URMAZI!

White Paper

10 Warning Indications in DNS Activity Logs

To safeguard digital assets and network communications, enterprises commonly deploy firewalls as a security barrier while maintaining connection and security event logs for organizational cybersecurity intelligence.

However, as the Domain Name System (DNS) serves as the backbone of all Internet services, organizations face common cybersecurity compliance issues—lack of detailed and easily interpretable DNS activity records. This deficiency makes it challenging to trace and investigate security incidents, potentially exposing enterprises to attack risks. Preserving comprehensive DNS query and response records provides valuable information about potential security threats, including access content and patterns for both normal and high-risk threats.

To effectively use DNS records for identifying normal and high-risk threats, the iSafer DNS Security Solution can be introduced to automate anomaly detection, provide real-time alerts, and conduct statistical analysis on DNS traffic content. This not only enables real-time identification and blocking of potential threats but also offers precise activity visibility for IT departments, serving as a technical basis for subsequent control strategy formulation and compliance with cybersecurity regulations. Additionally, maintaining the timeliness of DNS threat intelligence sources can further enhance your ability to detect and respond to high-risk threats in real-time.

 | www.urmazi.com | 16F, No. 80, Sec. 1, Zhongxiao W. Rd.,Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.) | SF-WP-31125

The following are specific indications based on DNS records for identifying high-risk threat access:

- **Unusual Query Patterns**
  Identify abnormal query patterns in DNS traffic, such as unusually high query counts for specific domains or frequent requests for non-existent domains (resulting in NXDOMAIN). These patterns may signify malicious activities, like malware exploiting Domain Generation Algorithms (DGA).

- **Blacklisted Domains**
  Maintain a list of known malicious or high-risk domains, comparing DNS query records in real-time. Observing DNS queries involving domains from the blacklist is a clear indication of potential high-risk threats.

- **Uncommon TLDs (Top-Level Domains)**
  Pay attention to uncommon or suspicious Top-Level Domains (TLDs) in DNS queries. Malicious domains often use less common TLDs, such as .xyz or .info, to evade routine security checks. Frequent queries to such TLDs may serve as a warning signal.

- **Rapid Changes or Domain Flipping**
  Monitor DNS records for domains associated with rapid changes or domain flipping techniques. Malicious actors often use these strategies to quickly alter IP addresses associated with domains, concealing their malicious activities.

- **Unusual Query Traffic**
  Sudden spikes in DNS query traffic or excessive DNS traffic to specific domains may indicate a Distributed Denial of Service (DDoS) attack or infected systems participating in a botnet.

- **Query Failures**
  Frequent DNS query failures indicate that the source may be conducting DNS query probing, checking for misconfigurations or protective mechanisms for further penetration and intrusion.

- **Excessive or Suspicious Subdomains**
  Analyze subdomains in DNS queries. Look for excessively long or suspicious subdomain strings, as they may be used to obfuscate malicious activities. For example, subdomains like "login.paypal.com.malicious.com" may indicate phishing behavior.

- **Reverse DNS Lookups**
  Perform reverse DNS lookups on IP addresses from DNS queries originating from your network. Check if IP addresses correspond to known malicious servers or are associated with suspicious activities.

- **DNS Tunnels**
  DNS tunnels are a technique malicious software uses for covert data exfiltration. Monitor DNS queries with abnormally long payloads or unusual characters, as they may be related to data leakage.

- **Time and Geographical Analysis**
  Analyze the time and geographical location of DNS queries. Unexpected DNS queries initiated from unusual locations or at unusual times may indicate malicious activity or compromised devices.

About URMAZI Networks Inc.

Specializing in DNS-based cybersecurity, we integrate extensive experience to develop iSafer, our flagship solution addressing enterprise cybersecurity needs. With the USRA research team leveraging AI for early threat detection, we swiftly respond to global challenges, making URMAZI your trusted partner for cutting-edge cybersecurity solutions.

