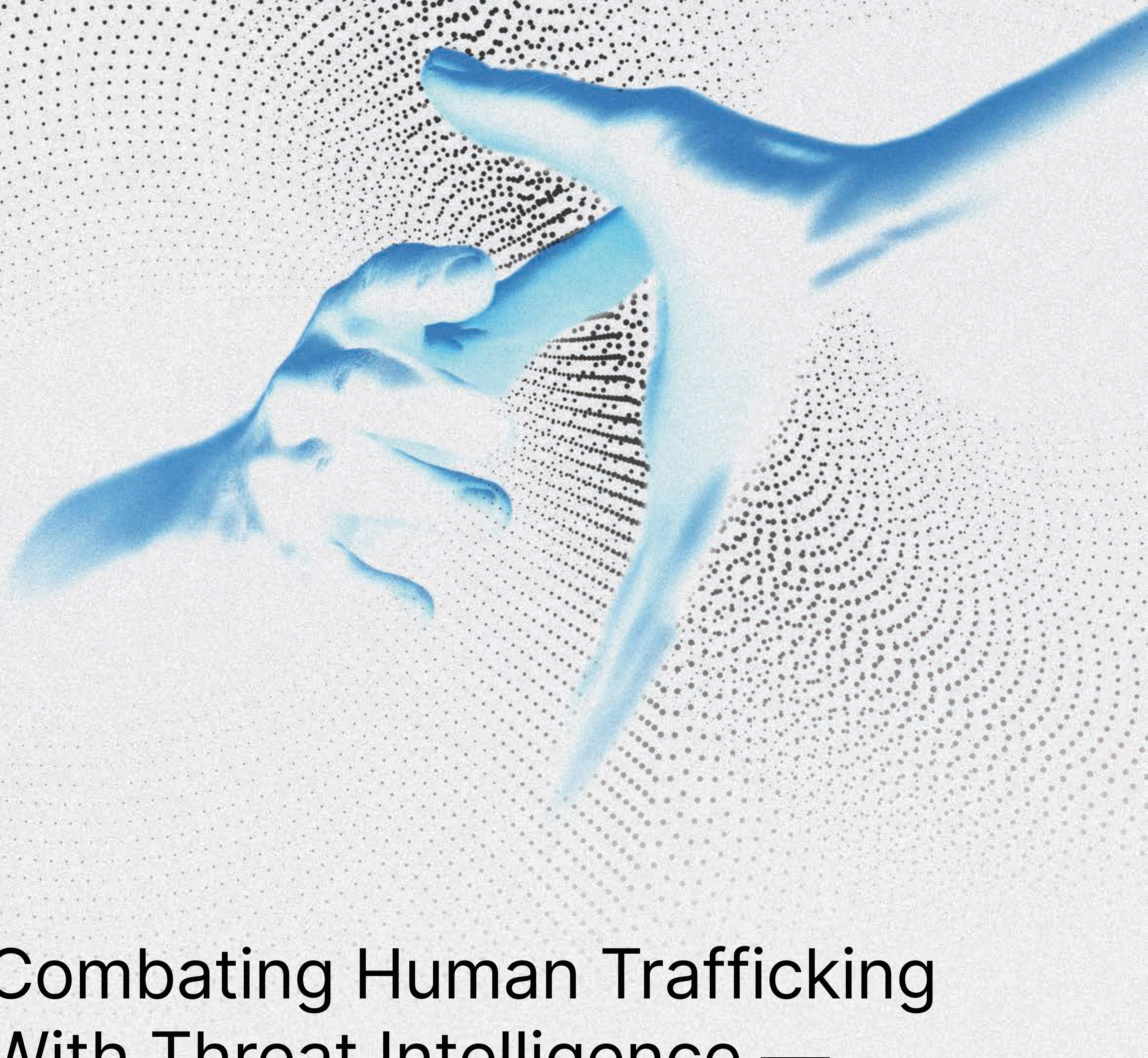
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 30, 2022



Combating Human Trafficking With Threat Intelligence — **Prosecution**

We analyzed current data from the Recorded Future® Platform, as well as both closed and open sources, to identify threat intelligence solutions to aid prosecution efforts in combating and mitigating human trafficking. This report is the second in a 4-part series; the first report focused on prevention and in subsequent months, we will publish 2 additional reports that cover protection and partnership efforts, offer threat intelligence solutions, where applicable, and provide mitigation recommendations.

Executive Summary

Threat intelligence solutions that help aggregate and analyze sources and data can support law enforcement efforts to investigate and prosecute human trafficking offenses. Human traffickers have historically used classified web pages, such as Backpage and similar websites, to advertise exploitative services. Following Backpage's closure, online ads for adult services moved to multiple, similar classifieds websites. Recorded Future harvested and analyzed information from 8 Backpage-like websites, collecting over 66,000 posts from adult classified ad pages. This data serves as a proof-of-concept (POC) study demonstrating that threat intelligence solutions can identify potential human trafficking indicators and leads to inform investigation and prosecution efforts.

When advertising exploitative services, human traffickers use various identifiers and points of contact such as usernames, email addresses, and phone numbers. Coupled with other indicators, warning signs, and behaviors associated with human trafficking, this information can aid law enforcement in generating valuable leads for initiating investigations and building cases.

From the dataset of over 66,000 posts collected from adult classified web pages, we identified 17,152 unique phone numbers and 3,357 unique email addresses. The analyzed sources predominantly catered their content to a US-based audience, with only a small fraction of listings referencing other countries and territories such as Canada, the United Kingdom (UK), Germany, France, Egypt, the Dominican Republic, the Cayman Islands, the Turks and Caicos Islands, and the Bahamas.

Email addresses can prove to be fruitful leads when coupled with various open-source intelligence (OSINT) tools that can help identify additional online accounts associated with them. In particular, the local part of an email address (the part that comes before the domain) can be searched separately to identify additional online accounts in which the local part is used as a username. Using this method, we built potential leads, uncovering full or partial names, physical appearance information, and a timeline of recent online activity. We found that similar methodology was used in recent anti-human trafficking efforts led by the Polk County Sheriff's Office Vice Unit in Florida, as well as the Anti-Human Trafficking Intelligence Initiative (ATII).

Key Findings

- The most referenced phone numbers were those with the prefix/area codes of the following US states: California, Florida, New York, New Jersey, and Texas. California prefix/area codes were the most referenced (at approximately 19%) of all identified phone numbers.
- Among identified email addresses, approximately 97% had gmail.com as their email domain. The remaining 3% of email addresses detected were from the following domains: yahoo.com, mail.com, mail.aol.com, protonmail.com, and a small number of disposable temporary email domains (such as mojzur.com and wgraj.com).
- In the analyzed datasets, we identified warning signs and potential human trafficking indicators in the form of commodifying and derogatory language describing people as objects, such as items that can be bought and sold.
- Based on our research and analysis, we built the following methodology for identifying potential human trafficking leads:
    - Identify and collect contact information from suspected human trafficking sources
    - Triage contact information to identify any commonalities or trends
    - Investigate contact information using various OSINT tools

Background

Human trafficking is a complex issue requiring a multifaceted approach, like the one set forth in the United Nations's Palermo Protocol. The Palermo Protocol serves as the foundation of the 4P paradigm which is composed of prevention, protection, prosecution, and partnership measures. In this framework, "prosecution" refers to both investigating and prosecuting human trafficking offenses.

Threat intelligence can aid law enforcement agencies' investigative efforts by gathering and identifying, or "surfacing", warning signs and potential indicators of human trafficking. Knowing where to look for leads on human trafficking and employing threat intelligence solutions that help collect, aggregate, and analyze sources and data can provide additional visibility, ways to identify the crime, and enable data analysis for additional insights.

As we noted in our first report, traffickers have historically used classified web pages, such as Backpage and similar classified websites, to market exploitative services. Threat intelligence can offer proactive research, monitoring, and analysis of suspected trafficking websites. Traffickers use various points of contact such as email and phone numbers as they advertise exploitative services on Backpage-like websites. Identified and known points of contact can be used to surface other posts, online communities, and threat actors that can further point to traffickers and behaviors associated with human trafficking.

Backpage (backpage[.]com) was a classified advertising website that was active in the US between 2004 and 2018. The website was owned by New Times Media (also known as Village Voice Media) and served as a similar service to Craigslist, allowing its users to post ads and listings under various categories including personals, automotive, rentals, jobs, and adult services. On April 8, 2018, Backpage was seized by the US Department of Justice for charges related to prostitution, including "ads depicting the prostitution of children" and money laundering. Critics have argued that the closure of Backpage has made it more difficult for sex workers to vet dangerous clients and for law enforcement to track potential traffickers. Following Backpage's closure, online ads for adult services did not end but instead moved to multiple, similar classifieds websites. The 2 bills that were created in response to the growing threat of internet-enabled human trafficking, Stop Enabling Sex Traffickers Act (SESTA) and Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), have also been criticized for their far-reaching consequences to free speech on the internet and First Amendment rights.

In our research, we have discovered websites that use the "Backpage" name in their domains and branding, as well as outlines and visuals similar to those used by Backpage. We harvested information from 8 Backpage-like websites, collecting over 66,000 posts from adult classified ad pages. Our analysis of collected information represents a POC study demonstrating that threat intelligence solutions can help law enforcement surface potential human trafficking indicators and leads to inform investigation and prosecution efforts.

We believe that with continuous monitoring of Backpage-like websites, researchers can surface further insights by correlating listings with publication dates. Continuous monitoring, such as daily data harvesting for months or years, can identify patterns, highlighting increases or decreases in activity over select periods of time. Since many Backpage-like websites do not date their posts, making it difficult to identify the specific day and time when a listing was posted, continuous daily data harvesting of the suspect sources can potentially address this evasive technique by building a timeline of new events. Even without continuous monitoring, researchers can still harvest information from the Backpage-like websites, creating valuable datasets representing active listings at the time of data scraping and using this data to conduct keyword- or location-specific searches.

Threat Analysis

From the dataset of over 66,000 posts collected from adult classified webpages, we identified 50,397 total phone numbers and, of these, 17,152 were unique. The most referenced phone numbers were with the prefix/area codes of the following US states: California, Florida, New York, New Jersey, and Texas. California prefix/area codes were most referenced (at approximately 19%) from all identified phone numbers (see Figure 1).

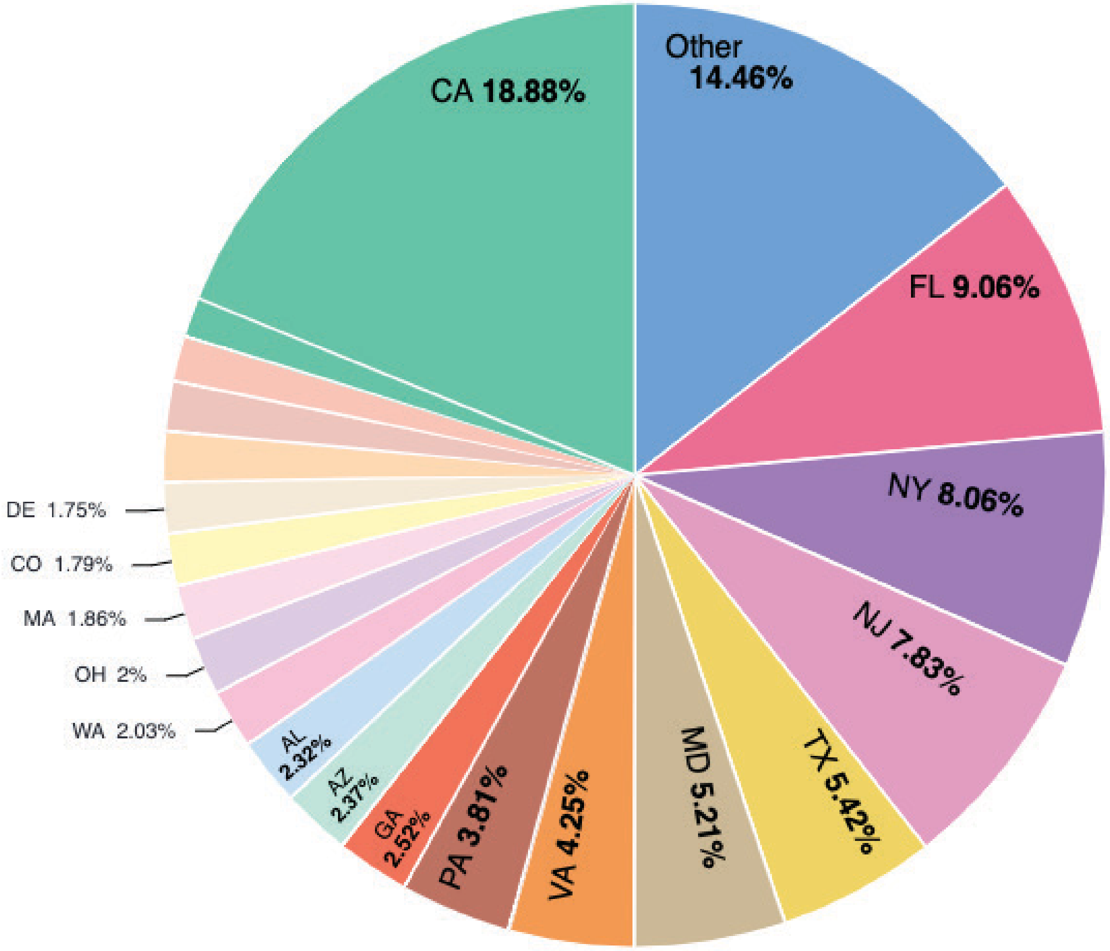
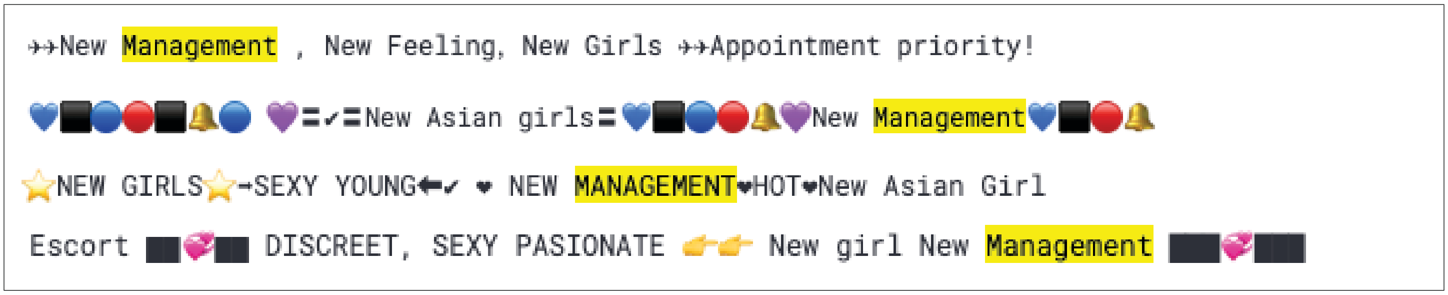


Figure 1: Top phone numbers based on their prefix/area code (Source: Recorded Future)

We found that the analyzed sources predominantly catered their content to a US-based audience. This was reflected in the references of locations found in the datasets as well as prefix/area codes of identified phone numbers. Besides the US (over 45,000 references), we detected mentions of the following countries and territories: Canada, the UK, Germany, France, Egypt, the Dominican Republic, the Cayman Islands, the Turks and Caicos Islands, and the Bahamas. Countries other than the US represented only a small fraction of listings in the analyzed data. Similar to the now-defunct Backpage, the analyzed sources were heavily focused on the US, with some only breaking up adult sections per state and city located in the US. Countries other than the US had dedicated sections only on 4 out of 8 analyzed sources.

We found that some of the same phone numbers appeared across multiple sources and posts. For example, a phone number with the 973 prefix/area code, associated with the state of New Jersey, was posted on 4 different sources and appeared in 55 listings.

Human traffickers are known for giving the impression that sexual exploitation is a voluntary, consensual choice of those engaged in providing adult services. According to the United Nations Convention Against Transnational Organized Crime, the consent of a trafficking victim is irrelevant. Human trafficking can take place even if the victim initially consented to provide exploitative services. Traffickers are notorious for advertising exploitative services as independent and unorganized. However, the volume of some of the posts with potential warning signs and human trafficking indicators, where the same phone number or email address appears hundreds of times, suggests that these advertisements are organized and managed. In some listings, we found warning signs and potential human trafficking indicators in the form of commodifying and derogatory language that is rarely, if ever, used by self-organized individuals. When querying the datasets by the English keyword “management”, we identified the organized nature of some of the advertised services.



➳➳New Management , New Feeling, New Girls ➳➳Appointment priority!

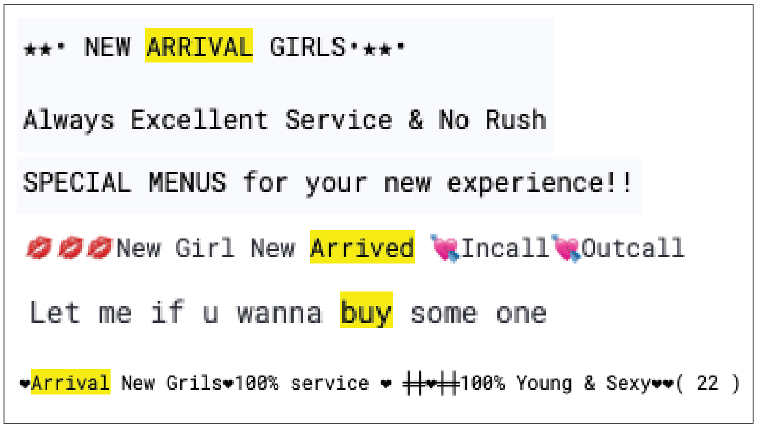
💙⬛🔵🔴⬛🔔🔵 💜〓✔〓New Asian girls〓💙⬛🔵🔴🔔💜New Management💙⬛🔴🔔

⭐NEW GIRLS⭐➡SEXY YOUNG⬅✔ ❤ NEW MANAGEMENT❤HOT❤New Asian Girl

Escort ██💞██ DISCREET, SEXY PASIONATE 👉👉 New girl New Management ███💞███

Figure 2: Examples of query results for the keyword "management" (Source: Recorded Future)

In other listings, we identified more instances of commodifying language in which people were described as objects, such as items that can be bought and sold.



★★• NEW ARRIVAL GIRLS•★★•

Always Excellent Service & No Rush

SPECIAL MENUS for your new experience!!

💋💋💋New Girl New Arrived 💘Incall💘Outcall

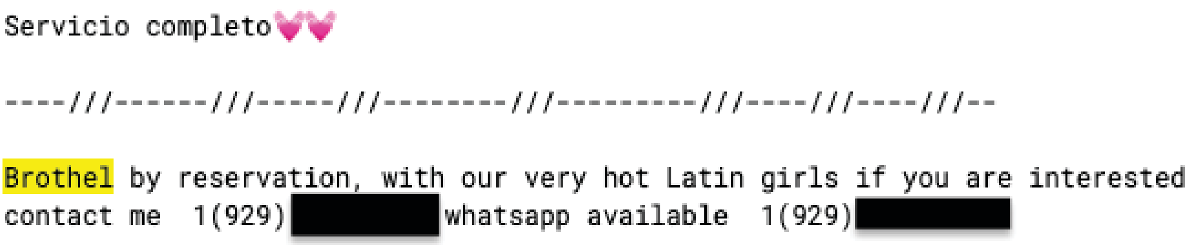
Let me if u wanna buy some one

❤Arrival New Grils❤100% service ❤ ╫❤╫100% Young & Sexy❤❤(22)

Figure 3: Examples of query results for the keywords "arrived" or "arrival" and "buy" (Source: Recorded Future)

We found numerous other examples of commodifying language, often used by traffickers and pimps, but chose not to include them as illustrations to this report due to their derogatory and explicit nature. In essence, the terms used (similar to the ones we illustrated above) reduce people to objects, commodifying and objectifying individuals as items for sale on a marketplace.

We queried harvested data against the list of human trafficking keywords in the English language provided in our first report and found references to some of the keywords, including "brothel", "buyer", "whore", "vic", and "purchase".



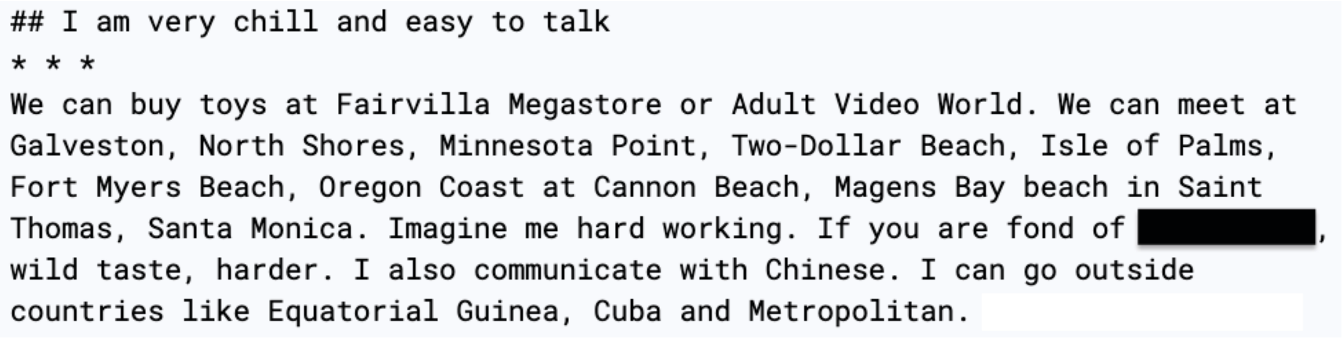
Servicio completo💓💓

----///------///-----///--------///---------///----///----///--

Brothel by reservation, with our very hot Latin girls if you are interested contact me 1(929)[redacted]whatsapp available 1(929)[redacted]

Figure 4: Example of a query result when searching for the keyword "brothel" (Source: Recorded Future)

Another potential human trafficking indicator is classified ads that list multiple locations as potential meet-up places (Figure 5), which are likely part of a circuit. For example, the West Coast trafficking circuit, which includes San Diego, Las Vegas, Portland, and the cities between these locations, is a popular route used by traffickers.



```
## I am very chill and easy to talk
* * *
We can buy toys at Fairvilla Megastore or Adult Video World. We can meet at
Galveston, North Shores, Minnesota Point, Two-Dollar Beach, Isle of Palms,
Fort Myers Beach, Oregon Coast at Cannon Beach, Magens Bay beach in Saint
Thomas, Santa Monica. Imagine me hard working. If you are fond of [redacted],
wild taste, harder. I also communicate with Chinese. I can go outside
countries like Equatorial Guinea, Cuba and Metropolitan.
```

Figure 5: Example of a listing referring to multiple cities, posted by a potential suspect of a trafficking circuit (Source: Recorded Future)

Identifying keywords of interest, such as those illustrated above, can aid law enforcement in generating valuable leads for initiating investigations and building cases.

Other than phone numbers, within our dataset of over 66,000 posts collected from Backpage-like websites, we identified 21,687 total email addresses, of which 3,357 were unique. Approximately 97% of email addresses used the gmail.com domain. The remaining 3% of email addresses were detected with the following domains: yahoo.com, mail.com, mail.aol.com, protonmail.com, and a small number of disposable temporary email domains (such as mojzur.com and wgraj.com).

The data points gathered from analyzing listings on Backpage-like websites can be further investigated by law enforcement to identify and locate potential victims or traffickers. By obtaining and serving subpoenas to public commercial communication service providers such as Google or Yahoo, it is possible to obtain further information about the account holder including name, account creation information, associated email address(es), phone number(s), sign-in IP address(es) and associated timestamp(s), email content, and more. While some of the information used for account registration can be inaccurate or fake, investigators can compel internet service providers (ISPs) to identify the individual who was assigned the IP address(es) used to sign-in to email providers. ISPs can provide the user's name, physical address, and other identifying information, which can be confirmed by conducting a mail cover or checking utility bills.

Similarly, for phone number records, investigators can use a subpoena to compel telecommunications companies to disclose basic subscriber and session information including the subscriber's name, physical address, local and long-distance telephone connection records, records of session times and durations, length of service (including start date) and types of service utilized, other subscriber numbers or identification, including any temporarily assigned network address[es], and the means or source of payment for such service (including any payment card or bank account number[s]).

In addition to phone numbers and email addresses, when analyzing collected data, we identified suggestive email addresses and usernames (local parts of the email addresses) that reflect an interest in advertising sexual services. Among the top 5 usernames / local parts of the email addresses, we identified the following: "sexygirlhere", "playgirl", "culfie", "bjfun", and "sexfun". In US case law (such as in United States v. Shields), the "suggestive" email address of "LittleLolitaLove" supported the probable cause needed for issuing a warrant to subpoena email account records due to suspected child pornography.

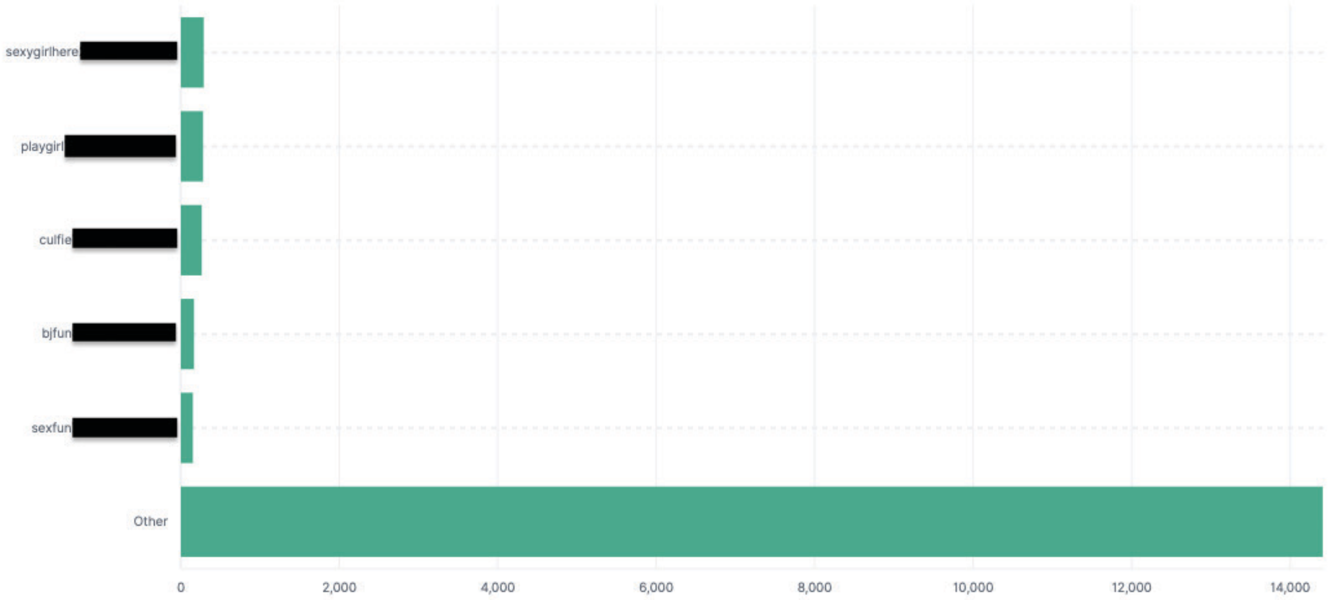
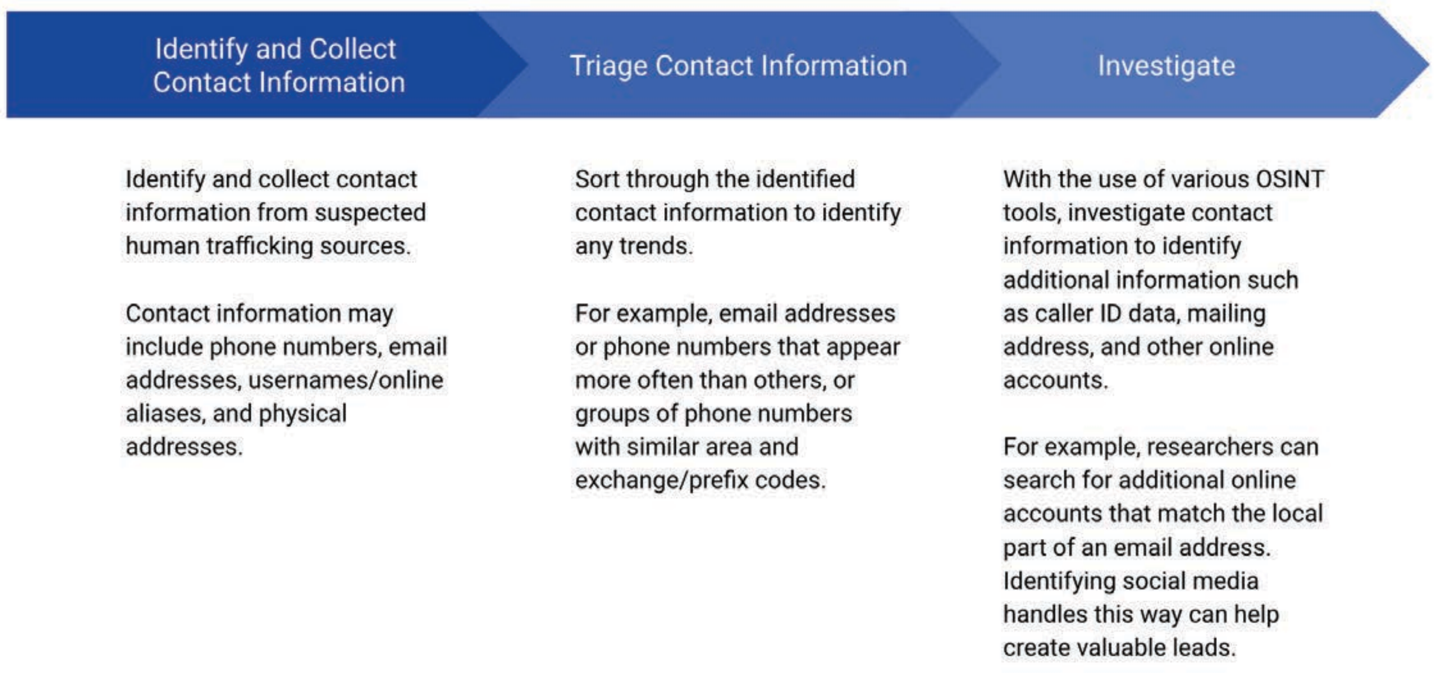


Figure 6: Usernames / local parts of the top 5 detected email addresses (Source: Recorded Future)

Identifying Potential Leads

We collected email addresses and phone numbers that were provided as points of contact on numerous Backpage-like sources. We then triaged this data, using various OSINT tools to identify potential leads that could trace back to either traffickers or victims themselves. An example of how human trafficking researchers can take initial steps to identify potential human trafficking leads is shown in Figure 7 below.



Identify and Collect Contact Information

Identify and collect contact information from suspected human trafficking sources.

Contact information may include phone numbers, email addresses, usernames/online aliases, and physical addresses.

Triage Contact Information

Sort through the identified contact information to identify any trends.

For example, email addresses or phone numbers that appear more often than others, or groups of phone numbers with similar area and exchange/prefix codes.

Investigate

With the use of various OSINT tools, investigate contact information to identify additional information such as caller ID data, mailing address, and other online accounts.

For example, researchers can search for additional online accounts that match the local part of an email address. Identifying social media handles this way can help create valuable leads.

Figure 7: Initial steps for identifying potential human trafficking leads (Source: Recorded Future)

We found email addresses to be more fruitful than phone numbers when searching for potential leads. An email address can be researched using various OSINT tools to identify other online accounts associated with that email address. Similarly, the local part of an email address can be searched by itself to identify additional online accounts in which the local part is featured as a username. Using this method, we were able to begin building potential leads, uncovering full or partial names, physical appearance information, and a timeline of recent online activity. In some cases, these searches led to videos, which can further be analyzed in an attempt to gather location information. Such leads can help law enforcement identify and locate potential victims or traffickers.

Use Case: Florida Law Enforcement Uses Similar Methods to Identify Trafficking Activity

A recent example of law enforcement using similar research methodologies to identify potential human trafficking activity includes the March 2022 arrest of 108 individuals by the Polk County Sheriff's Office Vice Unit in Florida. The 6-day operation, dubbed "Operation March Sadness 2", involved undercover detectives searching for, and identifying, online prostitution advertisements with the intent to identify any victims being forced into sex work and to arrest those participating in the trafficking of victims.

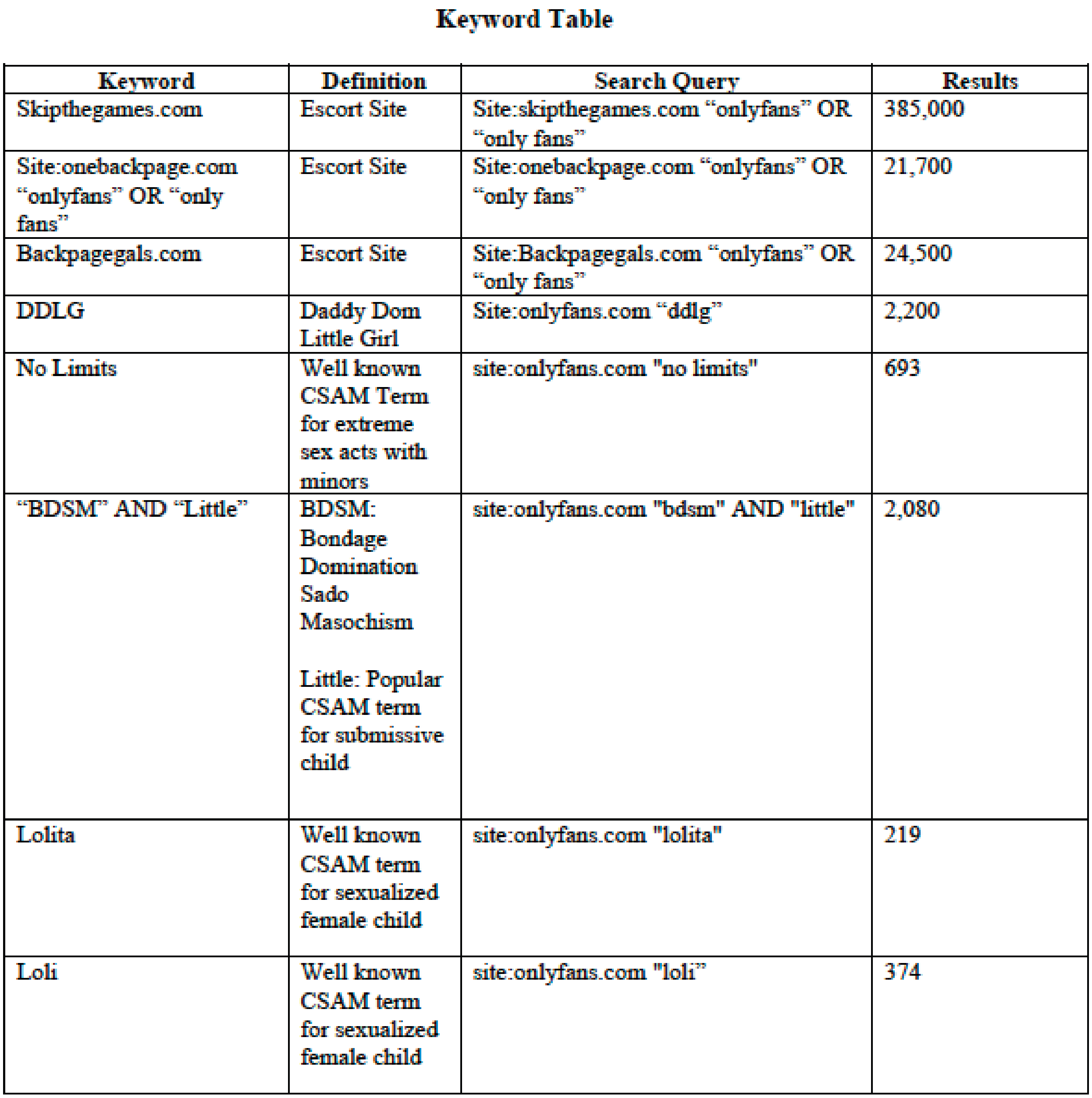
After identifying online advertisements, the detectives contacted individuals offering prostitution services and arranged to meet up, which subsequently led to their arrests upon arrival. The Polk County Sheriff's Office Vice Unit worked with anti-trafficking organizations that spoke with those offering prostitution services to determine if they were victims of human trafficking forced into sexual exploitation.

Use Case: ATII Uses OSINT Methodologies to Identify Potential Trafficking Leads Associated with OnlyFans

On April 3, 2022, the Anti-Human Trafficking Intelligence Initiative (ATII) published its findings regarding the use of OnlyFans as an online platform for human trafficking activity, particularly in regard to child sexual abuse material (CSAM). Included in this report are ATII's research methodologies for identifying potential trafficking leads. ATII noted that their research leads were generated using common search engines such as Google and "routine search techniques used in open-source investigations", such as searching known escort websites (similar to our investigation of Backpage-like websites) for CSAM and/or sex trafficking keywords. The ATII also used specialized dark web tools to identify connections between OnlyFans profiles and dark web sex predators. According to the ATII, "when searching keywords of 'OnlyFans' AND 'pedo' (aka pedophiles) 54,443 darknet results were identified. During ATII's research, references were found to children being sold for in-person physical contact sexual encounters". A summary of the ATII's keyword searches can be found in Figure 8 below.

Using this methodology, the ATII identified hundreds of thousands of potential leads. However, as stated by the ATII, and also noted in our report, the volume of results is complex and oftentimes does not involve obvious or probative evidence that illegal activity has occurred. The ATII provides the following insight into how potential leads can be investigated further:

> *Law enforcement personnel assess each potential case and weigh multiple "indicators" when deciding if a case warrants further investigation, but ultimately, pursuing an investigation is subjective. Certainly, any one or even two indicators present can sometimes be explained by, or attributed to, other factors that are not criminal. However, when there are multiple indicators present, it becomes more and more plausible (or even likely) that a person is being trafficked against their will.*



Keyword Table

Keyword	Definition	Search Query	Results
Skipthegames.com	Escort Site	Site:skipthegames.com "onlyfans" OR "only fans"	385,000
Site:onebackpage.com "onlyfans" OR "only fans"	Escort Site	Site:onebackpage.com "onlyfans" OR "only fans"	21,700
Backpagegals.com	Escort Site	Site:Backpagegals.com "onlyfans" OR "only fans"	24,500
DDLG	Daddy Dom Little Girl	Site:onlyfans.com "ddlg"	2,200
No Limits	Well known CSAM Term for extreme sex acts with minors	site:onlyfans.com "no limits"	693
"BDSM" AND "Little"	BDSM: Bondage Domination Sado Masochism Little: Popular CSAM term for submissive child	site:onlyfans.com "bdsm" AND "little"	2,080
Lolita	Well known CSAM term for sexualized female child	site:onlyfans.com "lolita"	219
Loli	Well known CSAM term for sexualized female child	site:onlyfans.com "loli"	374

Figure 8: Table created by the ATII depicting keywords their researchers used to identify potential sex trafficking activity (Source: Anti-Human Trafficking Intelligence Initiative)

Within our dataset of over 66,000 posts collected from Backpage-like websites, we identified mentions of the keywords used in ATII's research: "onlyfans" with 487 references, "no limits" with 280 references, "bdsm" with 608 references, "little" with 10,194 references, and "lolita" or "loli" with 7 references. We reported all identified sources covered in this report to law enforcement and the National Center for Missing and Exploited Children (NCMEC) CyberTip line.

Outlook and Conclusions

As exemplified by the prevalence of Backpage-like websites, human traffickers continue to use classified web pages to market exploitative services and target vulnerable people. We expect this advertising and recruitment method to continue to be popular in the future, due to the low bar for entry and the large number of similar websites available for use. Law enforcement agencies can monitor sources of interest for generating valuable leads for initiating investigations and building cases.

Targeted data collection and analysis can aid in the process of identifying leads and supporting investigative efforts by aggregating data points from multiple sources and surfacing potential indicators of human trafficking. While our data collection efforts encompassed a limited time period and limited sources, the results show that valuable insights and potential investigative leads can be generated if similar data collection methods are implemented on a continuous basis. Including more websites of interest in data aggregation will help capture additional information, thus enabling more opportunities to surface warning signs and identify crime.

Threat intelligence can offer proactive research, monitoring, and analysis of suspected trafficking websites. Traffickers use various points of contact, such as email addresses and phone numbers, as they advertise exploitative services on Backpage-like websites. Identified and known points of contact can be used to surface other posts, online communities, and threat actors to detect traffickers and behaviors associated with human trafficking.

Some of the prosecution challenges stem from the lack of appropriate training for law enforcement and within the criminal justice system. First responders, including police officers, should receive training on how to identify victims of human trafficking, including which warning signs and suspicious behaviors to look for and where to look for them. Human trafficking is no longer a hidden crime when first responders are trained to see it. Training examples for law enforcement can be found on the Department of Homeland Security (DHS) website (Blue Campaign), the Office for Victims of Crimes (OVC) website, the United Nations Office on Drugs and Crime (UNODC) website, the Organization for Security and Co-operation in Europe (OSCE) website, and other resources.

We recommend monitoring websites of interest, including adult classified service providers, to identify potential human trafficking indicators. Creating watchlists and alerting rules on the Recorded Future Platform can aid in monitoring underground, special-access, messaging platforms, and dark web sources that advertise and discuss human trafficking.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.