Infoblox

SOLUTION NOTE

Preventing DNS-based Data Exfiltration

SUMMARY

Theft of sensitive or regulated data and intellectual property is one of the most serious risks to an enterprise. DNS is frequently used as a pathway for data exfiltration, because it is not inspected by common security products such as firewalls, intrusion-detection systems (IDSs), and proxies. Infoblox Threat Insight is a patented technology that detects and automatically blocks attempts to steal sensitive data via DNS without the need for endpoint agents or additional network infrastructure. When used with Infoblox DNS Firewall, Threat Insight provides protection against both DNS tunneling and current sophisticated data exfiltration techniques. Infoblox is the only vendor to offer DNS infrastructure with built-in analytics for protection of your data.

DNS as a Pathway for Infiltration and Exfiltration

Several high-profile data breaches have been in the news recently. We read that millions of customer records are stolen, emails hacked, and sensitive information leaked. Most enterprises have multiple defense mechanisms and security technologies in place, such as next-generation firewalls, intrusion-detection systems (IDSs) and intrusion-prevention systems (IPSs). Yet somehow malicious actors find a way to appropriate data. What types of data are they after and why? Hackers try to steal personally identifiable information (PII) such as social security numbers and regulated data related to compliance and intellectual property that could give some other entity a competitive advantage. They can then post this data publicly to cause damage to reputation or they can turn around and sell it in the underground market for a nice profit.

Hackers can use multiple pathways to steal data, but the one that is often unknowingly left open is the DNS, or Domain Name System. DNS is increasingly being used for data exfiltration either by malware-infected devices or by rogue employees. According to a recent DNS security survey of businesses based in North America and Europe, 46 percent of respondents experienced DNS exfiltration and 45 percent experienced DNS tunneling.

DNS is not only used for data leakage, but also to move malicious code into a network. This infiltration is easier than you think. Hackers can prepare a binary, encode it, and transport it past firewalls and content filters via DNS into an organization's network. Hackers send and receive data via DNS—effectively converting it into a covert transport protocol.

DNS tunneling is the method of tunneling other protocols such as SSH or HTTP within DNS. DNS tunneling has been around for a long time, and popular toolkits include Iodine, OzymanDNS, SplitBrain, and TCP over DNS. Using a DNS tunnel, malicious actors can also fully and remotely control a compromised internal host or exfiltrate data.

Preventing DNS-based Data Exfiltration with Infoblox Threat Insight

Infoblox Threat Insight is a new patented technology that detects and automatically blocks attempts to steal intellectual property via DNS without the need for endpoint agents or additional network infrastructure. It uses real-time streaming analytics of live DNS queries and machine learning to accurately detect presence of data in DNS queries.

Available with Infoblox DNS Firewall, Threat Insight provides protection against both sophisticated data-exfiltration techniques and off-the-shelf tunneling toolkits. Infoblox is the only vendor to offer a DNS infrastructure with built-in analytics to detect and block DNS tunneling and data exfiltration.

Blocking of Data Exfiltration

Threat Insight not only detects but automatically blocks communications to destinations associated with data-exfiltrationattempts. The engine adds destinations associated with data exfiltration automatically to the blacklist in Infoblox DNS Firewall. In addition, Infoblox Grid-wide updates are sent to all Infoblox members with DNS firewalling/RPZ capability, to scale enforcement to all parts of the network.

No Additional Infrastructure or Endpoint Agents Needed

Unlike other approaches that analyze log data in batches and after the compromise, Threat Insight is built directly into the DNS infrastructure, which is in the path of exfiltration, and provides real-time detection, without the need for additional network infrastructure.

Visibility

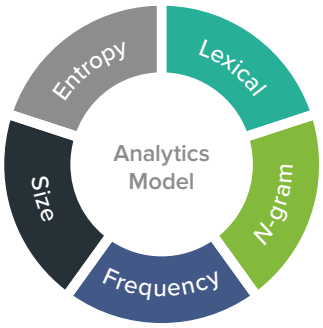
Infoblox provides visibility into the infected devices or potential rogue employees by providing detailed information such as device type, IP address, MAC address, and most importantly, the user associated with the device trying to exfiltrate data. This reduces time to repair and accelerates the remediation process.

Unique Patented Technology

Infoblox Threat Insight is a patented technology that uses machine learning to perform real-time streaming analytics on live DNS queries to detect data exfiltration. The analytics engine examines host.subdomain and TXT records in DNS queries and uses entropy, lexical analysis, time series, and other factors to determine presence of data in queries. This maximizes chances of detecting new methods of exfiltration, even those that don't have standard signatures, based on query behavior and patterns.

Automating Security Response through Integrations

In order to accelerate response to and remediation of data exfiltration threats, Infoblox integrates with leading endpoint solutions such as Carbon Black to provide indicators of compromise when an endpoint is trying to exfiltrate data. Using this intelligence, Carbon Black automatically bans the malicious processes from future execution and connection, thereby effectively quarantining the infected endpoint and preventing data from being exfiltrated, even if the device is outside the enterprise. Infoblox also exchanges security event information with Cisco Identity Services Engine (ISE) and provides robust restful APIs, which can be used to enrich your security information and event management (SIEM) with additional contextual data.



Don’t Become the Next Data Breach Victim

DNS is the perfect enforcement point to improve your organization’s security posture. It is close to endpoints, ubiquitous, and in the path of DNS-based exfiltration. While DLP technology solutions protect against data leakage via email, web, ftp, and other vectors, most don’t have visibility into DNS-based exfiltration. To maximize your chances of fighting back against these data theft attempts, complement traditional data loss prevention (DLP) solutions with a DNS-based solution. Infoblox Threat Insight complements traditional data-loss prevention (DLP) solutions by closing the gap and preventing DNS from being used a back door for data theft.

To learn about Infoblox security solutions, visit http://www.infoblox.com/security.

Infoblox

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70% of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com