Managing Attribution in Online Financial Crime Investigations

Like an undercover agent, a financial crime investigator needs to blend in to protect their identity while performing their research and collecting evidence. Tipping off a subject of an investigation can spoil months of work, ruin an entire case, prevent investigators from further pursuing leads and turn analysts and their organizations into targets for retribution.

And while the majority of researchers realize that anonymity during research is critical, many organizations still conduct investigations using a traditional browser on their local computers. The problem is that even when accessing sites on the open web, a regular browser reveals a lot of information about the user that could be used by an adversary to reveal the researcher's identity and compromise their mission. A single visit to a site may not raise immediate red flags, but over time, a savvy criminal who has something to hide could piece together an investigator's profile based on their browsing habits and the trail of breadcrumbs they leave behind.

Partial Solutions Won't Provide Meaningful Protection

Many financial institutions have policies and guidelines about which sites their analysts can access under what conditions, and the methods they can use to try and conceal their identity. Let's look at some of these and understand why many of the DIY approaches don't offer complete protection from a counterattack or counter investigation:

Banning Access to the Dark Web

Banning analysts from going on the dark web runs contrary to their mission. Researchers, especially those investigating financial crimes, need to be able to follow the criminals' activity into the deepest corners on the dark web, where a lot of stolen information is offered for sale and many clues can be collected by listening in on specific forums. Most importantly, the risk of exposure and malware is not limited to the .onion sites on the Tor network. Any site can leave an analyst susceptible to identification or introduce malware to their environment. So a ban on accessing certain sites not only hinders the investigator's productivity, it does very little to shield them from being exposed or attacked by adversaries.

Using "Dirty" Machines to Protect Corporate Networks

The idea is simple: instead of using their standard company-issued PCs, analysts may access "dirty" machines that are not connected to the company's network and are imaged in a way that doesn't reveal their company affiliation. Organizations construct and maintain entire parallel infrastructures to isolate these dirty machines, which can grow costly in terms of IT overhead. An IT team must create, maintain, reimage, wipe out and recreate a persona on a new machine every time an analyst may have picked up a virus or needs to "burn" their identity after it's been compromised. And as parallel infrastructure is maintained by people, that means there's room for human error, so cracks may form in the isolated environment or the rudimentary schemes to maintain analyst anonymity.

This approach also makes it difficult for analysts to retrace their steps, as well as to transfer files and evidence between the dirty machine and the corporate network for documentation and collaboration with other analysts.

Using VPN and Private Browsing Mode

While VPN and private browsing (e.g., Google's Incognito Mode) can modify some parts of an analysts' online identity and obscure their location, they don't offer complete protection and still leave sufficient information behind for an adversary to grow wise to the fact that they're under investigation. A VPN can spoof a location, but it can't disguise other aspects of the "location narrative" — obvious giveaways such as language, time zone and keyboard settings, as well as browser, OS and device details common to a target site's visitors. Similarly, a private browsing option blocks certain cookies and other trackers but leaves many others active. Without manipulating these aspects that VPNs and private browsing leave behind, an analyst won't blend in with the regular traffic and could put their investigation and organization at risk.

Even when using VPNs and private browsing, there are still many ways that users can be tracked online; for example:

- **Canvas Fingerprinting:** taking a fingerprint of an image rendering engine on your machine
- **E-tags:** continuous tracking of objects that a user has viewed/clicked on
- **Battery Status API:** a way to identify a mobile device across sites

Additionally, when using a private browsing mode, it practically signals to adversaries that someone is snooping, prompting them to look into that visitor's online activity even more.

Although using any (or any combination) of these approaches is better than going into financial fraud research completely unprotected, they don't provide complete protection, guarantee analyst anonymity or help financial services organizations comply with company and industry regulations.

What is Managed Attribution?

When conducting online investigations, the researchers' goal is to blend in and not attract any unwanted attention, while still being able to browse safely and engage with their adversaries to glean useful intelligence.
The best way to accomplish this is by managed attribution — a way to proactively control one's online identity and shape what others perceive about them, their position and intent while browsing. When researchers can completely disguise their digital fingerprint, they have a much easier time staying undercover and finding the truth behind shady financial dealings, illegal activity, suspicious behavior and potential threats to their organization and clients. With a managed attribution tool, combined with remote browser isolation, financial crime investigators can safely access any content, perform screen grabs for evidence collection, translate pages, engage in conversations and even download items from the web without introducing unnecessary risk into their organization.

Capabilities to Look for in a Managed Attribution Solution

A purpose-built solution for managing attribution needs to have the following key elements:

- **Isolation:** A cloud browser ensures that all code executes off of the physical device and the company's network, keeping the organization secure during online investigations
- **Manipulation:** Manage elements of the online fingerprint, such as the user-agent string, including geographical location, time zone, language and keyboard settings, operating system, browser, etc.

- **Workflow:** Make sure that evidence can be captured according to company and industry requirements, analyzed efficiently and stored and shared securely with collaborators
- **Integration:** Connect the managed attribution solution with existing OSINT tools in the organization to assist in the collection of data

These capabilities will not only help protect analysts and their organizations, they can significantly improve the researchers' productivity in uncovering and analyzing threats. With a purpose-built managed attribution solution, analysts and their organizations can improve investigation quality and efficiency, reduce program costs and prevent further financial crimes and fraud.

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.