

DNS Beacons

By DigiCert Team

Published: 2025-01-23 · Archived: 2026-04-05 14:35:35 UTC

As security operations centers (SOCs) have enhanced their capabilities in detecting malware command and control (C2) activities, the landscape of cybersecurity has evolved significantly. Initially, SOCs relied on signature-based detection methods, which could only identify known threats. Over time, advancements in threat intelligence and the integration of machine learning have enabled SOCs to detect and respond to previously unknown attack patterns. This continuous improvement in threat detection forced cybercriminals to innovate novel methods to maintain stealth. One such technique is DNS beaconing—a stealthy method used by attackers to maintain control over compromised systems via command and control (C2) servers. This article will demystify DNS beaconing, explain its intricacies, and provide actionable insights to help business professionals and organizations protect against this cybersecurity threat.

What Are DNS Beacons?

DNS beacons are a technique employed by malware to establish and sustain a persistent connection with a C2 server. This process relies on the DNS protocol as a communication channel between the compromised system and the attacker's server. Unlike other forms of DNS abuse that target the DNS infrastructure itself, DNS beaconing utilizes DNS as a transfer medium, allowing the attackers to operate under the radar without directly attacking the DNS system.

On the surface, DNS beaconing seems like DNS tunneling. However, a huge differentiator is its low-frequency communication pattern. This means that the malware interacts with the C2 server infrequently, making it difficult for traditional intrusion detection systems to identify the beaconing activity. By disguising their connections as benign DNS requests, cybercriminals have a fallback mechanism when their primary command and control is disabled and can continue to execute commands and exfiltrate data from the compromised system without raising alarms.

How Do DNS Beacons Happen?

DNS beaconing typically involves several stages to execute successfully. Initially, malware infiltrates a target system—often through phishing emails or exploit kits. Once inside, the malware establishes a communication channel with its C2 servers through HTTP, HTTPS, or DNS queries.

Throughout normal operation, the malware communicates with its C2 servers to receive commands and attack payloads and to exfiltrate data. These packets can be encrypted, making it challenging for security professionals to analyze the traffic and understand its true nature. The C2 server can then send commands back to the malware, directing it to carry out various malicious activities on the compromised system.

However, when malware frequently communicates with its C2 servers and performs network-intensive operations such as data exfiltration, that conversation is easier to detect and is blocked by SOC operations staff. As a result, malware developers started to add resiliency measures to keep control of their malware. One of those methods is DNS beaconing.

In DNS beaconing, malware uses DNS tunneling as a backup communications channel which it only uses when the primary communications have failed. They then typically transmit instructions to the malware to allow it to reconnect with their primary C2 and then go dormant. Some DNS beacons might only be used less than once a month or only when the primary C2 is unavailable.

This continuous primary and backup command and control setup allows attackers to maintain control over the system while evading detection by security measures that rely on identifying frequent or large data transfers.

DNS beaconing can also use domain generation algorithms (DGAs) and fast flux. DGAs generate many semi-random domains that malware-infected machines will try to connect to as a means to establish communication channels with C2 servers. Fast flux is a technique to modify DNS resource records rapidly using IP addresses of legitimate infrastructure providers in addition to the malware C2 IP addresses in a way to gain a positive reputation score for the domain. These techniques allow attackers to quickly switch between different domains in case one gets detected or taken down by security measures.

Examples of DNS Beacons

DNS beaconing is not just a theoretical risk; it is a real-world threat with numerous documented cases. For instance, Cobalt Strike's DNS Beacon feature leverages DNS requests to communicate with a C2 server. This Cobalt Strike payload uses DNS lookups against domains that the attacker's server has authority over. The DNS response then instructs the Beacon to either remain dormant or connect to the C2 server to receive tasks.

Numerous malware and attack groups have used DNS beaconing:

- **APT32 (OceanLotus):** Known for targeting entities in Southeast Asia, APT32 used DNS beaconing as a secondary method of communication with its command-and-control infrastructure, ensuring continued access even if primary channels were disrupted.
- **APT29 (Cozy Bear):** This high-profile group, suspected of being linked to Russian intelligence, has utilized DNS-based communications to maintain a resilient connection with compromised nodes, allowing for stealthy data exfiltration and remote control.
- **Sunburst (SolarWinds Hack):** Notably, the malware used in the SolarWinds attack incorporated DNS beaconing to discreetly communicate with its C2 servers, allowing attackers to receive commands and carry out espionage activities across high-value network segments.
- **Zloader:** A banking Trojan that has employed DNS beacons to update its C2 server configurations dynamically, ensuring persistence and adaptability in its operations across infiltrated networks.
- **PlugX:** This modular malware family has been observed using DNS-based tactics for C2 communication, allowing operators to manage compromised systems across Asia while evading detection through more conventional monitoring approaches.

How DNS Beacons Impact Your Business

DNS beaconing is intricately linked with malware, and its impact can be just as severe. When an attacker successfully compromises your network and employs DNS beacons, they can maintain a persistent and covert connection to their command-and-control infrastructure. This allows them to carry out various malicious activities over extended periods without being detected. Such activities may include data exfiltration, where sensitive information is stolen and transferred outside the network, lateral movement within the network to access additional systems and resources, and the installation of additional malware to further entrench their presence. This prolonged access can lead to devastating consequences, including data breaches, theft of intellectual property, and significant financial and reputational damage to the affected organization.

The use of DNS beaconing also presents a formidable challenge for incident response efforts. Traditional security solutions, which often rely on signature-based detection, may not effectively detect or alert DNS-based communications. This makes it difficult for defenders to accurately identify and respond to these threats in a timely manner. As a result, organizations may experience prolonged compromise, increased risk of sensitive data theft, and further damage to their reputation due to delayed response and mitigation efforts.

Moreover, the use of DNS beaconing can have additional impacts on business operations by adversely affecting network performance. With a marked increase in DNS traffic resulting from beaconing activity, legitimate network operations may experience delays or even disruptions. This can lead to operational inefficiencies, hampering productivity and potentially causing financial losses. The disruption of critical business processes due to slow network performance can have cascading effects, impacting customer satisfaction and business continuity.

To effectively combat the threat posed by DNS beaconing, organizations must adopt comprehensive security strategies that include advanced detection techniques capable of identifying anomalous DNS traffic patterns. Regular network monitoring, threat intelligence, and employee awareness training should be part of an organization's cybersecurity posture to minimize the risks associated with such sophisticated attacks.

Preventing DNS Beacons

Due to its stealthy nature, detecting DNS beaconing is challenging for traditional intrusion detection systems. However, there are some techniques that SOC operators and Cyber Threat Intelligence Teams can use to identify and mitigate this type of attack:

Use Protective DNS. Protective DNS services, also known as managed DNS firewalls, can be instrumental in safeguarding your network by preventing communication with malicious domains. These services work by maintaining a constantly updated list of known malicious domains, which is compiled through extensive threat intelligence and monitoring. When a request is made to access a domain, the service cross-references it against this list and blocks any that are identified as harmful. This proactive approach prevents potential cyber threats and helps reduce the risk of data breaches and other security incidents. By incorporating Protective DNS into your cybersecurity strategy, you can enhance your network's resilience against evolving online threats.

Endpoint Security

Implement comprehensive endpoint security solutions that can effectively detect and neutralize malware. These solutions should be capable of identifying malicious software that attempts to establish DNS beaconing channels on individual systems. By doing so, they help protect against unauthorized data exfiltration and ensure the integrity of the network's endpoints. Regular updates and monitoring of these security systems are crucial to adapting to evolving threats and maintaining robust protection.

Monitor DNS Traffic Patterns

Organizations should regularly monitor their network traffic for any unusual spikes or patterns in DNS activity that could indicate beaconing or other suspicious activities. This monitoring can be achieved using specialized tools designed to analyze DNS traffic or through manual analysis of DNS logs. By establishing a baseline of normal traffic patterns, organizations can more easily identify anomalies that may suggest malicious activity.

Implement Domain Whitelisting

By creating and maintaining a comprehensive whitelist of approved and trusted domains, organizations can significantly limit the potential for unauthorized communication with outside entities. This approach helps to detect attempts at DNS beaconing by blocking communications with domains that are unknown or unapproved. Regularly updating the whitelist ensures that it remains effective and relevant against evolving threats.

Educate Employees on Social Engineering Tactics

Attackers frequently use social engineering tactics to deceive employees and gain unauthorized access to an organization's network, which can lead to DNS beaconing. Educating employees about these tactics—such as phishing emails, phone scams, or impersonation techniques—empowers them to recognize and respond appropriately to potential threats. Regular training sessions and awareness campaigns can reinforce this knowledge and help prevent successful attacks.

Utilize Threat Intelligence

Staying informed about the latest cyber threats and attack vectors is crucial for preparing defenses against DNS beaconing attacks. Organizations should utilize reputable threat intelligence sources to gather information on emerging threats and share this intelligence with other organizations to create a collaborative defense strategy. By actively participating in information sharing, organizations can enhance their understanding of potential risks and improve their ability to respond to new and sophisticated threats.

Regular Software Updates

It is crucial to keep all software and systems consistently up to date as a proactive measure to safeguard against vulnerabilities. These vulnerabilities can be exploited by attackers to establish DNS beaconing channels, which are used to communicate with compromised systems. Regular updates ensure that known security flaws are patched, reducing the risk of unauthorized access and enhancing overall system security. By implementing a routine update schedule, organizations can better protect their network infrastructure and maintain the integrity of their data.

The Future of DNS Beaconing

As detection technology continues to evolve, so do the tactics employed by cybercriminals and the malware that they use. DNS beaconing is just one example of how attackers adapt and abuse existing protocols to achieve their goals. By understanding the nuances of DNS beaconing and implementing proactive defenses, businesses can protect themselves against this insidious threat and operate safely on a hostile Internet.

How Digicert Can Help

Digicert's [UltraDNS Detection and Response](#) (UltraDDR) is a leading protective DNS solution that preemptively blocks malicious queries and maps adversary infrastructure. It offers proactive security by integrating recursive and private DNS technologies, ensuring protection for employees in any location. UltraDDR detects and blocks threats in real time, intercepts malicious traffic, reduces security team burnout, enforces usage policies, and enhances security audits.

For further insights and resources on DNS beaconing and cybersecurity best practices, consider [reaching out to our expert team](#) for personalized guidance.

Source: https://vercara.digicert.com/resources/dns-beacons#page_top