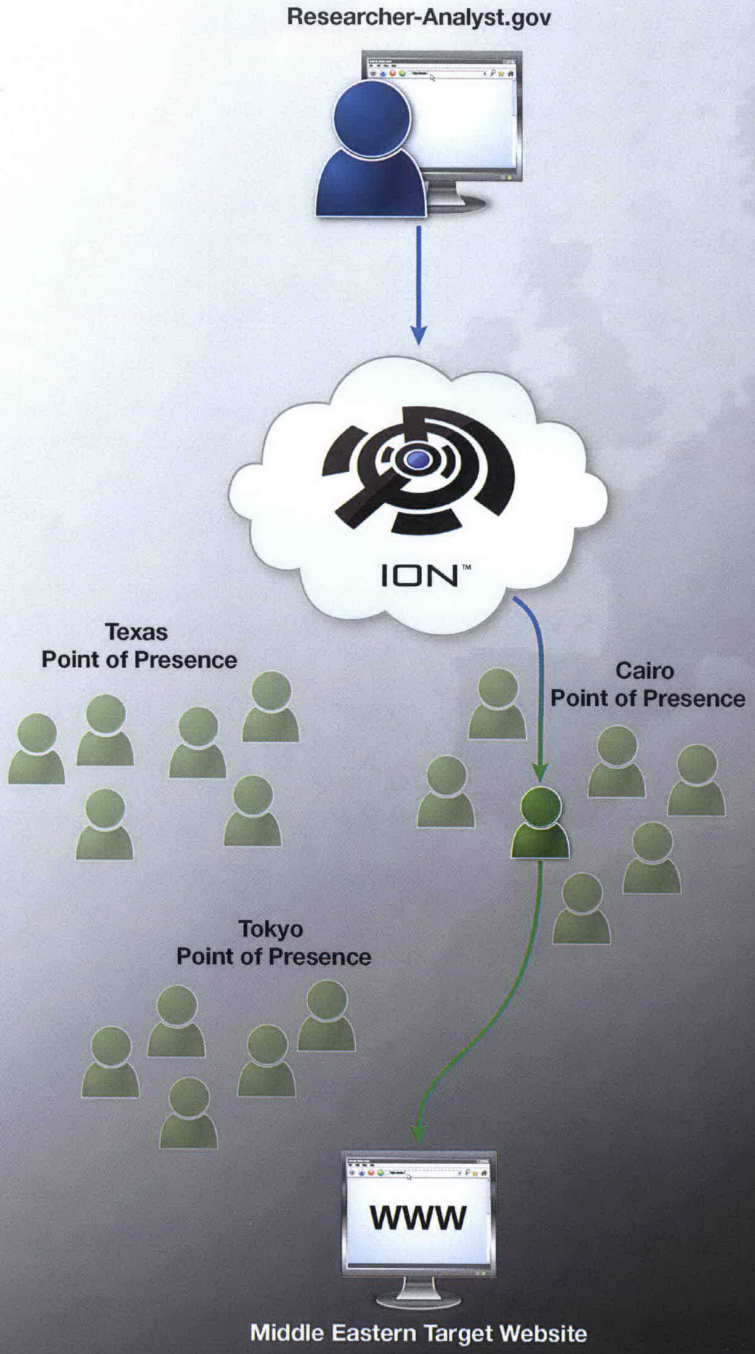
MISSION: RESEARCH & TARGETING

Enabling Secure Internet Operations

ION™

INTERNET OPERATIONS NETWORK



In the above diagram, all client Internet traffic is funneled through the *ION* network allowing the analyst in the U.S. to research and target enemy sites while appearing to originate from a foreign point of presence, in this case Cairo. The target website will never have reason to be suspicious of analyst visits, as all identifying HTTP information (location, operating system, language, etc.) will be appropriate and non-attributable to any U.S. entity.

Learn how ION can secure your Internet operations, contact us at

866-217-4072

Securing Research & Targeting Missions on the Internet

Ensuring Secure and Effective Research and Targeting on the Internet

Intelligence gathering on the Internet has become a critical component of modern collection and analytic efforts. Analysts must be able to collect reliable open source intelligence (OSINT), whether in support of criminal investigations, raw intelligence gathering, or advanced research and targeting. Without complete and secure access to target websites, the risk of being blocked or redirected to misleading information increases exponentially. These types of defensive tactics only scratch the surface of what targets can do as they become more aggressive and sophisticated in their abilities to detect unwanted visitors to their websites.

By using simple applications and other automated tools to obtain routinely updated and detailed lists of the unique IP addresses of any U.S. government entity, target website owners and other adversaries immediately gain an upper hand. Simply recognizing visitors from flagged government IP addresses allows targets to enact defensive tactics that prevent collection and compromise OSINT operations.

It's no longer enough to simply protect against "inbound" threats such as malware, viruses, and hacking. Non-attribution for "outbound" OSINT investigations is an operational necessity to remain anonymous and secure. Organizations that do not protect themselves are enabling criminals to uncover organizational affiliations, track online movement, and successfully counterattack based solely on the identification of the analyst's IP address.

Moving from Definitional to Operational Non-Attribution

Lightweight non-attribution solutions provide limited security and are only designed to protect Internet activity from being overtly tied to true identity. Solutions that provide no more than this minimum definitional standard of non-attribution are no longer sufficient to enable analysts to effectively conduct their online operations.

Government users need operational non-attribution capabilities that ensure critical information like real location, areas of interest, and patterns of activity cannot be detected. Simply stated, if a non-attribution solution does not provide security for these types of real world mission breaches, it isn't completely secure, and neither is the organization or its mission.

ION: The Internet Operations Network Non-Attribution for Research & Targeting

ION solutions provide critical capabilities that enable government organizations to collect reliable open source intelligence. Our proprietary technologies provide random, rotating IP addresses that are ordinary and untraceable, allowing analysts to blend in as "normal" visitors each time they conduct research on target websites.

In addition, *ION* offers multiple levels of indirection that provide a secure platform from which to conduct foreign and domestic research that is not attributable to any government entity, or anyone else that would raise suspicion. This capability is unique to our proprietary technologies, and is a critical component of a flexible, operational non-attribution solution.