

# SUSPECT IDENTIFICATION

A USE CASE ON GATHERING EVIDENCE FROM THE DARK WEB

## INTRODUCTION

Criminal activity increasingly crosses into the dark web, which means law enforcement need to be able to follow leads and conduct investigations seamlessly between the physical and digital worlds.

Officers have the difficult task of having to identify suspects based in an area of the internet that is used for its anonymity, where almost everyone operates under an alias. They also have the added complication of making sure that the digital evidence that they collect will stand up in a court of law.

How can investigators pull a criminal out of the dark web and into the light? They can start by working the actor's operational security (OPSEC).

OPSEC describes the process of identifying and obscuring information that could be gathered and exploited by an adversary. Originally a military term, today OPSEC is commonly used by the cybersecurity community, who are trying to stop organizations and individuals from inadvertently revealing critical or sensitive data to a cybercriminal.<sup>1</sup>



## HOW CAN INVESTIGATORS PULL A CRIMINAL OUT OF THE DARK WEB?

However, in this report we are going to turn the term on its head and think about the OPSEC of criminals operating online, as they try to hide information that could lead them to being personally identified when conducting their criminal operations.

From this point of view, the objective of law enforcement teams conducting dark web investigations is to unravel the OPSEC of cybercriminals; to identify the clues on the dark web that make it possible to track and identify suspects.

To illustrate how this can be done, this report looks at the case of USA vs Adams et al - a real criminal investigation that has led to a successful indictment in the US. We have recreated the investigation process with our dark web investigation tool Cerberus to show how you can undermine suspects' efforts to frustrate your tracking, and gather evidence from the dark web that helps you bring criminals to justice.

<sup>1</sup> <https://www.fortinet.com/resources/cyberglossary/operational-security>

## USE CASE: SUSPECT IDENTIFICATION

Criminals use the dark web because of the perceived anonymity it offers. The Onion Router (Tor), the most popular dark web network, encrypts traffic before redirecting it around nodes across the world. This makes it difficult to determine who a user on the dark web is, and what they are doing.

However, users do have to create profiles to use dark web services, such as marketplaces and forums discussing and selling illicit goods. This is where the OPSEC of criminals is sometimes flawed, providing law enforcement with an opportunity to identify users, track their activity, and ultimately bring them to justice for their crimes. Suspect identification describes the process of linking profiles, aliases, and usernames on the dark web to build a case that identifies an individual, and ties them to their crimes.

### THE CASE: USA VS ADAMS ET AL

In May 2022, Holly Adams and Devlin Hosner were charged by a Sacramento jury with conspiracy to distribute fentanyl and methamphetamine, possession with intent to distribute fentanyl and methamphetamine, and conspiracy to launder money.

This conviction followed an investigation by the Northern California Illicit Digital Economy (NCIDE) Task Force, which included Homeland Security Investigations, the FBI, the U.S. Postal Inspection Service, the U.S. Postal Service Office of Inspector General, and the Internal Revenue Service - Criminal Investigation.

In the course of the investigation it was found that Adams and Hosner had sold tens of thousands of counterfeit oxycodone pills containing fentanyl on dark web marketplaces.



Operating under the aliases “Iggorraawwr” and “its4real” they received the equivalent of more than \$800,000 in cryptocurrency payments, while shipping the fentanyl pills to buyers throughout the United States.

Their successful indictment was the result of many hours of law enforcement investigation, identifying not only the aliases by which these individuals operated on the dark web, but also the markets they sold on and the information they shared. This information was used alongside additional evidence compiled through investigatory and field activities in order to bring these individuals to justice.

### REPLICATING THE INVESTIGATION WITH CERBERUS

This report uses the information on the case that is in the public domain to demonstrate the capabilities of Cerberus, our dark web investigation tool, for identifying suspects based on gaps in the dark web OPSEC.

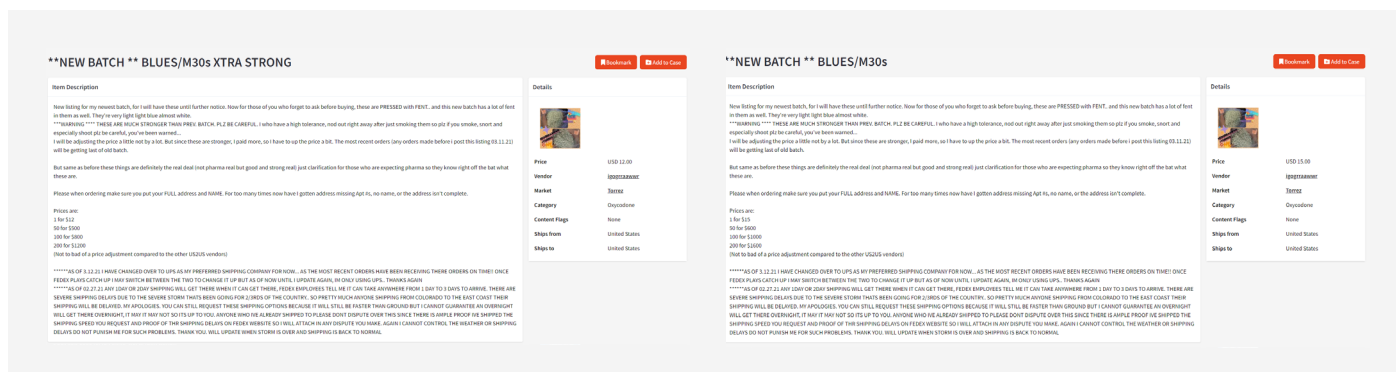
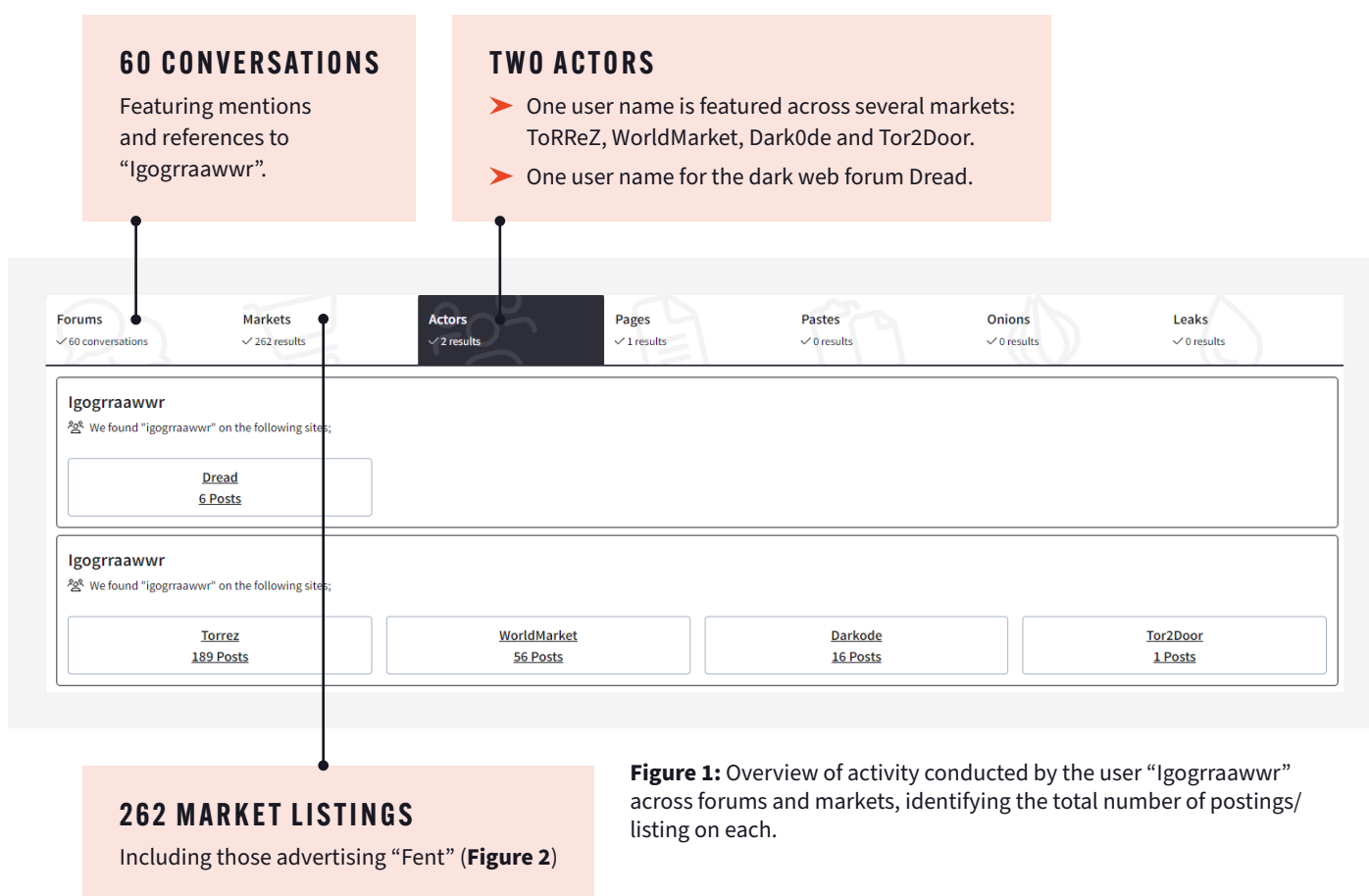
Cerberus was built with national law enforcement agencies to help them safely investigate live and historic dark web activity. It contains more than 15 years of data from marketplaces, forums, and leak sites with new deep and dark web activity updated live and provides law enforcement with a toolset to gather evidence on marketplaces, forums, sites, individuals, and groups.

<sup>2</sup> <https://www.justice.gov/usao-edca/pr/sacramento-grand-jury-indicts-riverside-county-man-and-woman-fentanyl-distribution-and>

# FOLLOWING DARK WEB LEADS

When tracking user activity across the dark web, investigating teams will usually start with one piece of information. This could be an email address, a PGP Key, a bitcoin address, or a user's alias.

In this case, the investigators knew the username "Igorraawwr", which is the first piece of information that we can query against Cerberus' dark web dataset. Searching "Igorraawwr" in Cerberus we find (**Figure 1**):



**Figure 2:** Listings from the account "Igorraawwr" on the dark web marketplace Torrez, including references to "pressed with fent" and "new batch has lots of fent in them".

## FOLLOWING THE TRAIL

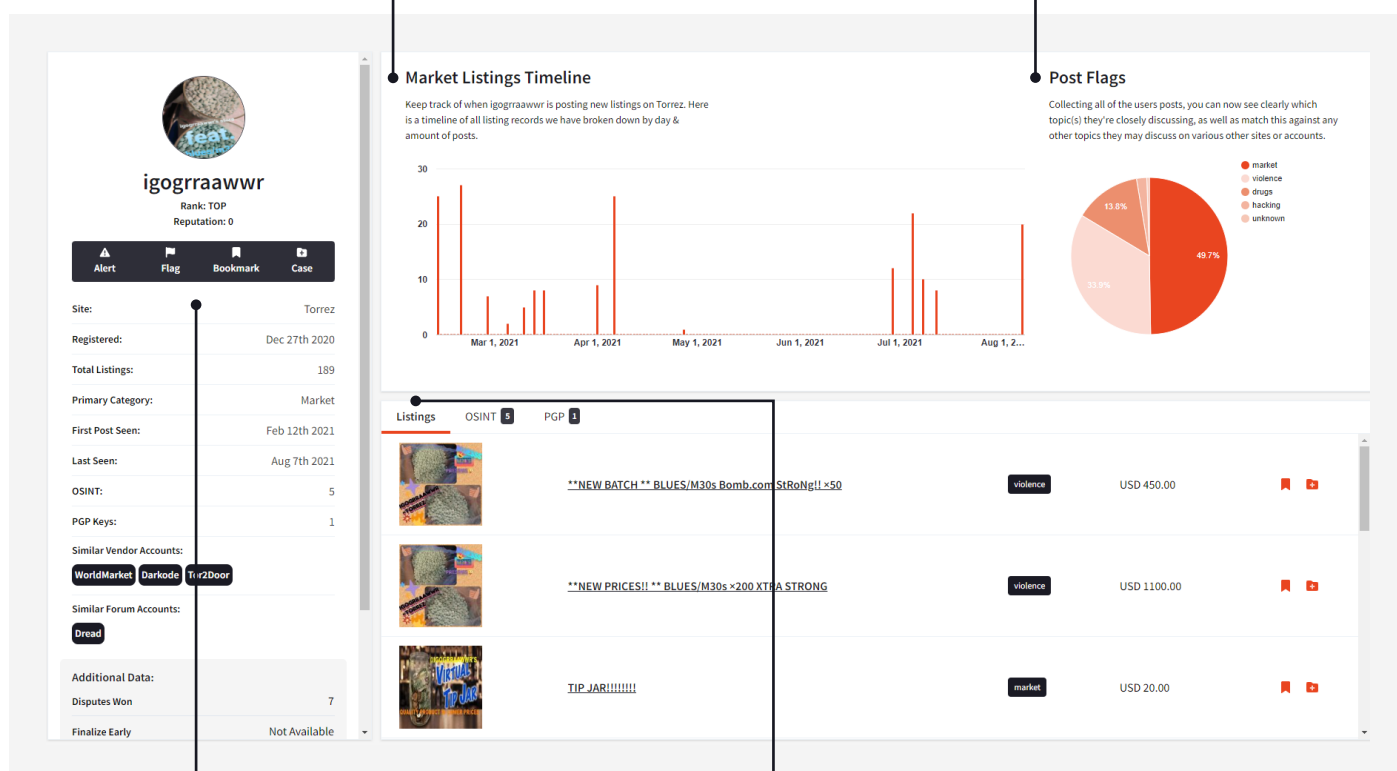
For the purposes of this report, we will zero in on the ToRReZ marketplace as this has the most “Igorraawwr” posts (189 in total). When investigating a user’s profile in a particular market or forum, Cerberus shows an overview of their activity, including:

### MARKET LISTINGS TIMELINE

A breakdown of their activity for the duration of their operations on the market. It shows that “Igorraawwr” was active on ToRReZ between February 12, 2021 and August 7, 2021.

### POST FLAGS

An indication of the type of activities the user is involved with.



### ACCOUNT INFORMATION

Details around the user such as when the profile was created, when they were last active, any OSINT or PGP keys associated with the profile, as well as other vendor or forum accounts the user is operating.

### LATEST LISTINGS

An overview of their most recent posts, which can be expanded to see all of their historical posts or listings.

**Figure 3:** The profile of the username ‘Igorraawwr’, highlighting their activity within the ToRReZ market.

Exploring the OSINT and PGP Keys tabs provides further useful information, such as a Telegram account name (@grraawwr760) and a PGP Key (9FE725B7262209ECCEBAA510E4535FF70FFA87C9FE725B7262209ECCEBAA510E4535FF70FFA87C4), which Cerberus has extracted from the postings and account.

Listings <b>OSINT 5</b> <b>PGP 1</b>			
Type	Value	Site	
Telegram	telegram @grraawwr760 <small>Found 4 times</small>	Torrez	<a href="#">View OSINT</a>
Pgp-Key-Public	9FE725B7262209ECCEBAA510E4535FF70FFA87C4 <small>Found 1 time</small>	Torrez	<a href="#">View OSINT</a>

**Figure 4:** Expanded OSINT tab showing multiple references to a Telegram username and a PGP Key.

Cerberus provides us with details associated with the extracted PGP Key, including the email address that was used to register the PGP Key, giving further information which could be built into the case file.

#### OSINT Details: "9FE725B7262209ECCEBAA510E4535FF70FFA87C4"

Metadata	
Type:	Pgp-Key-Public
Author:	igogrraawwr
Source Domain:	yxuy5oau7nugw4kpb4lclrqdbixp3wvc4iuiad23ebyp2q3gx7rtrgqd.onion
Source Type:	profile
PgpRaw:	-----BEGIN PGP PUBLIC KEY BLOCK-----  mQENBGDPbfBgBCADhxTjdinaOuEsmveJ91d1gU+8EZ8RHDreka500XbjZjiMckSc1 3wbm/5IQe0q6jhBrJBLkbqMdrTHP9AsCwGRH55J0r3Cm3zJCLD3HEzA2ue6rF9Mv HEDPWTi3WApFvAzBmXKLQIFnv0m9x9FQVcFKnz/NpLDby/g58HpSsURBreXKxBey f1fw9honPBc+4p2RYPf0CqMGnEEkGSrAcxnBFnnsOK23sGMK1Vv7HRss/upnIsHy hUmnocvmZRBNI05bVcI1BR/vH80+fHE15yzRqo4d0BXa2WpULrXnI/E1ld3Is/DK wXeutdNPj80I7+b5ISz6mth4cYmSLvpKonTABEBAAg0H0h1bnNsZXkgIDxncnJh YXd3cjC2QGdtYw1sLmIvbt6JAU0EEAEIACAFAmDPbfGcWkHCAMCBBUIcGIEFgIB -----
PgpKeyId:	E4535FF70FFA87C4
PgpKeyFingerprint:	9FE725B7262209ECCEBAA510E4535FF70FFA87C4
PgpType:	rsa2048
PgpUserId:	Hensley <grraawwr76@gmail.com>
PgpExpiry:	2021-06-20

**Figure 5:** Extracted PGP Key information, showing the PGPRaw and the email address used to register the account.

When conducting this investigation through the associated accounts, law enforcement can very quickly start to identify pieces of information that can be used both within Cerberus and outside of Cerberus to start identifying other links to this user.

In this scenario, very specific names were used for both a Telegram channel and two email accounts - "grraawwr76". Additionally, within the description of some of the market listings on ToRReZ, "Igogrraawwr" also references a Wickr account username, grraawwr760, which they indicated should be used for direct messaging.

## CROSSING INTO THE CLEAR WEB

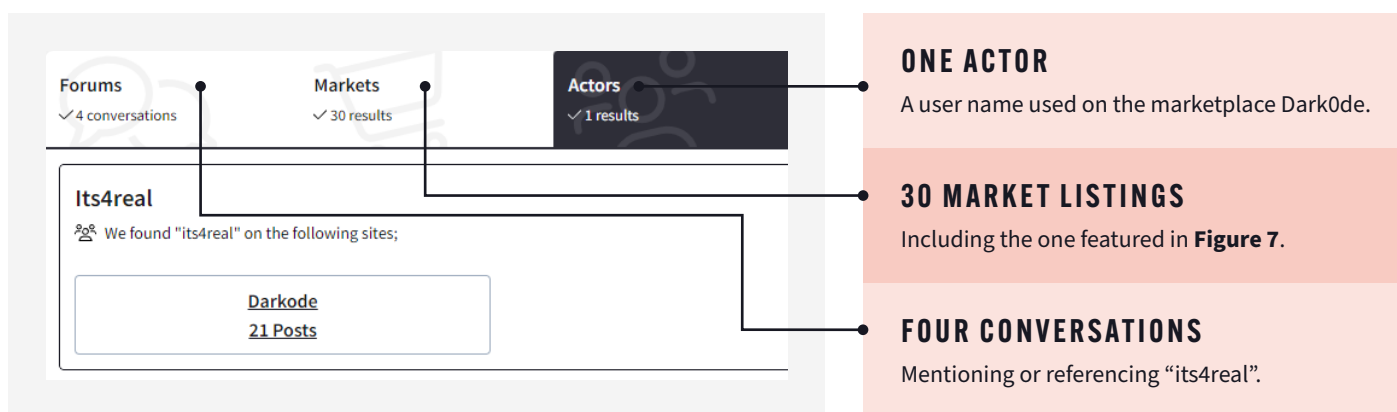
As the real investigation continued, it was identified that the username “grraawwr76” was also being used on clear web sites, some of which hosted images of the individual who owned the profile, enabling investigating teams to correlate this information with other sources to positively ID an individual in question, Holly Adams.

Searching “Igogrraawwr” in Cerberus, the following information was identified, which includes details that would be invaluable to investigators carrying out a similar investigation, saving hours of manual work in cross referencing accounts.

LOCATION	USERNAME	TELEGRAM	PGP KEY	PGP USER ID	WICKR
TORREZ (MARKET)	IGOGRRAAWWR	@GRRAAWWR760	9FE725B7262209ECCEBAA510E4535FF70FFA87C4	HENSLEY <GRRAAWWR76@GMAIL.COM>	GRRAAWWR760
WORLDMARKET (MARKET)	IGOGRRAAWWR	@IGOGRRAAWWR	9FE725B7262209ECCEBAA510E4535FF70FFA87C4	HENSLEY<GRRAAWWR76@GMAIL.COM>	
			0A2264A8438A36541467924F523BD7CE88709B4C	IGOGRRAAWWR <GRRAAWWR760H@PROTONMAIL.COM>	
DARKODE (MARKET)	IGOGRRAAWWR		D369CCE37B78BB8F3D849427C0E7EBA385EE73D5	A*****H*****513@GMAIL.COM	
TOR2DOOR (MARKET)	IGOGRRAAWWR				
DREAD (FORUM)	IGOGRRAAWWR		3E75E414313E6AA6	A*****H*****513@GMAIL.COM	

## ITS4REAL

Searching for the username “its4real” (the other alias identified by investigators) on Cerberus returned:



**Figure 6:** Overview of activity conducted by the user “its4real”.

**ups1day mexi oxys/m30 blues(1000qty)** Bookmark Add to Case

**Item Description**

For the 1000qty listing ONLY, and this is for every order not just the 1st time, we will be adding extra 100 to every 1000qty order!! a gift from us to you!


First off, these are not pharmacy products, they are **pressed** so do not ask us if they are pharmacy or pressed because we are telling you here and now, these are **PRESSED**. Secondly, these are much stronger than pharmacy kind, and so we give warning now, be careful on how you partake these as well as to how much and dont be stupid and give to someone who isnt opiate tolerant, you may be able to handle it but not everyone can.

We may be new to these markets but we know what quality is and we will always have quality product and once youve ordered, you will see for yourself. All our listings will have the price breakdown and you will notice that we dont go any lower than 100qty, but to make up for that there is going to be 2 listings for the 100qty because the 1st time you order it, it will be \$640... but you may only order this listing ONCE, if it is seen that you have ordered it for a second time, we WILL CANCEL THE ORDER IMMEDIATELY, and you may remake the order under the appropriate listing.

This special listing is for 1st time buyers, which should not be taken advantage of.


**Prices:**  
100 for \$725  
150 for \$950  
200 for \$1175  
300 for \$1650  
400 for \$2100  
500 for \$2500  
1000 for \$4700

**Details**



**Price** USD 4700.0  
**Vendor** [its4real](#)  
**Market** [Darkode](#)  
**Category** Opiods  
**Content Flags** None  
**Ships from** United States  
**Ships to** North America

**Figure 7:** “its4real” listing on the dark web marketplace Dark0de. The reference to “pressed” suggests the drugs have been produced with additional ingredients.

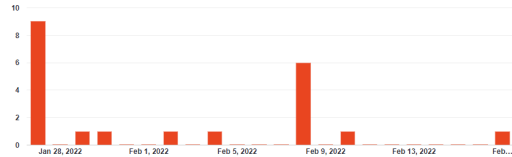


**its4real**  
Rank: 20  
Reputation: 5.0 / 5 (12 reviews)

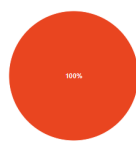
Alert Flag Bookmark Case

Site: Darkode  
Registered: Jan 25th 2022  
Total Listings: 21  
Primary Category: Spam  
First Post Seen: Jan 27th 2022  
Last Seen: Feb 17th 2022  
OSINT: 1  
PGP Keys: 1  
Similar Vendor Accounts: No Connected Accounts  
Similar Forum Accounts: No Connected Accounts




**Market Listings Timeline**  
Keep track of when its4real is posting new listings on Darkode. Here is a timeline of all listing records we have broken down by day & amount of posts.



**Post Flags**  
Collecting all of the users posts, you can now see clearly which topic(s) they're closely discussing, as well as match this against any other topics they may discuss on various other sites or accounts.



**Listings** OSINT 1 PGP 1

	<a href="#">pressed oxys/m30s hq+ups1day.x300 clone</a>	market	USD 1650.0	<span>Bookmark</span> <span>Add to Case</span>
	<a href="#">pressed oxys/m30s hq+ups1day.x400 clone</a>	market	USD 2100.0	<span>Bookmark</span> <span>Add to Case</span>
	<a href="#">pressed oxys/m30s hq+ups1day.x150 clone</a>	market	USD 875.0	<span>Bookmark</span> <span>Add to Case</span>

**Figure 8:** The profile of the username “its4real” highlighting their activity within the Dark0de market.

The “its4real” does not appear to have been active for very long, having registered the account on January 25th 2022 and being last seen on February 17th 2022. This was likely due to the fact that Dark0de exit scammed (closed and stole user funds) on February 2022, making this account unusable.

Further, whilst the PGP Key has been extracted, the information used to register the key offers much less than seen with the previous account “Ilogrraawwr”, showing just the “its4real” username and the PGPUserID. Whilst this may indicate that Holly Adam was trying to improve her OPSEC, law enforcement would likely have already collected enough information on the previous profile to hold her accountable.



## SUMMARY

This case demonstrates that it is possible to compromise the OPSEC of criminals even when they are operating under the “anonymity” of the dark web. Often there is evidence to be gathered that investigators can use to identify, track, and associate with suspects. The challenge for law enforcement is that finding this evidence can often be time consuming and difficult.

As this report shows, Cerberus can help law enforcement by automating much of the resource intensive parts of the investigation. With a starting point such as a username,

Cerberus correlates user accounts across multiple areas on the dark web to source new information, such as Wickr usernames and email addresses, which is automatically parsed from the conversations and market listings.

This can help investigators to quickly identify accounts using the same details. It is also evidence that can be collated and tracked in Cerberus’ case file system, allowing teams to collaborate on investigations, build comprehensive case files, and monitor individuals and accounts of interest.

## USE CERBERUS FOR DARK WEB SUSPECT IDENTIFICATION

Built in collaboration with law enforcement, Cerberus helps investigators:

### EFFECTIVELY ALLOCATE RESOURCES

With an intuitive toolset that can be used by officers of all technical levels, with features that can automate the surveillance of groups and suspects operating on the dark web.

### SAFELY INVESTIGATE ON THE DARK WEB

With a mirror view of dark web sites that allows investigators to gather digital intelligence without putting themselves at risk or requiring them to engage with criminal activity.

### ESTABLISH CONSISTENT POLICIES AND PROTOCOLS

With best practice for dark web data collection and retention built into Cerberus, so that digital evidence is beyond reproach and can be presented as clear and compelling evidence in court.

### COLLABORATE WITH OTHER AGENCIES

With the ability to securely share information in joint-task forces and deconfliction features built into the platform.

### REDUCE LEGAL CHALLENGES

With evidence preserved through our archive of more than 15 years of historic dark web data, which means that it remains available to investigators even if it is deleted from a dark web site.

**SEARCHLIGHT.  
CYBER**

VISIT **WWW.SLCYBER.IO** TO FIND  
OUT MORE OR BOOK A DEMO NOW.

#### UK HEADQUARTERS

Suite 63, Pure Offices,  
1 Port Way, Port Solent,  
Portsmouth PO6 4TY  
United Kingdom

#### US HEADQUARTERS

900 16th Street NW,  
Suite 450, Washington,  
DC 20006  
United States