



mxcx

Follow

Mar 30 · 4 min read

# DNS Data exfiltration—What is this and How to use?

*Summary: To test or exploit blind RCE, XXE,... the first thing which you think usually is outbound connection. Unfortunate, many importance servers are dropped the outbound connection. In such cases, you can use the DNS protocol to exfiltrate data. In this topic, I will talk about that technique. There are 2 parts:*

- 1. What is DNS Data exfiltration and how does it work.*
- 2. I will introduce my new product (the <http://requestbin.net>) which have a tool for Data exfiltration through DNS protocol.*

## 1. What is DNS Data exfiltration and how does it work?

**What is DNS Data exfiltration?**

Actually, this is not new technical, according to the Akamai, this technique is about 20 years old. In a simple definition, DNS Data exfiltration is way to exchange data between 2 computers without any directly connection, the data is exchanged through DNS protocol on intermediate DNS servers.

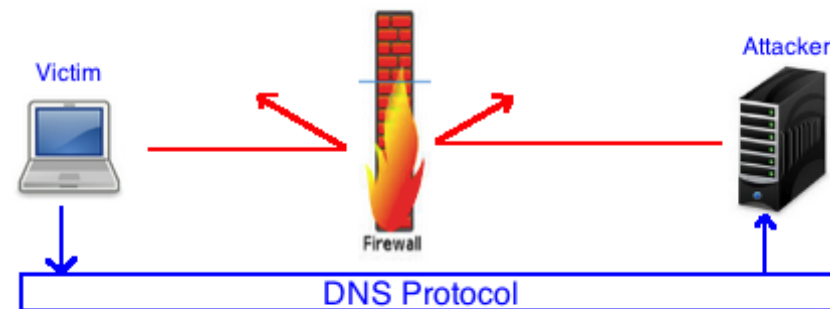
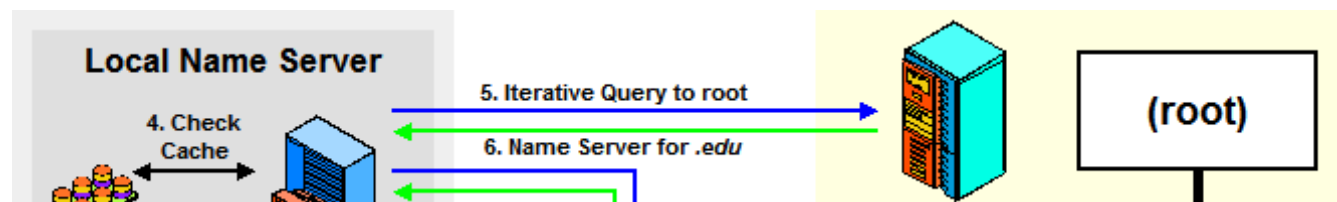


Figure 1. A simple definition of DNS Data exfiltration

## How does it work?

Back to basic, please follow a DNS resolution flow:



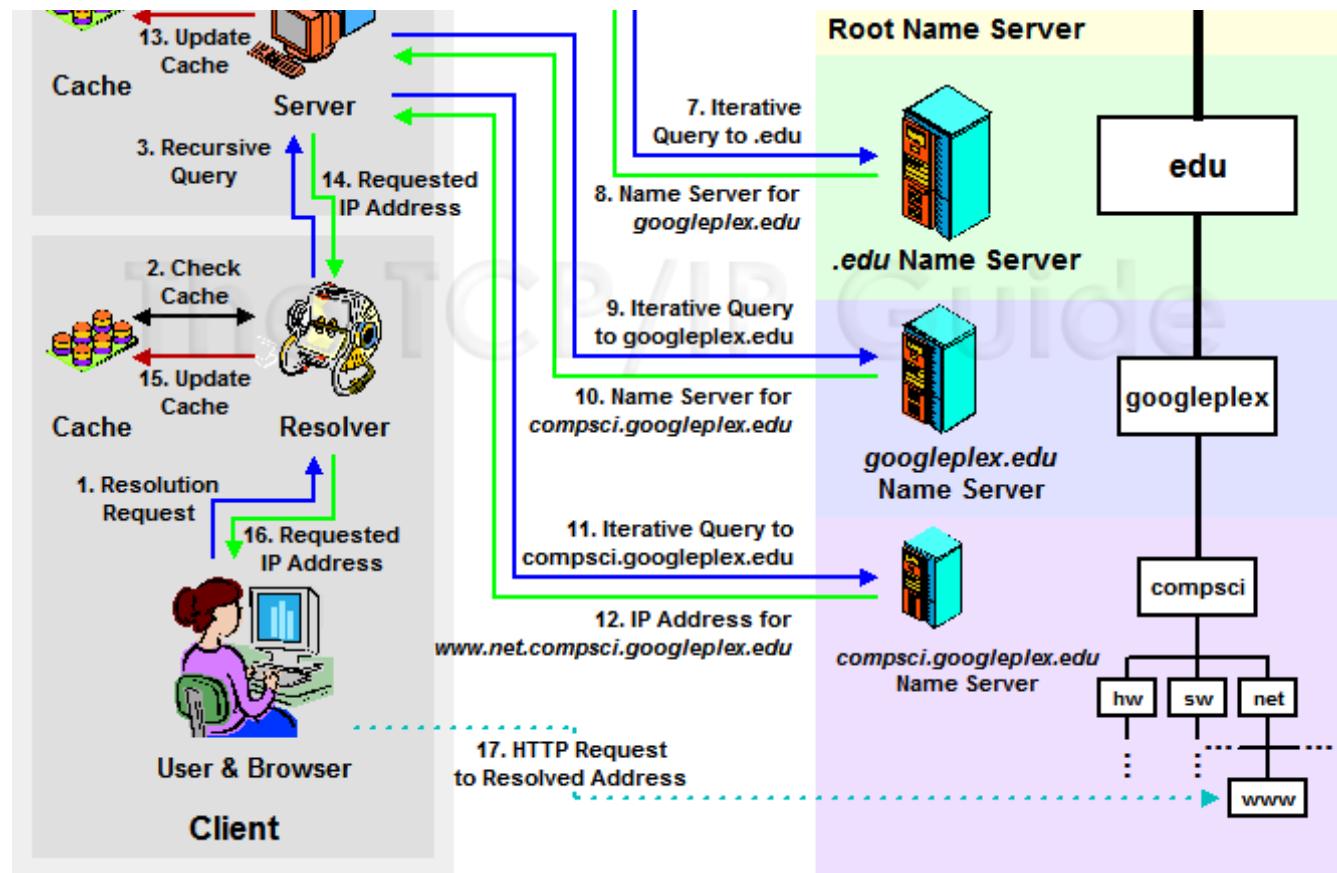


Figure 2. A DNS resolution flow (source: tcpipguide.com)

If you have managed a domain, please notice at step 9 and 11, client's DNS Server (for example 8.8.8.8) will connect to a name servers returned from step 8 and 10; These name servers is settable via the Registrar's DNS manager (for example: Go Daddy, Name Cheap,...). By setting the name servers (use

NS records) be your own server, you can inspect to the request from client's DNS Server.

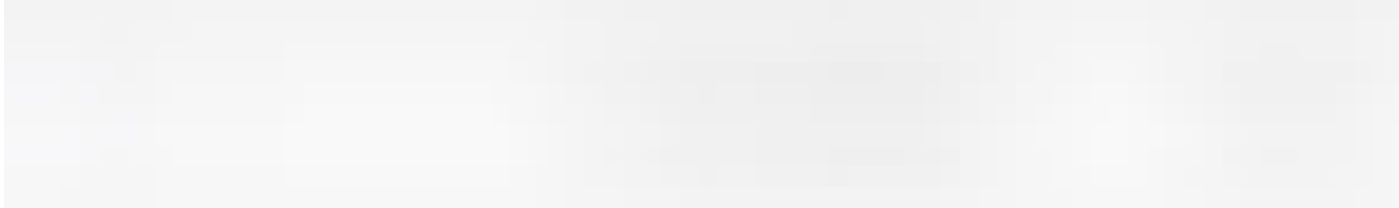


Figure 3. A setting of NS records

Follow above settings, if ns1.requestbin.net is yours, you can view all subdomain which client requested. Attacker will put data into subdomain and receive it at the name server side. So, that is way to send data from victim (client) to attacker (the name server).





Figure 4. An example which uses DNS Data exfiltration (source: [blogs.akamai.com](https://blogs.akamai.com))

In above example, the attacker wants to leak the password from compromised machine. The domain exfiltration.com is attacker's and already set NS record to a server he owns. The malware in this case will make a dns resolution a domain which includes text content of the password is subdomain of the exfiltration.com. After that, attacker will view log at name server to get the password.

### **How to send data from outside to inside?**

Similar to above technique, the client still make a dns resolution to exfiltration.com. However, instead of responding an A record, attacker's name server will response a CNAME or TXT record which allow large unstructured strings to be sent from attacker to victim.

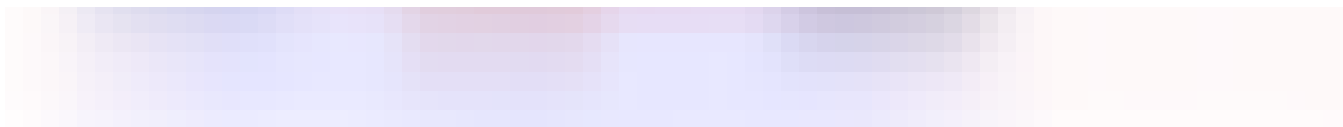


Figure 5. Use CNAME record to send data from outside

## So, about DNS Tunnel?

Of course, when you can send and receive data on DNS protocol, you can make a tunnel on that. With that technique, you will ssh, remote desktop or connect to any services of internal server. I will talk more about this technique in another topic.

In case you are interested in this, please read some bellow articles:

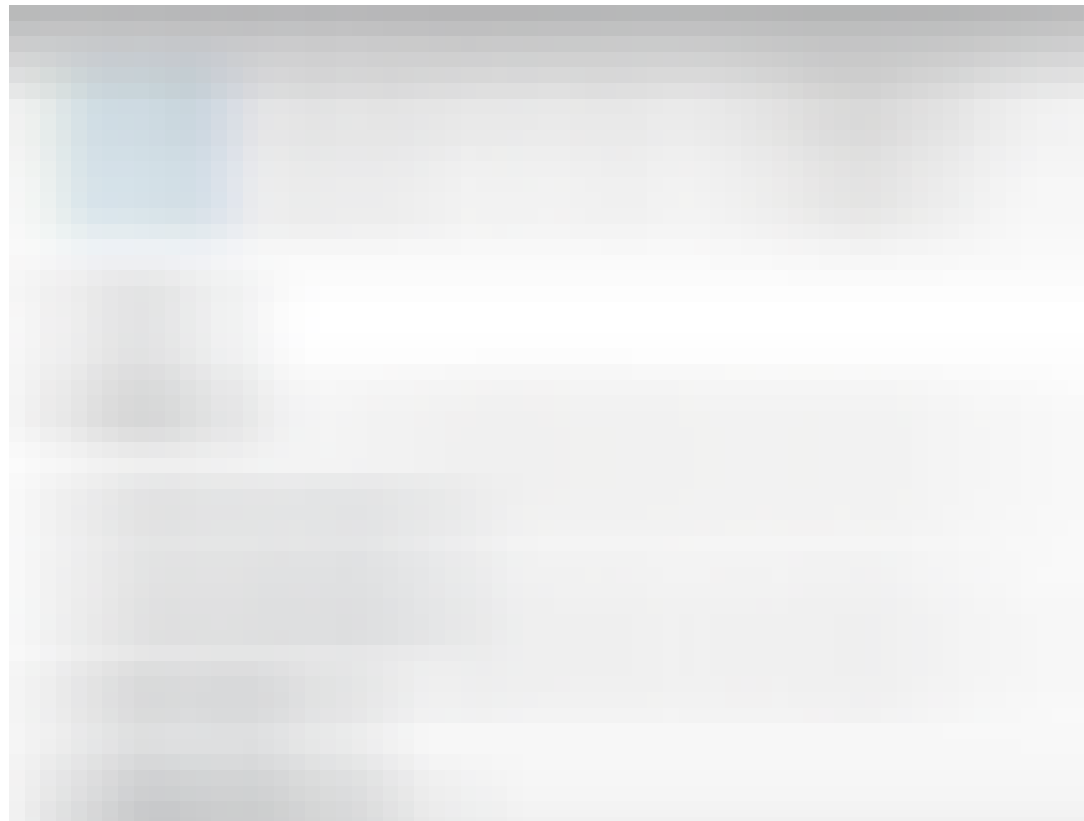
[DNS Data Exfiltration—How it works](#)

[Data Exfiltration \(Tunneling\) Attacks against Corporate Network](#)

## 2. How to use DNS Data exfiltration?

Follow the first part, to use the DNS Data exfiltration, you must at least have a domain and a name server which is setup to dns package inspection. It's not complicate but not easy for anyone.

So, I have built a website (<http://requestbin.net/dns>) which supports to check some cases like blind RCE, XXE,.. and supports to send/receive data between outside and inside. And in particular, it's very easy to use.



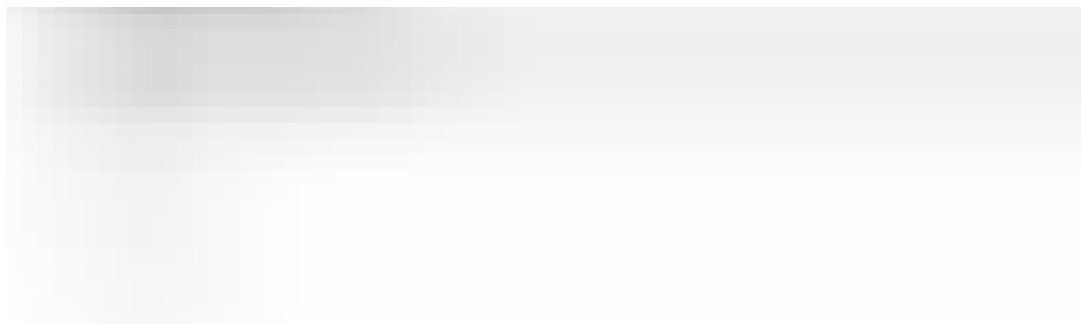


Figure 6. Screenshot of requestbin.net/dns

When visit the website, you maybe feel familiar about the interface. My website is based on requestb.in (<https://github.com/Runscope/requestbin>) which was down someday before and the code of DNS Data exfiltration is based on DNSBin (<https://github.com/HoLyVieR/dnsbin>)

In case you're interested in this code, please visit the repository:

<https://github.com/mxcxvn/requestbin.net>

Any feedback is welcomed, please contact me at [mxcxvn\[at\]gmail\[dot\]com](mailto:mxcxvn[at]gmail[dot]com)

DNS

Requestbin

Httpbin

Dnsbin

Data Exfiltration



---

## One clap, two clap, three clap, forty?

By clapping more or less, you can signal to us which stories really stand out.

72



**mxcx**

Follow




**FOSEC**

It's all about security

Follow

### Responses

 Write a response...