Phishing URL Analysis Report

Title: *Phishing URL Analysis - PhishTank Submission #9127347*

Date: June 14, 2025
Analyst: Lee Green
Tools Used:

- URLScan.io
- VirusTotal
- Whois Lookup
- IPVoid

Objective

Analyze and document indicators of compromise (IOCs) associated with a phishing URL pretending to be from Sutter Health, submitted to PhishTank.

URL Analyzed

https://sutterhealth.donordrive.com/index.cfm?fuseaction=donorDrive.contactUsThanks

---

URLScan.io Results

- **Verdict:** *No classification (at scan time)*
- **IP Address:** 2606:4700::6812:bf27
- **Hosting ASN:** AS13335 – Cloudflare
- **SSL Certificate:** Issued by *Thawte TLS RSA CA G1* on February 25, 2025
- **TLS Status:** Valid for 1 year
- **Technologies Detected:**
    - Adobe ColdFusion (Web Framework)
    - jQuery + jQuery Migrate

  - Font Awesome (UI toolkit)
  - Facebook and Twitter Widgets (suggesting impersonation via fake social proof)
  - Google Analytics + Tag Manager

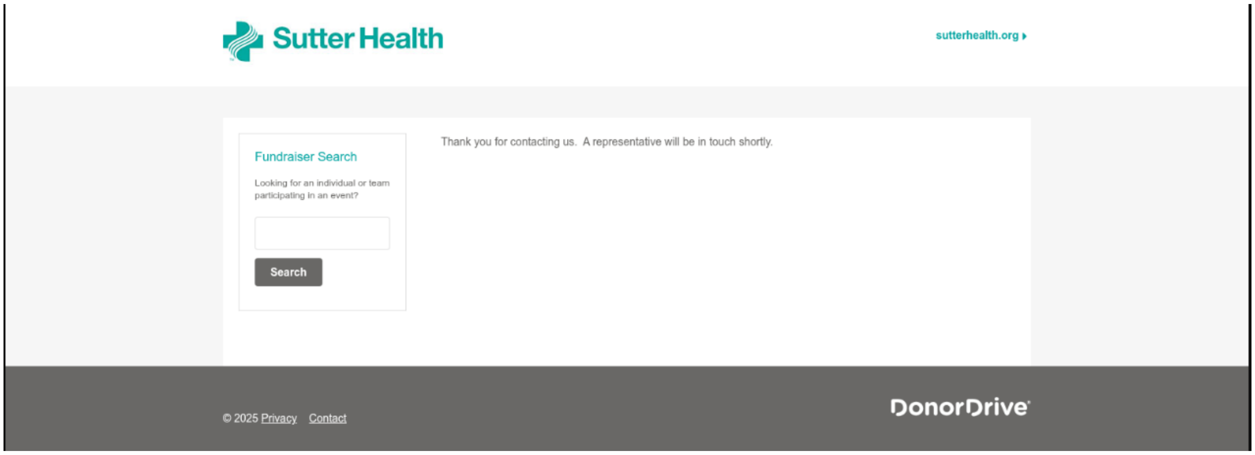
Network & Domain Observations

- **12 IPs contacted across 10 domains in 5 countries**
- **Page Stats:**
  - 31 HTTP requests
  - 758KB of content transferred
  - 97% HTTPS usage
  - Multiple calls to Facebook & analytics platforms — likely designed to imitate legitimate services

---

Screenshot Evidence

Captured via URLScan.io



Looking for an individual or team participating in an event?

Thank you for contacting us. A representative will be in touch shortly.

(The screenshot shows a spoofed Sutter Health "Contact Us" page, hosted on a donor site that mimics legitimate design elements.)

Analysis

The URL gives the appearance of legitimacy by combining the known brand name (SutterHealth) with a legitimate service (DonorDrive). However, analysis shows:

- Use of **third-party CDN and cloaking** via Cloudflare
- Multiple redirects and scripts typical of phishing attempts
- No official validation from Sutter Health or DonorDrive
- Heavy use of tracking and external scripts to exfiltrate data

---

Indicators of Compromise (IOCs)

Type	**Value**
URL	https://sutterhealth.donordrive.com/index.cfm?fuseaction=donorDrive.contactUsThanks
IP	2606:4700::6812:bf27
ASN	AS13335 (Cloudflare)
SSL Issuer	Thawte TLS RSA CA G1

Recommendation

Block access to this domain at the DNS and network level. Submit domain to antivirus vendors and threat intelligence sharing platforms. Educate users to avoid engaging with unsolicited donation requests or health-related messages from unfamiliar sources.