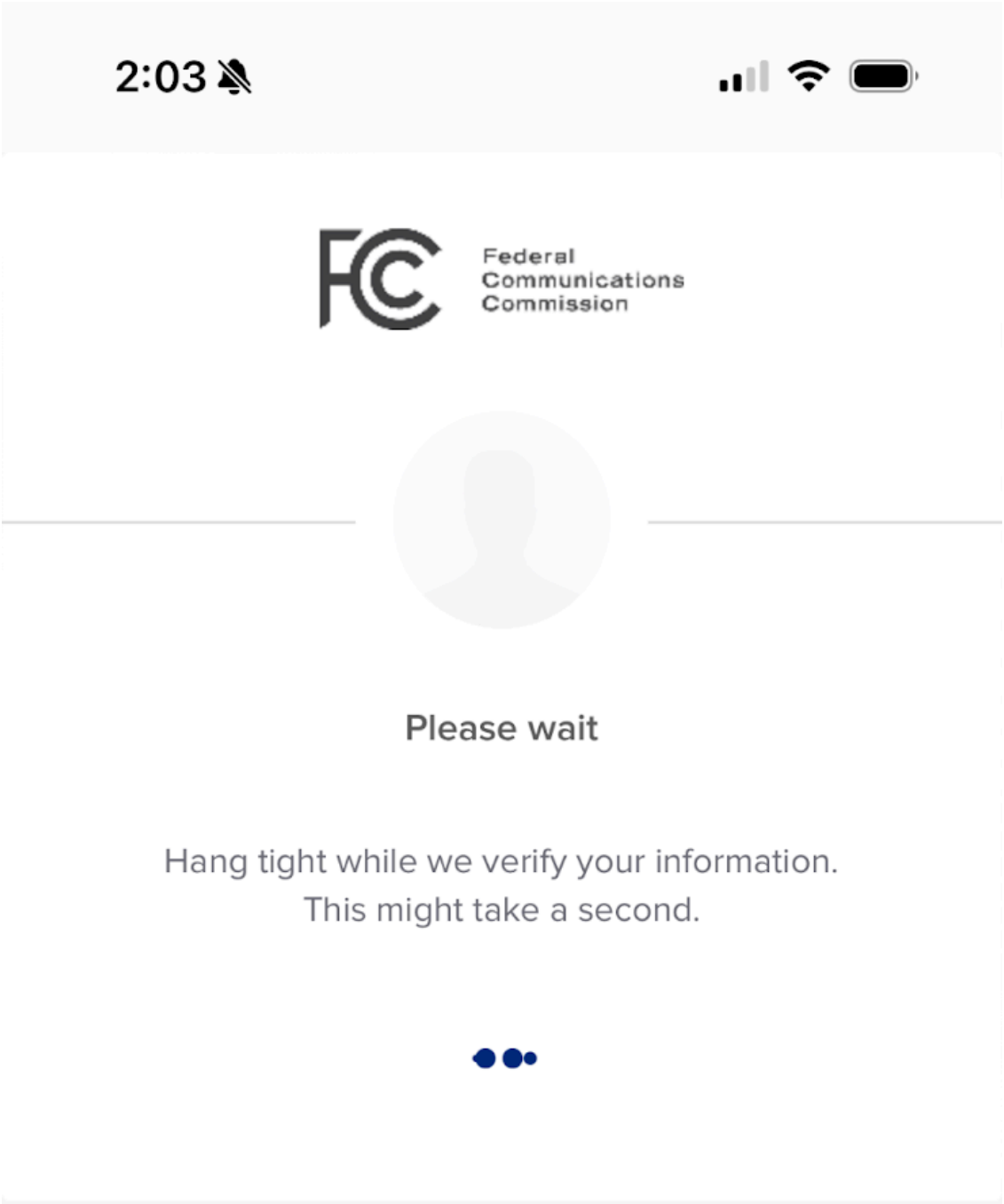
Once the captcha is completed, the login page mimics the FCC's legitimate Okta page.

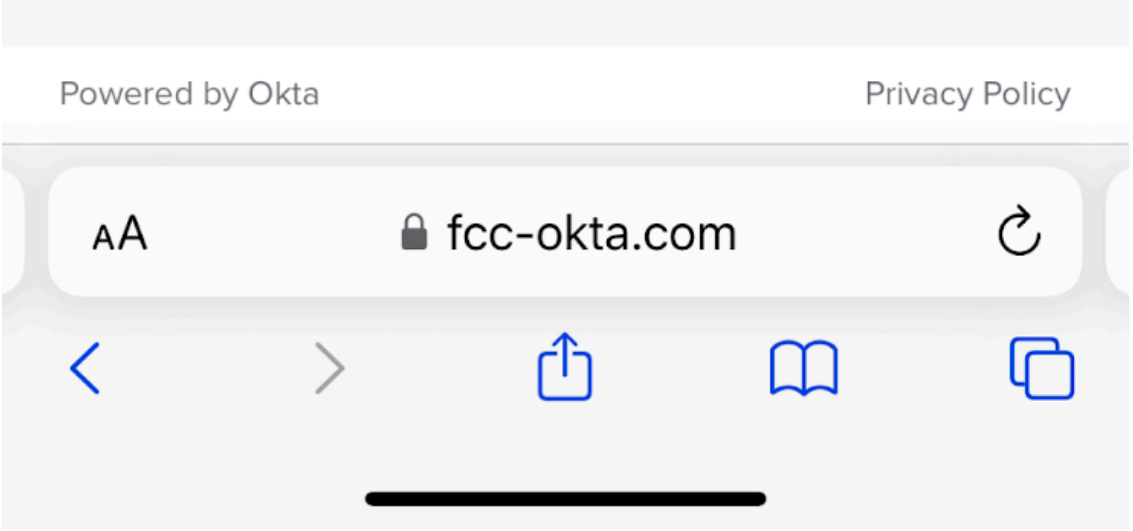

1:43
Federal
Communications
Commission
Sign In
Username
Password
Sign In



A very good replica of the official Okta page for the targeted organization.

Upon providing their credentials, the victim can be sent to wait, sign in, or ask for the MFA token.


2:03
Federal
Communications
Commission
Please wait
Hang tight while we verify your information.
This might take a second.



The victim is sent to a "loading" page to wait after entering their credentials.

Unlike typical phishing kits, which attempt to harvest credentials as quickly as possible, this one seems to be aware of modern security controls organizations have put in place such as MFA.

Lookout researchers saw that there is an administrative console that the operator uses to monitor the phishing page. While we were unable to directly access this console, we were able to access its javascript and css and piece together much of its functionality. Each time a victim visited the page and entered information, we observed that a new row was populated on a table. Once the victim enters their username and password, the admin is able to select from a long list of options of where to send them next.

The attacker likely attempts to log in using these credentials in real time, then redirects the victim to the appropriate page depending on what additional information is requested by the MFA service the attacker is trying to access, For example, they can be redirected to a page that asks for their MFA token from their authenticator app or a page requesting an SMS-based token.

```
<option>Select...</option>
<optgroup label="Okta">
    <option value="/signin">Sign in</option>
    <option value="/otp">OTP</option>
    <option value="/loading">Loading</option>
</optgroup>
<optgroup label="AOL">
    <option value="/aol">Password</option>
    <option value="/aol_otp">OTP</option>
    <option value="/loading_aol">Loading</option>
</optgroup>
<optgroup label="Gmail">
    <option value="/gmail">Sign in</option>
    <option value="/gmail_device">App</option>
    <option value="/gmail_otp">OTP SMS</option>
    <option value="/gmail_eotp">OTP email</option>
    <option value="/gmail_backup">Backup codes</option>
    <option value="/loading_gmail">Loading</option>
</optgroup>
```

```
<optgroup label="Outlook">
    <option value="/outlook_pw">Password</option>
    <option value="/outlook_otp">OTP</option>
    <option value="/loading_outlook">Loading</option>
</optgroup>
<optgroup label="iCloud">
    <option value="/icloud">Sign in</option>
    <option value="/icloud_otp">OTP</option>
    <option value="/icloud_2fa">2FA device</option>
    <option value="/loading_icloud">Loading</option>
    <option value="/icloud_verified">Verified</option>
</optgroup>
<optgroup label="External sites (leaves panel!)">
    <option value="/gmail_com">Gmail.com</option>
    <option value="/yahoo_com">Yahoo.com</option>
    <option value="/aol_com">AOL.com</option>
    <option value="/outlook_com">Outlook.com</option>
    <option value="/icloud_com">iCloud.com</option>
    <option value="/redirect">CUSTOM URL (NEW!)</option>
</optgroup>
```

The operator can choose various customizable pages to send the victim to next.

In some cases, when selecting an option, the operator will be prompted to provide more detailed information back to the victim. For example, when sending an SMS-based MFA token, the operator can provide the last digits of the

victim's actual phone number and customize whether the page should ask the victim for a 6 digit or 7 digit code to make it feel more legitimate.

```
if (selectElement.value === '/otp_sms' || selectElement.value === '/outlook_otp' || selectElement.value === '/twitter_sms'
    let digits = prompt('Enter last 2 digits of phone number');
    let e = confirm('OK = Show timed out error | CANCEL = No error');
    e = (e === true) ? 1 : 0;
    let format = confirm('OK = 6 digit code | CANCEL = 7 digit code');
    format = (format === true) ? 1 : 0;
    socket.emit('userAction', { user: user, response: selectElement.value, digits: digits, e: e, format: format });
```

The operator is prompted to customize the phishing page in real time by providing the last 2 digits of the phone number and selecting whether the victim should be asked for a 6 or 7 digit token.

Next, the operator would attempt to log in using the one-time password (OTP) token provided. At that point, the operator can direct the victim to any page, such as the real Okta sign in page, or a specific page with messages customized to different scenarios. For example, we found a page that tells the victim that their account is under review and to try to log in later at a time specified by the operator.

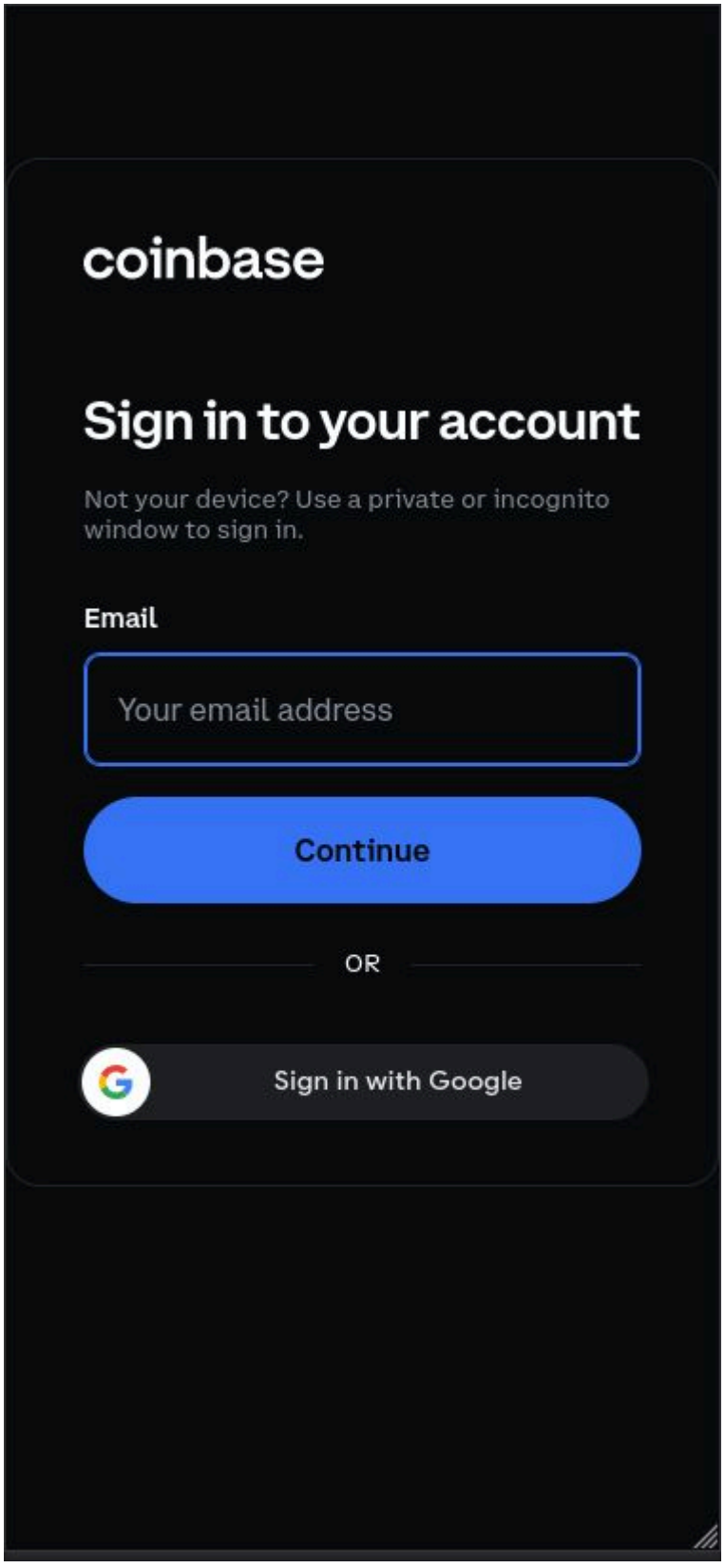
```
} else if (selectElement.value === '/pending_review') {
    let date = prompt('Enter date (e.g. July 15, 2023 7:00pm PDT):');
    if (!date) {
        let now = new Date();
        let futureDate = new Date(now.getTime() + (14 * 24 * 60 * 60 * 1000));
        let options = {
            month: 'long',
            day: 'numeric',
            year: 'numeric',
            hour: 'numeric',
            minute: 'numeric',
            timeZone: 'America/Los_Angeles',
            timeZoneName: 'short'
        };
        let formatter = new Intl.DateTimeFormat('en-US', options);
        date = formatter.format(futureDate);
    }
    socket.emit('userAction', { user: user, response: selectElement.value, date: date });
```

The operator would be asked to select a date when sending the victim to a page telling them their account was being reviewed.

While we were tinkering with the FCC Okta phishing site, the site was taken down and replaced with a racial slur.

Broader Phishing Kit Analysis

We were also able to investigate the phishing kit, which gave us additional insight into targets and tactics used. The kit contains numerous references to cryptocurrency platforms and SSO services. While the version of the kit targeted at the FCC impersonates the FCC's specific Okta page by default, the kit is able to impersonate many different company's brands.



The screenshot above displays this phishing kit's ability to impersonate Coinbase

Based on the phishing site characteristics, Lookout researchers were able to identify other websites using this phishing kit. Most of the websites use a subdomain of official-server[.]com as their C2, in addition to others listed at the bottom of this report. We also found Okta impersonation pages targeting employees of Binance and Coinbase, but the majority of the sites seemed targeted at users of cryptocurrency and SSO services. Coinbase is the most-frequently targeted service. Since February 21, some of the newly registered phishing domains use subdomains of a new C2 original-backend[.]com

Lookout researchers have also been able to gain ephemeral access to the backend logs, where we noted consistently high quality of the stolen credentials. Typically, when accessing a phishing site's data, it is filled with junk data that is obviously not someone's real email address or password. However, a high percentage of the credentials collected by these sites look like legitimate email addresses, passwords, OTP tokens, password reset URLs, photos of driver's licenses and more. The sites seem to have successfully phished more than 100 victims, based on the logs observed. Many of the sites are still active and continue to phish for more credentials each hour.

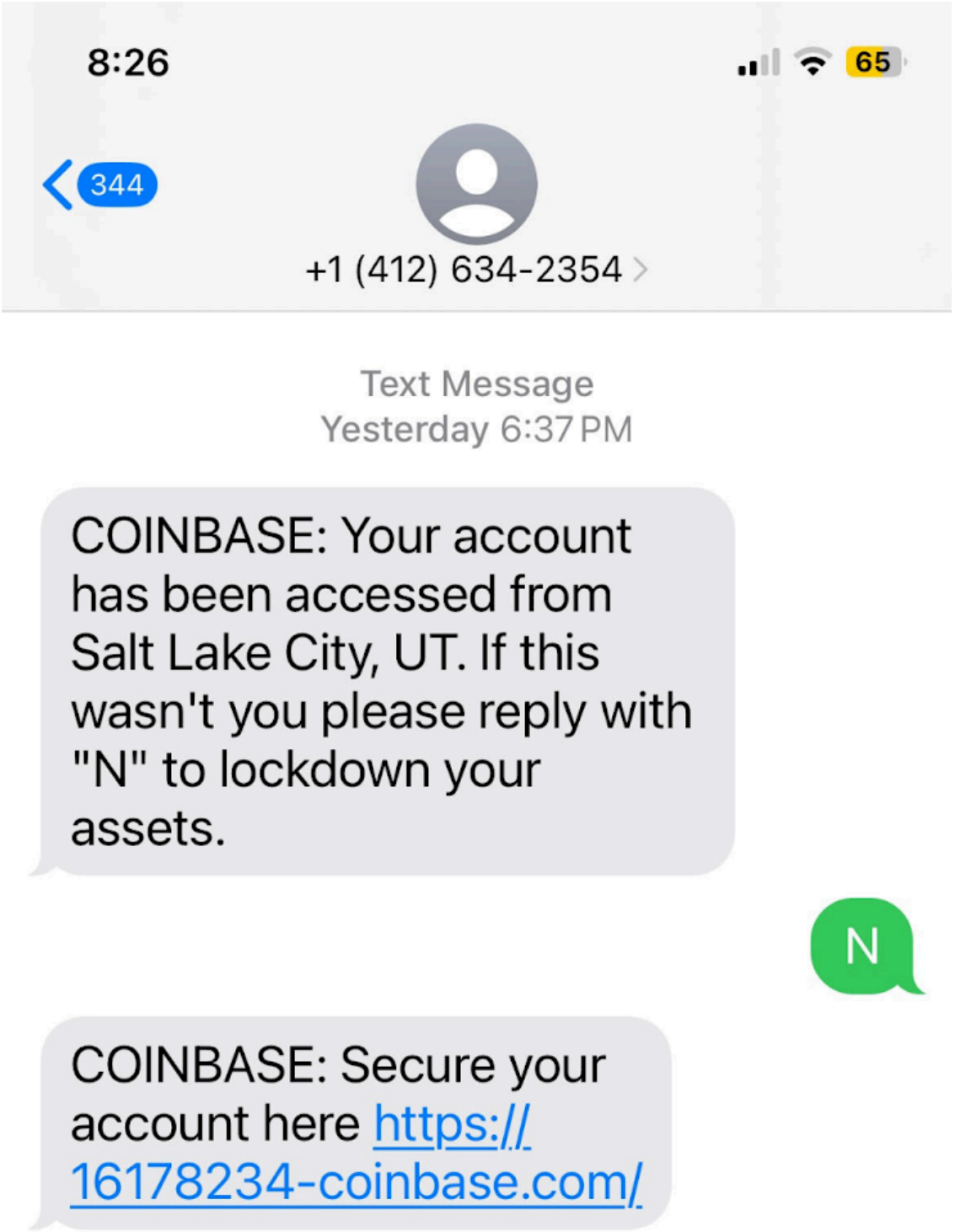
Some noteworthy files in the phishing kit include:

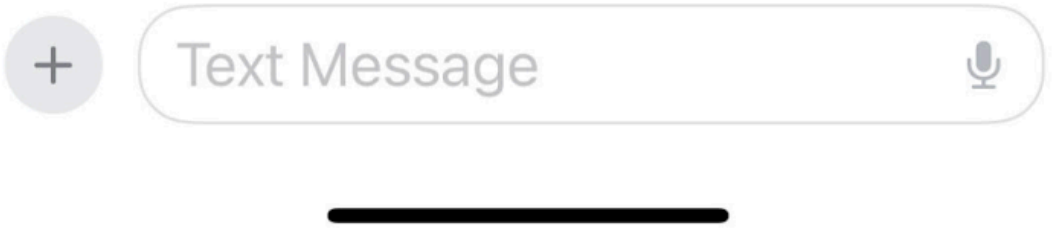
- /js/consts.js contains the URL for the command and control (C2) server
- /js/init.js contains the client-side logic for redirecting the victim and collecting the phished data
- /css/ contains the style sheets for impersonating the sites

The phishing websites have been deployed on various hosting networks. In November and December of 2023, Hostwinds and Hostinger were the cybercriminals' main choice of networks. However in January and February of 2024, most of the sites were hosted on RetnNet in Russia on IP 213.178.155[.]194. In general, it looks like sites hosted on RetnNet remain online longer compared to other hosting networks. This IP was active until February 17, after which the cybercriminals moved to new IP 185.12.127[.]233 on QWARTA LLC hosting services. On February 22, the cybercriminals moved to another IP 81.94.159[.]46 on OOO Westcall Ltd

Delivery Mechanisms Observed

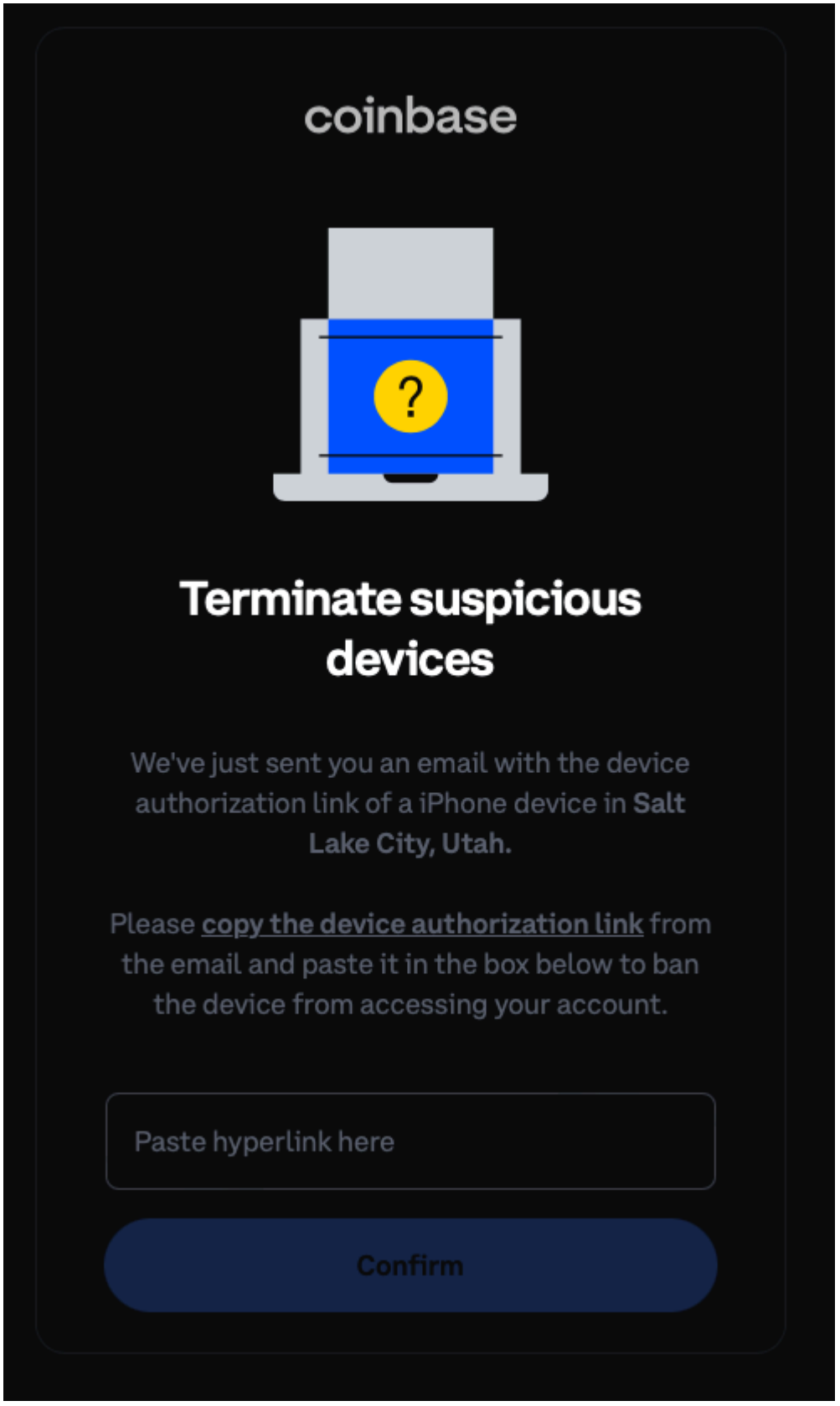
We were also able to speak directly with some victims, and in doing so we were able to ascertain that a combination of phone calls and text messages were used to encourage the victim to complete the process. In one scenario, a victim received an unsolicited phone call that spoofed a real company's customer support line. The person on the other end of the line was the threat actor, but sounded like a member of the support team from that company. They informed the victim that their account had been hacked, but that they would help them recover the account. While the victim was on the phone with the threat actor, they were sent a text message that linked them to the phishing page.


8:26
65
344
+1 (412) 634-2354
Text Message
Yesterday 6:37 PM
COINBASE: Your account has been accessed from Salt Lake City, UT. If this wasn't you please reply with "N" to lockdown your assets.
N
COINBASE: Secure your account here https://16178234-coinbase.com/



A text message provided by a victim, where they were alerted their account had been hacked (it had not) and to click on a phishing link to recover it.

While still on the phone with the victim, the threat actor encouraged them and helped them complete the steps. As a way to build credibility and trust, the actor consistently noted that the allegedly unauthorized device accessing the account was in Salt Lake City, Utah. This was mentioned in the text message, the phone call and on the phishing page itself (which is customizable to display different device types or locations).



The phishing kit contains specific references to the story being told to the victim on the phone and via text messages.

```
} else if (selectElement.value === '/device_auth') {
    let device = prompt('Enter device (e.g. iPhone):');
    let location = prompt('Enter location (e.g. Salt Lake City, Utah):');
    socket.emit('userAction', { user: user, response: selectElement.value, device: device, location: location });
```

When directing the victim to the page above, the operator can select the device type and location to be displayed on the page.

When we asked victims to describe the person on the other end of the line they characterize them as sounding “American”, “well spoken”, and “had professional call-center communication skills”.

We believe that the combination of high quality phishing URLs, login pages that perfectly match the look and feel of the legitimate sites, a sense of urgency, and consistent connection through SMS and voice calls is what has given the threat actors so much success stealing high quality data.

Sifting through the logs, the majority of victim data that looks legitimate comes from iOS and Android devices, which indicates the attack is primarily targeted at mobile devices. The vast majority of the victims are in the US.

Attribution

This attack follows similar techniques as Scattered Spider – in particular impersonation of Okta, registration of domains using *companyname*-okta.com, and homoglyph swapping. An example of homoglyph swapping would be switching capital Is and lowercase Ls to make AcmeInc.com (with a capital I) look identical to Acmelnc.com (with a lowercase L substituted for the capital I). One domain that is used (binance-okta[..]com) has been known in the past to be affiliated with Scattered Spider .

Despite the similarities to Scattered Spider, there are enough differences to indicate that this is likely not being operated by that group. For example, despite the URLs and spoofed pages looking similar to what Scattered Spider might create, there are significantly different capabilities and C2 infrastructure within the phishing kit. This type of copycatting is common amongst threat actor groups, especially when a series of tactics and procedures have had so much public success.

It is unknown whether this is a single threat actor or a common tool being used by many different groups. However, there are many similarities in the backend C2 servers and test data our team found across the various phishing sites.

Protection

Based on similarities and similar infrastructure of previous attacks, Lookout customers have been protected against these phishing sites since before we identified this threat actor in January 2024. We have continued to track the general behaviors and techniques used to ensure protection against additional sites that use this kit and will continue to update protections through automated means as necessary.

Indicators of Compromise

Command and Control servers

commandandcontrolserver[.]com
lookoutstop[.]com
officialbackupserver[.]com
original-backend[.]com
thebackendserver[.]com

lookoutsucks[.]com

official-server[.]com
server694590423[.]tech
island-placid-bromine.glitch[.]me
circular-noon-farmhouse.glitch[.]me
talented-friendly-price.glitch[.]me
dflfmgsdokasdcpl[.]com
original-backend[.]com

Phishing websites

147253-exodus[.]com
156253-gemini[.]com
157253-kucoin[.]com
158253-kraken[.]com
113712-coinbase[.]com
12518234-coinbase[.]com
125194-coinbase[.]com
12595-gemini[.]com
125980-binance[.]com
127253-ledger[.]com
128594-gemini[.]com
129581-coinbase[.]com
129645-coinbase[.]com
142685-coinbase[.]com
142724-coinbase[.]com
142746-coinbase[.]com
142786-coinbase[.]com
143516-coinbase[.]com
143784-coinbase[.]com
145126-coinbase[.]com
14522564-coinbase[.]com
14572176-coinbase[.]com
146784-coinbase[.]com
147852-kraken[.]com

148942-coinbase[.]com
149024-google[.]com
149253-coinbase[.]com
1502759-ledger[.]com
151294-kraken[.]com
151924-coinbase[.]com
1519845-kraken[.]com
152674-coinbase[.]com
154236-coinbase[.]com
156283-coinbase[.]com
157142-kraken[.]com
157192-uphold[.]com
157194-gemini[.]com
1581932-coinbase[.]com
158248-gemini[.]com
158712-coinbase[.]com
159120-coinbase[.]com
159823-coinbase[.]com
16159867-coinbase[.]com
1645079-coinbase[.]com
167243-coinbase[.]com
167253-binance[.]com
17224652-coinbase[.]com
17384624-coinbase[.]com
173912-coinbase[.]com
17412627-coinbase[.]com
17503-apple[.]com
1750314-apple[.]com
17512657-coinbase[.]com
1751654-coinbase[.]com
17591024-coinbase[.]com
1759654-coinbase[.]com
17612416-coinbase[.]com
17612418-gemini[.]com
17612486-coinbase[.]com
17618412-coinbase[.]com
176425-coinbase[.]com
17682192-coinbase[.]com
176822-coinbase[.]com
176823-coinbase[.]com
17691-coinbase[.]com
177250-cb[.]com

177250-kraken[.]com
177253-coinbase[.]com
17825-coinbase[.]com
178492-coinbase[.]com
178526-coinbase[.]com
17913-coinbase[.]com
17916-cb[.]com
17916-cbwallet[.]com
17916-coinbase[.]com
17919-coinbase[.]com
179325-coinbase[.]com
17943564-coinbase[.]com
1827235-coinbase[.]com
1835246-coinbase[.]com
18364712-coinbase[.]com
184124-coinbase[.]com
184625-trezor[.]com
1847039-coinbase[.]com
185126-coinbase[.]com
18532063-coinbase[.]com
185417-coinbase[.]com
185421-coinbase[.]com
18547-coinbase[.]com
185614-coinbase[.]com
185617-coinbase[.]com
185914-coinbase[.]com
185924-uphold[.]com
187253-uphold[.]com
187421-coinbase[.]com
18925-coinbase[.]com
19045-coinbase[.]com
191284-coinbase[.]com
191284-gemini[.]com
19175234-coinbase[.]com
19243652-coinbase[.]com
1925876-coinbase[.]com
19265-coinbase[.]com
19453264-coinbase[.]com
19463752-coinbase[.]com
1947245-google[.]com
194857-kraken[.]com
195024-coinbase[.]com

195102-coinbase[.]com
195127-coinbase[.]com
19513657-coinbase[.]com
19524624-coinbase[.]com
195824-swanbtc[.]com
195827-binance[.]com
19584-coinbase[.]com
19642-coinbase[.]com
197253-trezor[.]io
197287-coinbase[.]com
19783221-coinbase[.]com
19784-coinbase[.]com
1985204-coinbase[.]com
19854-coinbase[.]com
229123-coinbase[.]com
235252-cb[.]com
27954383-coinbase[.]com
283272-coinbase[.]com
298193-coinbase[.]com
391215-coinbase[.]com
421424-cb[.]com
421424-cbwallet[.]com
489912-coinbase[.]com
53201-coinbase[.]com
592013-apple[.]com
7226119-coinbase[.]com
783927-coinbase[.]com
83730493-coinbase[.]com
848312-coinbase[.]com
85439-cb[.]com
884394-coinbase[.]com
90251-gmail[.]com
90251-icloud[.]com
917260-coinbase[.]com
923852-coinbase[.]com
96329-coinbase[.]com
account-help-icloud[.]com
adfs-seic[.]com
administration-icloud[.]com
adsupport-google[.]com
appie-pay[.]com
appleassist[.]org

applepayhelp[.]net
applepayhelp[.]org
authorize-okta[.]com
authorizing-coinbase[.]com
binancesecurity[.]com
binancetickets[.]com
blocked-cb[.]com
blocked-coinbase[.]com
cancel-google[.]com
coinbase-login[.]com
coinbasehelpdesk[.]com
coinbasetickets[.]com
com-ticket[.]info
compensate-cb[.]com
compensation-coinbase[.]com
dashboard-cbwallet[.]com
dashboard-kraken[.]com
dashboard-kucoin[.]com
defend-cb[.]com
defend-cbwallet[.]com
deposit-coinbase[.]com
finance-coinbase[.]com
firewall-cb[.]com
firewall-coinbase[.]com
gamdomrewards[.]com
gamdomsecurity[.]com
googie[.]support
googlehelpdesk[.]com
guard-cbwallet[.]com
handle-coinbase[.]com
help-applecare[.]com
help-cbwallet[.]com
help-coinbasesupport[.]com
help-lastpass[.]com
help-swanbtc[.]com
helpdesk-google[.]com
helpdesk-microsoftonline[.]com
icloudtickets[.]com
idmsac-apple[.]com
idmsac1-apple[.]com
idmsac2-apple[.]com
idsmac-apple[.]com

indentity-coinbase[.]com
iticket-apple[.]com
lastpasshelp[.]com
linkedin-okta[.]com
lockdown-coinbase[.]com
lockup-coinbase[.]com
login-swanbitcoin[.]com
msfthelpdesk[.]com
mypasskey[.]info
nexotickets[.]com
passkeysetup[.]com
portal-cb[.]com
portal-exodus[.]com
portal-trezor[.]io
privacy-cb[.]com
protect-cbwallet[.]com
protection-cb[.]com
protection-kraken[.]com
receipt-coinbase[.]com
recovery-cb[.]com
recoveryportal-kraken[.]com
refund-cb[.]com
revert-kraken[.]com
reverts-coinbase[.]com
s-binance[.]com
s-gemini[.]com
s-kraken[.]com
s-kucoin[.]com
secureaccess-coinbase[.]com
secureunlock-coinbase[.]com
securing-coinbase[.]com
shield-cb[.]com
shield-cbwallet[.]com
signin-swanbitcoin[.]com
swan-bitcoin[.]com
swan-help[.]com
swap-coinbase[.]com
tickets-lastpass[.]com
ticketsupport-coinbase[.]com
trezor-recovery[.]io
unlink-ledger[.]com
unlink-trezor[.]com

unlock-kraken[.]com
verification-gemini[.]com
verification-trezor[.]com
verify-gemini[.]com
verify-ledger[.]com
verify-trezor[.]io
www-cb-wallet[.]com
www-cbwallet[.]com
www-help-apple[.]com
x-okta[.]com
yahoohelpdesk[.]com
yourapplecare[.]com

help-lastpass[.]com

113712-coinbase[.]com
113912-coinbase[.]com
129045-coinbase[.]com
142724-coinbase[.]com
142746-coinbase[.]com
142764-coinbase[.]com
142786-coinbase[.]com
145126-coinbase[.]com
146282-coinbase[.]com
146784-coinbase[.]com
148942-coinbase[.]com
1502759-ledger[.]com
1519845-kraken[.]com
157192-uphold[.]com
157194-gemini[.]com
16159867-coinbase[.]com
16275-coinbase[.]com
167243-coinbase[.]com
17224652-coinbase[.]com
17384624-coinbase[.]com
173912-coinbase[.]com
17412627-coinbase[.]com
17512457-coinbase[.]com
17512657-coinbase[.]com
1751654-coinbase[.]com
1751854-coinbase[.]com
1751954-coinbase[.]com
17591024-coinbase[.]com

1759654-coinbase[.]com
17612416-coinbase[.]com
17612418-gemini[.]com
17612412-coinbase[.]com
17612486-coinbase[.]com
17618412-coinbase[.]com
17625-coinbase[.]com
17682192-coinbase[.]com
176822-coinbase[.]com
176823-coinbase[.]com
176824-coinbase[.]com
17691-coinbase[.]com
17825-coinbase[.]com
17913-coinbase[.]com
17916-coinbase[.]com
185417-coinbase[.]com
185421-coinbase[.]com
18547-coinbase[.]com
185614-coinbase[.]com
185617-coinbase[.]com
185914-coinbase[.]com
185924-uphold[.]com
187421-coinbase[.]com
18925-coinbase[.]com
191284-coinbase[.]com
192854-gemini[.]com
192856-coinbase[.]com
195102-coinbase[.]com
195127-coinbase[.]com
19524624-coinbase[.]com
19562-coinbase[.]com
19582-coinbase[.]com
195827-binance[.]com
197287-coinbase[.]com
83730493-coinbase[.]com
90251-gmail[.]com
90251-icloud[.]com
account-help-icloud[.]com
appie-pay[.]com
appleassist[.]org
applepayhelp[.]net
applepayhelp[.]org

blocked-coinbase[.]com
bofa-help[.]com
coinbase-login[.]com
coinbase-ticketsupport[.]com
coinbaseticketsupport[.]com
com-175691[.]help
com-83730493[.]help
com-fraud[.]management
com-ticket[.]info
compensation-coinbase[.]com
deposit-coinbase[.]com
finance-coinbase[.]com
firewall-coinbase[.]com
handle-coinbase[.]com
help-lastpass[.]com
indentity-coinbase[.]com
lockdown-coinbase[.]com
lockup-coinbase[.]com
login-nexo[.]com
nexotickets[.]com
officialbackupserver[.]com
original-backend[.]com
protection-kraken[.]com
receipt-coinbase[.]com
refunding-coinbase[.]com
reimburse-coinbase[.]com
reverts-coinbase[.]com
secureunlock-coinbase[.]com
securing-coinbase[.]com
swap-coinbase[.]com
ticketsupport-coinbase[.]com
transfers-kraken[.]com
unlock-kraken[.]com
verify-trezor[.]io
www-cb-wallet[.]com
www-cbwallet[.]com
www-coinbasewallet[.]com
www-help-apple[.]com
www-help-coinbase[.]com
bofa-help[.]com
suite-trezor[.]io
compensate-coinbase[.]com

142784-coinbase[.]com
ss-icloud[.]com07159889-coinbase[.]com
10195-coinbase[.]com
11246-coinbase[.]com
11247-coinbase[.]com
11248-coinbase[.]com
11258-coinbase[.]com
11259-coinbase[.]com
113912-coinbase[.]com
11472-coinbase[.]com
11923-coinbase[.]com
11957-coinbase[.]com
128147-coinbase[.]com
12958-coinbase[.]com
12984-okta[.]com
12985-coinbase[.]com
13130-coinbase[.]com
13247-coinbase[.]com
13247-icloud[.]com
13267-coinbase[.]com
146271510-coinbase[.]com
146282-coinbase[.]com
146284-coinbase[.]com
147260-coinbase[.]com
14765-coinbase[.]com
14817582-coinbase[.]com
14871904-coinbase[.]com
14891902-coinbase[.]com
1492864-coinbase[.]com
158312-coinbase[.]com
158372-coinbase[.]com
158702-coinbase[.]com
16171675-coinbase[.]com
16171832-coinbase[.]com
16178234-coinbase[.]com
16178237-coinbase[.]com
16178434-coinbase[.]com
162178-coinbase[.]com
162478-coinbase[.]com
162782-coinbase[.]com
162812-coinbase[.]com
162814-coinbase[.]com

16442580-coinbase[.]com
16450107-coinbase[.]com
16450207-coinbase[.]com
16458207-coinbase[.]com
16478202-coinbase[.]com
164872942-coinbase[.]com
16590-coinbase[.]com
16594373-coinbase[.]com
16624831-coinbase[.]com
16642124-coinbase[.]com
16642172-coinbase[.]com
16642580-coinbase[.]com
16642721-coinbase[.]com
16642724-coinbase[.]com
16642871-coinbase[.]com
16642872-coinbase[.]com
16712942-coinbase[.]com
16718672-coinbase[.]com
16728342-coinbase[.]com
16728348-coinbase[.]com
16728442-coinbase[.]com
16728472-coinbase[.]com
167285-coinbase[.]com
16729042-coinbase[.]com
16748272-coinbase[.]com
16782942-coinbase[.]com
16827420-coinbase[.]com
16827423-coinbase[.]com
16847145-coinbase[.]com
16893924-coinbase[.]com
17182-coinbase[.]com
17255030-coinbase[.]com
17259-kraken[.]com
172486-coinbase[.]com
17284652-coinbase[.]com
17286-coinbase[.]com
17334522-coinbase[.]com
17334522-kraken[.]com
17384522-coinbase[.]com
173912-coinbase[.]com
17494976-coinbase[.]com
17512854-coinbase[.]com

17512857-coinbase[.]com
1751954-coinbase[.]com
17525030-coinbase[.]com
17529580-coinbase[.]com
17614-coinbase[.]com
17618412-coinbase[.]com
17619-coinbase[.]com
176284-coinbase[.]com
17823920-coinbase[.]com
178253-coinbase[.]com
178294-coinbase[.]com
17912-coinbase[.]com
17914-coinbase[.]com
17917-coinbase[.]com
17954-coinbase[.]com
17958-coinbase[.]com
182043-coinbase[.]com
18275-gemini[.]com
18276-coinbase[.]com
18290185-coinbase[.]com
182967-coinbase[.]com
18560-coinbase[.]com
18571-coinbase[.]com
185912-coinbase[.]com
185914-coinbase[.]com
18592176-coinbase[.]com
18594162-coinbase[.]com
18594962-coinbase[.]com
18597162-coinbase[.]com
18719562-coinbase[.]com
1875290-coinbase[.]com
1882730-coinbase[.]com
18902-coinbase[.]com
18903-coinbase[.]com
189126-coinbase[.]com
18952-coinbase[.]com
192854-coinbase[.]com
192856-coinbase[.]com
19287-binance[.]com
19572-coinbase[.]com
195812-coinbase[.]com
195826-coinbase[.]com

1958262-coinbase[.]com
195827-binance[.]com
1958297-coinbase[.]com
19582970-coinbase[.]com
19582971-coinbase[.]com
19583-coinbase[.]com
19592653-coinbase[.]com
197304-coinbase[.]com
19730492-coinbase[.]com
19764162-coinbase[.]com
19803-coinbase[.]com
201784289-coinbase[.]com
210823644-coinbase[.]com
21158-coinbase[.]com
21509-coinbase[.]com
25985-coinbase[.]com
27699-coinbase[.]com
28367-coinbase[.]com
28676-coinbase[.]com
29185-coinbase[.]com
29195-coinbase[.]com
2a-coinbase[.]com
2b-coinbase[.]com
2c-coinbase[.]com
2f-coinbase[.]com
2fas-coinbase[.]com
2o-coinbase[.]com
2r-coinbase[.]com
2s-coinbase[.]com
2sv-coinbase[.]com
352134951-coinbase[.]com
38468-coinbase[.]com
39590-coinbase[.]com
41260-coinbase[.]com
427883-coinbase[.]com
43017-coinbase[.]com
47562-coinbase[.]com
50195-coinbase[.]com
5247-coinbase[.]com
54765-coinbase[.]com
57197-coinbase[.]com
58176-coinbase[.]com

58297-coinbase[.]com
61250-coinbase[.]com
61835-coinbase[.]com
61851-coinbase[.]com
61937-coinbase[.]com
71925-coinbase[.]com
72957-coinbase[.]com
72985-coinbase[.]com
74651-coinbase[.]com
754668948-coinbase[.]com
76159869-coinbase[.]com
76153-coinbase[.]com
81758-coinbase[.]com
81920-coinbase[.]com
81926-coinbase[.]com
81958-coinbase[.]com
826298-coinbase[.]com
83216-coinbase[.]com
837613-coinbase[.]com
83956-coinbase[.]com
87157-coinbase[.]com
87312-coinbase[.]com
89304-coinbase[.]com
89375-coinbase[.]com
91723-gemini[.]com
91752-coinbase[.]com
91756-coinbase[.]com
91782-coinbase[.]com
91835-coinbase[.]com
91845-coinbase[.]com
91923-coinbase[.]com
92758-coinbase[.]com
948122061-coinbase[.]com
978941-coinbase[.]com
accountrecovery-coinbase[.]com
action-shakepay[.]com
adjust-coinbase[.]com
admin-kraken[.]com
applechargebacks[.]com
authenticate-gemini[.]com
authorize-gmail[.]com
binance-okta[.]com

captcha-coinbase[.]com
cd-coinbase[.]com
coinbase-heip[.]com
coinbase-live[.]support
coinbase-reject[.]com
coinbase-ticket[.]com
coinbaseheip[.]com
com-2fa[.]help
com-2fa[.]support
com-3845[.]support
com-connect[.]help
com-fraud[.]support
com-help[.]support
com-reset[.]help
com-reset[.]net
com-ticket[.]live
com-ticket[.]support
contact-nexo[.]com
convert-coinbase[.]com
customerservice-coinbase[.]com
default-coinbase[.]com
defend-coinbase[.]com
deny-coinbase[.]com
disconnect-coinbase[.]com
escalate-coinbase[.]com
establish-coinbase[.]com
fcc-okta[.]com
fraudulent-coinbase[.]com
guard-apple[.]com
guard-icloud[.]com
guardian-coinbase[.]com
guide-gemini[.]com
help-bitfinex[.]com
help-shakepay[.]com
helpdesk-apple[.]com
helpdesk-gemini[.]com
helpdesk-icloud[.]com
identification-coinbase[.]com
lockdown-coinbase[.]com
login-nexo[.]com
keys-coinbase[.]com
messages-coinbase[.]com

newpassword-coinbase[.]com
prompt-coinbase[.]com
protect-apple[.]com
protect-coinbase[.]com
protect-gmail[.]com
protect-kraken[.]com
recoverme-coinbase[.]com
recoveryportal-coinbase[.]com
refunds-coinbase[.]com
reset-okta[.]com
restore-coinbase[.]com
return-coinbase[.]com
reverts-coinbase[.]com
secure-binance[.]us
secure-icloud[.]com
secure-nexo[.]com
secure-shakepay[.]com
security-umusic[.]com
server694590423[.]tech
session-coinbase[.]com
startrecovery-coinbase[.]com
signin-kraken[.]com
suite-trezor[.]io
supportportal-coinbase[.]com
tech-icloud[.]com
threat-coinbase[.]com
ticket-apple[.]com
ticket-coinbase[.]com
tickets-apple[.]com
tokens-coinbase[.]com
unblock-coinbase[.]com
unlink-coinbase[.]com
your-coinbase[.]com
welcome-coinbase[.]com
www-coinbasewallet[.]com
www-help-coinbase[.]com
www-help-gemini[.]com
