In Obscura
Vincent M. Nasti, Founder, Chief Executive Officer, Consultant
In Obscura, LLC | Threat Intelligence | Security Countermeasures | Investigations
https://inobscura.org/

INTELLIGENCE THREAT WARNING
(TLP-C) HIDDEN RESIDENTIAL SURVEILLANCE CAMERAS, SAN GABRIEL VALLEY, LOS ANGELES, 18 MAY 2026

KNOW THE TARGET – WATCH THE TARGET – LOOK DEEPER -EXPECT THE UNEXPECTED

IN OBSCURA THEAT LEVEL – IMMINENT

CAVEAT: THIS INTELLIGENCE PRODUCT RELIES ON OPEN-SOURCE MEDIA OR GOVERNMENT RELEASED UNCLASIFIED INFORMATION. RECOMMENDED ACTIONS ARE INCLUDED FOR CLIENTS FOR INFORMATION AND ACTIONS DEEMED APPROPRIATE.

EXECUTIVE SUMMARY

This intelligence warning is amongst several prior In Obscura reporting on corroborated insurgent surveillance and intelligence collection of churches. It is with medium confidence that the following criminal operational tradecraft described here probably has already been used against churches in fixed, stationary positions, undetected.

Importantly because church security teams rarely communicate and share information, and various levels of law enforcement are apprehensive about sharing, the threat is exacerbated. This is because of a lack of liaison, sharing, and training, a sense of urgency and lack of tenacity.

CONTEXT

The Los Angeles area suburban neighborhoods have for years been targeted by “South American Burglary Crews.” These are stationery installed devices, battery powered and remotely controlled. This is for continual surveillance of the target from as many positions and cameras as the crew deems necessary. In Obscura assesses with high confidence, it

is only a matter of imagination and time, if not already operational, this tradecraft will be replicated by insurgents targeting the church[1].

BACKGROUND

Bolded Text is for church emphasis and intelligence value.

Local thieves partly responsible for an increase in the number of home break-ins around Los Angeles have adopted high-tech tactics police first observed being used by so-called tourist burglars **to disable security systems and remotely surveil target homes.**

"They're replicating the tactics and MO of the South American burglary crews, using **jammers, and more sophisticated pre-incident surveillance,"** LAPD Chief Jim McDonnell said Tuesday, describing the modus operandi of some LA-based burglary crews **arrested during recent investigations**.

"They may have cameras laid out on the property or on a car parked on the street across from the target house for a period of time, to be **able to determine a pattern of life, to determine when a person is going to be home, when they're going to be gone,"** he said. Police said they **recently discovered some of the stake-out cars, including Teslas, that have built-in cameras that can be remotely monitored, and other types of cars, with small cameras aimed towards streets and homes of interest.**

This includes cameras connected to a portable hotspot and external battery pack, cellphone connected to a power bank and wrapped in green camouflage tape, with artificial plants attached[2].

---

[1] LA burglars adopting new techniques to select homes, avoid capture In addition to jamming WiFi and cutting data lines, some thieves are leaving parked cars with cameras to remotely stake-out potential targets By Eric Leonard • Published July 29, 2025 • Updated on July 29, 2025 at 7:06 pm https://www.nbclosangeles.com/investigations/la-burglars-adopting-new-techniques-to-select-homes-avoid-capture/3755898/

[2] Hidden cameras found tucked in bushes in San Dimas neighborhood, authorities say KABC TV, Friday, May 15, 2026, 7:49PM https://abc7.com/post/hidden-cameras-found-tucked-bushes-san-dimas-neighborhood-authorities-say/19108827/

Those and other techniques, such as the **severing phone and data utility lines**, have been seen by detectives investigating some of the recent residential burglaries in Encino and the west San Fernando Valley[3]. The reports are also being made from the LA County areas outside the city limits.

INDICATIONS AND WARNING

As assessed in this intelligence warning, two concerning elements appear: the foreign nexus and the technology tradecraft. In Obscura reporting has emphasized, repeatedly the targeting tradecraft of churches and their nexus to the insurgent operations escalating inside the U.S., which empowers and enables various attack scenarios targeting churches. This includes the surveillance of security systems, and the security staff operations. These might involve testing these systems by insurgents as part of intelligence collection. These will decide the ability to neutralize the security and detection systems, by testing them. Known as tests of security. Among them might be bomb threats, unattended items, suspicious mail pieces, swatting calls. Disabling (jam) security duress alarms, church surveillance cameras during attack operations all come to mind.

RECOMMENDED ACTIONS

It is reported that most of these residents never detected these devices, landscapers and utility workers happened upon them. Neighbors do not seem to have reported suspicious activities prior to these discoveries, as their emplacement require time and cover for action of the suspects, which are undisclosed.

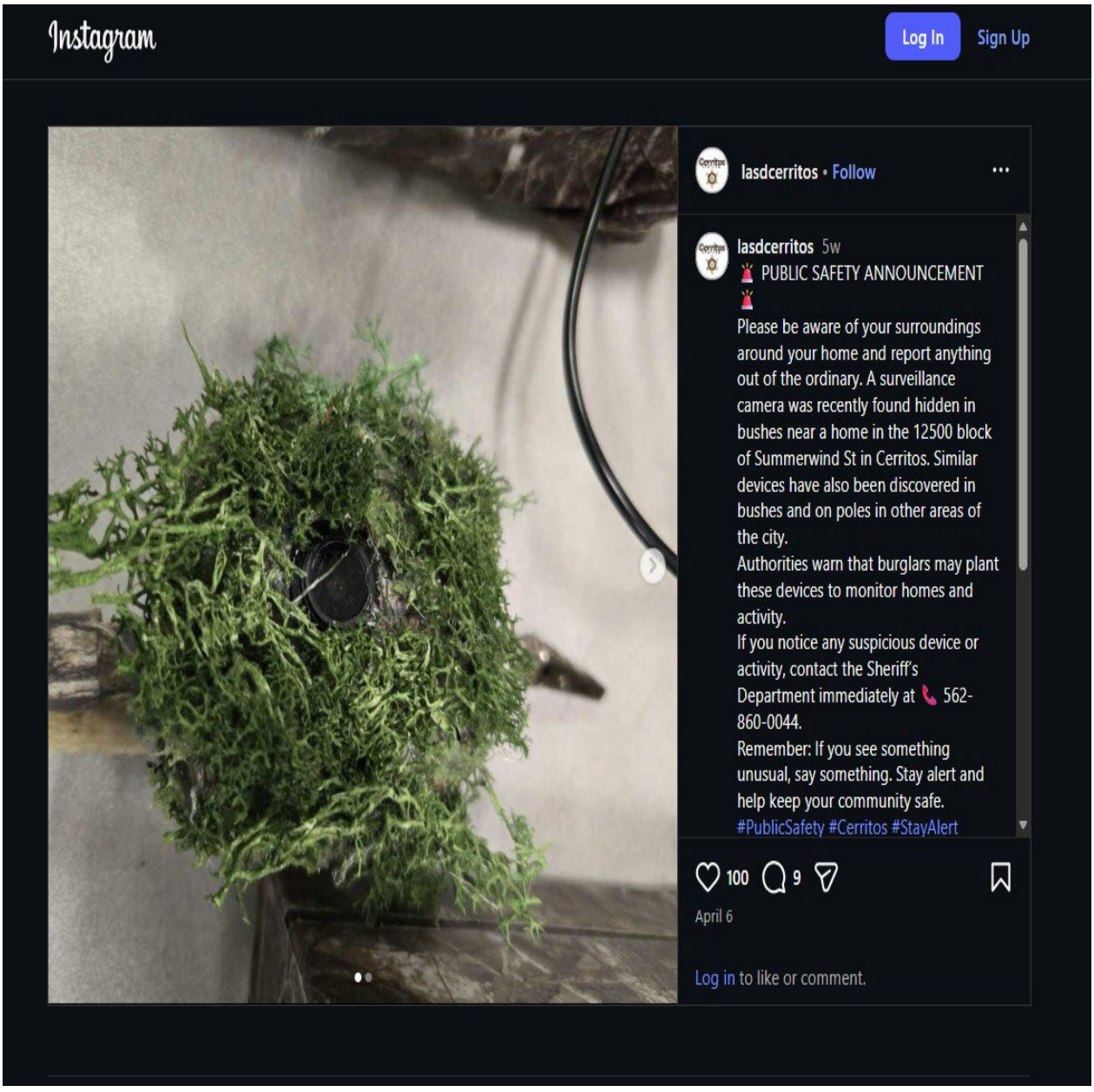
The ability to use the depicted technology in this report to conduct undetected systematic intelligence collection to identify a range of church personalities, their vehicles, and security team routines and habits are left to the mind of the insurgent. Security teams must be as adept and imaginative as regards the potential attack scenarios and how to defend against them. Appropriately, checks for suspicious items, possible IED are mandatory as well as parked, unoccupied and unfamiliar vehicles or people. These are

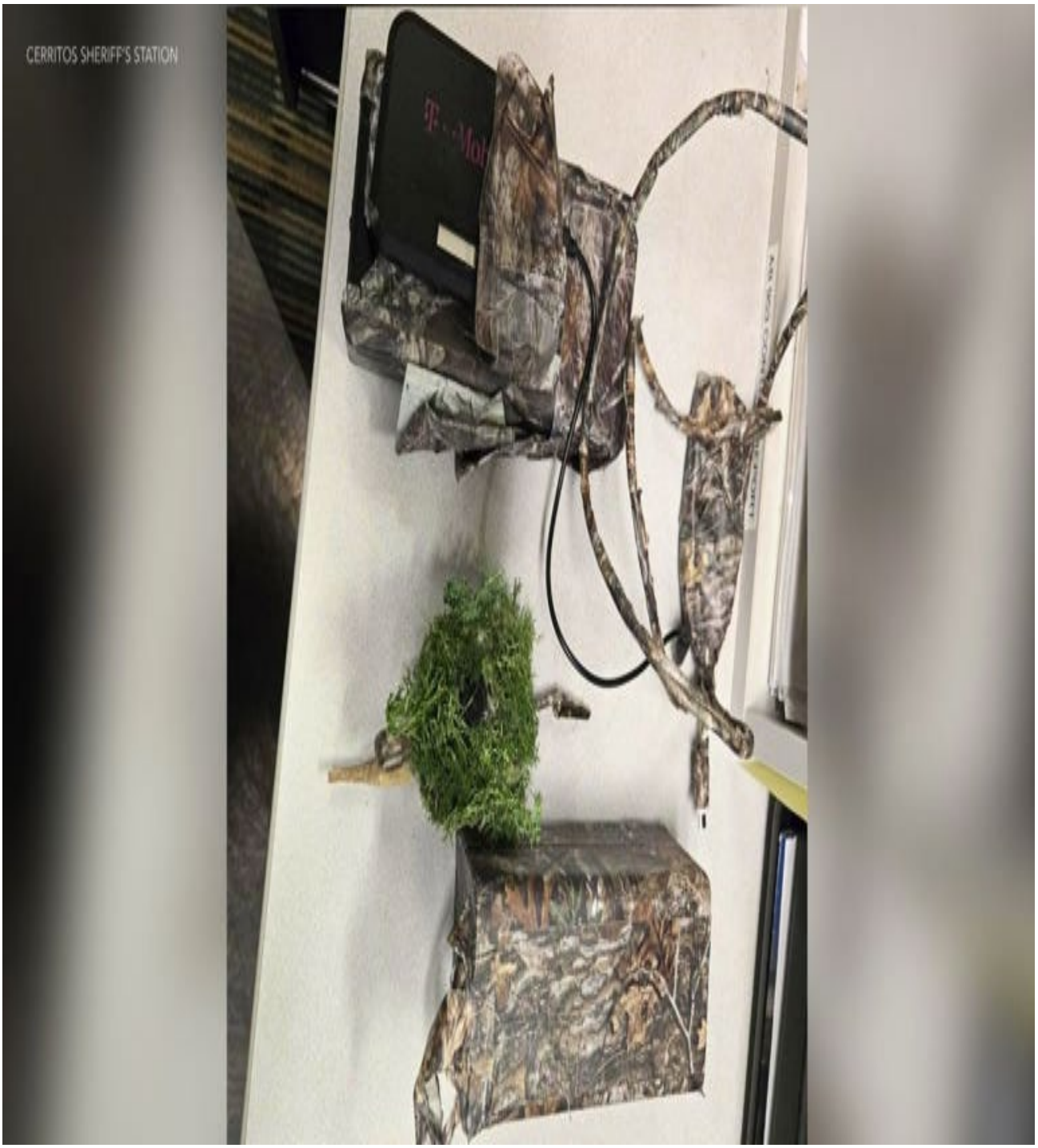
[3] LA burglars adopting new techniques to select homes, avoid capture, in addition to jamming WiFi and cutting data lines, some thieves are leaving parked cars with cameras to remotely stake-out potential targets, By Eric Leonard • Published July 29, 2025, • Updated on July 29, 2025, at 7:06 pm https://www.nbclosangeles.com/investigations/la-burglars-adopting-new-techniques-to-select-homes-avoid-capture/3755898/

among numerous church activities which security learn the normal routine and then be able to detect anomalies and then expand to investigate.

IMAGERY

From various local media outlets





LOS ANGELES COUNTY SHERIFF'S DEPARTMENT

SPECIAL BULLETIN

SHERIFF ROBERT G. LUNA

SITUATIONAL AWARENESS

BE ON THE LOOKOUT FOR HIDDEN CAMERAS

On Tuesday, May 12, 2026, deputies from San Dimas Sheriff's Station responded to a residential burglary call in the 800 block of Via Gregorio in San Dimas. During the preliminary investigation, deputies discovered a concealed surveillance device hidden inside bushes across from the victim's residence (see Photos 1). The device consisted of a hidden camera connected to a portable hotspot and an external battery pack.

Approximately one week earlier, a landscaper working in the same neighborhood located another suspicious device concealed in hedges while trimming vegetation. That device consisted of a cellular phone connected to a power bank and wrapped in green camouflage tape with artificial plants attached to it (see Photo 2).

These hidden cameras are typically placed in or around bushes, planters, trees, or flower beds and are often camouflaged to blend into the surrounding landscaping. Suspects may use these devices to observe when residents leave their homes, identify valuables, or determine the best time to commit burglaries.

Here are some steps you can take to protect your home:

- Inspect your property regularly and stay alert for suspicious activity
- Keep trees and bushes trimmed to reduce hiding spots for cameras or suspects
- Use and regularly monitor home security cameras
- Keep outdoor areas well-lit at night
- If you find a suspicious camera or device, contact law enforcement immediately
- Do not touch or move the device; wait for police to collect it

IF YOU ARE A VICTIM OF THIS CRIME, PLEASE CONTACT:

San Dimas Sheriff's Station at (909) 450-2700

If you prefer to provide information anonymously, you may call "Crime Stoppers" by dialing (800) 222-TIPS (8477), use your smartphone by downloading the "P3Tips" Mobile APP on Google play or the Apple App Store or by using the website http://lacrimestoppers.org

Wednesday, May 13, 2026

Created by FCCB/CAU/SDM

///END///

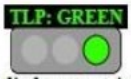
==========

IN OBSCURA HAS ADOPTED THE OSINT CLASSIFICATION SYSTEM OF DEPARTMENT OF HOMELAND SECURITY CLASSIFICATIONS 'TRAFFIC LIGHT PROTOCOL' RELEASE CAVEATS. THESE REGULATE IN OBSCURA REQUIREMENTS FOR PUBLIC RELEASE TO PROTECT CLIENTS AND IN OBSCURA SOURCES, METHODS, AND TECHNQIUES. IN OBSCURA RELEASE PROHIBITION MARKINGS ALSO APPLY. NONE ARE RELEASABLE TO NEWS MEDIA OR JOURNALISTS WITHOUT WRITTEN REQUEST AND PERMISSION.

==========

REQUEST WRITTEN PERMISSION, EMAIL, PRIOR TO DISSEMINATING ANY IN-OBSCURA PRODUCTS OR INFORMATION. TRAFFIC LIGHT PROTOCOL REQUIREMENTS FOR DISSEMINATION FOLLOW...

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 For the eyes and ears of individual recipients only, no further disclosure.	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
 Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP:AMBER+STRICT.
 Limited disclosure, recipients can spread this within their community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
 Recipients can spread this to the world, there is no limit on disclosure.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.