Protecting Corporations from Internet Counter-Intelligence

Understanding new information threats to the Enterprise and how it impacts your organization now.

An Anonymizer White Paper

Executive Summary

The media has made us aware of the endless barrage of harmful security risks to our computer information infrastructure. Viruses, adware, spyware, pop-ups, Trojan horses, embedded spam messages, and cookies threaten to destroy or alter the online user experience. These threats have made anti-virus, anti-adware, anti-spam, firewall, and cookie removal solutions required protection for every PC user who wants to surf the Internet — from the first-time home user, to the largest FORTUNE 500 enterprise.

But administrators can't get too comfortable with their security initiatives, just yet — a new and more dangerous threat has arrived on the Internet landscape. *Internet Counter-Intelligence* involves using a series of sophisticated tools called *Web Analytics* to uncover corporate user identities by analyzing and tracking enterprise surfing habits, and capturing IP address and network identities. Analysis of this data is then used to reveal sensitive business, financial or network information — information that could be used by a competitor or hacker to gain a commercial, financial, investment-related, or public relations advantage. Here are just five of these types of threats:

IP-Based Blocking – This is the process of blocking the access of specific IP addresses and/or domain names. (*Example* - your marketing research team is unable to access your competitor's Web site, limiting their ability to conduct industry and competitive intelligence for your firm.)

IP-Based Cloaking – A Web site that changes its online content based on a user's IP address or geographic location. (*Example* – Your competitor recognizes one of your technical employees surfing their site and displays incorrect product information to your IP address, making it impossible to obtain accurate competitive intelligence.)

Industrial Espionage – Web administrators use tools to monitor and track the various pages and objects that are accessed on their Web site. (*Example* – Your competitor detects a large amount of traffic coming from your IP to their product page and concludes that you will be coming out with a similar product. They counter by launching a new promotion to blunt the impact of your new product campaign.)

Confidential Information Leakage – Your organization is protected from external threats by your firewall and anti-virus solutions. However, your company is not protected from the internal threats that occur everyday when your employees surf the Internet and inadvertently give out confidential information over time.(*Example* – Your competitor can determine your strategic initiatives, such as a hostile takeover, based on the information that your employees pull from their Web site.)

Cyber Terrorism – Cyber Terrorism refers to the direct intervention of a threat source towards your enterprise Web site. (*Example* – In 1997, the Pentagon simulated a cyberattack and found that attackers using ordinary computers and widely available software could disrupt military communications, electrical power, and 9-1-1 networks in several American cities. Hacking tools and expertise have become only more widespread since then.)

"Today's IT managers must recognize the need to proactively protect their company's identity when online," says Brian Burke, research manager at IDC. "Each time an employee accesses the Internet, they leak pieces of information to watchful competitors, hackers and online predators. Anonymizer effectively mitigates these threats with their identity protection and information assurance solutions."

Anonymizer® solutions circumvent these threats by completely masking the network identity while users are online. This is accomplished by combining a series of techniques such as secure high-performance network access, the use of variable IP addresses, and the application of pre-registered domain names. These features make it statistically impossible for any organization to trace back and uncover their true corporate identity.

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

Table of Contents

Introduction

Friday, March 26, 1999. Do you remember the day when enterprise computing changed? On that date six years ago, corporations around the world first became aware of the insidious threat imposed by computer viruses spread by the Internet — and the impact that these viruses would have on enterprise information worldwide. With the introduction of *Melissa* — a virus that attacked the heart of corporate infrastructure, Microsoft Office — enterprises first understood not only how vulnerable their computer networks were, but how these relatively minute pieces of code could wreak havoc on their information assets. The virus proliferated by kidnapping Microsoft Outlook e-mail address books, crippling tens of millions of PC's, servers, and networks around the world and costing enterprise businesses billions of dollars in lost commerce, productivity, and revenue.

Since *Melissa*, the media has continued to make us aware of an endless barrage of new, more harmful viruses — adware, spyware, pop-ups, Trojan horses, embedded spam messages, and cookies — that threaten, destroy, or alter computer information. Because of this higher threat awareness, anti-virus, anti-adware, anti-spam, firewalls, and cookie elimination solutions have become standard components of the online experience for every PC user, from the first-time home user to the largest FORTUNE 500 enterprise. In fact, it is now standard for computer manufacturers to ship some version of these solutions with every new PC, to prevent such threats from spoiling the online experience.

Corporations must now protect against the threats posed by *Internet Counter-Intelligence*, and take them as seriously as viruses, spyware, hacker intrusion, and spam.

By erecting barriers to these threats, enterprise IT departments have made the issue of intrusion and security a top priority. But just at a time when many are feeling comfortable with these efforts, a new and more dangerous threat has arrived. Corporations must protect against the threats posed by *Internet Counter-Intelligence,* and take them as seriously as viruses, spyware, hacker intrusion, and spam.

What is Internet Counter-Intelligence? This new threat involves using the Internet and a series of sophisticated tools called *Web Analytics* to uncover corporate user identities by analyzing and tracking enterprise surfing habits, and by capturing IP addresses and network identities in an effort to obtain sensitive business or financial information. This information can be used by a competitor to gain a commercial, financial, investment-related, or public relations advantage.

Today, enterprise users would never consider surfing the Internet "naked" — without a reliable anti-virus software and firewall solution installed on their PC's and networks. However millions of enterprise users are surfing the Internet and visiting Web sites equally unprotected in other ways, exposing their IP addresses and corporate network identities to competitors and Web site operators. In fact, when a user visits a Web site, they also disclose their operating system, browser version, physical address and anything that might be saved to their clipboard. Millions in revenue could be lost directly, through damage to a company's image. Additionally, indirect costs could arise from the exposure of strategic research being performed, especially in the areas of new product development, prospective mergers and acquisitions, investments or R&D.

Anonymizer, the leader in corporate identity protection and information assurance, wants enterprise users like yourself to be aware of the threat of Internet Counter-Intelligence and help you understand the magnitude of the dangers that are inherent when surfing the Internet without protection.

Analyzing the Variety of Threats to Enterprise Information

Until recently, the term "enterprise security" referred to breaches, intrusions, or destruction of enterprise data from **within** the enterprise or coming **into** the enterprise infrastructure from an outside hacker or predator. These areas are the focus of the bulk of IT security strategy and solution funding. These security threats and risks can be categorized by the following table:

Threats and Risks to Enterprise Computing

External Threats *(Hacker Penetration)*	
Type of Threat	**Risk Level**
Serious "Ethical" "Just for kicks"	 Minor to Moderate Nuisance Adverse publicity
Malicious Data theft/corruption/destruction Fraud	 From Minimal to Disastrous Very serious
Internal Threats *(Improper Access)*	
Type of Threat	**Risk Level**
Accidental Breach of Confidentiality Security loophole created	 Potentially serious Probably critical
Malicious Data theft Data corruption Fraud Data destruction	 Very serious Very serious Very serious Potentially disastrous
Denial of Service Loss of commerce/image	 Potentially disastrous

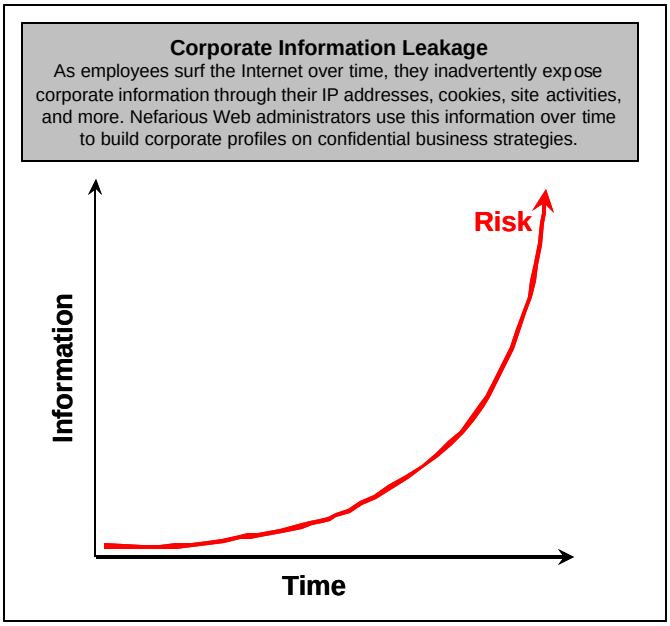
(Source: IDC)

These threats incur losses that are generally related to data destruction or corruption. "Denial of Service" threats receive less press coverage than the more malicious issues mentioned, but are still critical for enterprises that conduct much or all of their business in the online environment, are bound by Service Level Agreements (SLAs), or have highly visible Web sites (i.e. eBay, Amazon, etc).

The threat posed by Internet Counter-Intelligence, on the other hand, rearranges the entire security playing field because it involves protecting the most basic part of the corporate online user experience: IP addresses, domain names, and other basic network information relating to the enterprise identity. Unfortunately, this type of threat is often carried out without the enterprise user being aware that it is taking place.

Corporate identities are uncovered by using Web Analytic tools that analyze and report on Web site traffic. Web administrators can use these tools to analyze the surfing behavior of visitors to their sites. Much of the information that is gathered about visitors is tracked from their IP addresses. When you visit a Web site that uses analytics, it is possible for the administrators at these locations to trace your identity and monitor your click-through activities.

From an enterprise perspective, once a competitor knows your company's network ID, they can employ Internet Counter-Intelligence on your network. With this capability, the site can build a detailed profile of your interests and make a determination as to why you are viewing that particular set of information. Once a probable reason is determined, the competitor can take a series of counter measures such as posting false or misleading information, changing prices, skewing dynamic pages, routing you to an alternative version of their Web site or blocking you from their site altogether.



In the next section, we will provide some examples of how malicious entities, competitors and online snoops can use Web analytics to capture your corporate identity along with of the types of activities they can employ against your users and your enterprise as a whole.

Understanding the Seven Threats from Internet Counter-Intelligence

Most of today's enterprise IT organizations are ill-equipped to appropriately manage the problems posed by Counter-Intelligence. The chart below outlines the different ways that companies utilize the Internet and the threats that they face when their employees are online.

Application	Threats Faced	Recommended Solution
Entire organization surfs the Internet for business information and personal use.	? IP-based cloaking ? Personal and corporate leakage ? Cyber terrorism	Anonymizer Enterprise Chameleon
Analysts scour the Internet and conduct intense competitive and market research.	? IP-based cloaking ? Personal and corporate leakage ? Cyber terrorism	Anonymizer Enterprise Chameleon
Company utilizes unstructured data management (UDM) tools to harvest large amounts of data from the Internet.	? IP-based blocking ? IP-based cloaking	Anonymizer Intelligence Chameleon
Remote users and laptop users access the Internet from remote locations.	? IP-based cloaking ? Personal and corporate leakage	Anonymizer Enterprise Client Chameleon

Following are examples of the most common situations and/or threats that enterprise users may encounter by exposing their corporate identities on the Web:

1. **IP-Based Blocking** - The corporate firewall or Web proxy is used to prevent an identified user or domain from accessing some or all of the company's network resources, such as Web sites or FTP servers. For example, an organization could create a list of IP addresses that do not have access to their Web site, such as those of competitors. This tactic is used by companies in direct competition within the same industry, such as airlines, automobile manufacturers, and consumer products.

2. **IP-Based Cloaking** – IP-Based Cloaking enables an HTTP server to serve different Web pages once a specific IP address and/or domain name has been identified. For example, if a company detects a significant amount of traffic coming from a competitor's IP address, it can set up scripts to show misleading content to any traffic coming from that address. In a well-publicized example from the late-90s, 3Com Corporation detected visitors to their Web site from their competitor, Cisco Systems. Once identified, visitors from Cisco Systems would be immediately redirected to 3Com's employment page, where they would see various open positions along with instructions on how to get in touch with 3Com's human resources department.

   IP-based cloaking may also be used to present information tailored to a viewers' geographic location or apparent national affiliation. 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. For example, a well-known Arab news service posted different editorial content depending on the IP address of the Web site visitor. Web surfers from the U.S., Britain, or Australia were presented with pages representing a certain point of view regarding events in the Middle East. When the same Web site was accessed by Web surfers from an Arabic or Islamic country, a completely different set of editorials were presented, touting anti-Western, anti-Israeli, and anti-Semitic views.

Geographic IP-Based Cloaking

3. **Personal Identity Leakage** – Personal ID Leakage refers to the unauthorized redistribution of a person's confidential digital information, either accidentally or intentionally (such as employee theft, accidental distribution, hackers, changes in trust, lost devices, etc.). For instance, some software includes a "phone home" validation. When you install this software on your PC, it sends a signature from your computer to a data warehouse. This signature is like a fingerprint for your computer and contains information such as your IP address, host name and operating system.

   As a real-life example of this threat, a government employee working in a high security facility purchased software with his personal credit card while surfing the Internet at home. He later installed the software at his work office. A year later, he received a phone call at work reminding him to renew

his software subscription. He had never provided the software company his work number. Even though the customer purchased and registered the software using his home address, he installed the software at work. The software developer received his IP address from the "phone home" validation and with a simple reverse IP lookup, they were able to identify where the employee worked. They simply called the main number and asked for him by name (which he provided when he registered his software).

4. **Corporate Information Leakage** - Leakage can also apply to your corporate identification through the monitoring of a company's online search activities. Once your enterprise IP address has been detected via a competitor's use of Web analytics software, that address can be traced back to its source to uncover a host of additional details including your domain name and address, browser version, operating system, even departmental or location information. Corporate Identity Leakage is most harmful to an enterprise in three key business areas:

    - *Mergers and Acquisitions (M&A)* - Companies looking to acquire or merge often perform a heavy degree of due diligence and research before making their decisions known. Part of this function is performing Internet research on the target organization without the target company's knowledge that this research is taking place. To do so would compromise the final negotiated purchase price. Using Web analytics, if a competitor notices that there is an unusually high degree of traffic coming from your finance department or your investment banker, and they are downloading annual reports or 10K filings, they might be able to surmise that a merger or acquisition is afoot and take subsequent action that could financially impact that strategy for your organization.

    - *Use of Confidential Information* – Under SEC requirements, public corporations must take great care to ensure that confidential information does not leak out to the general public. To do otherwise would give some investors an unfair advantage and increase the likelihood that your organization could face severe financial sanctions as a result. Having an exposed IP address provides Web site owners and online predators with the ability to build profiles based on Internet surfing activity that can be used to determine what additional types of activities a company is performing (such as M&A, new product releases, etc). The purloined information could be used for the personal financial gain of the information gatherers. If exposed, the threat of a class-action lawsuit from other stockholders could deal a significant financial, legal, and/or public relations blow to the corporation.

    - *Security* - Just as corporations have adopted virus security as an essential requirement for conducting e-business, identity security will be the next requirement that enterprises will need to embrace as a standard requirement of being on the Web. Without Internet privacy, evildoers can not only see what Web sites a particular organization visits, but also their physical location, division, operating systems, browser versions and anything saved to their clipboard. This opens the organization up to potential security threats from hackers and other nefarious users. With this information they would have a better understanding of the target organization's infrastructure, making it easier to hack their systems.

5. **Harvesting Risks** – Many companies utilize Web harvesting tools to automatically gather and organize unstructured information from Web pages in order to show develop a complete picture of the marketplace. These extraction tools automate the reading, organization and analysis of data, and have proved useful for pulling together vast amounts of information on competitors, pricing reviews, trademark infringements investigations, etc. However, these tools can also raise a red flag for companies that monitor their site traffic and notice that an inordinate amount of traffic is coming from a particular IP address or range of IP addresses. For example, if your primary competitor recognizes a large amount of traffic coming from your domain, they can block your organization from accessing their site, thus limiting your ability to conduct any further intelligence on your competitors without being recognized. Worse, your users could receive false information because your competitors are utilizing IP-based cloaking to serve up incorrect information.

6. **Industrial Espionage** – Industrial Espionage refers to using Web analytics to analyze, track, and catalog online behavior that can be used to acquire trade secrets from business competitors. With an exposed IP address your competitors can determine your company's possible strategies and tactics by analyzing the Web surfing habits of your employees. For example, using analytical tools such as HitWise™ and Urchin™, companies can generate reports that give them the number of clicks occurring on each page and all of the items on those pages. If your competitor, for example, notices that your employees are spending a considerable amount of time viewing Web pages devoted to one particular product, they could determine that you plan to come out with a similar, competing product in that category. This could cause that competitor to accelerate a new competitive marketing campaign, which would then influence the outcome of your own marketing or pricing strategy.

7. **Cyber Terrorism** – Cyber Terrorism is the one of most malicious examples of Internet Counter-Intelligence. It involves direct intervention from the threat source towards an online domain or enterprise. In March of 2001, Condoleezza Rice, then National Security Advisor to President George W. Bush stated, "Today, the cyber economy is the economy. Corrupt those networks and you disrupt this nation".

Anonymizer Enterprise Solutions and their Advantages

Protecting the enterprise from these identity threats involves completely hiding your corporate network identity from the prying eyes of competitors and others who have intentions of "ill will" against your organization. To provide true masking capability entails more than another hardware or software enhancement for your existing network infrastructure. It requires a complete solution that today's most sophisticated Web analytic tools will be unable to thwart.

"Today's IT managers must recognize the need to proactively protect their company's identity when online," says Brian Burke, research manager at IDC. "Each time an employee accesses the Internet, they leak pieces of information to watchful competitors, hackers and online predators. Anonymizer effectively mitigates these threats with their identity protection and information assurance solutions."

Anonymizer provides enterprise customers true anonymity by combining four key components that aid in protecting corporate identities:

- **Anonymous IP Addresses** - Anonymizer utilizes thousands of IP addresses from several sources to protect and hide the identity of all its customers while they are using the Anonymizer Network.

- **Rotating IP Addresses** – Anonymizer uses a variety of techniques that alter how IP addresses are assigned to customers when they sign on to the Anonymizer Network. Since the user's IP address changes on a frequent basis, it is impossible for another site to detect your true identity.

- **Discreet Domain Names** – Anonymizer uses a number of pre-registered small business domain names that appear like everyday traffic and cannot be traced back and reveal your actual domain identity. This ensures complete protection from unwanted surveillance.

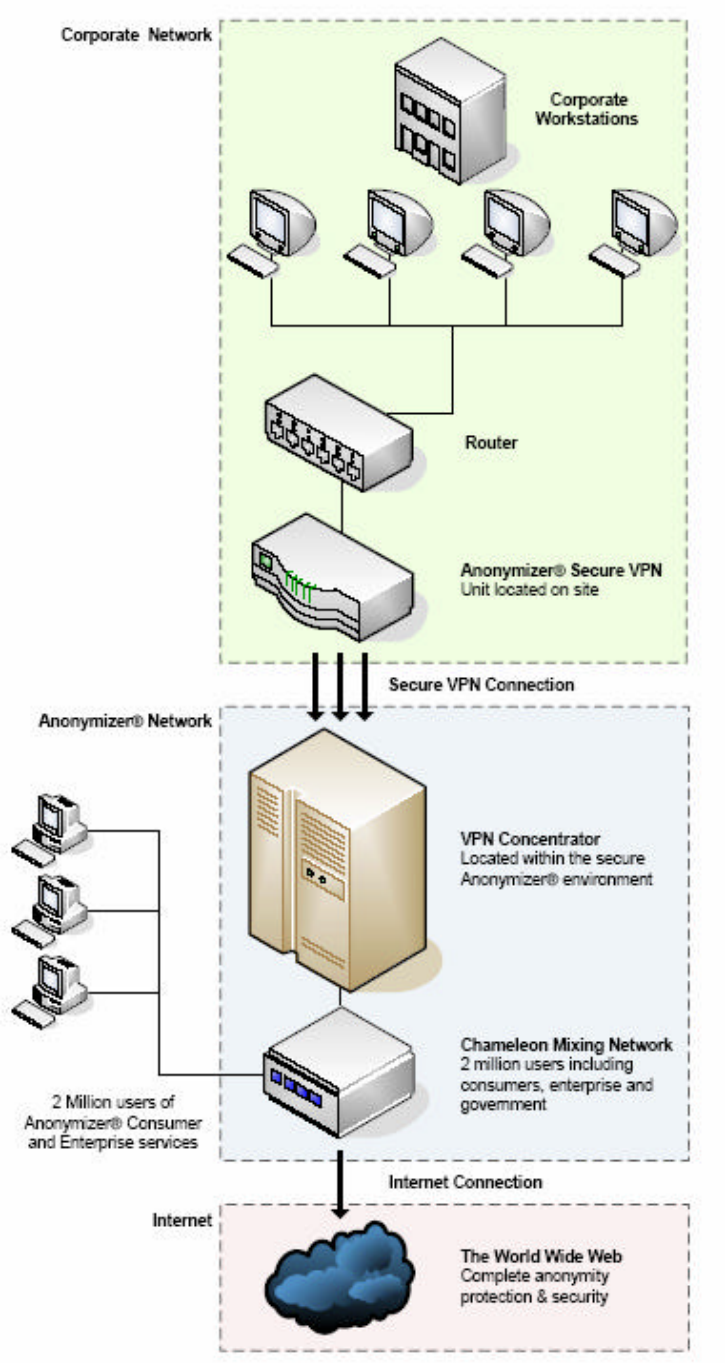
- **Fast and Secure Network Infrastructure** – Anonymizer combines ample bandwidth along with a highly secure VPN encryption to ensure that your network identity is afforded fast and secure communications, which cannot be traced back or identified in any way. In addition, Anonymizer provides full data redundancy, ensuring that your web-based information is safe and secure.

- **Trusted Protection –** Anonymizer has been the trusted leader in identity protection and information assurance since 1995, without a single security breach to date.

The features that Anonymizer builds into its network design to ensure corporate privacy make it statistically impossible for any organization to uncover your true identity.

To provide enterprise businesses with the widest possible choice of solutions to meet their information gathering needs, Anonymizer provides three levels of identity protection and information assurance solutions geared toward the organization's anticipated usage requirements.

The first is The Anonymizer Enterprise Chameleon which is explained in detail below.



The Anonymizer Enterprise Chameleon

Anonymizer Enterprise Chameleon is the perfect solution for companies to protect their identities while engaging in Internet activity. This solution can be implemented to protect individual analysts, single departments or entire organizations. It works with all ports and protocols, ensuring fast and flawless Internet access.

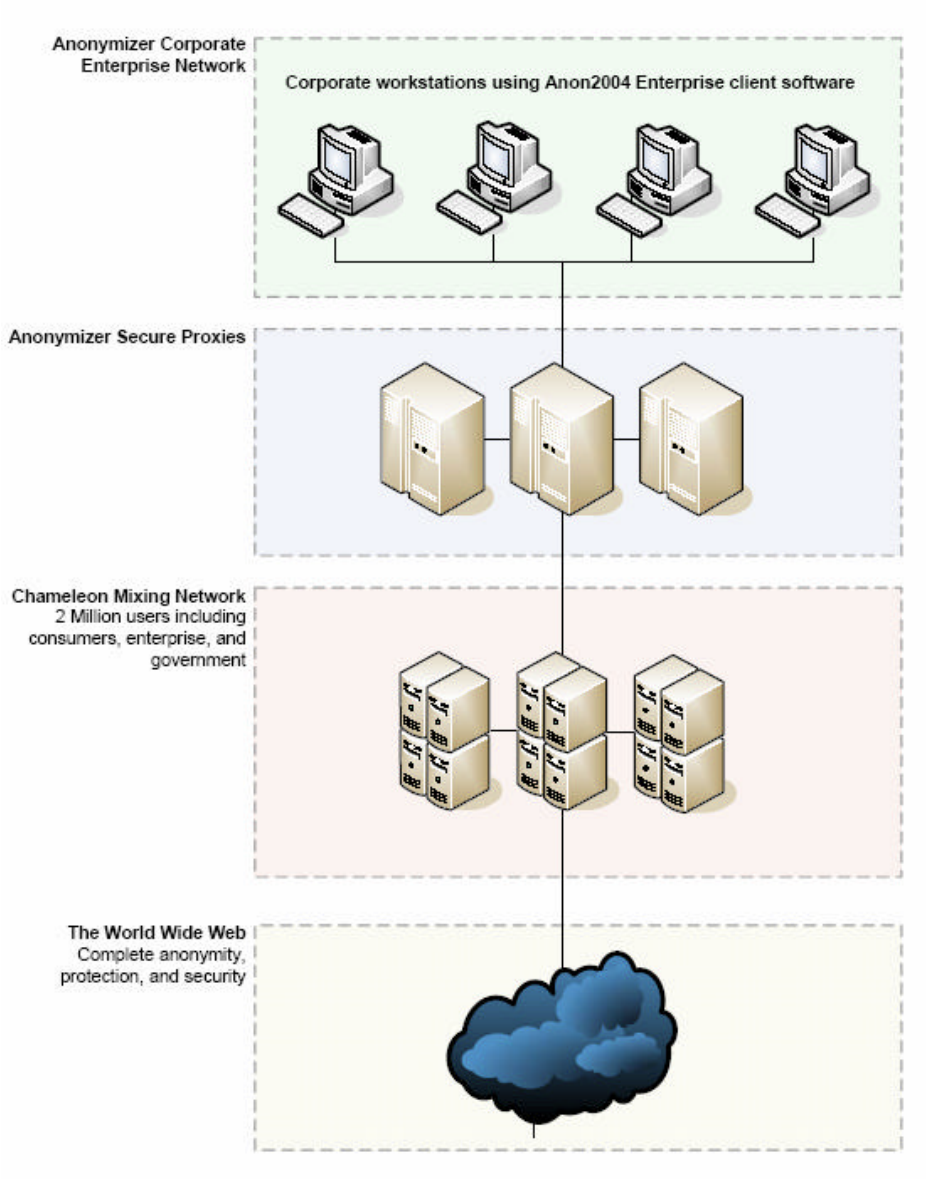
With the Enterprise Chameleon, a secure Virtual Private Network (VPN) network router is attached to the enterprise network. All network traffic is then rerouted to Anonymizer's Chameleon Network, protecting users 24/7.

The Anonymizer Enterprise Chameleon uses a technique called "IP Rotation" where the IP address that is used for the subscribers' network is changed on a daily or periodic basis. This is best suited for organizations that perform a significant amount of competitive analysis on the web and need to covertly access competitive or industry Web sites without their knowledge.

A Network Access Translation module (NAT) dynamically controls what IP address is presented to the outside world. The IP addresses are rotated daily and custom rotation frequencies are available for an additional fee.

IT organizations can determine how many users will be allowed to tunnel through this VPN at any given time, whether executives only, the analysts, or the entire enterprise user community.

The second identity protection solution for the enterprise is The Anonymizer Enterprise Client Chameleon.



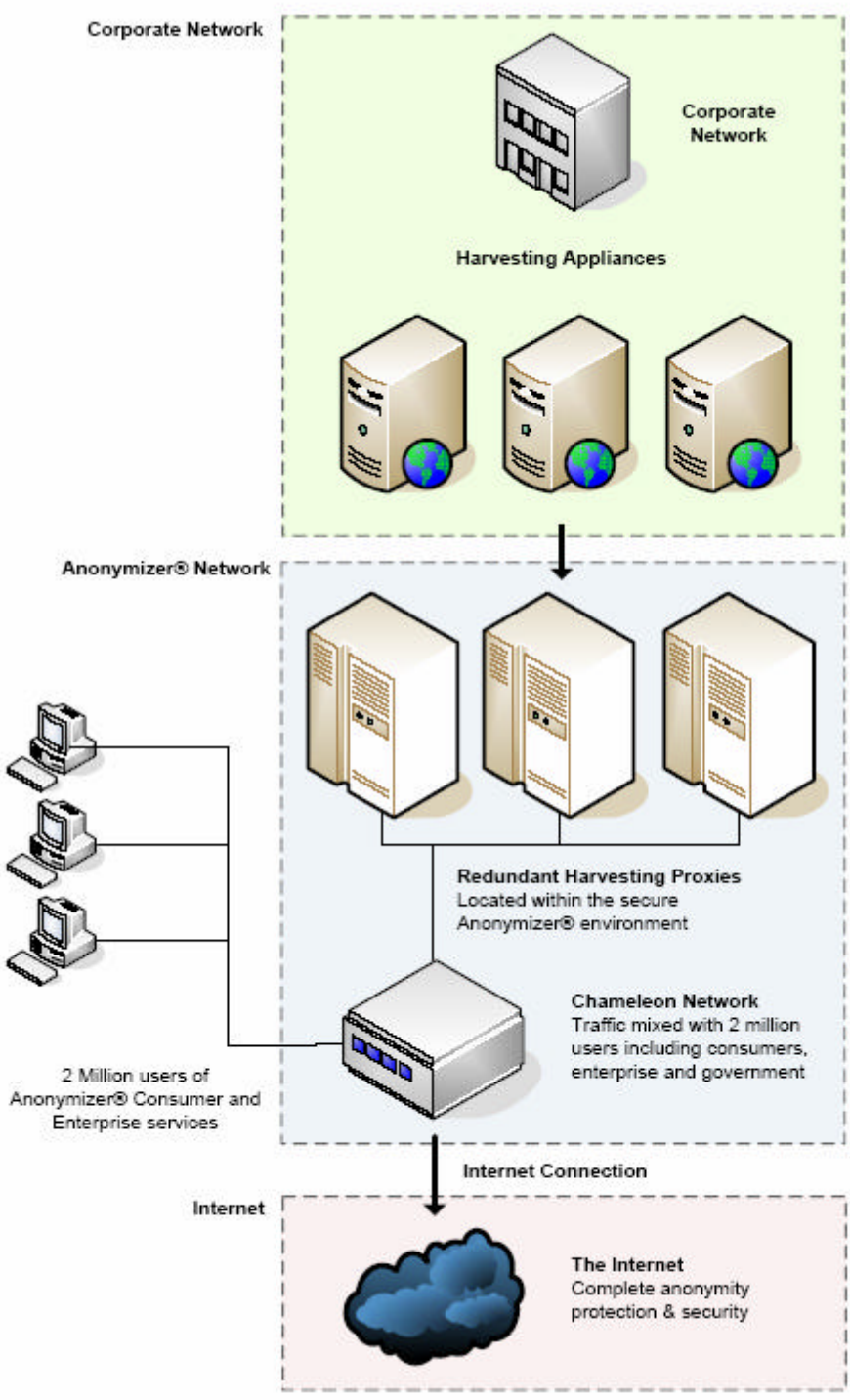
The Anonymizer Enterprise Client Chameleon

The Anonymizer Enterprise Client Chameleon is a must-have for those who work remotely and want to protect their identity while surfing the Internet.

The Enterprise Client Chameleon is provided as a CD that is installed on select client devices. This solution provides a "toggle-like" software switch that allows the user to turn the solution on or off at will. This is especially useful for remote or mobile users who have laptop or notebook computers. These users may access enterprise information from home or on the road, raising the risk of exposing their identities in unprotected network environments such as wireless cafes or hotels.

This solution is also useful for smaller organizations that don't have a large enterprise infrastructure and require a simple solution for a limited number of employees.

The third identity protection solution for the enterprise is The Anonymizer Intelligence Chameleon.



The Anonymizer Intelligence Chameleon

The Anonymizer Intelligence Chameleon is the perfect solution for any government organization or business enterprise that uses Unstructured Data Management (UDM) tools to conduct automated Web harvesting research.

For example, online travel services need to search and compare millions of competitive prices from many sites in order to determine a competitive rate for their services, while keeping their identity completely hidden from those other entities.

The Intelligence Chameleon uses a technique called "IP Explosion" which causes each TCP network connection to go out on a randomly selected IP address from a pool of thousands of addresses.

The Intelligence Chameleon can be used with or without an attached VPN, providing organizations flexibility in setup.

Summary

Our computer identity is something we take for granted each time we log onto the Internet. The ease of accessing information on the Web has created a false sense of security that can be exploited by business competitors using new and powerful tools at their disposal. Just as businesses woke up to the threat of viruses, cookies, and spyware on a few years ago, these enterprises must now become more aware of the threats imposed by Internet Counter-Intelligence. The only way to circumvent this threat is to completely mask user identities, making this a new requirement while online.

The Anonymizer Chameleon Network allows your enterprise employees to discretely gain uninterrupted access to public information. By leveraging discreet domain names and IP addresses, Anonymizer prevents outside parties from distinguishing your enterprise identity from any other Web site on the Internet. This 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 four advantages associated with using Anonymizer for your Identity security:

- **Protects Enterprise Identity** – Anonymizer ensures that your surfing behaviors and Internet destinations remain anonymous to prying eyes or competitors.
- **Enables Accurate Corporate Research** – With Anonymizer, the accuracy of your competitive intelligence is guaranteed without concern that your identity will expose your users to false information that is being "spoofed" by your competitors.
- **Prevents Preemptive Competitive Action** – Anonymizer ensures that your identity will remain completely anonymous to your competition, preventing them from taking any pre-emptive actions that might cause harm to your company or your marketing efforts.
- **Lowers The Risk of Hacker Attack** – Anonymizer provides protection from unauthorized users intercepting your corporate IP address and/or domain name and sending harmful or unwanted information into your enterprise network.

About Anonymizer

Anonymizer, the most trusted name in privacy, defends consumers, businesses and government agencies with comprehensive online identity protection solutions ensuring their privacy while using the Internet. Anonymizer identity protection solutions have secured millions of users since 1995 without a single security breach, while providing information assurance and control over their online identities.

As Internet technology advances, online threats such as identity theft, user profiling, IP-based cloaking and cyber-terrorism grow exponentially. Anonymizer identity protection solutions mitigate these threats and ensure a safe and secure Internet experience. For more information, please visit our Web site at www.anonymizer.com/enterprise.

ANONYMIZER®

5694 Mission Center Road #426
San Diego, CA 92108-4380 (888) 270-0141
www.anonymizer.com/enterprise