Employing Disinformation Security™ to Protect Corporate Networks with NetBait™

A NetBait Whitepaper
June 2003

Employing Disinformation Security™ to Protect Corporate Networks with NetBait™

EXECUTIVE OVERVIEW

Security in the enterprise has of late become the primary concern of both IT managers and other executives. The challenges of securing enterprise networks in the face of intruders armed with the tools of compromise have become overwhelming and yet, they still grow. In their own defense, organizations have sought the most obvious solutions in firewall, VPN, and intruder detection variants. All of these solutions, however, continue to leave proprietary data accessible to determined intruders.

Moreover, many of the more advanced current network security solutions require a good deal of administration, with consistent needs for re-configuration, management, and report analysis. With security administrators supporting an ever-growing number of users, such consistent interaction with security mechanisms has become impractical. Therefore, today's enterprise requires a security solution that will not only thwart the most unflappable intruder but will as well accomplish this with minimal configuration and supervision.

In consideration of these needs, NetBait offers a security solution based on the concept of Disinformation Security™, or providing intruders with inaccurate information in terms of the configuration and number of nodes on your network. NetBait allows you to:

- Statically or dynamically alter the types and number of nodes appearing on a network segment, with up to fifteen thousand NetBait Nodes per host.
- Deploy real operating systems, databases, web/mail servers, etc. on NetBait Nodes to allow for their true "compromise" in deference to the uninterrupted operation of your actual servers and applications.
- Implement the entire NetBait Infrastructure on-site or install only the core components and utilize our outsourced NetBait Service to complete the solution.
- Apply NetBait Nodes to your entire enterprise network or just to individual segments that require greater security.
- Improve productivity by reducing time spent on intrusion and attack issues.
- Utilize NetBait Micro-Deployments for specific monitoring, configuration, and testing applications.

- Minimize intruder chances of successfully compromising a particular network object or all objects network-wide to any desired level. These are the chances of access before the response of any supplemental intrusion detection system.

Companies in all industries benefit from NetBait's Disinformation Security™ architecture. Our customers range in industry from Education to Financial Services to Telecommunications. However, they all have one thing in common: they employ a network security solution that proactively prevents unauthorized access to their systems by confusing, diverting, and preoccupying intruders with a subterfuge of pseudo-networks and systems.

THE NETWORK SECURITY PROBLEM

Network Security

Networks have become indispensable for conducting business in government, commercial, and academic organizations. Networked systems allow organizations to access needed information rapidly, improve communications while reducing their cost, collaborate with partners, provide better customer service, and conduct electronic commerce. At the same time, businesses, large and small, continue to suffer from their networks' vulnerabilities to both casual and deliberate intruders.

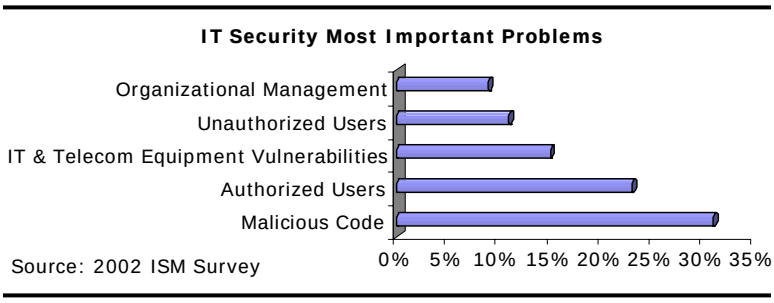
While computer networks have revolutionized the way companies do business, the risks they introduce can be devastating. Attacks on networks can lead to losses in revenue, reputation, intellectual property and other sensitive information.

The Computer Security Institute/FBI *2002 Computer Crime and Security Survey* indicates that the number of computer crime incidents is rising and that the cost of the damage they cause is increasing. For example:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months, compared to seventy percent reported in the 2000 survey;
- Eighty percent acknowledged financial losses, compared to sixty-four percent reported in the 2001 survey;
- For the fifth year in a row, corporate Internet connections were cited as the most frequent point of attacks; and
- Acknowledged financial losses topped $450 million, a twenty percent increase from 2001.

The Nature of Security Breaches

While security practices vary greatly from small to very large organizations, security practitioners generally agree about their most pressing problems. Nearly a third mention malicious code, while another quarter worry about securing authorized users. According to one of the respondent's of the 2002 ISM Survey, one of the greatest threats is "the lag time between the time a new virus is recognized and [when] the fix is posted."



As more companies migrate to a "brick-n-click" business model, the single most important security project or program is the security of Web and/or e-commerce operations. Not surprisingly, only twenty-five percent of the 2000 Information Security survey respondents said that secure e-commerce was their number one priority, while over forty percent and sixty percent said the same thing in 2001 and 2002, respectively.

The two types of security breaches that constitute the growing level of anxiety among security professionals are internal and external attacks. While internal breaches may arguably be easier to quantify, external attacks can significantly damage loyalty, trust, and shareholder value in a vulnerable organization.

Internal Breaches

The Information Security Survey confirms that, in many ways, insiders present a far greater risk than outsiders. It's not purely a "bits and bytes" problem, but one that involves human psychology and complicated workplace dynamics. And the problem is getting worse, not better.

While the media tends to focus on "sexy" cyber attacks such as denial-of-service, buffer overflows and Web defacements, the frequency of these attacks is considerably lower than insider access control breaches, software/hardware misuse and abuse of Internet use privileges.

Outsider Breaches

While internal security incidents are arguably more obvious to a business, external/outsider security breaches seem to be more prevalent and problematic. One of the reasons for this dichotomy has to do with the potential for public exposure. External breaches in security tend to get high-profile headlines more frequently because internal breaches and misuse, if detected, are often handled quietly in-house. Internal violations that are discovered usually result in employee reprimand or dismissal, most of the time without public disclosure.

It is natural to be more concerned about things you can't control vs. things you can control. In most cases, companies can keep a lid on insider security breaches, which helps minimize damage control no matter how serious the actual breach is. But it is usually impossible to control how outsider incidents are discovered and get covered in the media. As a result, a company experiencing a Web defacement, for instance, has to deal with the fallout on two fronts: resolving the technical vulnerability that led to the hack (relatively easy), and restoring shareholder and consumer confidence in the company's electronic and physical security (much more difficult).

Current Approaches

The prevalent methodology in approaching network security is to place a "wall" (i.e., a firewall or other network gatekeeper) between the public and private sides of an organization's network. As a baseline security, these guards work well in defense of attacks from unsophisticated would-be intruders. However, they fail when faced with a knowledgeable and determined hacker, whose mission is to overcome and compromise a given information security system and gain access to an internal network.

Indeed, regardless of the apparent impenetrability of security that an organization may implement, a sophisticated intruder will always be able to gain, at a minimum, a picture, or understanding, of the organization's network and it's structure. It is through this picture, with time and study, that an intruder is likely to find a pathway to exploit the systems' vulnerabilities.

NETBAIT'S SOLUTION -- DISINFORMATION SECURITY™

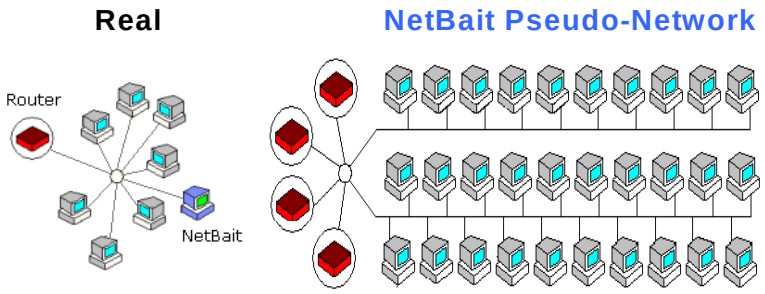
Network Pictures

Every network presents an organizational picture to a would-be intruder. This picture is made up of the actual workstations, servers, printers and other nodes on the network and typically shows a firewall as the only "public" node. This picture is employed by intruders to map an organization's network and, once this is accomplished, to determine probable vulnerabilities.

If the network picture remains unchanged for a period of time, the likelihood of successful intrusion grows with each day. The static nature of networks provides for a virtual schematic for the effective compromise of the systems that they interconnect. In order to truly secure a network, its picture must be changed on a regular basis – preferably minute by minute.

Secure Your Network with Disinformation

When NetBait is employed, it does not become part of an organization's existing network picture. On the contrary, NetBait generates its own picture – or a pseudo-network. The pseudo-network consists of the real network objects and any number of NetBait Nodes strategically placed throughout. Each NetBait Node may contain differing operating systems, applications and databases which, depending on an administrator's configuration, may be representative of the real systems in the organization.

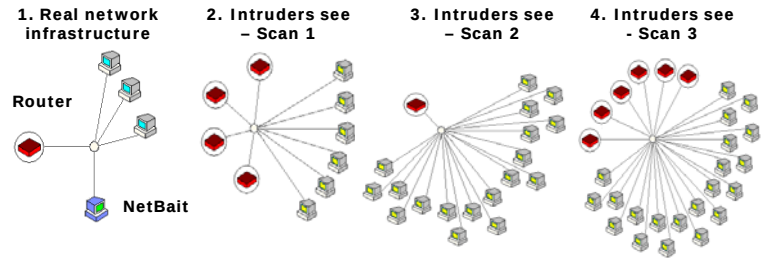


It is up to the company's security administrator to decide which network assets require which level of protection. While typically not every IP address needs to be protected, those that do can project any number of NetBait Nodes.

Therefore, if you provide NetBait protection for one hundred critical network objects at, for example, ten thousand NetBait Nodes per object, you will have developed a pseudo-network of 1,000,100 nodes. With this number and range of targets from which to choose, the chances of an intruder accessing a real system become nearly infinitesimal. In the typical scenario, an intruder spends time accessing "data" on NetBait Nodes, while the organization's actual systems continue to perform mission-critical functions without interruption

Dynamic Behavior Limits Risk

As we alluded earlier, a static network picture can be a security flaw in its own right. Every known "honeypot-derived" solution offers ways to configure objects; however, they are all static in nature – they stay the same until an administrator changes the configuration, after which they remain static.



NetBait, on the other hand, can dynamically change its configuration at desired intervals, based on the administrator's specifications during initial configuration. NetBait's Dynamic Behavior leaves intruders without an effective mapping of an

organization's network. Moreover, it continues to leave them guessing about which systems to target and through which methodology to attempt such intrusion.

Hack-Proof Infrastructure

Whether you decide to outsource NetBait operations through NetBait Service or implement an your own infrastructure through NetBait Enterprise, you will maintain complete privacy over the actual network environment. Even a deliberate compromise of NetBait's infrastructure will not allow an intruder to attack your or any other organization's network. Contrary to offerings from all other known providers, no one can use NetBait Nodes as a proxy to launch attacks against their host or other networks – not intruders, not us, not even a systems administrator.

Intruder Data – Take it or Leave it

When an intruder attacks a NetBait Node, security administrators garner comprehensive information on the origin of the intruder, specific systems on which access was attempted, the intruder's methods, and the date, time, and duration of the attack. This information can be logged, forwarded to the administrator, or simply turned off. NetBait provides all of this in a seamless, web-based service model, as well as in a dedicated and supported enterprise version.

Realize True Scalability

The overall value of NetBait is in its patent-pending centralized architecture. This architecture provides for a multi-variable platform where applications share a common engine with variable behavior and configuration patterns. This framework allows for the deployment of NetBait across the entire enterprise network as well as for Micro-Deployments™ on particular network segments. NetBait is every bit as scalable as an organization needs it to be.

CONCLUSION

NetBait is the security solution for companies that seek the state of the art in enterprise network protection and monitoring. NetBait Enterprise is defining this class of solution and the number of NetBait-based applications continues to grow. NetBait allows you to truly take control of the security of your network and inter-networked systems from the standpoints of preventing unauthorized access and monitoring should such access occur. NetBait Enterprise allows you to:

- Implement a Disinformation-based network defense mechanism to guard against the loss of sensitive corporate information.
- Determine an initial configuration once, leaving the work of surreptitious re-configuration to NetBait's dynamic behavior.
- Implement the entire solution in-house, or only the basic framework using our outsourced NetBait Service to fulfill node requests, limiting investment in additional hardware.
- Free administrators for other network and security management tasks with NetBait's simplicity in configuration and maintenance-free execution.
- Reduce corporate exposure to the risks of systems compromise and data theft, thereby protecting your organization from the costs associated with such losses, in terms of both revenue and reputation.

What is your goal in securing your network? If it is to deter intruders and protect intellectual property, and you are seeking a solution that requires little in the way of constant management and administration, then the perfect choice is right before your eyes. NetBait - the Evolution of Disinformation Security™