

[Subscribe](#)[Past Issues](#)[Translate ▼](#)

News, Resources, and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.



Toddington International Inc.

Online Research and Intelligence Newsletter

JUNE 2020 EDITION

In This Edition

- [Welcome to the Newsletter](#)
- [e-Learning: "Using the Internet as an Investigative Research Tool"](#)
- [More Self-Paced e-Learning Programs](#)
- [Featured Article: "Why Digital Investigations Are the Future of Policing"](#)
- [Upcoming Select Public Courses](#)
- [Tools and Resources for the OSINT Professional](#)
- [How-To's and Articles of Interest for the OSINT Professional](#)

Welcome to the Newsletter

Free Drop In and Learn ("DIAL") Webinars

We are pleased to present our **FREE** Drop In and Learn ("DIAL") weekly webinars. From best practices in preserving and presenting online sourced evidence to essential critical thinking skills, OSINT techniques, and through provoking cyber security practices, each week we feature a different expert guest to keep you informed.

[Subscribe](#)[Past Issues](#)[Translate ▼](#)**Upcoming DIAL sessions (note all times are in UTC):****June 4 (1500 hrs UTC)**

["Getting the Most Out of Google"](#) with Nico Dekens

June 11 (1700 hrs UTC)

["Medical Intelligence, Pandemics and Global Health Emergencies: A Practitioner's Perspective"](#) with Chelsey Goodman

June 18 (1700 hrs UTC)

["Cyber Risks During COVID: Small and Medium Business Edition"](#) with Dominic Vogel

Running time of the DIAL webinars ranges from 30 to 45 minutes and registration is **free**. To sign up and find out about upcoming webinars please visit dropinandlearn.org - past editions are available on the DIAL [YouTube Channel](#).


"Hunted" Now Available on Amazon Prime

The first four seasons of the BAFTA nominated, hit UK television series "Hunted" have arrived on Amazon Prime. Watch TII's David Toddington (Seasons 1, 2 and 3), Colin Crowden (Seasons 3, 4 and 5) and Yaniv Pereyaslavsky (Season 5 when available) as they track ordinary British citizens who attempt to go on the run and drop off the grid for 28 days.

Subscribe

Past Issues

Translate ▼



Hunted

Season 3 ▼

2015 6 episodes 13+ 🗨

Languages: Audio (1), Subtitles (1) ▼

14 ordinary members of the U.K. public are challenged to go on the run, and to drop off the grid for up to 28 days. This is a twist on the reality TV genre, with simulated 'state' tracking by professional investigators, hackers, profilers and ex-police officers. With limited financial resources, those hunted must do whatever they can to maintain a low profile against.

Episodes (6) [More details](#)

prime
Included with Prime

[▶ Play S3 E1](#)

[+ Watchlist](#)

[⬇ Download Season 3](#)

[🔗 Share](#)

E-Learning Graduates

Congratulations to the following students who are among those who successfully completed an e-learning program with TII this month:

- Myra Pagé
- Paula Gyte
- Roger Charles
- Angus Naismith
- Donna Warren
- James Fisher
- Richard Peterson
- Beverly Morton
- Joshua Pike
- Dorothy Groves
- Ellis Pasterkamp
- Paul Higgins
- Isaac Wallis
- Aaron Humphries

Subscribe	Past Issues	Translate ▼
<ul style="list-style-type: none">• Sunita Paulina• Duane Allen• Sandra Cunningham• Nathan Wilburn• Jeannette Duguay		

Important Note: As we respect the privacy of our students, we only publish the names of students who have provided express permission to do so. Many of our students are unable to share their completion due to the nature of their employment, or due to online privacy concerns. If your name did not appear in the above list and you wish to announce your completion of the course with TII, please [contact us](#).

"Using the Internet as an Investigative Research Tool™" Self-Paced e-Learning



Take Your Online Research and Intelligence Skills to New Levels with TII's Comprehensive e-Learning Program, ["Using the Internet as an Investigative Research Tool™"](#)

The most comprehensive and up-to-date internet research and investigation e-learning program available, ["Using the Internet as an Investigative Research Tool™"](#) is designed to enable investigators, researchers, and intelligence professionals to find better online information, in less time, at less cost, with less risk™.

For a fraction of the cost of classroom-based training, our flexible and interactive virtual classroom environment allows candidates to progress at their own pace and competency level, with a qualified personal instructor on hand at all times to ensure success. Initially launched in 1998, this highly-acclaimed and continually updated online course has been successfully completed by well over eight thousand investigators and knowledge workers around the world.

[Subscribe](#)[Past Issues](#)[Translate ▼](#)

group discounts and licensing options are available for five or more registrants. Visit the [course page](#) to find out more and instantly register, or [contact us](#) directly with any questions.

Bonus: Tuition fee includes special access to select OSINT resources.

As a HRSDC certified educational institution, TII provides Canadian students with a T2202A Tuition Tax Receipt.

More Self-Paced e-Learning Programs



Social Media Intelligence & Investigations

30-Hour E-Learning Program

COMING SOON This highly-anticipated program will introduce research and investigative professionals to a variety of essential tools and techniques necessary to locate, collect, and utilize social platform-sourced information, while reminding participants of the considerations and implications of leveraging this type of information safely and appropriately. **Sign up for the waitlist or learn more [here](#).**

Introduction to Intelligence Analysis

40-Hour E-Learning Program

This program provides a rich and interesting opportunity to explore the key concepts and intellectual foundations which inform intelligence analysis activity. Students will develop awareness of, and gain experience in, using common tools and methodologies to

[Subscribe](#)[Past Issues](#)[Translate](#) ▼

[up or learn more here.](#)

Criminal Intelligence Analysis

40-Hour E-Learning Program

This program is designed to equip aspiring and inexperienced analysts, as well as other interested law enforcement and investigative professionals, with the knowledge and skills required to undertake criminal intelligence analysis work, and to understand criminal intelligence analysis products when encountered. **Sign up or learn more** [here](#).

Strategic Intelligence Analysis

40-Hour E-Learning Program

This program is intended for professionals working in public sector enforcement, intelligence, national security, and regulatory compliance roles, or those aspiring to do so. Students will be equipped with the skills and knowledge required to effectively conceive, plan, and implement strategic analysis projects, and deliver impactful strategic advice to clients and other end users. **Sign up or learn more** [here](#).

Why Digital Investigations Are the Future of Policing



[Subscribe](#)[Past Issues](#)[Translate ▼](#)

Examples and images in this document contain disturbing content related to human and drug abuse.

“It is rare that a case does not involve some kind of cyber or computer element that we prosecute in our office.”¹

—Cyrus Vance, Manhattan District Attorney

Criminal strategies are rapidly evolving alongside technology. More crimes, from child exploitation to financial fraud, are planned and executed in some capacity online —particularly on the dark web and less-regulated social networks. Individuals and organizations, including law enforcement agencies, are also increasingly grappling with targeted cyberattacks and data theft.

These trends are driving fundamental shifts in criminal investigations. Agencies are now responsible for processing digital forensics and online data. The success and speed of most cases rely on law enforcement’s ability to process this data thoroughly and efficiently, even though many agencies aren’t equipped to cope with the quickly advancing digital aspects of crime.

What does this process currently look like, and how are specialized search tools improving it in the field?

Digital Investigation Efficiency Is a Priority

The proliferation of smart technology, IoT, and digital communications is rapidly expanding the volume of data available to law enforcement, increasing industry demand for digital investigators. Without the staff and tools required to efficiently process this information, agencies risk prolonging criminal activity and reducing public trust in their efforts.

According to a survey requested by the Fairfax County PD in 2017, training and equipping a digital forensics examiner takes about 18 months and \$95,000.² These roles also tend to require continuous tool upgrades and training to keep up with new technologies and adaptive criminal strategies.

There are thousands of sources on the “hidden internet,” including deep and dark websites, as well as less-regulated social networks (e.g. Gab, 4chan), where criminals publicly and anonymously discuss and advertise their activities. These include drug and human trafficking, financial fraud, identity theft, child exploitation, terrorism, gang activity, and targeted cyberattacks.

The hidden internet is integral to contextualizing real-world crimes and other digital

queried by conventional search engines.

They also produce an overwhelming volume of data that is impossible to manually search and classify efficiently. Networks like the dark web also require skill to navigate without exposing law enforcement systems to further risk. These factors make finding relevant investigative data extremely time-consuming and risky—which is why specialized tools are necessary for law enforcement investigators.

Specialized Search Software Is Essential to an Agency's Toolkit

This landscape points to a need for investigative search tools that:

- Filter relevant, public data safely and efficiently from the deep and dark web and other social networks where criminals or witnesses operate
- Access a broad spectrum of mainstream and niche networks where relevant data can be overlooked
- Get digital investigators up-and-running quickly, even if they aren't technical experts
- Protect law enforcement agencies themselves from digital and physical harm

Data discovery software enables law enforcement to quickly and easily find relevant online data to support their investigations. There are a number of emerging web-based tools on the market that allow criminal investigators to narrow in on relevant data that isn't easily searchable through Google or in-site navigating—whether it's a dark web forum thread or public social media content.

These tools work by aggregating and indexing data from a number of sources relevant to law enforcement. These include social media platforms, dark web forums and marketplaces, and deep websites like obscure image boards and paste sites.

Once the data is indexed, users can efficiently refine search results using keywords, advanced filters, and with some tools, machine learning capabilities. Depending on the tool, indexed data is made available within a platform's user interface, or delivered to an agency's or fusion centre's existing platform through an API.

These tools help agencies reduce investigation training costs and timeframes. They also help law enforcement personnel sort through overwhelming data volumes more efficiently, and ensure that they don't miss out on any critical content.

Data Discovery Software: Common Use Cases

Law enforcement can use these tools for investigating crimes in almost every category, from personal to white-collar crimes. The following examples highlight common law enforcement use cases using data discovery software.


Subscribe





Past Issues

Translate ▼

Dark web marketplaces enable the flow of illicit substances within and across international borders. By routing internet traffic through multiple nodes, dark web networks like Tor are designed to keep users anonymous. However, vendors often disclose the country and sometimes state of origin. Dark web search software allows law enforcement personnel to query location-based keywords (for example, “ships from United States”) across multiple marketplaces to locate and engage covertly with drug trafficking networks.

7G. PUREST CLEANEST BLACK TAR HEROIN AVAILABLE





Sold by

69

5.00 ★

Trust Level 3

FEATURES

Product class	Physical Package	Quantity left	10000
Ships from	United States		
Ships to	United States		
Views	110	Visibility	Public
Ends In	Never	Payment	Escrow

Total Purchase Price : USD 551.2

Shipping : USPS PRIORITY SHIPPING 3 Days - USD +15.1

Buy Now

DescriptionFeedbackRefund policyTerms & Conditions

Product Description

we now have the best bth available at a discounted price. Take advantage of our superior products and fast shipping

US-based vendor offering black tar heroin domestically—discovered on Nightmare Market using Beacon

Data discovery tools aid in trafficking investigations by correlating user activities on disparate networks. For example, vendors often reuse usernames and language across their suite of online accounts—not only on the dark web, but sometimes on the surface web as well. Law enforcement can pivot off of data, such as vendor usernames, to create links between a suspect’s surface and dark web activities to support a case.

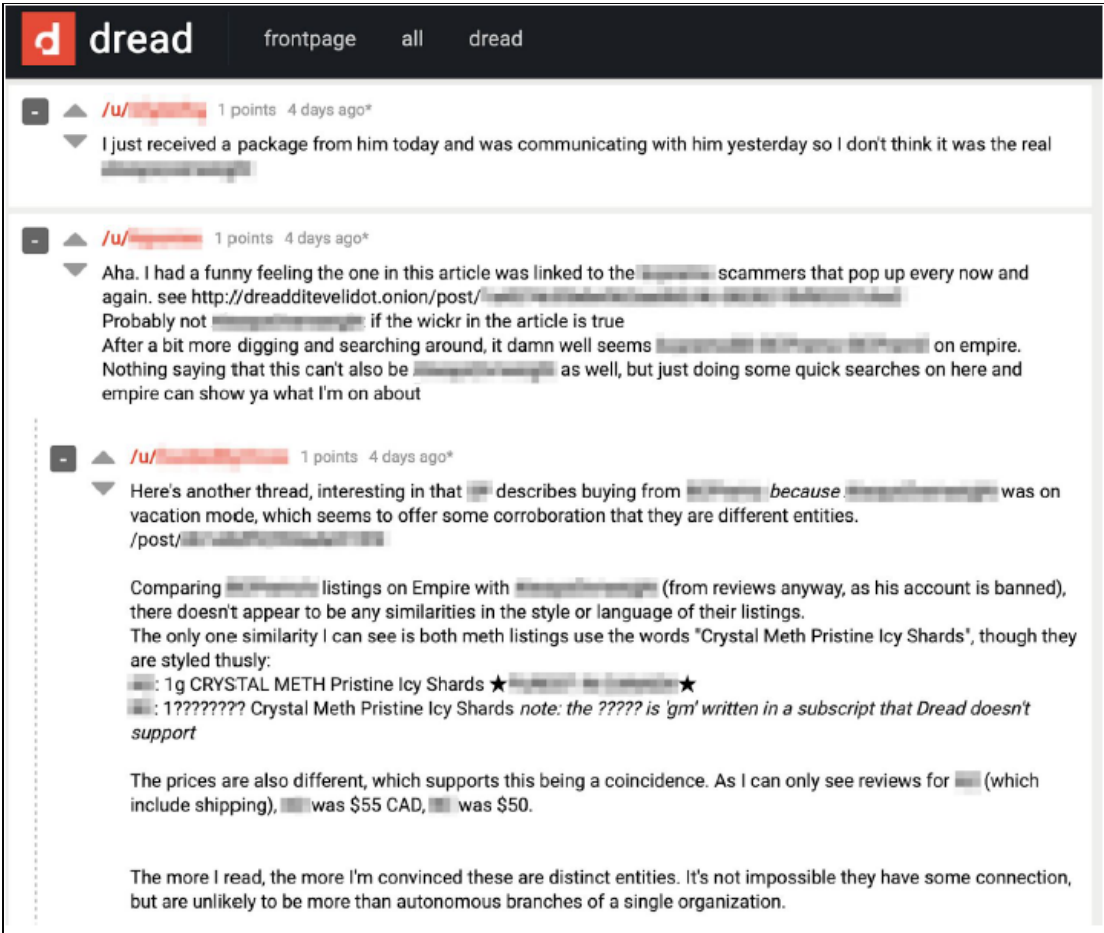
The dark web also contains discussions about drug trafficking strategies and vendor

Subscribe

Past Issues

Translate ▼

- Which vendors are popular, what they sell, and where and how they operate
- How-to discussions on drug manufacturing and trafficking



Users on the dark web forum Dread discussing dark web vendors potentially linked to a recent drug bust—discovered using [Beacon](#)

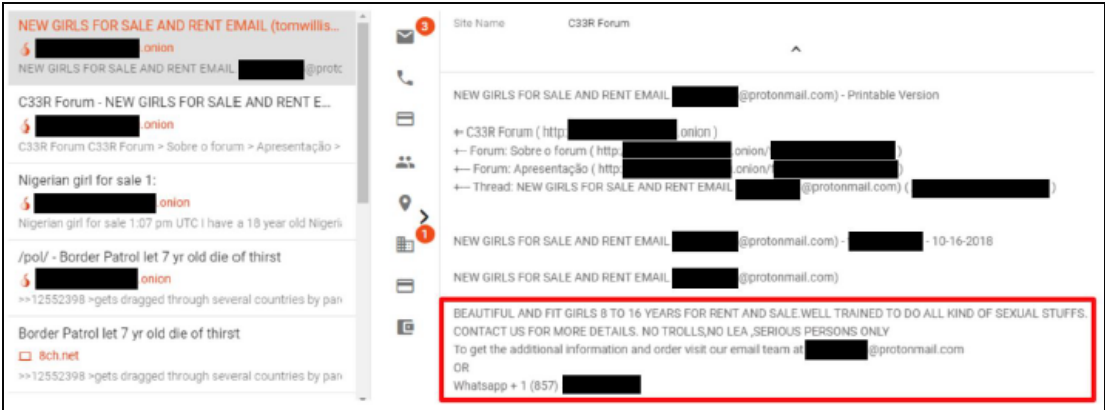
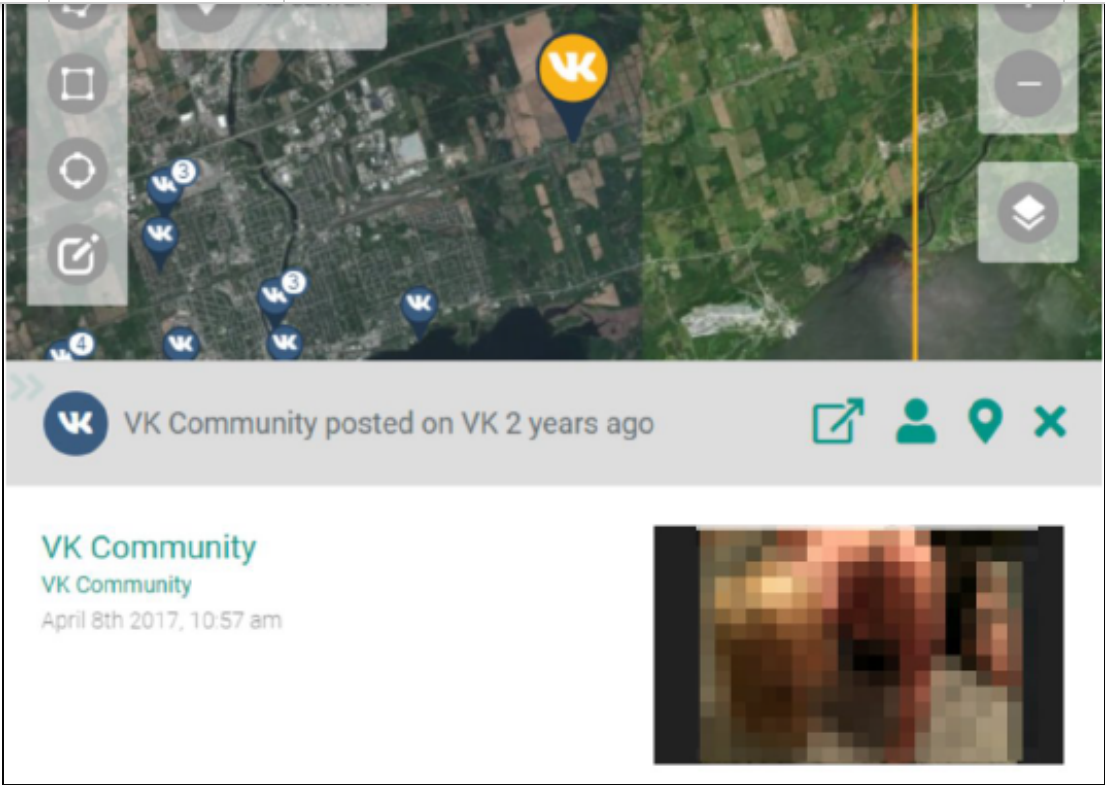
Human Trafficking

Online networks also offer valuable information to support human trafficking cases. Data discovery software allows law enforcement to search adult ads on classified sites like skipthegames.com and social networks like Vkontakte. These ads often contain indicators of transient human trafficking rings, such as “one night only” and “new in town.”

Subscribe

Past Issues

Translate ▼



Echosec user locates public adult services post on VK (above) and links the user to a dark web human trafficking operation in

Beacon (below)

Again, pivoting on key data is a powerful tool for connecting the dots in a human trafficking investigation. Data points such as username, phone number, or location are often shared between surface and dark web networks and give law enforcement a broader lens into human trafficking activities in their region.

Violent Crime and Gang Activity

Similar to trafficking investigations, dark web forums and social media networks can also reveal information about gang activity and violent crime in specific areas. Dark web forums and less-regulated social networks like 4chan are useful for finding discussions about current gang activities.

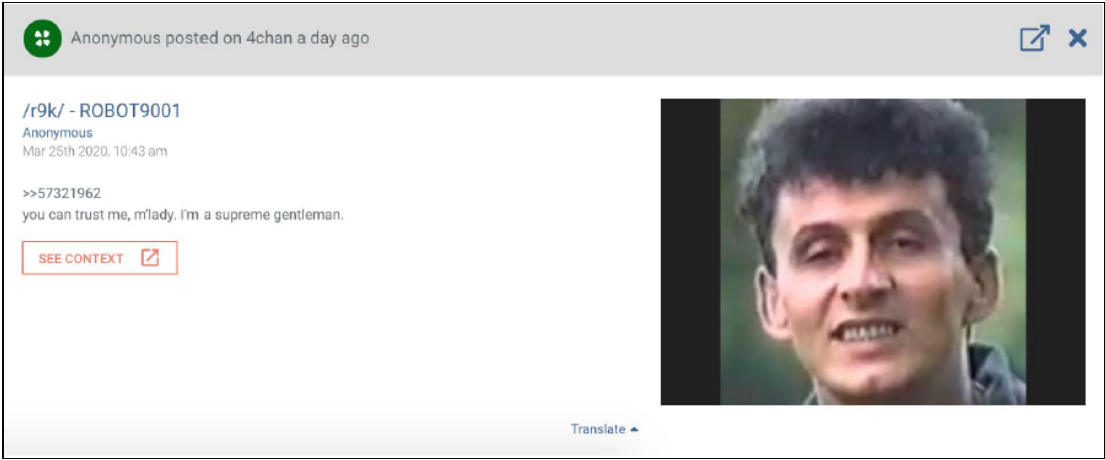


Deep web forum user discussing Hell's Angels activity in a specific location—as viewed in [Beacon](#)

Witnesses and insiders often use social media to post live streams or other public information related to criminal activity, such as a drive-by shooting. Law enforcement can use search tools to find and monitor this content across multiple networks to stay alerted to breaking incidents or find digital evidence.

Hate Crimes and Radicalization

Unfortunately, politically-motivated hate crimes, such as public mass shootings, are a common occurrence across North America. Perpetrators are often radicalized on anonymized online networks where content is less moderated. Hate-based discussions and manifestos, which often reference previous shooters and radical texts, are valuable for both predicting potentially violent incidents or individuals, and investigating post-incident.³

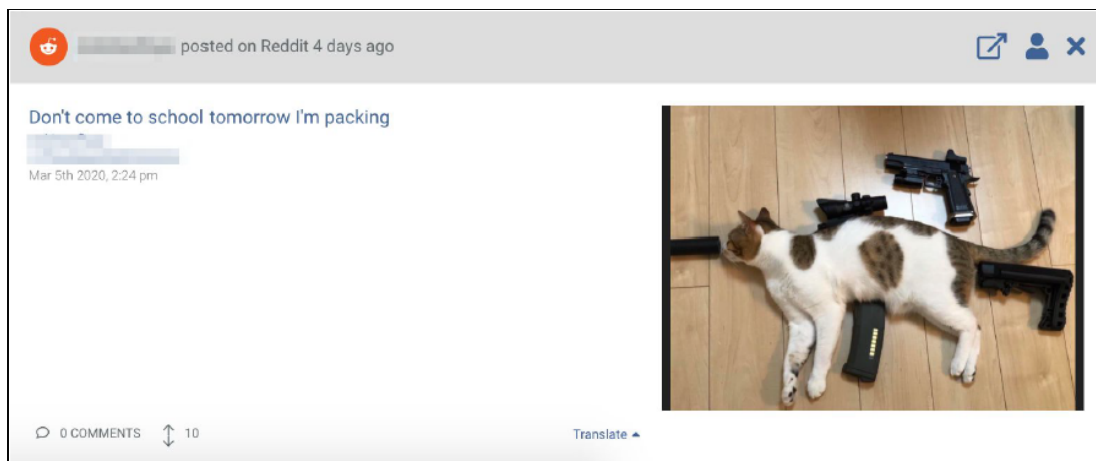


The active shooter reference “supreme gentlemen” posted by a 4chan user—discovered using [Echosec](#)

Specialized data discovery tools also allow law enforcement to search for phrases like

[Subscribe](#)[Past Issues](#)[Translate ▼](#)

they turn out to be pranks.



"Don't come to school tomorrow" post on Reddit—discovered using [Echosec](#)

Law Enforcement Is a High-Value Target for Cybercriminals

Beyond leveraging online data to support investigations, law enforcement is also faced with defending their personnel and data against cyber attacks and forms of targeted harassment.

In general, cyber attacks are becoming more advanced and widespread for most sectors. A total of 8.5 billion records were compromised in 2019, a 200% increase from 2018.^{[4](#)} The public sector, including law enforcement, is a high-value target for both malicious hacking groups and nation-state threat actors. In a 2016 survey, 44% of local governments reported daily attack attempts. Shockingly, a majority were unaware of how often they are attacked and by whom, suggesting a problematic cybersecurity oversight.^{[5](#)}

Attacks are often motivated by acquiring valuable classified intelligence, disrupting services as a form of hacktivism, or monetizing breached data either on the dark web or through ransomware. Public sector-targeted attacks have increased exponentially in the first few months of 2020 in response to the COVID-19 pandemic.^{[6](#)}

The public sector is commonly compromised as a result of successful phishing attacks, in which adversaries pose as a reputable entity and send malicious links or request sensitive data. Phishing is a lucrative strategy for attackers: in a 2018 Michigan-based security audit, 25% of randomly selected state employees clicked a phishing link.^{[7](#)}

As a result of a targeted attack, law enforcement agencies face:

- Loss of digital evidence^{[8](#)} and other internal data, such as login credentials
- Disrupted services, such as dispatch systems^{[9](#)}
- Slower investigation cycles

Subscribe

Past Issues

Translate ▼

- Millions in financial costs[10](#)
- Doxxing and harassment campaigns targeted at police officers

Protecting Law Enforcement Agencies

Like other criminal activities, law enforcement-targeted threats can be better prevented and investigated with access to relevant information from the right online sources. What does this process look like?

Locating Breached Data

The earlier an organization detects breach indicators, the more likely they are to reduce associated costs and impacts from any of the secondary consequences listed above. Some threat intelligence tools allow security teams to detect infrastructure vulnerabilities or suspicious network activity early on.

However, because of increasingly advanced attack techniques, detection often isn't possible until breached data is out in the world. When breach indicators go public, they tend to appear in obscure and unindexed online spaces that law enforcement may already be using to support other criminal investigations.

These sources include:

- **Paste sites**, which are popular on the deep and dark web for publicly and anonymously sharing blocks of plain text. Nefarious paste site use involves exposing breached data. Popular paste sites include Pastebin, PasteFS, and DeepPaste.
- **Dark web forums and marketplaces**. These sites offer users total anonymity, making them abundant sources of breached data dumps. Dark web marketplaces typically state where the data came from and offer a preview of available data, while dark web forums can act more like paste sites, where users dump breached data lists.

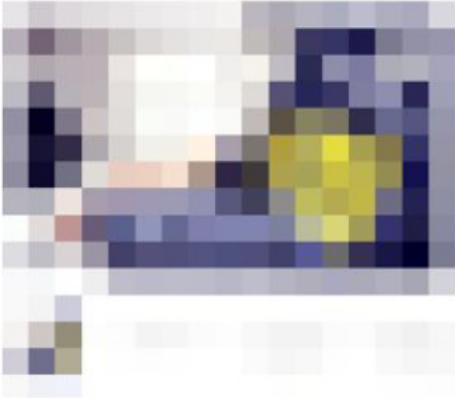
Subscribe

Past Issues

Translate ▼


Shop ▼AnnouncementsAboutTerms and conditionsMy accountHelp ▼

Home > Data Leak > FBI leak



leak

\$7.00

Breach to three sites associated with the 




Add to cart


Category: [Data Leak](#)

Description >

Reviews (0)

Description

Breach to three sites associated with the , a coalition of different chapters across the U.S. promoting federal and law enforcement leadership and training located at the 
 Exploited flaws on at least three of the organization's chapter websites allowed to download the contents of each web server.

Files from three websites:


Federal law enforcement breached offered for sale on the dark web—discovered using [Beacon](#)

- **Breached data repositories.** These repositories are publicly-available databases aggregating over 10 billion leaked records from known breach incidents. Repositories are continuously evolving as new breach events are discovered on the dark web and other hidden sources.

15 of 20

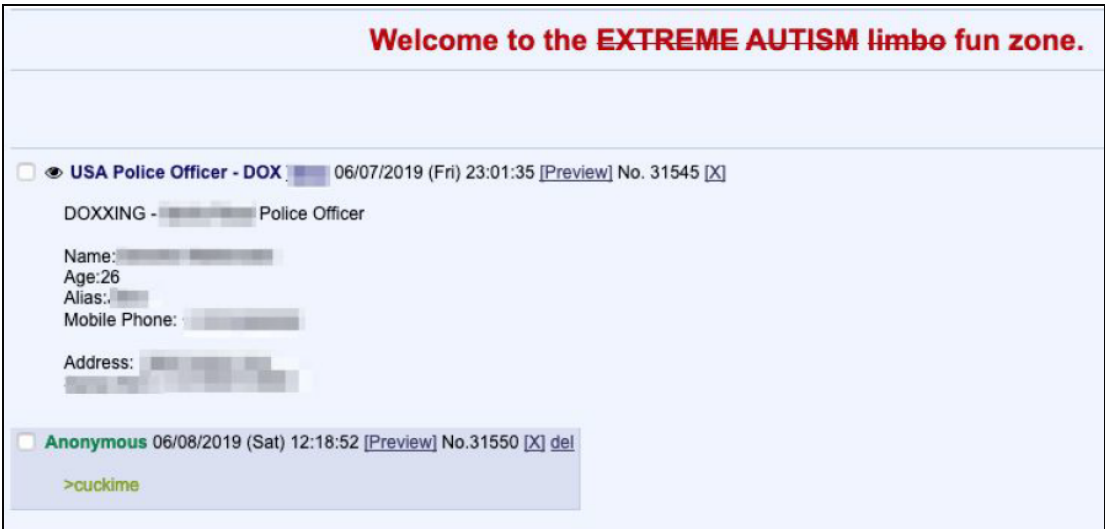
2020-11-16, 9:03 a.m.



Specialized search software allows law enforcement personnel to search these source types for entities unique to their organization, such as email handles, phone numbers, and names.

Finding Officer-Targeted Harassment

Breached data is often published on these unindexed sources in the form of a dox. A dox is a public disclosure of an individual’s personally identifiable information intended as a form of harassment. Doxxes often include full names, addresses, phone numbers, emails, and passwords, of the targeted individual and their immediate family members.



Officer-targeted dox on a dark web image board site—discovered using [Beacon](#)

Law enforcement personnel are often targets of these types of attacks as a form of hacktivism—for example, after a controversial incident or case in which a known officer was involved. Doxxing can expose law enforcement personnel and their families to harm. They can also compromise an agency’s network security if doxxed information is

[Subscribe](#)[Past Issues](#)[Translate ▼](#)

Doxxes are most commonly published on unindexed paste sites and deep and dark web forums, which are only searchable through specialized data discovery tools.

Identifying Service Disruptions

If a dispatch system or other critical infrastructure goes down in a cyberattack, alerts often reach social media faster than other sources as individuals become affected. Data discovery tools allow law enforcement officers to aggregate and search for content related to hacking or service outages across multiple sources so interruptions can be identified faster.

Reviewing Criminal Strategy Discussions

Anonymous dark web forums are often used to discuss current cyber attack techniques. These can be incredibly valuable for law enforcement as they offer up-to-date information about risks such as targeted malware, ransomware, phishing, and other attack vectors relevant to law enforcement. The ability to search for this information efficiently with search software allows security personnel to improve their infrastructure and inform personnel based on trending attack methods.

Conclusion

The public relies on law enforcement to maintain public safety and identify, investigate, and resolve crimes as quickly as possible. More crimes of every type involve some level of online activity, and investigators must adapt their strategies accordingly.

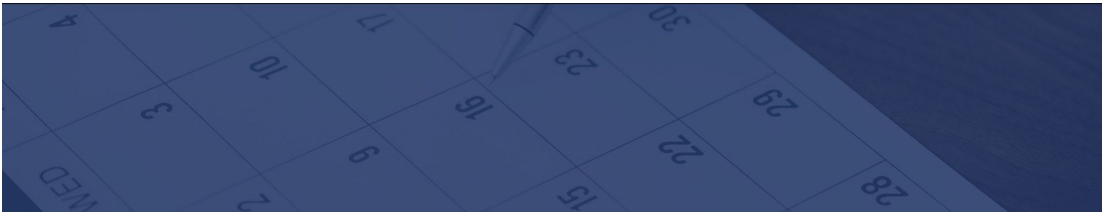
Unindexed areas of the internet, which include social networks (both widespread and less-regulated), deep and dark websites, and breached data repositories, are highly valuable data sources for law enforcement agencies. They offer a variety of threat data to support criminal investigations, as well as threat alerts targeted at law enforcement systems and personnel directly. Specialized search software enables safe and efficient access to relevant information from these sources—which produce an overwhelming amount of data on a daily basis.

As the demand for digital forensics and online data investigation grows alongside the rate of targeted cyber attacks, data search software is likely to become essential to agencies across the US and around the world.

Authored by: [Echosec Systems Ltd.](#)

To schedule a training course for your organization or team, please [contact us](#). To join

Upcoming Select Public Courses



Dates	Location & Time	Courses
July 24, 2020	Remote Delivery 1000-1800 EDT (1400-2200 UTC)	Investigating the Dark Web
August 19, 2020	Remote Delivery 0900-1700 AEST (2300-0700 UTC)	Investigating the Dark Web
August 24-25, 2020	Remote Delivery 1000-1700 EDT (1400-2100 UTC)	Social Media Intelligence & Investigation
September 14-15, 2020	Remote Delivery 1000-1700 EDT (1400-2100 UTC)	Advanced Internet Intelligence & Online Investigations

Don't see the course you're looking for? TII is pleased to offer a number of specialized and customizable in-house training programs for both the public and private sectors internationally. To learn more about what we can do to empower your workforce, [contact us](#).

Tools and Resources for the OSINT Professional



[Video DownloadHelper](#) - Firefox (and Chrome) extension for downloading videos on YouTube and similar sites

[Subscribe](#)[Past Issues](#)[Translate ▼](#)

around the world, including active cases and recoveries, and compare with global trends

[Image Search Options](#) - Firefox reverse image search extension

[Covid-19 Bibliometrics](#) - Database developed by scientists from UK and Malaysia to provide access to Covid-19 research publications

[Undo Close Tab](#) - Firefox extension that allows you to restore the tab you just closed

[Infotagion](#) - Independent, fact-checking service for Coronavirus information

[uBlock Origin](#) - Firefox extension that blocks content such as ads, trackers, and more

[Google Trends](#) - Milkshakes, pizza, and beach closures, top Coronavirus search trends

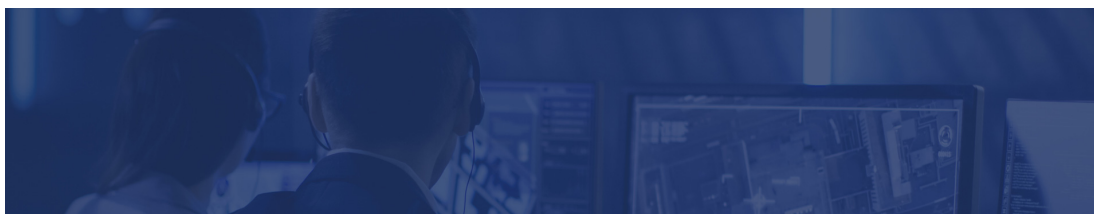
[Enhancer for YouTube](#) - Firefox add-on for improving the YouTube user experience

[Vaccine Mapper](#) - COVID-19 Vaccine Knowledge Base, designed to track the development of vaccines

[TripsGuard](#) - Database/listing of entry restrictions, rules, and quarantine information for different countries

Follow us on [Twitter](#) for our resource of the day, or visit our [Free Resources Knowledge Base](#) to see more resources like these.

"How-To's" and Articles of Interest for the OSINT Professional



["Find the Exact Date When a Google Maps Image was Taken"](#)

["5 great apps to keep your kids learning at home"](#)

[MIT launches 'Covid Tracing Tracker' project to track the deluge of Covid-19 apps](#)

[Subscribe](#)[Past Issues](#)[Translate ▼](#)

[A double-edged sword? "An official government mobile phone app could soon track millions of people in the UK in order to prevent a second wave of coronavirus infections"](#)

["How to spot a conspiracy theory when you see one" - How do we know when questions about the origins of Coronavirus are legitimate concerns and when they should be dismissed as a conspiracy theory?](#)

[Using AI, Bing can now return a "Yes" or "No" answer for certain natural language queries. This new search feature includes the one-word answer as well as a number of related excerpts from various sources.](#)

[YouTube takes action against conspiracy theorist spreading disinformation about Coronavirus, deletes David Icke's channel](#)

["Netflix Will Now Cancel Your Account Unless You Use It"](#)

["Our health data can help stop COVID-19-but we need strong safeguards to protect it"](#)

["How police are using technology like drones and facial recognition to monitor protests and track people across the US"](#)

Follow us on [Twitter](#) for daily articles and other interesting industry updates.

[follow on Twitter](#) | [friend on Facebook](#) | [forward to a friend](#)

Copyright © 2020 Toddington International Inc., All rights reserved.



[unsubscribe from this list](#) | [update subscription preferences](#)