efficient iP®

Solution Paper

Ensuring Data Confidentiality

Techniques to Protect Against Data Breaches via DNS

Contents:

Data exfiltration can be extremely difficult to detect as it often closely resembles typical network traffic. Substantial data loss incidents therefore only become noticed long after data exfiltration has already been achieved. DNS has been found to be one of the most discrete options for cyber criminals to carry out data theft[1].

The potential consequences of data exfiltration can be disastrous. They include:

- Theft of sensitive data or Intellectual Property
- Severe corporate brand damage and public media management costs
- Huge impact on customer/partner trust and associated increase in customer churn
- Regulatory non-compliance (GDPR, CCPA, NIS2, PDPA etc..), with associated massive fines

The aim of this paper is to describe how EfficientIP's innovative solutions can be used to effectively protect data confidentiality.

As summarized by Duncan Brown in the IDC Technology Spotlight: *"Enhanced DNS security is an added layer of protection when considering security and privacy for the network, data, and customers, while preserving reputation and enabling regulatory compliance such as GDPR."*

[1] According to a recent IDC survey, 29% of businesses experienced data exfiltration via DNS in the past 12 months.

The Importance of DNS in Network Infrastructures

In today's world of ever-evolving networks, the DNS service is recognized as one of the most critical IT services for any company in any industry. Being at the core of application routing makes it a fantastic source of information for getting accurate visibility and understanding of network activities/traffic. However, a non responding DNS service often leads to network blackout.

Despite this fact, DNS security is often overlooked. Taking advantage of this negligence, the threat ecosystem has become adept at launching attacks on or via DNS that can result in:

- Failed or slow access to Web sites and applications
- Denial of Service, impacting access to required data
- Re-routing Web traffic to unauthorized sites, resulting in stolen data or identity fraud
- Data Exfiltration

It's importance makes DNS extremely vulnerable to attacks, therefore requiring that DNS services be a major part of any company's security plan.

Why DNS is So Easy to Exploit for Data Theft

Since DNS isn't generally associated with data delivery, it is often overlooked. Cyber criminals benefit from this assumption to bypass security mechanisms for transporting sensitive data from inside to outside the enterprise.

The DNS protocol is manipulated to act either as a tunneling protocol or as a 'file transfer' protocol. Most businesses don't even know that data is being exfiltrated until it is too late.

The three main reasons why DNS is so easy to exploit are:

1. DNS traffic is not often analyzed (by 68% of companies - Cisco Security Report)
2. The Service is Open by Design and often not filtered properly at the network edge
3. It is connectionless (UDP) - and therefore difficult to track with existing network inspection tools, especially considering the high volume of DNS traffic.

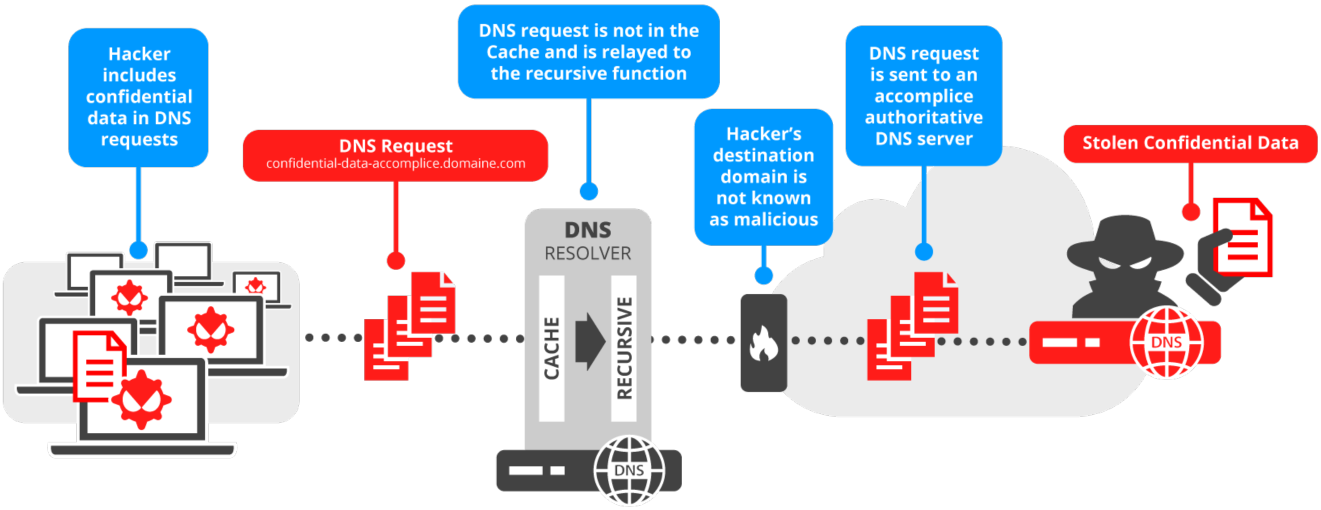
Standard Security Solutions Are Unable to Effectively Protect Against DNS-Based Data Exfiltration

Threats are dynamic by essence, meaning filtering rules need to be constantly updated. Firewalls are not adept at ensuring IP-based filtering rules are kept relevant in near-real time, so often the updates occur far too late to mitigate attacks. In addition, simply blacklisting a remote malicious IP is not an effective solution to prevent DNS exfiltration.

Furthermore, traditional detection algorithms focus only on DNS packet frequency, payload, data encoding, or entropy of the requests. Whilst this has the benefit of easily filtering part of the malicious traffic, it is easily abused, leaving existing security solutions blind to advanced DNS attacks. Standard security solutions also have no insight, at the heart of the DNS protocol, of sequences of query exchanges for every single DNS transaction across cache and recursive functions in order to understand the client's context . This peripheral analysis will never provide enough information to safely identify DNS tunneling, and security countermeasures can only be based on fragmented information. DNS tunneling therefore often goes completely unnoticed, allowing confidential data to be exfiltrated without triggering any alarms.

The countermeasures themselves are limited to merely blocking traffic or dropping suspect queries from suspected IP addresses. This leads to a high risk of legitimate traffic also being blocked (false positives) which will have significant impact on your business operations and bottom line.

Demonstrating that standard DNS security solution are not adapted is very easy. Simple tests, using hacker tools available on the web, enable passing through Next-Gen Firewall, proxy or DLP systems.


Hacker includes confidential data in DNS requests
DNS Request
confidential-data-accomplice.domaine.com
DNS request is not in the Cache and is relayed to the recursive function
DNS
RESOLVER
CACHE
RECURSIVE
DNS
Hacker's destination domain is not known as malicious
DNS request is sent to an accomplice authoritative DNS server
Stolen Confidential Data
DNS

Abnormal use of the Cache Function by Clients Cannot be Detected by NGFW

DNS Guardian: Advanced Protection for Data Confidentiality

EfficientIP is a leading provider of appliance-based DNS security solutions for network protection. We offer a purpose-built threat detection solution, with adaptive countermeasures. Built directly into the DNS server, which is in the path of exfiltration, the DNS Guardian solution provides real-time detection, without the need to add additional network infrastructure or agents.

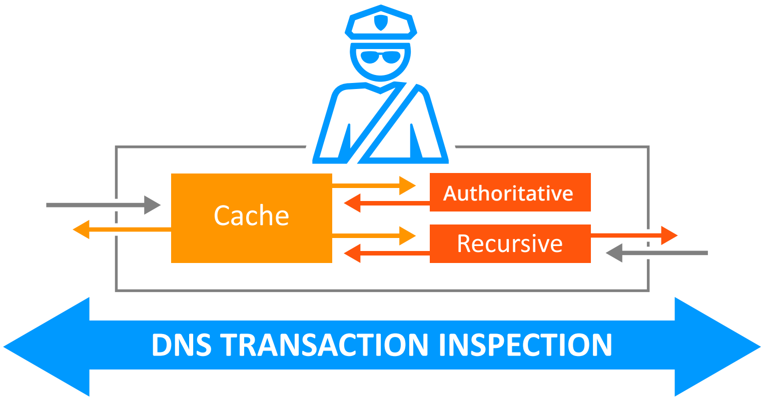
Our approach to data protection consists of: 1) Use of real-time DNS analytics for behavioral threat detection 2) Deployment of adaptive countermeasures to block DNS-based data exfiltration.

Fast remediation and centralized reporting functionalities are then added to enhance the data confidentiality protection process.

Real-time DNS Analytics for Behavioral Threat Detection, with No Performance Impact

The DNS protocol allows for a large variety of queries and records to be exchanged between a client (via his browser) and external servers. Although this facilitates data exfiltration, such queries look atypical compared with normal traffic.

DNS Guardian is the first and unique market solution offering complete DNS Transaction Inspection (DTI), in real-time and without any performance impact. Because the DNS Guardian solution sits deep down between the local cache and the recursive DNS server, it is able to assess the validity and correctness of DNS traffic in the specific context of each enterprise. In essence, DNS Guardian assesses how a normal and benign DNS request/response looks and acts, and then compares this baseline against traffic.



DNS Guardian DTI

> *« Importantly, EfficientIP continuously monitors complete DNS transactions, which may incorporate multiple request/response pairs. This means that hackers attempting to stay below the radar in terms of, for example, record length or frequency, are still very likely to be detected quickly by the system. »*
>
> - IDC Technology Spotlight: Dealing with DNS-Based Data Breaches to Avoid GDPR Non-Compliance

The DTI innovation allows for a complete understanding of the client's context, overcoming limitations of signature-based security systems that only offer limited peripheral traffic visibility. This is key for delivering true DNS analytics and behavioral threat detection capabilities.

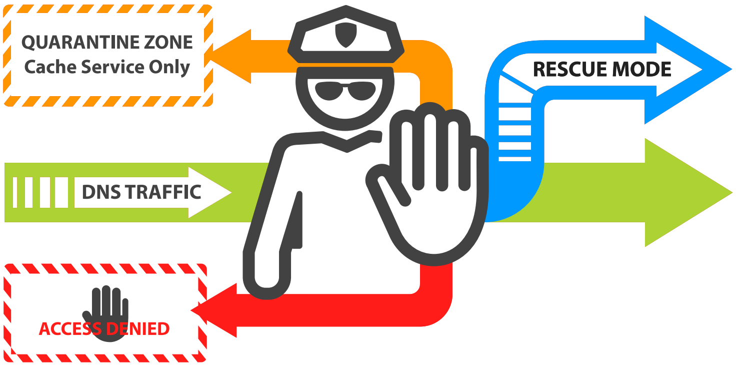
This complete DNS Transaction Inspection (DTI) allows build up of a powerful, substantial base of intelligence around DNS services. It provides an adaptive capability that is kept current despite new domains being created and registered (for example, using DGAs). This means that a suspect client activity can be detected even before the related domain has been specified as being malicious. It also helps eliminate the risk of blocking or quarantining legitimate traffic, as it can interpret the difference between a legitimate customer and a malicious actor.

Near Real-time Threat Intelligence for countering exfiltration for countering exfiltration can be obtained by combining DNS Guardian with EfficientIP's DNS Firewall. This maximizes threat response efficiency, permitting permanent blackholing of locally identified suspicious domains. Additional benefit can be obtained from external security feeds e.g. SURBL, that provide security intelligence from global traffic analysis, leveraging machine learning and predictive analytics. This provides enhanced protection against malware and advanced persistent threats (APTs) by disrupting the ability of infected devices to communicate with command-and-control (C&C) sites and botnets.

Contrary to most other solutions on the market, statistics are collected globally and trends are analyzed on a per-client basis. This global approach helps security operations take the best course of action for mitigation. Furthermore, when integrated with the security ecosystem, the IP data provided helps to find and isolate the suspicious client.

Adaptive Countermeasures: Protect DNS Services Continuity and Data Confidentiality

DNS Guardian provides a variety of solutions that act as countermeasures (examples listed below) against data exfiltration and more general DNS-based attacks, practically eliminating the risk of false positives whilst protecting against non-identifiable attack sources. A key feature of the solution is the separation of the DNS cache and recursive functions. This allows each function to be individually protected, enabling the cache-based function to operate independently of the state of the recursive function.



- Block source IPs of the attacks
- Rate Limit DNS traffic per IP source
- Quarantine Mode (patented): Malicious IP addresses given unrestricted access to cache data only - recursive requests are blocked. Reduces the risk of blocking legitimate clients
- Rescue Mode (patented): Ensure service continuity even if attack source is unidentifiable. Ensures 100% accessibility to most critical business applications and services

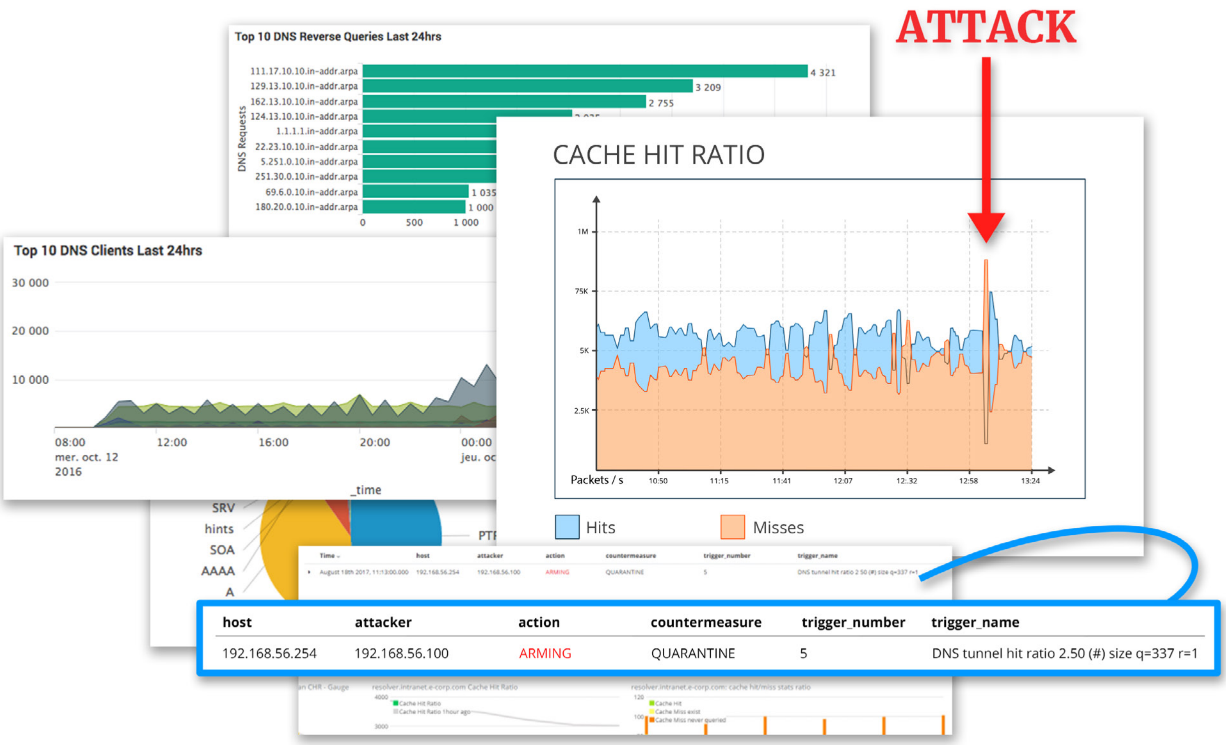
Smart adaptive countermeasures

Fast Remediation

Visibility into the infected devices or potential rogue employees provides detailed information such as device type, IP address, MAC address, and most importantly, the user associated with the device trying to exfiltrate data. This reduces time to repair and accelerates the remediation process.

Centralized, detailed reporting: to monitor & analyze your network, devices and applications

Details are provided on malicious activities and infected devices. Log enrichment via SIEM is possible when Splunk is used (alerts used to create enhanced log).



host	attacker	action	countermeasure	trigger_number	trigger_name
192.168.56.254	192.168.56.100	ARMING	QUARANTINE	5	DNS tunnel hit ratio 2.50 (#) size q=337 r=1

Detection of Data Exfiltration - Example Information

EfficientIP Interaction with Other Security Components

Working with Data-loss Prevention Solutions

The majority of data-loss prevention (DLP) solutions protect against data leakage via email, web, FTP etc. by monitoring data. However, they never consider DNS-based exfiltration. EfficientIP complements traditional DLP solutions by closing this gap, thus preventing DNS from being used as a back door for data theft. The most effective way to address DNS-based data exfiltration is to build intelligent detection capabilities directly into the DNS infrastructure. Both sets of information gathered can then be sent to SIEM to provide enhanced reporting.

Automating Threat Response through Integration

As well as performing the critical functions of detecting and blocking data exfiltration attempts, lightning-fast remediation of the infected devices is necessary. This can be achieved by tighter integration between detection technologies and endpoint remediation solutions or NACs such as Cisco ISE to provide indicators of compromise when an endpoint is trying to exfiltrate data. Via this intelligence, the malicious process is automatically banned from future execution and connection. The infected endpoint is quarantined, even if it is outside the enterprise, and data theft prevented.

Conclusion

DNS data exfiltration is an effective means of sending data outside an organization.This paper has highlighted that everything should be considered to be a potential threat to your network operations and more importantly to data confidentiality within your company. The introduction of stricter regulations like NIS2, DORA, PIPEDA and HIPAA adds another dimension to data theft, affecting organizations globally.

Businesses need to look beyond traditional security solutions which have proven to be ineffective against data exfiltration via DNS. Fortunately, the innovative technologies provided by EfficientIP offer comprehensive protection against data breaches. Security is now embedded in the DNS servers themselves, and uses the DNS's own mechanisms to protect against attacks. Being cost-effective (no additional components or agents required) and having no impact on DNS performance, the DNS Guardian and DNS Firewall solutions go a long way towards protecting data confidentiality, helping ensure your company avoids serious brand damage or massive fines from regulatory non-compliance.

efficient iP®

REV: C-230223

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752