Brochure

Free DNS Data Exfiltration Test

Proactively Protect Your Network Against Data Theft & Ransomware

Benefits

- Detect risk of data exfiltration
- Avoid data theft fines (GDPR, US CLOUD, PDPA...)
- Reveal weaknesses in your current security layer and receive recommendations
- Learn from proven security experts about improving reliability of your DNS
- Discover adaptive countermeasures to protect your network

24% of companies suffer data theft via DNS

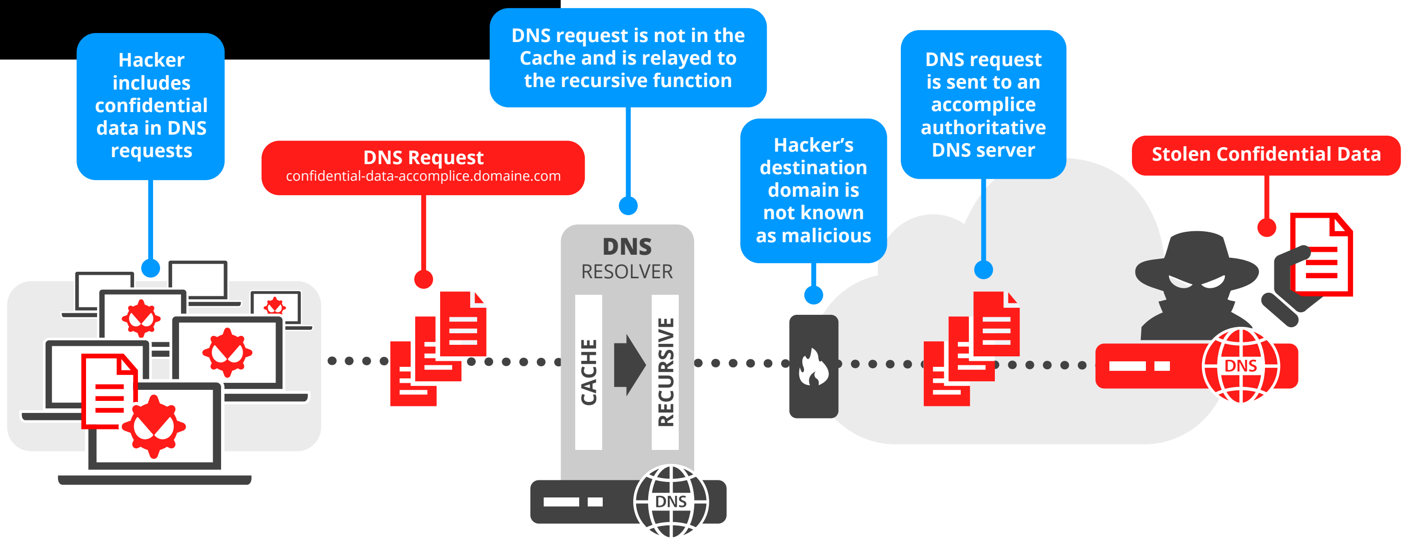
- IDC 2022 Global DNS Threat Report -

Understanding Why DNS is a Favorite Target 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 used as either a tunneling protocol or as a 'file transfer' protocol.

Firewalls and Data Loss Prevention (DLP) systems find it difficult to detect this exfiltration in a timely manner, so most businesses don't even know that data is being stolen until it is too late.

To protect data confidentiality, organizations need to look beyond traditional security solutions which have proven to be ineffective against data exfiltration via DNS.


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

How hackers exfiltrate data via DNS

efficient iP®

Test Your Protection Against Data Breaches via DNS

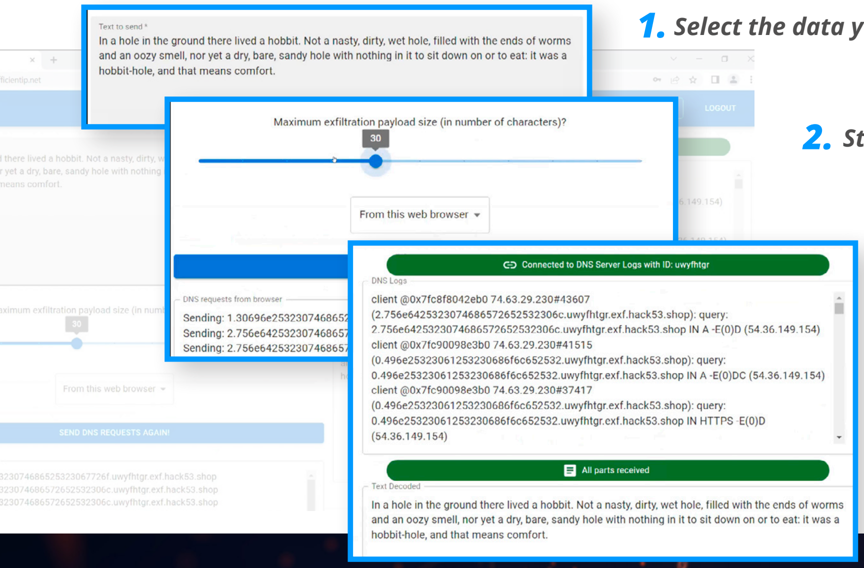
EfficientIP provides you access to a web tool using a URL for you to conduct a data exfiltration test on your network.

The test is a structured “ethical attack” on your DNS system to identify if data exfiltration using DNS is possible. It uses the same non-intrusive tools and techniques that real attackers use to break into networks, without impacting your infrastructure.

3 Quick, Easy, Non-Intrusive Steps

To perform the test, a website unknown to all DNS services will be used.

The web tool, maintained by EfficientIP, will generate different DNS requests to exfiltrate your data on the client side, execute them directly from the browser, and display the result in real time on the DNS server side eg. outside of your network. From the web interface as illustrated below, you will be able to:



Text to send *
In a hole in the ground there lived a hobbit. Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat: it was a hobbit-hole, and that means comfort.

Maximum exfiltration payload size (in number of characters)? 30

From this web browser

DNS requests from browser

```
Sending: 1.30696e2532307468652
Sending: 2.756e642532307468657
Sending: 2.756e642532307468657
```

Connected to DNS Server Logs with ID: uwyfhtgr

DNS Logs

```
client @0x7fc8f8042eb0 74.63.29.230#43607
(2.756e6425323074686572652532306c.uwyfhtgr.exf.hack53.shop): query:
2.756e6425323074686572652532306c.uwyfhtgr.exf.hack53.shop IN A -E(0)D (54.36.149.154)
client @0x7fc90098e3b0 74.63.29.230#41515
(0.496e25323061253230686f6c652532.uwyfhtgr.exf.hack53.shop): query:
0.496e25323061253230686f6c652532.uwyfhtgr.exf.hack53.shop IN A -E(0)DC (54.36.149.154)
client @0x7fc90098e3b0 74.63.29.230#37417
(0.496e25323061253230686f6c652532.uwyfhtgr.exf.hack53.shop): query:
0.496e25323061253230686f6c652532.uwyfhtgr.exf.hack53.shop IN HTTPS -E(0)D
(54.36.149.154)
```

All parts received

Text Decoded
In a hole in the ground there lived a hobbit. Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat: it was a hobbit-hole, and that means comfort.

***1.** Select the data you want to exfiltrate*

***2.** Start the exfiltration test*

***3.** Watch the data being exfiltrated in real-time!*

By running the test, you will know if your network and data are at risk against data exfiltration then be able to decide how to improve your security posture.

What is Included

Pre-briefing with your team:

- ✓ Understand your DNS configuration - authoritative & recursive DNS
- ✓ Explanation of scope and objectives of the test

DNS data exfiltration test on your DNS servers:

- ✓ Check for lack of protection against data exfiltration
- ✓ Read-only actions performed, no configuration modifications
- ✓ Carried out using EfficientIP’s specifically-designed tool

Post-briefing:

- ✓ Explanation of test results
- ✓ Recommended actions & countermeasures

Test duration:
5 to 15 Minutes

Cost:
Free of Charge

To sign up for your Free DNS Data Exfiltration Test, please contact us.

efficient iP®

REV C-220112

www.efficientip.com