silo
BY AUTHENTIC8

WHITE PAPER

Going After Criminals on Their Own Turf: The Internet

How law enforcement can stay safe in online Investigations

Protecting the integrity of an investigation is more difficult than ever online

Today, nearly all criminal investigations — not just cybercrime investigations — have the potential to include online research. Law enforcement professionals routinely look up persons of interest on open-source databases, social media, online marketplaces and web forums. They scour court websites, find personal records and uncover connections through simple as well as complex web searches.

Online research is crucial to building a thorough case, but it comes with an array of challenges that could affect the outcome of the investigation or put the investigator — or their organization — at risk. With every click in a traditional web browser, law enforcement professionals are giving away important details about their identity and their mission. And if the subjects of their investigation catch wind of either, they could go into hiding, disinform or retaliate.

To protect investigations, the law enforcement professionals that conduct them and the agencies they represent, it's vital to be aware of the inherent risks of online research — and what tools and tradecraft can be used to overcome them.

Why are online investigations risky?

The cybersecurity risks of the internet are well documented in daily headlines of ransomware attacks, dangerous vulnerability exploits and massive data breaches. In July 2019, the Los Angeles Police Department was involved in a data breach that released thousands of current aspiring police officers' personal records. A year later in July 2020, the BlueLeaks archive exposed the personal information of 700,000 cops.

These and other cyberattacks show the risk law enforcement agencies are up against simply because of devices and corporate networks connecting to the internet.

But there's another risk to those conducting online investigations: attribution.

Attribution could reveal your identity and intent

Attribution refers to all the identifiable details that websites collect each time you visit. These details are passed to websites by different sources, including the device and browser you're using. Combined, attribution details create a digital fingerprint that is extremely unique and can easily be used to uncover your actual identity.

Traditional browsers like Chrome, Firefox or Safari are built to track users and obtain an array of information about their device, browsing activity and more. These functions exist to tailor browsing experiences based on your location, device settings, browsing history, browsing behavior and details of the browser itself. Most of this information is monetized and resold.

While a bit creepy, most internet users tolerate such tracking. But for law enforcement professionals using the web as a resource for their investigation, it can cause major problems.

Details of your digital fingerprint are passed to websites from different sources, including:

- **Internet address and connection:** registered owner, subscriber information
- **Browser and device type:** OS, software/plugins installed, time zone, audio/video devices, cookies, HTML5 local storage, HMTL5 canvas fingerprinting, audio rendering
- **Unique online behavior:** social media connections, shopping interests, websites visited, account activity

This information ensures compatibility with the content that will be displayed (for example, if you're requesting from a mobile device, the website will display differently than on a desktop, or the language of the displayed content will match the language setting of your device).

Separately, these components may be insignificant, but all together they can help websites — and their webmasters — track and identify who you are, who you're working for and what your interest is in a certain site.

Learn more: **What's in your digital fingerprint and how to control it**

Using social media in law enforcement investigations

Social media has become one of the most robust sources of information for law enforcement investigators to quickly gain insight on persons of interest and their affiliates. However, social media brings with it another layer of risk due to the information it gathers about you. Here's an example:

Facebook receives "off-Facebook" activity; even while you're not on Facebook, it can collect information about apps you're using and sites you're visiting. So it's possible for Facebook to see you have an interest in aviation, you read Denver news, you've shopped at Galls.com (a law enforcement supplier), that you have an AT&T FirstNet account, you're interested in firearms, real estate investing and have been looking at events in the Washington D.C. area.

Take a break and disconnect your off-Facebook activity now

So even if your profile doesn't say you work for law enforcement, the details provided to Facebook could make it easy to guess that you do. This can be a problem when it comes to the friend recommendation feature.

Hazards of the friend recommendation

When a social media platform suggests a new friend, they look at your location, your mutual friends and searches you've completed. But if you're using your own profile while performing your investigation, the platform may suggest friends based on the person you've searched.

And if it's happening to you, you can bet it's happening to your subject — they see you pop up as a friend recommendation. You may also be appearing as a friend recommendation to confidential sources, putting them in jeopardy.

Learn more: Social media's value and danger to law enforcement investigations

5 challenges of online investigations

BLOCKED ACCESS

Cybersecurity teams block untrusted websites. While this is good IT hygiene, it can mean that investigators sitting behind the firewall can't access websites that may be useful to their case. Even if you're able to get an exception from the security team, you've lost valuable time, and you're still working in an unsafe environment.

UNTRUSTED CONTENT

Investigations could involve websites that deliver malware or malicious code, enabling infections or further tracking of activity on your device. If your machine isn't properly segregated, infections could spread through your network.

CHAIN OF CUSTODY

Collecting information online is just the beginning. It must be cataloged and stored securely to meet chain of custody requirements. If you want to collaborate and share information, it adds even more complexity.

ALERTING THE SUSPECT

Most websites track visitors in some degree of detail. Also, advertisers use visitor information to serve ads and make recommendations. If these trackers can see you, your suspect can see you.

RETALIATION

Once suspects know you're watching, they can decide how to respond. They may keep things in the cyber realm and launch an attack against your device or your network. Or they can take things offline and come after you in the real world, using the details of your digital fingerprint to uncover your true identity and personal information. Other retaliatory tactics are to go dark — as in shutter a website or social media account — or disinform to spoil the investigation.

Using the dark web in law enforcement investigations

Of all internet traffic, the dark web only composes a very small amount. But to leave the information past the surface web untouched is to miss out on information that could prove to be essential.

If information on the dark web is relevant to your investigation, you'll need to use special software to access it. Tor is often the tool of choice. While it does a great job of obfuscating your IP address, Tor still has some tracking mechanisms. The Tor Project website even hedges claims of complete anonymity saying, "Tor Browser aims to make all users look the same, making it difficult for you to be fingerprinted based on your browser and device information" (italics added for emphasis).

So if you think browsing Tor is automatically anonymous, think again. Details of your digital fingerprint are still attributed to you and passed to the dark website.

The dark web is also notorious for booby-trapping websites with malware built to track activity like keystrokes. If your browsing environment isn't isolated from your device or network infrastructure, you could be risking infection from these websites — for yourself and your organization.

WHAT'S THE DIFFERENCE? SURFACE, DEEP AND DARK WEB

Surface web: the internet most of us use daily (a.k.a open web, clear web). It's the traditional format of the web, composed of open pages easily accessed by search engines on any browser.

Deep web: sites that require login or subscription services, such as court record databases.It has some barriers to accessibility while being adjacent to the surface web and is typically accessed via the same browsers.

Dark web: the area of the internet that can only be accessed by using a specific software. There are different versions available, from the most well-known (e.g., Tor/ The Onion Router) to the lesser used (e.g., Freenet, I2P, ZeroNet).

Learn more: Understanding the dark web and how it can aid your investigation

Traditional safeguards no match for today's risks

Tools that used to be effective in protecting law enforcement networks and professionals are no longer working. Cracks can form in the patchwork methods that aim to provide airtight security, completely managed attribution and steadfast compliance.

Segregated network

Some organizations set up a different network exclusively for online investigations to limit organizational exposure to web-borne threats. This requires investment to set up and maintain. As it's run by people, it's also subject to human error. Investigators may find this setup cumbersome, too, as they have to switch services, machines or even locations to access the network or analyze evidence they've collected while using it.

And without lots of additional, equally resource-intensive measures, adversaries can still identify exactly who you are.

Private browsing

Most people use private browsing to keep others from seeing internet activity on that specific device. It clears cookies and data you've entered into forms. The problem is that information is still collected by supercookies and other tracking mechanisms that private browsing does nothing to prevent. Private browsing also does nothing to protect against web-borne threats.

VPN

With a VPN, you get a bit more anonymity as it changes your IP address and location, and it's still better than using your network, but there are many identifying details VPNs are helpless to disclose. And unfortunately, it still executes directly on your machine. Even if you do click on a malicious link using a VPN, you can still download malware.

Neutralizing security and attribution risks in online investigations

To protect investigations, the law enforcement professionals conducting them and the agencies they represent, you need the right tools for the job. The solutions discussed below address the security and attribution risks of online investigations, but also are built to support the tradecraft and expertise that their users exercise every day.

Cloud-based browsing to eliminate persistent tracking and maintain security

Cloud-based browsers execute all web code remotely, so it never reaches the endpoint, giving users a benign video display to interact with. Because of this isolation, cloud-based browsers can be used on any device or any network without the risks of web-borne threats.

Using a cloud-based browser not only enables law enforcement to isolate their investigative browsing from their device and network — protecting them from malicious content — it can also segregate browsing itself.

While all cloud-based browsers provide protection from malware to your device/network, not all provide anonymity during browsing investigations. Some can obfuscate connection to your organization, attributing to the cloud service provider, while others can obfuscate even that. To avoid persistent tracking between web sessions, these more advanced cloud-based browsers can provide a fresh, non-attributed browsing session every time they're launched; and paired with managed attribution, they can control tracking and attribution within a session.

Cloud-based browsers can also support multiple sessions with each executing its own virtual container and using different digital fingerprints at the same time. This can help investigators segregate and not cross-contaminate browsing sessions for different sites of interest, different investigations and different purposes (i.e., personal browsing vs. browsing for investigative purposes).

Managed attribution to conceal identity and intent

Managed attribution lets you control and customize how your digital fingerprint appears to sites that you interact with online. It gives you the ability to manipulate any number of identifiable details, such as keyboard and language preferences, time zone selections, browser and OS settings, and lots more. By matching these details to average site visitors of sites you're investigating, analysts and law enforcement professionals can blend in with the crowd and avoid tipping off investigative targets.

Managed attribution is delivered through purpose-built browsers for online investigations.

Spoofing geolocation to further change your digital fingerprint

Websites may block users coming from certain regions or IP addresses, or they may display different information to these visitors which could impact investigations.

In addition to changing digital fingerprint settings, investigators looking to manage their attribution can benefit from using a global egress network to spoof geolocation and appear as an in-region visitor.

Leveraging a network of internet egress nodes lets you adjust the location from which you appear to be visiting, showing a local IP address that doesn't refer to you or your agency. This ensures you can view and collect data as the visitor you desire to be, not the visitor you are.

Workflow tools to increase productivity

To keep up with caseloads, online investigators need tools of the trade at their fingertips. This means built-in solutions to the browser where investigations are conducted that support the key stages of research — access, analysis, capture and audit.

As described above, cloud-based browsers can simplify secure access to the web from any device or network.

In the analysis stage, built-in packet capture, source viewing and translation capabilities in the investigative browsing environment can greatly increase the efficiency. Automating multi-search workflows (preferred groups of specialized sites for different types of analysis) can also improve productivity, letting investigators run frequently used searchers across multiple sites in a single click.

When capturing data, small inefficiencies can add up. The ability to capture screenshots and videos, tag assets with URLs and timestamps, and save assets into case files from within the investigative browsing environment can save time every day. Automating data collection by scheduling recurring collections on various sites can also greatly improve efficiency; in addition, automated collections help investigators maintain tradecraft — even when they're not performing the capture themselves (due to time constraints, odd hours, etc.).

SECURE STORAGE

Data collected online must be securely stored off-network in the cloud to protect the organization from malware or similar risks. Using shared storage in the cloud also improves efficiency in collaboration, ensuring fellow analysts can properly access necessary information.

Lastly, to maintain compliance during investigations, all web activity must be logged, and all logs must be encrypted with organization-managed keys. If usage policies can be applied to a user and their cloud-based browser (rather than a device), the organization can seamlessly enforce and log investigator activity on any device or network.

For investigations that may lead to more formal reviews — by courts, regulators or internal teams — presenting evidentiary logs may be required. Presenting these logs and case materials requires centralized processes with strict custodial records. Investigators need the tools in place to track collections and monitor their workflows throughout their research.

Learn more: 13 tools to improve online law enforcement investigations

Protecting investigations in a data-driven world

The role of online research in law enforcement investigations will only increase. The time for erecting the right strategy around secure web use and best-practice search protocol is now. This will require consideration in terms of policy as well as which tools will support investigator tradecraft and organizational security. With the right solutions, law enforcement agencies can protect their network, their personnel and the integrity of their investigations and keep their communities safer.

About Silo for Research

Silo for Research enables law enforcement to gather intelligence and evidence securely and anonymously across the surface, deep and dark web. Built on Authentic8's patented, cloud-based Silo Web Isolation Platform, Silo for Research provides 100-percent protection from all web-borne threats and complete oversight of all research activity. Investigators can count on full online anonymity in an isolated browsing environment, and increase efficiency with an integrated suite of workflow productivity tools.

State, local and federal law enforcement agencies across the country rely on Silo for Research every day to protect their investigations. See how its managed attribution capabilities can make a powerful difference for your organization — visit our Experience Center now.

silo
BY AUTHENTIC8

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com