

NetBait™ • The Evolution of Disinformation Security™

NetBait offers a new paradigm in information security. As opposed to traditional informational security measures, NetBait does not exist as the secured primary public node in the overall picture of an organization's network. On the contrary, NetBait plays a critical role in generating the view of the client's network, with one important caveat: the picture that NetBait generates is not that of a client's network per se, but a highly modal fabrication that can be seamlessly reconfigured to provide differing representations of what appears to be the actual network environment - we call it a pseudo-network.

This picture is exposed to the intruder and it maintains the identical hurdles for entry that must be overcome to gain access to the real network. Once, and only if, access to the pseudo-network is gained, the intruder is confronted with any number of nodes running differing operating systems, applications, and databases. With persistence and the appropriate skill, the intruder may be able to find a path to entry on a particular node and also gain access to "data" on that node. However, no matter how many hours that intruder devotes to the effort, his work will have been in vain as he has gained access to nothing more than an immense void existing within the confines of the real network.

Within this void lie tempting NetBait Nodes that appear to represent your network's internal and external systems, providing an expanded range of targets from which the intruder may choose. In addition, NetBait captures information on the origin of the intruder, the systems that the intruder attempted to access, the method by which the attempt was made, and the date, time, and duration of the attempt.

This information can be logged, forwarded to an administrator, or simply turned off if it is not required. NetBait provides all of this in a seamless, web-based, off-site service model as well as in a dedicated and supported on-site enterprise solution.

NetBait™ Technology

NetBait is modal and modular, two characteristics that form the basis for a completely secure network environment. In engineering our solution, we took into account the inherent weaknesses in existing security solutions, such as intrusion detection systems (IDS), firewalls, and honeypot technologies. The result of our design work is NetBait - a virtually non-hackable and undetectable network security solution, which is based on a distributed network of multiple systems independently communicating with a main server to perform attack detection and traffic redirection according to a customized set of rules.

NetBait's greatest advantage is in the absence of user interaction points and/or externally accessible services. Its infrastructure is completely transparent to outsiders. While certain sub-network modules of NetBait can be easily compromised, acting as the "bait" for the intruder, NetBait's sub-network structure cannot be compromised, hacked, or flooded (even by DOS or DDOS attacks). Moreover, NetBait offers no fingerprint because it is not attempting to mimic or emulate any particular operating system. On the contrary, it displays real operating systems through a mode which would be analogous to that of a film projector.

Because of NetBait's indefinite routing and dynamic architecture, intruders have no concept of their location. This means that, while a prospective intruder may receive an answer to his request, the origin of that answer could come from any number of hosts - but all through the same IP address. This methodology confuses any denial of service attack and renders it harmless to the NetBait Nodes. While packet traffic may increase temporarily on the host network, the servers that were targeted in the attack will function normally and continue to respond to legitimate requests.

In the end, NetBait isolates the intruder in a sub-network environment from which he can go nowhere. With NetBait's LockDown™ topology, an intruder cannot gain access to the host network nor can he utilize the NetBait infrastructure as a base for any attack or to escalate any attack. NetBait is a virtual vortex for intruders, allowing them entrance but denying them residence or effective exit. That is, they can gain access to NetBait, although once they do, their only available path is retreat. An intruder or NetBait can end the session at any time and there is no path through NetBait to any other network. This leaves intruders, well, "hackless," and with no viable means to utilize NetBait, or the host-network that it protects, as a target or as a path to attack another target.



NetBait™ Implementation

NetBait is offered as a cost-effective, easily configurable, off-site service for small to large companies. We provide the infrastructure in our data center and you configure only your host/s, which can be as economical as the old i386 in your storage room. For the service, you pay a monthly subscription fee based on the number of IP addresses that you are utilizing.

For the enterprise, we offer NetBait as a pre-configured hardware and software solution which you may lease or purchase directly from us or through one of our partners. While you manage the solution in-house, we provide all hardware and software maintenance and support. The solution is flexible in that, if you have unutilized existing hardware, we can employ that hardware in the infrastructure to lower your overall cost. This provides a best-of-both-worlds implementation scenario for your organization.

Want to know more? Contact us or your NetBait Solutions Partner by visiting <http://www.NetBaitInc.com>.

Or call us at 1 866 NETBAIT.

