WildFire Decryptor
(c) 2016 Intel Security
---

August 23, 2016

The WildFire Decryptor is a command line tool that can decrypt some files encrypted by the WildFire ransomware family.

Commands:
---

| | |
|---|---|
| -e : -- extractid [File Path] | Extracts the User ID from an unaltered ransom note. |
| -f : -- file [File Path] | This is the file to decrypt. |
| -h : -- help | Prints tool instructions to the console. |
| -p : -- password [Password File Path] | Indicates the password file to be used to decrypt. |
| -u : --userid [User ID] | Indicates the User ID to locate a potential decryption key. |

Usage:
---

To use this tool, you must have access to the User ID created by the ransomware sample. The User ID is a 10 character alphanumeric string found within the ransom note. In many cases, it is in a text file on the system's desktop (e.g. HOW_TO_UNLOCK_FILES_README_(2a321bd202).txt.). If you wish to have the tool extract the User ID, use the extract command. Switch the file name to the ransom file name generated on the system:

```
>wildfiredecrypt.exe –e HOW_TO_UNLOCK_FILES_README_(2a321bd202).txt
```

1. Run the command with the User ID:

```
>wildfiredecrypt.exe -u 2a321bd202
```

You will receive a URL output to the console. Copy this URL into a browser and download the linked text file. If you get a message such as "404 file not found" or "[Error] Cannot find file", then we have been unable to locate the private key that encrypted the files.

In this example, you have downloaded the private key file 2a321bd202.txt. You can now run another command to decrypt the files. Suppose you wish to decrypt the file

```
"2016 Taxes #WildFire_Locker#3615a1##.pdf.wflx"
```

2. Run the command with the private key file and the file you wish to decrypt

```
>wildfiredecrypt.exe -p 2a321bd202.txt -f "2016 Taxes #WildFire_Locker#3615a1##.pdf.wflx"
```

The tool will attempt to decrypt the contents of the file and the file name. If successful the decrypted file will be located in the same directory.