

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Seizure of
(Briefly describe the property to be seized)
The Domain TSOI-ZHIV.COM as further described
in Attachment A-1

Case No. 3:25-MJ-485-BK

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Eastern District of Virginia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

The Domain TSOI-ZHIV.COM as further described in Attachment A-1.

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property and that an order under 21 U.S.C. § 853(e) is not sufficient to assure the availability of the property for forfeiture.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 05/29/2025

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to

United States Magistrate Judge Renée Harris Toliver

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

5/16/2025 at 1:22pm [Signature]
Judge's signature

City and state: Dallas, Texas

United States Magistrate Judge Renée Harris Toliver

Printed name and title

Return

Case No.:

3:25-MJ-

485-BK

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A-1

With respect to “tsoi-zhiv.com” (“SUBJECT DOMAIN NAME 1”), VeriSign, who is the domain registry for SUBJECT DOMAIN NAME 1, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAME 1:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the FBI, by associating the SUBJECT DOMAIN NAME to the following authoritative name-server(s):
 - a. hans.ns.cloudflare.com;
 - b. surina.ns.cloudflare.com; and/or
 - c. Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to VeriSign.
2. Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAME 1 pending transfer of all right, title, and interest in SUBJECT DOMAIN NAME 1 to the United States upon completion of forfeiture proceedings, to ensure that changes to SUBJECT DOMAIN NAME 1 cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

Some time after SUBJECT DOMAIN NAME 1 is associated with the authoritative name-server(s), but no later than May 21, 2025, the Government may display a notice on the website to which SUBJECT DOMAIN NAME 1 will resolve. That notice may consist of law enforcement emblems and the following text (or substantially similar text):

“This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued by the United States District Court for the Northern District of Texas as part of a law enforcement action against the LummaC2 malware service, its administrators, and its subscribers.

This action has been taken in coordination with the National Security Division of the Department of Justice.

The FBI also acknowledges that private sector actors seized other domains in a separate and independent operation pursuant to civil injunctive relief granted by another federal court.

Information about LummaC2, their affiliates, or activity can be submitted through the following Tor-based tip line:
he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion.”