

REVERSING ANTI-REVERSE PROXY: DROPBOX



► The reCAPTCHA challenge

The screenshot shows a web browser window for the Dropbox sign-in page (<https://www.dropbox.com>). The page has a dark red background on the left side containing promotional text:

Put your creative energy to work with Dropbox

Dropbox is a modern workspace designed to reduce busywork – so you can focus on the things that matter.

The right side of the page is the sign-in form:

Sign in or [create an account](#)

Email

Password

This page is protected by reCAPTCHA and is subject to the [Google Privacy Policy](#) and [Terms of Service](#).

Remember me

[Sign in](#)

[Sign in with Google](#)

[Forgotten your password?](#)

A red rectangular box highlights the reCAPTCHA notice at the bottom of the sign-in form.

REVERSING ANTI-REVERSE PROXY: DROPBOX



► The reCAPTCHA challenge

The screenshot shows a browser window with two tabs: "Dropbox" and "Dropbox". The main content is a phishing page for "Dropbox" with a maroon background. The heading reads: "Put your creative energy to work with Dropbox". On the right side, there are fields for "Email" and "Password". Below them is a message: "This page is protected by reCAPTCHA and is subject to the Google Privacy Policy and Terms of Service." Underneath is an error message: "ERROR for site owner: Invalid domain for site key" from "reCAPTCHA". The "Privacy - Terms" link is also visible.

The developer tools (Elements tab) are open at the bottom, showing the following JavaScript code snippet:

```
> <head></head>
<body>
  <script type="text/javascript" nonce="zPF3NdXifa0Zm5Mp0Jj4Fw">
    recaptcha.anchor.ErrorMain.init("[\x22ainput\x22,null,null,null,null,[1,1,1]\n,\x22Invalid domain for site\nkey\x22,6,null,null,[\x22https://drb-17.phishing.anti/intl/en-GB/policies/privacy\x22,\x22https://drb-17.phishing.anti/intl/en-GB/policies/terms\x22]\n\n");
    == $0
  </script>
  <div class="rc-anchor rc-anchor-normal rc-anchor-light">
    <div id="recaptcha-accessible-status" class="rc-anchor-aria-status" aria-hidden="true">Invalid domain for site key. </div>
    <div class="rc-anchor-error-msg-container" style="display:none"></div>
    <div class="rc-anchor-content">
      <div class="rc-inline-block">
        <div class="rc-anchor-center-container">
          <div class="rc-anchor-center-item rc-anchor-error-message"></div>
        </div>
      </div>
    <div class="rc-anchor-normal-footer"></div>
  </div>
</body>
```

The browser's address bar shows the URL: <https://www.phishing.anti/#>.

REVERSING ANTI-REVERSE PROXY: DROPBOX



► The reCAPTCHA challenge

The screenshot shows a browser window with three tabs, all titled "Dropbox". The middle tab is active and displays a phishing page at <https://www.phishing.anti/#>. The page content includes a cookie consent message: "We use cookies so that Dropbox works for you. By using our website, you agree to our use of cookies. [Learn more](#)". Below this is the Dropbox logo and navigation links for "For teams" and "For individuals". On the right, there are "Sign in" and "Download" buttons. The browser's address bar also shows the URL <https://www.phishing.anti/#>.

Below the browser window, the developer tools Network tab is open, showing network traffic for the URL </recaptcha>. The "General" section of the Network tab details the request:

- Request URL:** <https://drb-17.phishing.anti/recaptcha/api2/anchor?ar=1&k=6LdnLyIUAAAA0iGPtdhh-g3KijRoDGGPD-6dqXo&co=aHR0cHM6Ly93d3cucGhpc2hpbmcuYw50aTo0NDM.&hl=en-GB&v=v1555968629716&size=invisible&cb=aq13mkssrpdt>
- Request Method:** GET
- Status Code:** 200 OK
- Remote Address:** 127.0.0.1:31337
- Referrer Policy:** origin-when-cross-origin

The "Response Headers" section shows:

- Alt-Svc: `quic=":443"; ma=2592000; v="46,44,43,39"`
- Cache-Control: private, max-age=0
- Connection: close

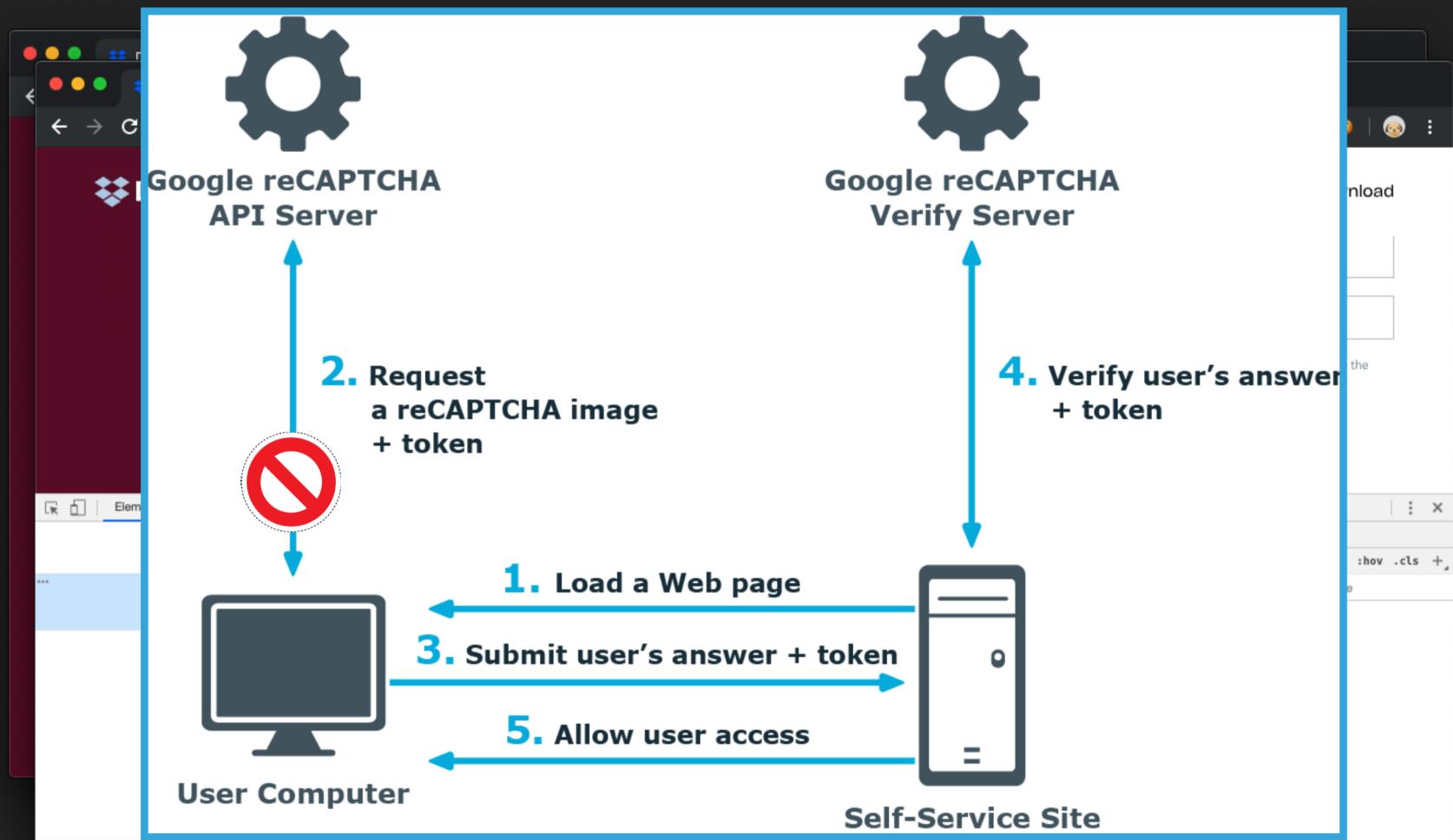
The bottom of the developer tools shows the console output:

```
atob('aHR0cHM6Ly93d3cucGhpc2hpbmcuYw50aTo0NDM')
"https://www.phishing.anti:443"
>
```

REVERSING ANTI-REVERSE PROXY: DROPBOX



► The reCAPTCHA challenge



REVERSING ANTI-REVERSE PROXY: DROPBOX



- ▶ The reCAPTCHA challenge
- ▶ The fix: base64 transformation support:

```
"transform": {  
    "base64": {  
        "enabled": true,  
        "padding": [  
            "=",  
            ".."  
        ]  
    },
```

WHERE TO FIND THE CODE



<https://github.com/muraenateam>