

The average citizen's Internet activity is easily tracked, information that in the hands of tech-savvy marketers may be helpful or merely annoying. But in the hands of cyber adversaries, it's downright dangerous.

The Internet delivers so much information to our fingertips that it's no surprise the "Google it" phenomenon has expanded to our professional lives. Government employees, particularly in the fields of intelligence, law enforcement, national security and defense, make highly effective use of the Internet as a research tool, but more emphasis needs to be placed on ensuring cyber adversaries can't follow someone's online and open source searches back to sensitive government networks.

Even the U.S. intelligence community may not be doing a good enough job in helping Web-surfing analysts hide their open source research, and some government agencies don't attempt to hide their research tracks at all.

A perfect storm of conditions has brought this danger to the forefront: Overstretched intelligence collection resources have spurred the growth of open source intelligence, or OSINT, now referred to as the "source of first resort"; the digital information explosion has made open source research highly lucrative; the high operations tempo of intelligence analysts has cut severely into training time and tradecraft development; and cyber adversaries have grown tremendously in sophistication.

For intelligence analysts competing for scarce traditional collection resources, the growth of the Internet provides ample new digital information that can help meet information requirements. A recent Cisco Visual Networking Index found that about one-quarter of all Internet traffic consists of published reports, documents, website content, comments and other postings on accessible Web pages, including social networking sites. The law enforcement community also benefits from open source research, particularly publicly shared information on social networking sites.

The danger is that not everyone is adequately informed of the threats such Internet activity can pose. While professional intelligence analysts (those conducting first-level analysis) are usually well-trained with strict oversight and control of their research methods, all-source, fusion or "ops intel" analysts at the unit level frequently don't have the same access to training or emphasis on open source tradecraft. They often use open source research to plug intelligence gaps in support of operational planning or assessment, and sometimes even operational staff planners are tempted to Google their way through intelligence gaps when intel support lags.

Internet users must understand that unprotected open source research, conducted from attributable network domains (those that reveal the type of organization you are affiliated with, for example a .gov or .mil network), invites operational and cybersecurity risks. Today's cyber-savvy adversaries can easily determine that they are the subjects of online research from government Internet proxies. Not only does this create an operations security threat, tipping off operational focus areas, but it opens the door for malicious actors to adopt cyber countermeasures or mount exploitation campaigns against government networks to gain access to unclassified sensitive information.

Widely deployed network defense tools such as anti-virus software and firewalls protect networks from incoming threats, but they do nothing to mask an organization's IP address when users venture onto the Internet. Government users (particularly OSINT novices) operating on the Internet in an unprotected manner leave a trail that can lead cyber adversaries back to high-payoff, data-rich government networks.

One of the best ways to mitigate this vulnerability is to use non-attributable Internet connections, a solution many workers in the intelligence community have used for years. However, existing non-attribution measures may not stand up well to sophisticated cyber adversaries, and they need to be upgraded or modified to meet current cybersecurity needs.

Non-attributable access allows government users to conduct open source research and Internet

operations in an environment where their government affiliation is obscured. There are many reasons why government personnel should not reveal their analytic interest in particular topics and subjects on the Internet. The cover of anonymity is essential for intelligence analysts conducting open source foreign intelligence, or homeland security and law enforcement officials investigating hacking activity or monitoring an extremist Web forum.

Non-attributable networks are critical to conducting cyber reconnaissance of adversary networks or tracking criminals via their social media posts. Analysts supporting diplomatic or information operation missions may need quick and reliable access to foreign websites when developing sociocultural understanding in support of strategic communication, humanitarian or crisis operations.

Beyond national security, organizations such as the Department of Agriculture may need to research foreign crop or livestock conditions, trade markets, etc., but their users don't know they might be stumbling onto malicious websites or can be tracked by foreign intelligence services through their own digital footprint.

Not only can visited websites be a source of malware, but browsing activity alone reveals sensitive information — a digital footprint — about your computer and network, particularly if the research activity is persistent or repetitive. Every time a user visits an Internet site, their Internet Protocol (IP) address is recorded in that site's Web server log. Basic analysis of such logs enables administrators to establish cyber personas of their frequent visitors.

In addition to your IP address, US-CERT, in its “How Anonymous Are You?” security guide, explains that the following specific information is revealed every time you visit a website:

- Date and time of visit.
- Domain name, such as .mil or .gov
- Software details, including which browser and operating systems you use.

“If a website uses cookies, the organization may be able to collect even more information, such as your browsing patterns, which include other sites you've visited,” US-CERT notes.

When aggregated, organizational users who reside on common network IP addresses, with a characteristic network configuration and similar data handling practices, leave a highly targetable digital footprint for adversaries to pursue.

Once a cyber-savvy adversary is tipped off to “suspicious” monitoring of their websites, a little further cyber exploitation of suspect IP addresses can reveal even more computer and network details that contribute to the cyber profile of a government user. Once adversaries identify a suspicious “footprint,” a quick search of the IT systems and suites purchased, installed or maintained by U.S. government organizations completes the puzzle, and a particular IP address is tagged as government or law enforcement affiliated.

Think this is hard? Check out the “Careers & Employment” sections on corporate websites of vendors who provide IT support to your organization. High turnover in the IT field means frequent job advertising, and those employment ads list required skills specific to IT products and services affiliated with your organization's networks — valuable details used in compiling a digital footprint.

## **Adversary Countermeasures**

Once a digital footprint is established, critical information about your organization's mission sets and operational focus is revealed through the analysis of visited websites, and analysts can become victims of cyber countermeasures.

At a minimum, research subjects alerted to government interest can block access to their websites from incoming .gov or .mil addresses, or they can move or take down their site altogether. Going a

step further, adversaries can spoof government research efforts by re-directing “suspicious” IP addresses to fake websites that provide minimal or even false information. Worst case: Cyber adversaries introduce malware on the spoofed website, ensuring that unwanted visitors download malicious code upon accessing the page. The malware might be spyware that facilitates further reconnaissance, or worse, delivers malicious code that exploits unpatched vulnerabilities in network systems.

The government user's network now becomes a target for intelligence collection and social engineering. This can take the form of well-crafted spear phishing campaigns, using reference terms from your own browsing history to gain your trust and penetrate your network.

## **Protection Shortfalls**

So what has traditionally been done to protect government networks from dangerous Internet practices? The simplest measure involves local base network administrators blocking access to foreign or other “dangerous” websites; government users get an “Error: your firewall blocked access” message when trying to browse certain sites. While this is a sound network defense measure, it can severely impair research efforts.

More often, one or two government computer terminals are connected directly to a commercial Internet service provider. Users are then allowed access to the Internet through a virtual local area network on the government domain. These open access terminals tend to be located in common areas or near the IT Help Desk, sometimes a considerable distance from analyst workspaces, making them rather inconvenient to use. Depending on the configuration of the VLAN, performance and connection reliability may also be affected, hampering research efforts.

Furthermore, the associated IT equipment and network configurations in use usually conform to government standards because the ISP-connected computers come from regular IT stock and therefore match the profiles of known “government” boxes.

Finally, the commercial Internet connection in use resolves to a single IP address in a particular city. A cyber adversary who sees an IP address whose computer and network details match established government profiles simply Googles known government facilities and organizations hosted within that geographic area, and develops a list of possible matches.

More robust legacy non-attribution measures were implemented by the IC to “anonymize” Internet activity through the use of proxy or anonymizing servers or virtual private networks. In the case of anonymous network proxy servers or software, several limitations exist: The proxy can be slow in loading desired information, browser add-ons can still be used to reveal the source IP address, and websites being researched can choose to block access from users browsing via anonymous proxy servers.

Furthermore, if anonymizing services make use of U.S.-based servers for their connection, users still divulge a U.S.-centric digital footprint — problematic when researching foreign websites. VPNs also reveal information about the user's cyber profile, namely the browser, the operating system and the language-related character set in use, all of which can reveal a U.S.-centric cyber presence.

Other more exotic solutions such as Tor, which combines encryption and multiple proxy server hops, may unknowingly compromise users by routing them through rogue exit nodes. These nodes are hosted by adversaries who act as members of the Tor network, all the while intercepting and logging your Web traffic.

A final consideration is: “How do I want my cyber profile to appear on the Web?” Yes, a user may appear “anonymous,” but guess who else uses anonymization measures: cyber criminals, traffickers and child pornographers. The effort to achieve anonymity can itself draw unwanted attention to online activities — users begin to look suspicious in their effort to “not look suspicious.”

Today's cyber adversaries are complex and sophisticated professionals with access to funds and resources. They freelance and rent their services and tools to international criminal networks, foreign intelligence services and extremist groups, and understand anonymization far better than users do.

Users need to find different and more effective non-attributable Internet solutions that are also agile enough to keep up with evolving cyber threats. Contrary to most current approaches, the goal of today's open source researchers shouldn't be an anonymous profile but rather an inconspicuous one.

Effective non-attribution can be achieved when Internet users apply a multipronged approach that helps them to inconspicuously blend in to, rather than try to hide in, the World Wide Web. Any government agency that has a need for open source Internet research should implement a secure and comprehensive non-attribution program to minimize cyber vulnerabilities and maximize open source research opportunities. n

*Retired U.S. Air Force Lt. Col. Andrea L. Hlosek is a cyber-security and operations consultant to Webhead Inc., based in San Antonio.*

Source: