SOLUTION NOTE

Malware Containment and Control

Malware: The Monster Lurking inside Your Network

Several high-profile data breaches have been in the news It's one of the most common attack vectors in use today, and it doesn't show signs of stopping. As malware becomes more sophisticated and continues to circumvent traditional defenses, the daily challenges faced by network and security professionals are increasing at an alarming rate.

Commonly employed security defenses—such as antivirus, firewalls, and even newer sandboxing approaches—are insufficient for containing and controlling malware that uses the universal DNS protocol to exfiltrate data from networks. And the task of rapidly isolating and remediating infected devices is a headache of epic proportions. Additionally, security teams often lack actionable network and device context that, combined with threat intelligence, could help expedite threat response.

Send Malware Packing and Keep Your Network Functioning Optimally

Infoblox solution for Malware Containment and Control helps organizations more effectively mitigate malware by leveraging DNS infra-structure and threat intelligence, and by sharing contextual threat data and indicators of compromise with leading security technologies to automate and accelerate threat response.

Benefits

Prioritize the myriad of threat alerts

- Leverage a rich set of business relevant data: endpoint (MAC address, device type, device OS, DHCP lease history, etc.), device user, and DNS queries and responses to help prioritize threat alerts

Leverage Existing DNS Infrastructure for Protection

- Detect compromised endpoints by identifying DNS requests to known infected Internet sites
- Protect your network with the DNS infrastructure you have in place; no "bolting on" required
- Combine advanced threat intelligence with network context to take action against malware at the control point of the network: the DNS

Predict and Defend

- Defend your network with threat intelligence from our threat research team, with years of experience monitoring DNS and malware threats
- Use the federated platform for threat data sharing to predict threats that may hit your network

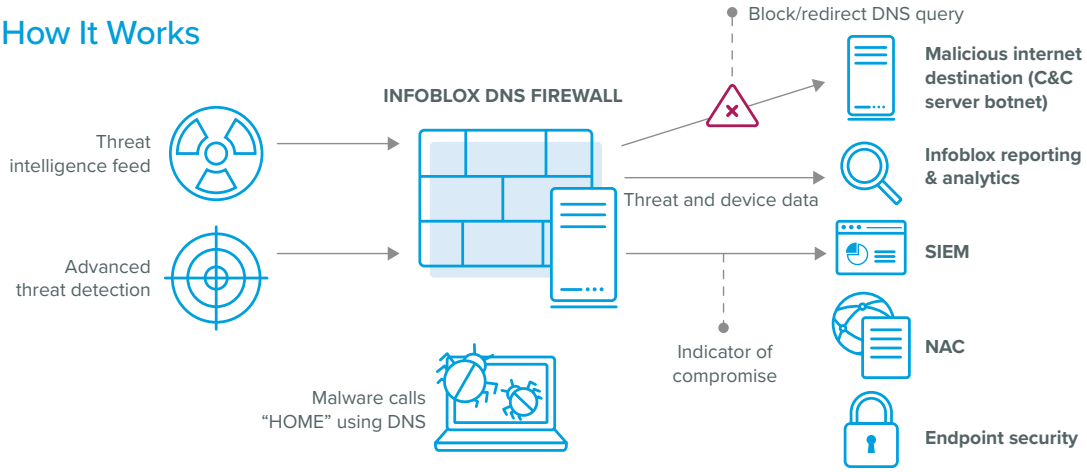
Get More out of Current Security Investments

- Retain current security investments and up-level your security quotient
- Integrate with leading security technologies—endpoint security, advanced threat detection, and SIEM
- Limit malware longevity in network and automate threat response and containment

Detect the Threat. Respond Quickly. Stop Malware in Its Tracks.

Because all malware uses DNS to communicate with its command and control (C&C) server, DNS is ideally suited to contain and control malware. Good thing the Actionable Network Intelligence Platform has a native emphasis on DNS-security. The Infoblox solution focuses on DNS as a point of attack and responds accordingly, to contain and control malware. Furthermore, it shares threat information to the broader security ecosystem via easy-to-consume ecosystem APIs, syslog, and SNMP.

How It Works



KEY COMPONENTS

Infoblox Products

DNS Firewall with Optional Threat Insight

- Protects against malwareby utilizing a high-quality and automated threat intelligence feed
- Leverages threat intelligence which categorizes (20+ categories including malware, APT, exploit kits) and classifies threats (300+ classifications) to provide insight

Reporting and Analytics

- Displays the top malicious hosts that devices try to communicate with
- Enables operators to quickly understand the nature of the threat they are experiencing
- Provides details on infected devices: DHCP fingerprint, IP address, MAC address, device type, OS and users

Ecosystem Products

Advanced Threat Detection

- Leverage indicators of compromise (e.g. newly discovered threats) from advanced threat detection technologies
- Automatically take action using DNS as an enforcement point

Endpoint Security

- Provide indicators of compromise (e.g. malicious hostname an endpoint attempted to communicate with) to endpoint security technologies
- Automatically respond to threats and kill responsible malicious processes or quarantine endpoints

NAC

- Provide indicators of compromise with NAC for automation of threat responses

SIEM

- Share security events with SIEM as part of a comprehensive threat view for analysis and automation of response workflows

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com