silo
BY AUTHENTIC8

WHITE PAPER

Why Online Investigators Need Managed Attribution

silo
BY AUTHENTIC8

Online research practices could jeopardize investigations

Online investigators often face hidden dangers that can jeopardize their mission. If subjects of investigations catch on to their work — by piecing together details about their identity and intent — they risk similar outcomes to an undercover agent whose cover has just been blown: danger to themselves, danger to their organization and a botched case.

That's why it's important that online investigators blend into digital environments and remain anonymous to the target of their investigation. Using private browsing or a VPN isn't enough. You need to understand how your online activity can reveal your online identity — what's "attributed" to you — and how to ensure anonymity to protect yourself, your mission and your organization. "Managed attribution" is key to minimizing risk, giving you greater control over the online identity you reveal to websites, social media and other internet activity in the course of your investigation.

Financial fraud, cybersecurity intelligence and law enforcement are some of the dominant drivers for online investigations. However, the practice of specialized online research has been expanding into dedicated teams that tackle fraud and brand misuse, corporate security and the emerging practice of trust and safety.

Understandably, the IT management and cybersecurity policies that oversee these teams block access to untrusted sites, leaving much of the deep and dark web off-limits, or with extra hurdles for entry. Yet those are hotbeds for criminal activity, and can be critical areas of research. Accessing unsafe online territory, though, often creates friction between analysts and IT, in addition to both cyber and real-world risk.

But even when necessary sites can be accessed, an often bigger and more complicated problem is concealing an analyst's identity and intent. Everything you do online — the sites you visit, the browser you use, the way you browse, the device you're on, where you're searching from — says something unique about you. With enough details, adversaries can understand who you are, the organization you represent and the mission at hand. They can then act to thwart or threaten your work.

To ensure successful, secure investigations, controlling the details of your digital footprint has become a vital capability. In this paper, we'll look at how managed attribution delivers that control and minimizes risk in online investigations.

INVESTIGATIONS COMMONLY AT RISK

- **Intelligence and evidence gathering:** For federal, local and private investigators building case files on specific targets, preserving chain of custody and evidence integrity is crucial. Tradecraft can fail without an airtight infrastructure and total anonymity.
- **Trust and safety:** Protecting web communities from harmful impacts may require online socializing with bad actors, making it essential to have an ironclad false digital identity to minimize risk.
- **Fraud and brand misuse:** Analysts need to rapidly identify and mitigate fraudulent activity targeted at a brand and its customers. All too often, fraudsters get tipped off and even retaliate.
- **Financial crime and compliance:** While payment card fraud, money laundering and related activities are escalating, many investigators are unequipped to follow leads to all corners of the web.
- **Security intelligence:** Whether investigating cyberthreats, malware, phishing, war-gaming or even physical threats, analysts face sophisticated adversaries who are likely skilled at uncovering online identities, and may respond with malicious attacks.

Understanding how you're tracked online

To protect systems and investigations against potential risks or threats, you need to securely access online content **without linking the research to yourself or your organization**. That starts with understanding how your online activity can be attributed to you, and how to minimize that exposure.

In a typical online connection, even if you cloak your IP address for web browsing, there's a significant amount of data collection ongoing in the background that many people never know about.

For example, websites and browsers can track:

- **Your internet address**: location and IP address, including registered owner and subscriber information
- **Attributes of your browser and device**: device type, operating system, audio/video devices, software/plugins/ custom fonts installed, device battery status, time zone and language settings, cookies and other unique identifiers (e.g., session IDs and employee number) and local storage of cached data
- **Behavior unique to you**: search terms used, websites visited, browsing patterns, time of use, social media connections, account activity and shopping preferences

Online research requires the same care as going undercover in the physical world. Regular browsers track your online presence, even when using private browsing and VPN.

Learn more about how you're tracked online and how to stop it in our Naked and Exposed webinar.

REGISTER NOW →

Combined, this information creates an extremely unique profile and can be used to identify you and your organization. As a consumer, it can be valuable for personalizing ads and content you receive. But as an investigator, it can be used against you, exploited by adversaries or targets of your research.

In addition to the above sources of identifying information, advanced tracking techniques like canvas, audio and battery fingerprinting also happen behind the scenes. Through these methods, browsers and websites gathering granular data about your device that help single you out as unique. When you stack up all the possible identifiers, you and your online investigation may be substantially more exposed than you think.

What does attribution risk look like?

Too often, investigators or organizations may think the online risks are exaggerated. Or they consider private browsing or using a VPN safe enough. But for sensitive research, particularly in the deep or dark web, leaving any attribution trace of your online activity can have severe repercussions, including:

- **Infect devices and networks with malware**: If your browsing environment is not isolated from your computer or network, malicious content could execute locally on your machine and potentially infect other assets on the same network.

REAL-WORLD EXAMPLES

Let's look at a few actual incidents that illustrate the impact of attribution risk:

- **Location, location, location:** A Fortune 100 company was plagued with malware through a phishing email from a foreign site. Even using a "dirty" network with a VPN, investigators were blocked from internet access because attackers saw requests coming from outside their geographic region. With a managed attribution service, analysts were able to obfuscate their online identity to blend in with local web traffic, and gain insights to understand the threat and execute preventive measures.

- **A visit from the FBI:** An analyst at on of the world's largest tech companies was investigating terrorism-related social posts in chat rooms frequented by terrorists. Working from home, the analyst believed the company VPN obfuscated their identity. However, an FBI agent in one of those chat rooms was able to identify participants, and showed up at the analyst's home as part of their own investigation.

- **You've been swatted:** At a leading tech company, analysts investigate alleged criminals who may be using their service, such as hate groups and cartels. Targets uncovered the name, phone number and home address of two analysts and retaliated by having them "swatted." Spoofing an analyst's identity, adversaries called 911 and reported a dangerous incident in progress, which triggered a SWAT team to descend on the analyst's home.

- **Endanger investigators**: Maintaining anonymity is crucial to both the analyst and the organization. If bad actors realize they're under scrutiny, they may retaliate with cyberattacks, or worse, physical harm or damage.
- **Destroy credibility with misinformation**: Another retaliatory tactic is to feed false information to analysts, which can destroy the integrity of an investigation.

How managed attribution is different

Managed attribution gives you greater control over what is or is not left behind as a traceable digital footprint. It is not the same as mis- or non-attribution, so let's clarify the difference:

- **Non-attribution** is when you try to stay anonymous for web browsing. But whether you use a VPN, dedicated network or "dirty" device, none of those solutions provide a fully cloaked environment. You are still at risk because browsers, websites and search engines collect data on many variables that can identify you.
- **Misattribution** refers to intentionally misleading your investigation targets about your identity and intent. Even with private browsing or "burner" machines, identifying data can still reside on the device that could be used by trackers and jeopardize your mission. Misattribution also does not alleviate the risk of malware in the course of the investigation.
- **Managed attribution** helps you blend into web environments by customizing how you appear to sites and people you interact with online. You can substantially reduce risk using a location-specific and context-specific digital disguise, with investigative work isolated from your business and personal browsing.

LEARN MORE IN OUR BLOG: MISATTRIBUTION VS. MANAGED ATTRIBUTION →

How managed attribution minimizes risk

Managed attribution gives you all the benefits of misattribution, but in a uniquely tailored and safer way. What should you look for in a managed attribution service?

The right purpose-built solution gives you the power to improve the results and impact of your investigations with capabilities that enforce tradecraft best practices, including:

- **Isolate online research:** Ensure your personal and everyday business browsing is separate from your investigative work. It's key to avoid specific actions and behavior patterns that can be used to identify you, and erode any intentional misattribution you've put in place. A managed attribution service (such as Silo for Research) enables you to use the same computer every day, but isolate your investigations in a securely anonymized, cloud-based environment.

  This web isolation platform ensures web code never reaches the endpoint, keeping your device and network safe from malware. Investigation evidence can be safely collected, stored, translated and shared through the solution, with a full audit trail.
- **Manipulate your online appearance**: Like a physical undercover agent, your online identity needs to blend in as appropriate to your investigation. Your solution should enable you to change your location, time zone and language settings to align with the region of your targets. You'll also want to avoid standing out by using that region's most common search engines and social media networks, and conducting searches using terms in the local language.

  TIP! To see the most popular OS/browsers around the world CHECK OUT THIS TOOL →

- **Use disposable browser sessions**: To minimize attribution risk, start fresh each time you browse. At the end of each session, have a system that clears all cookies and tracking data, erasing any evidence of your device or your online activity.
- **Automate for efficiency and productivity**: Your managed attribution solution should make it safe and easy to work efficiently, such as scheduling jobs, automatically downloading sites for later research, capturing content in isolation, as well as built-in tools for translation and audit trails you may need.

Safe and anonymous access to all areas of the web

Increasing the success rate of investigations relies on secure, anonymous access to credible information. Minimizing risk is key — and that requires a solution purpose-built to protect analysts, organizations and the integrity of data collected as evidence.

A managed attribution service like Silo for Research conceals identities during online research, providing the anonymity and access investigators need. From financial fraud specialists, to corporate security or trust and safety teams, to law enforcement, analysts can more safely, easily and efficiently conduct anonymous research to maximize productivity and improve outcomes.

See how managed attribution can make a powerful difference — schedule a demo today.