



SEACOAST
Cybersecurity Group



SEACOAST CYBERSECURITY GROUP WHITE PAPER

Protective DNS (PDNS): A Cybersecurity Best Practice and Requirement

By Jon Oltsik, Principal Security Researcher

June 2025

Whalebone Immunity White Paper

This White Paper was commissioned by Whalebone and is distributed under license from Seacoast Cybersecurity Group.



Contents

Contents.....	2
Executive Summary	3
DNS is a Critical Aspect of Cyber-attacks.....	3
PDNS: A Security Best Practice and Requirement	3
Whalebone PDNS.....	4
Next Steps.....	5



Executive Summary

DNS is ubiquitous, acting as a network directory for brokering Internet connections. Unfortunately, this also makes DNS an essential part of cyber-attacks like social engineering, malware distribution, and command-and-control (C2) communications. To address this situation, organizations can (and should) deploy protective DNS (PDNS) solutions that block malicious connections, continuously update threat intelligence blacklists, enforce policies, and integrate seamlessly into their networks. PDNS is a security best practice and is often recommended or even required as part of various industry and government regulations. As organizations evaluate PDNS, they may want to consider solutions from Whalebone – a PDNS leader.

DNS is a Critical Aspect of Cyber-attacks

The Domain Name System (DNS) is a foundational component of the Internet and World Wide Web, as it acts as a universal directory, brokering connections from client (and non-human identity assets) to servers and Internet-based services. Beyond this altruistic function however, DNS is also a critical part of most cyber-attacks. In fact, over 90% of malware uses DNS resolution at some point in its lifecycle (e.g., for command-and-control communication, data exfiltration, or resolving phishing domains, source: Splunk). Examples of the malicious use of DNS include:

- **DNS Spoofing (Cache Poisoning):** This involves injecting false DNS data into a DNS resolver's cache. When users try to access a legitimate website, their queries are resolved with the incorrect (malicious) IP address, redirecting them to a fake website that mirrors the original. This is often used for phishing or to deliver malware.
- **DNS Tunneling:** This attack uses the DNS protocol as a covert communication channel. Attackers encapsulate malicious traffic (like command-and-control communications or data exfiltration) within legitimate DNS queries and responses.
- **DNS Hijacking (Domain Theft):** This involves maliciously gaining control of a domain name by stealing the owner's login credentials for the domain registrar or exploiting vulnerabilities in the registrar's system. Once hijacked, the attacker can redirect traffic, steal sensitive information, or use the domain for other malicious activities.

Aside from these types of attacks, DNS is used as part of cyber-adversary tactics, techniques, and procedures (TTPs) for another reason. Malicious use of DNS circumvents typical security controls like firewalls and endpoint detection and response (EDR) software, while DNS logs won't provide any clues of an attack in progress to security information and event management (SIEM) systems. Thus, DNS-based attacks like those described above are often invisible to the security team – until it's too late.

PDNS: A Security Best Practice and Requirement

With DNS regularly used in social engineering attacks, malware distribution, and C2 communications, it would be safe to assume that CISOs and security teams are actively building appropriate countermeasures. Unfortunately, this isn't always the case. In fact, only 31% of security professionals feel very confident in handling a DNS attack (source: G2 Learning Hub).

Fortunately, there is a simple way to address DNS-based attack vulnerabilities. How? Through the deployment of protective DNS technology. As proof, a pilot program by the United States National Security Agency (NSA) determined that PDNS could reduce the ability of 92% of malware attacks to successfully deploy malware on a given network.

PDNS acts as an inspector for all internet traffic. Normally, a browser (or application, IoT device, etc.) sends a request to a DNS server to find the numerical IP address for that website. Cyber-adversaries usurp this process through social engineering attacks or by compromising assets at either end of a DNS query. Protective DNS inserts itself within this process as it checks the requested website against a continuously updated list of known malicious sites (e.g., those hosting malware, phishing scams, or command-and-control servers for cyberattacks). If the requested website is on that blacklist, Protective DNS blocks the connection, preventing a malicious connection. In this way, PDNS acts as a first line of defense.

In terms of feature/functionality, PDNS solutions provide:

- **Malicious Domain Blocking:** PDNS maintains extensive, frequently updated blacklists of domain names associated with various cyber threats, including malware distribution sites, phishing scam pages, command-and-control servers used by botnets, and ransomware delivery points. When a user tries to access one of these blacklisted domains, the protective DNS resolver intercepts the request and blocks the connection.
- **Threat Intelligence Integration:** To stay effective against constantly evolving threats, protective DNS solutions continuously integrate with various threat intelligence feeds. These feeds keep organizations safe with real-time updates on new and emerging malicious domains, attack campaigns, and attacker infrastructure.
- **Content Filtering:** Beyond just blocking known threats, many protective DNS solutions offer content filtering capabilities. This allows organizations to define policies that restrict access to specific categories of websites, such as adult content, social media, gambling sites, or other categories that fall outside of an organization's acceptable use policies.
- **Reporting and Analytics:** Leading PDNS solutions provide detailed logging, reporting, and analytics. This includes information on blocked threats (what was blocked, when, and from where), attempted access to malicious or restricted sites, and overall DNS query patterns. These insights are invaluable for understanding network security posture, spotting trends, or pinpointing negligent users.

Additionally, PDNS can help organizations in achieving and maintaining various regulatory compliance requirements. By proactively blocking access to malicious websites, it helps satisfy data protection mandates in regulations like GDPR, HIPAA, and PCI DSS. PDNS is especially relevant to requirements within the Network and Information Systems 2 Directive (NIS2) designed to enhance the overall level of cybersecurity across the EU's Member States. NIS2 mandates that entities implement "appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems." Protective DNS directly contributes to this by offering proactive prevention, enhanced visibility, supply chain security, and other NIS2 requirements.

Whalebone PDNS

While there are many commercial and even free PDNS solutions available, Whalebone stands out as an innovative leader – especially for EU-based organizations. As CISOs compare PDNS solutions, they will discover that Whalebone stands apart with:

- **Proactive Threat Blocking:** Whalebone can block a wide range of cyber threats (malware, phishing, ransomware, C2) at the DNS level, preventing them from ever reaching endpoints.
- **Minimal Latency & High Performance:** Rather than get in the way of Internet connections, Whalebone is engineered to process DNS queries extremely quickly, ensuring no noticeable traffic latency.



- **Simple Deployment:** Whalebone doesn't require agent deployment, software changes, or network configuration adjustments, easing implementation and accelerating time-to-value.
- **Granular Control & Policy Management:** Whalebone can be customized and tailored for content filtering for different user groups or organizational needs.
- **Scalability:** Whalebone is designed to handle the DNS traffic of organizations of varying sizes, from small businesses to large enterprises and government agencies.

Whalebone also supports the other requirements defined above including continuous threat intelligence integration, detailed reporting, and strong alignment with government and industry regulations. Whalebone is also a DNS4EU consortium leader/solution provider, and an active participant in the DNS4GOV initiative, a part of the DNS4EU vision that focuses on how a secure, EU-based DNS infrastructure can be tailored and deployed for government agencies and public institutions.

Next Steps

Organizations face a dangerous threat landscape, and things will only get worse as threat actors adopt AI tools as part of their TTPs. PDNS is an effective, and easy countermeasure with a proven track record of blocking all types of malicious traffic. CISOs should begin pursuing a PDNS strategy by:

- **Evaluating their DNS-layer visibility.** This can help them understand what's in place and how DNS has been utilized for cyber-attacks on your organization and industry.
- **Comparing PDNS capabilities to their current stack.** This comparison should include network latency, ease-of-use, efficacy, etc. Even organizations with free or basic commercial PDNS may determine that there are more effective options available.
- **Reviewing regulatory compliance alignment and PDNS.** As previously stated, PDNS is mandated or recommended in many regulations such as the US government's Office of Management and Budget (OMB) Memorandum M-22-09, the US Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC), ISO/IEC 27001:2022, and the European Union (EU) NIS2 Directive (Directive (EU) 2022/2555). Organizations considered critical infrastructure should be especially proactive.
- **Piloting PDNS solutions like Whalebone as a proof-of-concept project.** CISOs should set up test beds and control sites to gauge the effectiveness of PDNS while comparing different options. Efficacy metrics should include things like blocking rate, false positive incidents, mean-time-to-detect (MTTD), threat intelligence integration, DNS logging visibility, and reporting. Ease of installation and operations should be a high priority for organizations with small security teams.