SPOTLIGHT REPORT

Issue 5

Your Online Fingerprint

You may want to think twice about that trail of digital breadcrumbs you're leaving behind...

What is it?

Your online attribution, or fingerprint, is the combination of technical indicators and behavioral patterns associated with your activities online. Technical indicators are things like IP addresses, cookies, and browser configurations, which are viewable by websites you visit. Technical measurements are easy for adversaries to monitor, but can be managed with secure managed attribution platforms. Behavioral patterns comprise your digital pattern of life: the websites you visit, how frequently you visit them, the times of day you are active online, and the kinds of searches you run. These are more difficult for adversaries to collect and analyze, but can also be more difficult and time consuming for you to convincingly control.

So What?

Left unmanaged, your online fingerprint allows adversaries to trace your activities over time, differentiate your accounts from typical users, or even attribute activities directly to your organization—putting you and those around you in harm's way.

Consider a few examples:

- **You access an adversary's website with your real IP address**. You've now revealed your approximate location and organization to anyone who's looking.
- **You access a website using an IP address that geolocates to Germany, but your browser reports a US time zone**. This not only indicates that you are in the US, but also that you are also trying to obfuscate your location.
- **You are operating a social media profile that presents itself as based in Singapore, but only posts online between 9-5pm, Monday to Friday in Eastern Standard Time**—a not-so-subtle indication that you are not truly in Singapore.

Now What?

Perhaps you can relate to some of the scenarios mentioned above. If you or someone you know is struggling to manage their online fingerprint, you may want to address the technical and behavioral information you're revealing about yourself.

Identifying your adversary, or who may impose scrutiny on your activity, is also an important consideration. Is your adversary an internet service provider? A website administrator? Maybe a social media user or even the platform itself? Whatever your answer, there may be times when you need to hide your fingerprint altogether, and other cases in which you purposefully create a misleading one. Either way, you'll want to choose the right tool to control those digital breadcrumbs, position the mission for success, and protect your personal safety.

Interested in learning more about the technical elements behind your online fingerprint? Take a look at these components, and keep in mind how they may make you vulnerable to adversaries when combined with your unique browsing behavior.

	What Is It?	Implication
IP Address	An Internet Protocol (IP) address is assigned to your computer by the operator of the network it is attached to. Your computer has an internal IP that identifies it on its local network and an external IP that identifies its network internet. Your external IP is often shared between all computers on your local network.	IP addresses identify either a single computer or the egress point of a larger network. IPs can indicate the rough geographic origin of network traffic.
Hostname	Hostnames are human-readable names mapped to the IP address of a computer using the Domain Name System (DNS). Not all computers have a hostname, but internet service providers often map hostnames to all IPs they control. Your hostname can be retrieved by a third party using a Reverse-DNS lookup of your computer's IP.	Hostnames can associate an IP with a corporate network, an internet service provider, a cloud provider, or a geographic area. Not all IPs are associated with a public hostname.
Cookies	Cookies are text files that contain identifying information stored in your browser by websites.	Cookies are used to identify a user or computer across sessions and websites.
Tracking Pixels	A 1x1 image hosted on a social media service or advertising network that is embedded in a third-party website. The image is loaded when your browser visits the third party website, transmitting cookies and any other identifying information to the social media service.	Tracking pixels allow social media services to monitor your activity across the internet for advertising and anti-fraud purposes.
DNS Servers	When you enter a website address into your browser, like www.google.com, your computer makes a request to a Domain Name System (DNS) server to translate the human-readable address into an IP address. Unless properly configured, your computer may send DNS queries to your local internet service provider rather than your geosite host.	Websites can check what DNS servers your computer is using to detect a discrepancy between the geolocation of your IP address and the geolocation of your DNS servers.
MAC Address	A unique serial number associated with the network interface of your computer. Used to identify your computer on a local network when negotiating a connection with a router or switch. MAC addresses must be unique on any given network.	Your MAC address is not normally visible to third-party websites, but is potentially discoverable by plugins (Java, Flash, ActiveX, Silverlight) or by desktop applications.
User-agent String	A string of text containing basic information about your browser and operating system transmitted by your browser when establishing a session with a website. It is commonly used by websites to determine whether you should receive the mobile or desktop version of a page.	Variation in operating systems and browser version numbers, when combined with other pieces of information, can be used to identify you across sessions.
HTML5 Canvas	A method for drawing 2D and 3D graphics on a webpage using HTML5 and JavaScript. Different computers will produce subtly different outputs when rendering the same set of instructions based on their graphics card and installed fonts. Differences in canvas image output can be measured with JavaScript and are particular to your computer.	When merged with other information, HTML5 canvas data can potentially identify your machine across sessions without storing information on your computer.

Ntrepid's Spotlight Reports are a series of research articles that examine emerging social media platforms and trends of interest to online analysts and operators.

NTREPID®