



| Flash |

Threat Actors Seeking to Exploit California Wildfires Recovery Funds

F-2025-01-24a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Fraud, Deep and Dark Web, Threat
Actor

January 24, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on January 24, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Actors Seeking to Exploit California Wildfire Recovery Funds

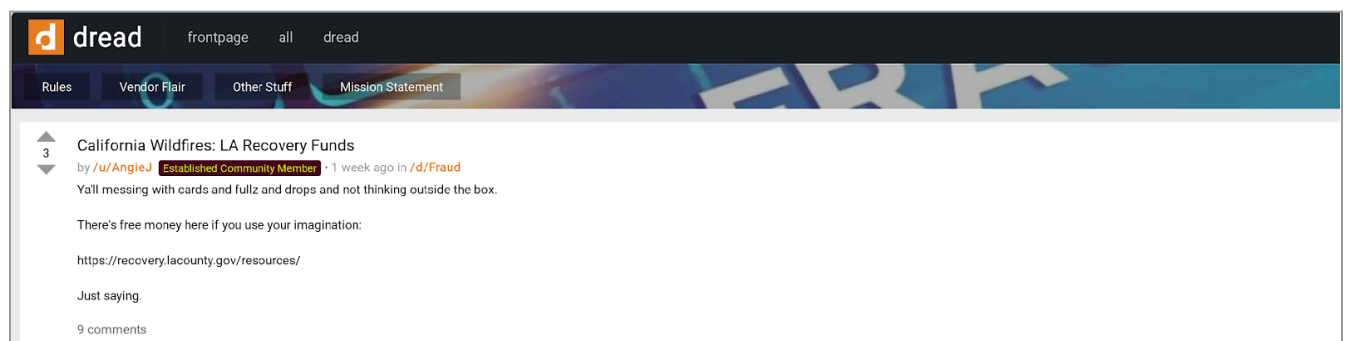
| Key Findings

- ZeroFox has identified threat actors actively discussing methodologies to exploit California wildfire recovery funds for financial gain on the dark web.
- In a thread identified on the Dread forum, threat actors discussed methodologies for successful scams, stating that this is “free money”, as well as the importance of exercising patience to avoid early scrutiny during the verification process.
- Based on previous behavior and attitudes towards disaster relief funds, it is very likely that a broader array of threat actors are interested in exploiting these funds than those identified to date.
- Although ZeroFox has identified no evidence that threat actors are actively—and successfully—leveraging wildfire recovery funds in financial scams, such activity could result in financial and reputational damage for state or local government authorities and reduce the availability of relief funds for those legitimately affected by the wildfires, as well as perpetuate the idea that these funds are a viable attack vector.

Details

On January 15, 2024, an untested threat actor known as “AngieJ” initiated a topical discussion regarding the exploitation of California wildfire recovery funds on the dark web forum Dread. The actor suggested that these funds could be leveraged to fraudulently illicit payouts from government authorities. AngieJ drew attention to the website `hXXps://recovery.lacounty[.]gov/resources/`, highlighting it as a potential focus for exploitation. It is very likely that some financially motivated actors perceive these funds as having inadequate verification processes, making them fertile ground for financial gain and posing very little risk to the scammers applying.

- Following the outbreak of the January 2025 wildfires across California, authorities have made Federal Emergency Management Agency (FEMA) assistance funds available for residents impacted by wildfires in Los Angeles (LA) County.
- In the thread, AngieJ criticized other members of the Dread forum for relying on outdated fraud methods, such as using financial mules and stolen payment cards.
- The post almost certainly indicates ongoing threat actor interest in exploiting these funds via financially motivated scams. Based on previous behavior and attitudes towards disaster relief funds, it is very likely that a broader array of threat actors are interested in exploiting these funds than those identified to date.



AngieJ’s original post on Dread, where actors mention LA County’s wildfire recovery program as a potential target for fraud

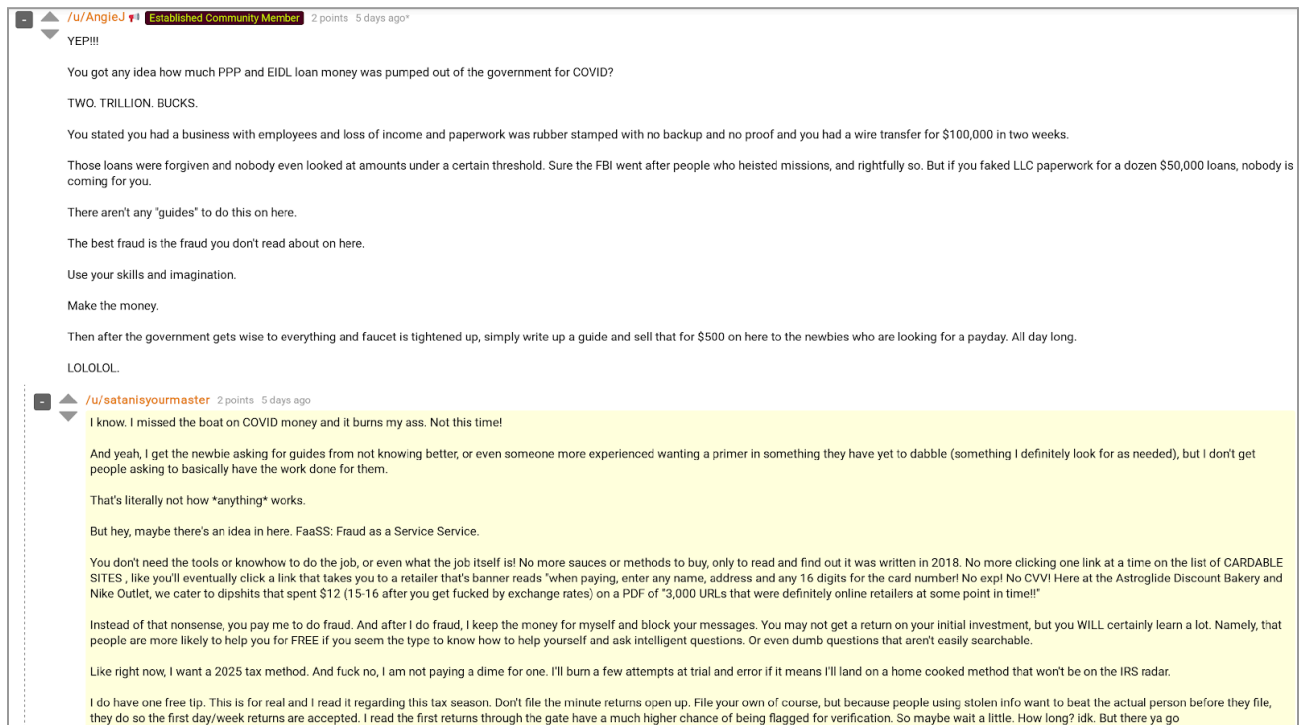
Source: Dread

AngieJ alluded to scams conducted during the COVID-19 pandemic as a blueprint for exploiting wildfire recovery funds. The actor elaborated on their initial post, stating that trillions of dollars in loans had been obtained from the U.S. government during the

COVID-19 pandemic, specifically through the Paycheck Protection Program and Economic Injury Disaster Loans. The actor implied that some of these loans were obtained fraudulently and that similar scams could possibly be leveraged again, with potentially low risk to the threat actor.

- According to AngieJ, individuals who forged limited liability company (LLC) paperwork to secure USD 50,000 loans were often not pursued by authorities if they disappeared after receiving the funds, barring a few exceptions.

An untested actor known as "satanisyourmaster" replied to AngieJ with a lengthy post that garnered significant attention, the most relevant part of which addresses fraud related to LA wildfire recovery funds. The actor remarked, "I read the first returns through the gate have a much higher chance of being flagged for verification. So maybe wait a little. How long? Idk. But there ya go." This highlights a strategic approach for improving the success rate of applications for relief funds related to the LA wildfires, emphasizing threat actor patience to avoid early scrutiny during the verification process.



/u/AngieJ  **Established Community Member** 2 points 5 days ago*

YEP!!!

You got any idea how much PPP and EIDL loan money was pumped out of the government for COVID?

TWO. TRILLION. BUCKS.

You stated you had a business with employees and loss of income and paperwork was rubber stamped with no backup and no proof and you had a wire transfer for \$100,000 in two weeks.

Those loans were forgiven and nobody even looked at amounts under a certain threshold. Sure the FBI went after people who heisted missions, and rightfully so. But if you faked LLC paperwork for a dozen \$50,000 loans, nobody is coming for you.

There aren't any "guides" to do this on here.

The best fraud is the fraud you don't read about on here.

Use your skills and imagination.

Make the money.

Then after the government gets wise to everything and faucet is tightened up, simply write up a guide and sell that for \$500 on here to the newbies who are looking for a payday. All day long.

LOLOLOL.

/u/satanisyourmaster 2 points 5 days ago

I know. I missed the boat on COVID money and it burns my ass. Not this time!

And yeah, I get the newbie asking for guides from not knowing better, or even someone more experienced wanting a primer in something they have yet to dabble (something I definitely look for as needed), but I don't get people asking to basically have the work done for them.

That's literally not how *anything* works.

But hey, maybe there's an idea in here. FaaS: Fraud as a Service Service.

You don't need the tools or knowhow to do the job, or even what the job itself is! No more sauces or methods to buy, only to read and find out it was written in 2018. No more clicking one link at a time on the list of CARDABLE SITES, like you'll eventually click a link that takes you to a retailer that's banner reads "when paying, enter any name, address and any 16 digits for the card number! No exp! No CVV! Here at the Astroglide Discount Bakery and Nike Outlet, we cater to dipshits that spent \$12 (15-16 after you get fucked by exchange rates) on a PDF of "3,000 URLs that were definitely online retailers at some point in time!"

Instead of that nonsense, you pay me to do fraud. And after I do fraud, I keep the money for myself and block your messages. You may not get a return on your initial investment, but you WILL certainly learn a lot. Namely, that people are more likely to help you for FREE if you seem the type to know how to help yourself and ask intelligent questions. Or even dumb questions that aren't easily searchable.

Like right now, I want a 2025 tax method. And fuck no, I am not paying a dime for one. I'll burn a few attempts at trial and error if it means I'll land on a home cooked method that won't be on the IRS radar.

I do have one free tip. This is for real and I read it regarding this tax season. Don't file the minute returns open up. File your own of course, but because people using stolen info want to beat the actual person before they file, they do so the first day/week returns are accepted. I read the first returns through the gate have a much higher chance of being flagged for verification. So maybe wait a little. How long? idk. But there ya go

Relevant comments in the chatter for LA wildfire recovery funds fraud

Source: Dread

Flash Threat Actors Seeking to Exploit California Wildfire Recovery Funds

F-2025-01-24a

TLP:CLEAR



Although ZeroFox has identified no evidence that threat actors are actively—and successfully—leveraging wildfire recovery funds in financial scams, the thread indicates threat actor interest in exploiting such relief funds for this purpose. If such scams are successful, not only could it result in financial and reputational damage for state or local government authorities, it would also very likely reduce the availability of relief funds for those legitimately affected by the wildfires—as well as perpetuate the idea that these kinds of schemes are a viable attack vector for bad actors..

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY 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 that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%