Protect Your Company
By Taking Your Network Undercover

An Anonymizer White Paper

Introduction

The Internet has become an indispensable way for people to obtain critical information for both their business and personal needs. The Internet drives the hottest stocks on Wall Street, shapes technological innovation, and fills the pages of the world's presses. The Internet also creates new ways for citizens to communicate, congregate, and share information of a social nature. It is obvious that the Internet has and will continue to change the way we live.

Unfortunately what many web surfers may not be fully aware of is the fact that they are often providing valuable information to the websites that they visit. Through the use of Internet surveillance technology, web administrators are able to gather information such as the visitor's domain name, IP address, or even the visitor's geographic location. One of the main purposes that companies use these surveillance tools is to prevent certain visitors, such as competitors, from accessing a site to obtain business information that can be used against them.

When a competitor is detected accessing a website, the web administrator can completely block access to that site or post a custom tailored website specifically designed to mislead the competitor with false information. For example, when one low-cost airline first detected that their website was being viewed by a competitor they used their counter-intelligence tools to block access from that domain location. Now they have the capability to post inaccurate fare information intended to mislead the competitor.

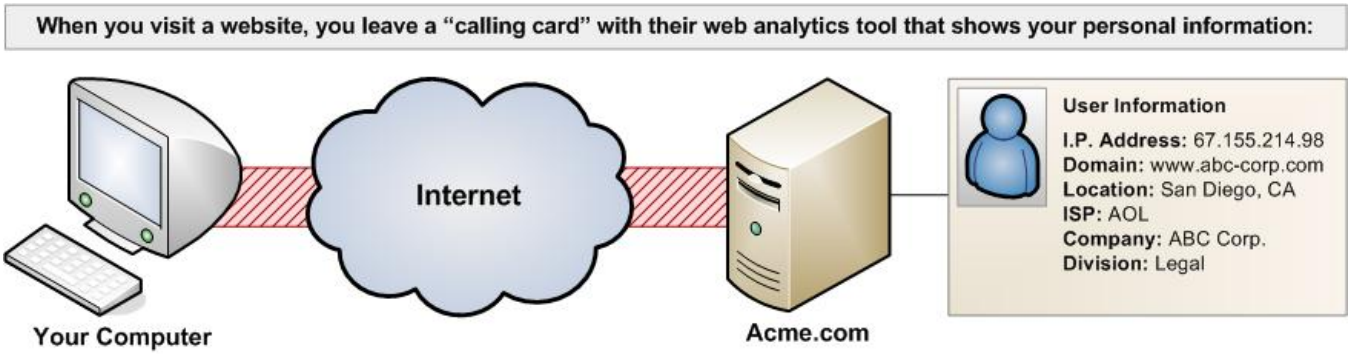
In another instance, an Arab news service posted different editorial content depending on the IP address of the website visitor. For example, Web surfers from the U.S, Britain, or Australia were presented with pages representing a certain point of view about events in the Middle East. When the same website was accessed by web surfers from an Arabic-speaking or Islamic country, a completely different set of editorials were presented, touting highly anti-Western, anti-Israeli, and anti-Semitic views.

The Anonymizer enterprise architecture coupled with Chameleon Network technology enables users to maintain a level of anonymous access to public information. Through the use of this technology, Anonymizer has become a leading enterprise service provider for businesses that require unobstructed access to specific sources of public information for focused research. This service allows businesses to take immediate action on opportunities and events without disclosing their corporate identity to competitors.

To better understand the advantage that Anonymizer Chameleon provides to its customers, it is important to understand how some enterprise organizations use tools and technologies to recognize, block and alter their web content. This white paper will accomplish this by presenting the Anonymizer Chameleon Network and the methodologies that are employed to mask corporate identification, restoring full access to all publicly available web-based information.

How Enterprises Recognize and Exploit Internet User Information

When you surf the Internet, your computer makes a direct and unprotected connection to the server where the information that you request is stored. For that server to send Web content back to you, it must know your computer's IP address. Once that address is obtained, it can be used to obtain additional information such as your domain name, the part of the world that you are located in, the name of your ISP, and additional details about your corporate network. (See diagram on next page.)



Web administrators can analyze your surfing behavior when you visit their sites. Much of the information that is gathered about you is tracked from your IP address. When you connect to a web page, you may also be implicitly connecting to other servers which can monitor your click-through activities. For example, most banner ads on commercial websites are actually served by servers run by specialized advertising companies. From an enterprise perspective, once a competitor knows your company's network ID, they can employ a technique called "Internet Counter-Intelligence" on your network. With this capability the site can build a detailed profile of your interests and likely future plans as well as provide misleading information, including different prices, skewed dynamic pages, or even complete alternate versions of the entire web site in extreme cases.

Additional Internet Counter-Intelligence Threats	
Competition • Inadvertent exposure of confidential research and Software can be provided to your competition. • Early warnings can be provided to competitors of possible or planned mergers and/or acquisitions. • Exposure of new product development plans from research activities.	**Data Integrity** • Planted or misleading information may be received, based on the source of queries. • Obstructed access to "specific" research by outside sources can be launched, blocking your IP address.
Security • Advance warnings to the targets of confidential investigations or exposure of research can be generated. • Unintended leaks of investor information or warnings that specific stocks are being targeted by the financial sector. • The potential for possible exposure of sensitive client information is increased.	**Operations** • IP addresses can be traced back to the originating computers on which on-line research is performed. • Hacker attacks against networks can be enabled through automated counter-probes launched by Web sites. • The risk of subjecting your organization and your employees to an influx of spam email, which degrades network performance and wastes server resources. • Possible exposure of your covert operations and/or operatives.

Enterprise Web administrators have a number of analysis tools at their disposal that give them the ability to not only detect and analyze inbound traffic to their websites, but also to perform many of the Internet Counter Intelligence techniques that have been described. These tools are commonly referred to in the IT industry as "Web Analytics."

Web Analytics employs tools and services that can gather user data from the Web server logs or collect it directly from the visitors' browsers. These services are particularly adept at providing a global view of visitor activity on multiple enterprise sites. Performing Web Analysis makes it possible to track visitor activity, including the geographic locations of visitors. In addition, web administrators have the ability to view an individual's click path while surfing their website.

Web Analytics can also analyze the surfing behavior of visitors to a website, tracking the pages within the site that are most frequently accessed, and the files that are downloaded. The result of the information that is collected is provided in the form of tables, charts, and graphs. It is this aspect of Web Analytic functionality that can identify specific IP addresses and domain names, which in turn can be used to prevent access from locations that are deemed a competitive threat.

Some of the most popular Web Analytic tools that are found in the business marketplace today include:

- **WebSideStory®**
- **Urchin™**
- **Core Metrics™**
- **Click Tracks™**
- **Deep Metrix®**
- **WebTrends®**

Case Study: A Costly Lesson to Learn When Your Web Activities are Being Monitored

Note: The details of this case study are based on actual customer circumstances. Due to Anonymizer's non-disclosure policies, the names of these companies and their industry focus have been changed to protect their true identities.

Customer Profile: Hilboro Software, an enterprise software development company.

Customer Environment: Web Analytic software exposes Hilboro's covert research activity conducted on a competitor website.

Customer Situation: Awareness of pre-acquisition activity by the competitor has created a competitive bidding war for the firm.

A large enterprise software company, Hilboro Software, held a meeting with its lawyers, merger and acquisition (M&A) consultants, investment bankers and board members to develop a plan on purchasing one of their major competitors, JRASoft, a firm specializing in the development of Java J2EE-based portals. All the attendees left the meeting and scoured JRASoft's website for more information on their upcoming acquisition. As part of their investigative process, they looked at the firm's investor relations information, white papers, press releases, technical spec sheets, and other financially-related information that had been posted on the site.

Due to the use of their Web Analytics tools, JRASoft noticed a substantial amount of traffic coming from the Hilboro Software domain, as well as other IP addresses representing the domains of organizations that JRASoft was familiar with. This included Hillsboro's investment bank, legal offices, and their M&A consultants. Over the past year, JRASoft had identified these series of IP addresses which the JRASoft

system administrators placed on a competitor "watch list". Digging deeper, they discovered that this particular set of IP addresses were accessing a variety of web pages representing information from their legal department, investor relations, strategic partnerships, financial affiliations as well as the backgrounds of all of their board members. Based on their observations of this activity, coupled with the identification of the IP addresses, JRASoft concluded that they were about to be purchased by Hilboro Software.

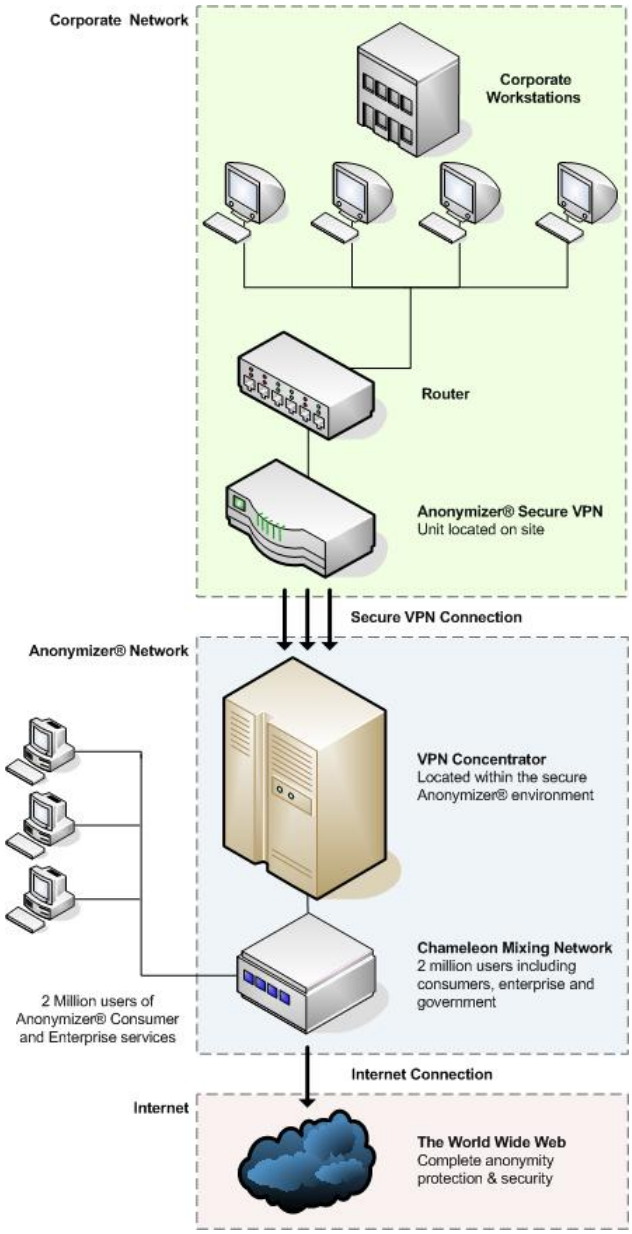
That afternoon JRASoft contacted a third competitor in their industry, Mercurial Development, a software firm specializing in .NET application development. JRASoft informed them of their analysis and the possible acquisition that they believed was about to take place. As a result of this information, JRASoft encouraged Mercurial to begin negotiations with them or risk being shut out of this portion of their industry all together. Mercurial gathered their executives together, developed an acquisition plan of their own, and begin negotiations with the chairman, chief executive officer and the rest of the board at JRASoft. When Hilboro found out that Mercurial was negotiating separately with JRASoft for a possible acquisition of their own, a bidding war broke out between Hilboro and Mercurial.

In the end, Hilboro "won" the bid and purchased JRASoft, however the final closing price was elevated by $15 million more than they originally had planned on paying. Unfortunately, this was a costly lesson for Hilboro to learn but a lesson that any company in a similar situation only has to learn once.

Achieving Inconspicuous Access with the Anonymizer Chameleon Network

The key to achieving completely discrete Internet surfing is a function of being able to use an IP address or a domain name that appears to be anonymous to the websites that are being visited. This is achieved by providing users with IP addresses and domains that remain unrecognized by the website, appearing to them as an ordinary website visitor. This is the concept behind the Anonymizer Chameleon Network.

Anonymizer provides this covert capability by licensing numerous legitimately registered domain names. Then, using various external ISPs, Anonymizer establishes a series of IP addresses for this large group of domains that are used by the subscribers to the Anonymizer Network. Each time a subscriber logs onto the Anonymizer Network they are assigned an "identity" from a large pool of thousands of IP addresses which they can use while they are surfing the Internet. This mix of IP addresses and domains is constantly exchanged and re-purposed for all of the subscribers that are logging in and out of the Anonymizer Chameleon Network. In addition, the Anonymizer user has complete control over this IP assignment process, which can be changed at a specified frequency. This provides the user with complete discretion, preventing any outside organization from detecting the actual identity of their computer or their corporate network.



The Anonymizer Chameleon Network provides Internet anonymity in the following way:

1. An Anonymizer Secure Virtual Private Network (VPN) network router is attached to your corporate network where all outbound Internet traffic is re-routed to the Anonymizer Chameleon Network.

2. Once inside the security of the Chameleon Network, a VPN Concentrator consolidates the network traffic, and securely assigns it to one of Anonymizer's servers (SSL) using Triple-DES or AES Encryption, two of the most secure encryption standards used today.

3. Next, the corporate network traffic is sent to a Chameleon Network Mixing Server where it is mixed with tens of thousands of different IP addresses and hundreds of registered domain names. The server randomly chooses an anonymous IP address and assigns it to the user from your corporate network.

4. Using this new generically masked IP address, your users access the World Wide Web with complete anonymity, protection, and security.

5. When a Web administrator attempts to identify your domain name or IP address, your users blend discretely into the general visitor population, in a "Chameleon-like" fashion.

While surfing with Anonymizer, users are protected from website logging, tracking by online advertisers, hacker attacks and exploits, network monitoring by ISPs, and other threats. Since Anonymizer's core technology is server-side and platform-independent, end users don't have to download client software or adjust their system configurations.

Security is one of the key issues that are frequently on the minds of many new users to the service. The Anonymizer Network allows users' access to the Internet through a series of servers and proxies that never write any data to disk. This provides Anonymizer customers with total privacy and security from identity disclosure. Because user information or the sites that are visited are not recorded on any network server, Anonymizer can guarantee its members complete user privacy even in the event of a breach situation. As a result, Anonymizer is unable to provide information on any of our clients' Internet history or surfing habits to any law enforcement or regulatory organization.

An additional advantage that The Anonymizer Network provides is the ability to change a user's designated regional location, a feature that is referred to as "Geographic Distribution". Certain portions of an IP address designate the country from which a web surfer resides. Under certain situations, web sites that contain governmental, geo-political, media-related, pricing or censored information will alter

their content based on a user's regional IP address. In the case of the official Chinese government website for example, web surfers in China will see a different set of content than web surfers in Taiwan.

Anonymizer allows a user to choose to use IP addresses for a different geographic location so that the site's web server will think that the visitor originates from that country or location. This feature is especially useful for researchers, such as the news media, that would like to compare the internal web content of a targeted site, to the information than is being presented to the outside world.

Anonymizer Enterprise Solutions and Service Advantages

Anonymizer offers a series of solutions that help small, medium, and large enterprise customers combat the Internet Counter-Intelligence problem for their business.

Anonymizer Enterprise Chameleon – An organization-wide protection solution provisioned via the Anonymizer Chameleon Network and its VPN/Traffic Mixing systems. Anonymizer routes all traffic from your corporate LAN to the Internet through the Privacy Proxy network, effectively hiding the source of the traffic and blending it with the traffic from millions of other users. The Chameleon Proxies™ prevent the destination site from knowing the true identity of the Anonymizer customer visiting it. The process is completely transparent, allows 100% functionality for all Web sites, and requires no software on the end user's computer. Only a single server is installed at the client facility.

Anonymizer Enterprise Client Chameleon – In situations where it is not possible to use the Chameleon Network router, such as the case of frequent business traveler or an enterprise that prohibits the installation of "un-approved" network hardware, Anonymizer offers the Anonymizer Enterprise Client Chameleon, a software-based solution with the complete functionality of the Enterprise Chameleon router. The Enterprise Client Chameleon is also useful in situations where the systems that access the Anonymizer Chameleon Network may be located in geographically diverse offices or locations apart from the central location where the Chameleon network router is located. The Client Chameleon solution offers the same level of online anonymity without compromising any "trace-back" capability. This ensures that the discrete identification of the client on any of the corporate workstations is retained, similar in functionality to the features of the Enterprise Chameleon solution.

The Anonymizer Enterprise Client Chameleon is also highly effective for employees that use wireless-enabled notebooks. These devices have been shown to be highly insecure and are often open to outside intrusion and identification. With the Anonymizer Enterprise Client Chameleon, secure tunneling technology is employed that ensures that each wireless Internet connection is 100% secure.

Anonymizer Intelligence Chameleon – A network-wide solution that allows corporations, law firms and government agencies to safely and privately perform a large volume of repetitive or automated research in conjunction with their web harvesting tools. Some examples might include the collection of competitive pricing, analysis of large volumes of dialog within chat rooms, or automated media tracking. Anonymizer's privacy technology facilitates this type of on-line research in a safe and anonymous fashion without requiring the intervention of IT personnel.

Anonymizer has also built into the Chameleon Network several infrastructure advantages that ensure consistent uptime, robust security, and complete network discretion. These specific advantages include:

- Biometric access control systems restrict and regulate access to the Chameleon Network facility.
- All network and server equipment is contained in locked cabinets within the network facility.

- Optional round-the-clock, 24/7, and "spare in the air" support programs are available to all Anonymizer customers.

- High-security network firewalls and intrusion detection systems are installed throughout the network to prevent unauthorized network access.

- All required network hardware is provided preconfigured by Anonymizer to facilitate deployment when installed at customer facilities.

- Anonymizer's proven security has been trusted by government and law enforcement agencies since 1997.

- An emergency generator is in place for fast power switching in the event of a catastrophic power outage.

- Physically redundant network feeds ensure connectivity to the Anonymizer Chameleon Network with more than 99% up-time.

Summary

The key to ensuring that the Internet remains an open source of information is a function of access and accuracy. Users need to be assured that the information that they see on a public website is unrestricted to access, and once the information on that site is obtained, that the content is accurate and consistent for all of its public visitors. With the evolution of new Web-based detection technologies, many companies have instituted the means to prevent certain users from accessing certain portions of this publicly available information. As an additional tactic, many of these companies "spoof" or present false public information designed to mislead certain "unwelcome" users from accessing the same information that the rest of the general public can see. The ability for any person, regardless of their affiliation, to visit a website that is free from spying, blocking and spoofing is becoming an issue of increasing importance to all Internet users today.

The Anonymizer Chameleon Network allows your enterprise employees to discretely gain uninterrupted access to public information. By leveraging many domain names and IP addresses, Anonymizer prevents outside parties from distinguishing your enterprise identity from any other Web surfer on the Internet. This capability provides a level of assurance that your employees will have completely accurate and unfettered access to all forms of Internet-based information without tipping off a competitor.

To summarize, there are three advantages of The Anonymizer Chameleon Network:

- **Restores Internet Integrity** – The Anonymizer Chameleon Network enables you to conduct effective, accurate and unobstructed research and intelligence on the Internet.

- **Protects Enterprise Identity** – The Anonymizer Chameleon Network ensures that your surfing behaviors and Internet destinations remain anonymous to prying eyes.

- **Prevents Pre-Emptive Competitive Action** – The Anonymizer Chameleon Network ensures that you remain anonymous to your competition, preventing them from taking any pre-emptive actions that might cause harm to your company or your marketing efforts.

About Anonymizer

Anonymizer, Inc. is a leading provider of Internet Privacy and Security solutions for consumers, corporations and the government. The company was established in 1996 with a mission to create user-friendly technologies that make the Internet a safer place to surf, shop, learn and explore. The Anonymizer.com core service, referred to as Anonymizer Private Surfing, has been used to privacy-protect over 4 billion Web page views for millions of unique users.

For more information about Anonymizer and Anonymizer Chameleon solutions, please visit our website at www.anonymizer.com/enterprise

5694 Mission Center Road #426
San Diego, CA 92108-4380
800-921-2414

www.anonymizer.com