Brochure

Free DNS Risk Assessment

Maximize Your Network Security & Efficiency

87% of organizations suffer attacks via DNS

IDC 2021 Global DNS Threat Report

Identify Vulnerabilities: Expert Assessment of Your DNS Traffic

Getting an accurate visibility and traffic analysis capacity is key to understanding, preventing and protecting against security threats.

In order to help you better understand the usage context and behavior of your DNS clients, EfficientIP offers an expert assessment involving analysis of real DNS traffic.

Benefits

- Reveal gaps in your current security layer and receive recommendations
- Identify threats already on your network, such as:
  - Malicious domains
  - DGA domains
- Discover how to mitigate different attack types
- Identify usage behavior and anomalies of your DNS, including:
  - Top requested domains
  - Query requests by type
    e.g. NX Domain Errors
- Learn how to improve functioning of your DNS

How it Works

1. User DNS data dumped in PCAP format (tcpdump, netsh, ...)
2. Data uploaded or shared with EfficientIP contact
3. Analysis performed off-site to check DNS usage and identify suspicious behavior

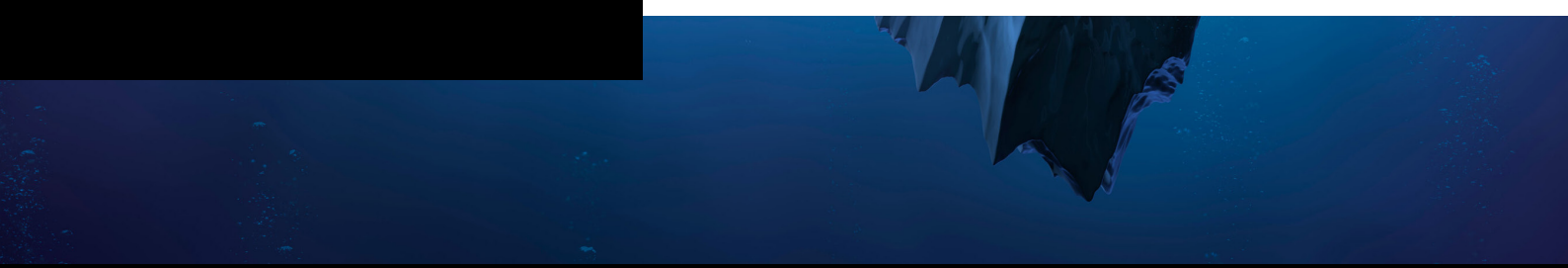
What You'll Receive:

A Detailed Assessment Report Containing:

- Checks performed & summary of results
- Details about DNS clients' behavior / malicious domains identified
- Recommended actions to improve protection against data theft, security of resources and user experience

Results Presentation to Your Technical and Management Teams

- Explanation of assessment results
- Review of recommended actions



efficient iP®

91% of malware are using DNS

Cisco 2016 Security Report

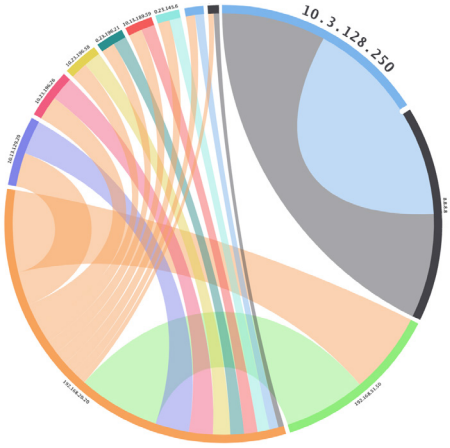
Understanding DNS: Mission-Critical for Network Services & Application Access

Managing network services has become incredibly complex with trends such as Cloud, BYoD and Shadow IT. DNS service is mission-critical for controlling access to applications & services, hence considered the cornerstone of network infrastructures. However, DNS is open by nature and is rarely monitored or analysed, making it one of the primary targets for cyber criminals to gain command and control, exfiltrate data or redirect traffic.

Signature-based and traffic-threshold security solutions such as firewalls, anti-DoS or IPS are not designed to ensure DNS service availability and integrity. They have proved to be insufficient, even against some basic attacks and, of greater concern, are very susceptible to blocking legitimate clients (false positives). The consequences can be serious for your organization: business impact/downtime, data theft, embezzlement of money, brand damage.

The efficiency and security of your network, and hence your business services, depends largely on the integrity, performance and availability of your DNS.

Example Report Information You'll Receive



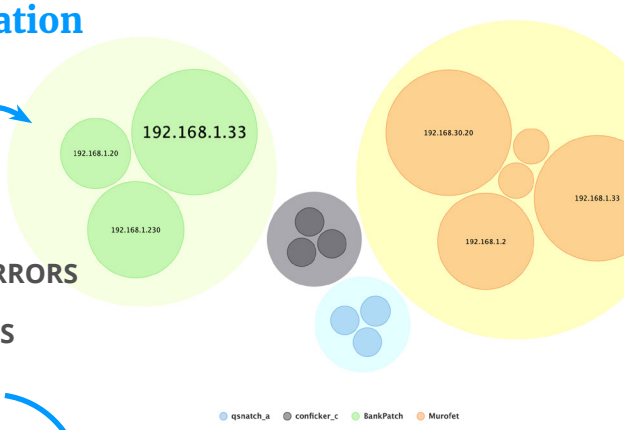
DGA DOMAINS

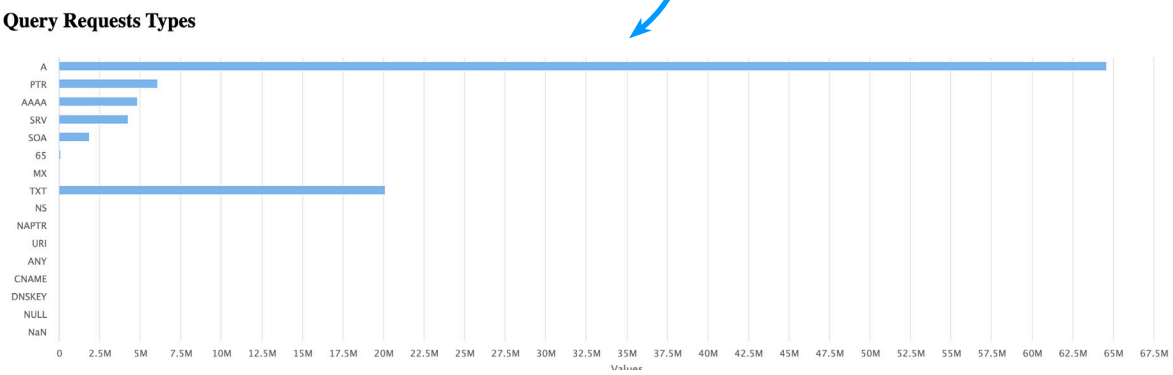
MALICIOUS DOMAINS

NX DOMAIN ERRORS/CONFIG ERRORS

TOP 100 COMMUNICATIONS

QUERY REQUEST TYPES





To sign up for your free DNS Risk Assessment, please contact us.

efficient iP®

REV C-220112

www.efficientip.com