Shade Decryptor
(c) 2016 Intel Security

July 25, 2016

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

Commands:

-f : --file [File Path]	This is the file to decrypt.
-h : --help	Print tool instructions to the console.
-k [Key File Path] : --keyfile [Key File Path]	Supply the private key file path to decrypt files.
-u [User ID] : --userid [User ID]	Supply 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 20 character alphanumeric string found within the ransom note. In many cases, it is in a text file on the system's desktop (Readme1.txt, Readme2.txt, etc.). Here is an example message from a ransom note:

> To decrypt files you should send the following code:
> F7AB2CA6D04AC4DA110C
> to e-mail address xxxxxxxx@xxxx.com

In this example, "F7AB2CA6D04AC4DA110C" is the User ID.

1. Run the command with the User ID:

```
>shadedecrypt.exe -u F7AB2CA6D04AC4DA110C
```

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 F7AB2CA6D04AC4DA110C.txt. You can now run another command to decrypt the files. Suppose you wish to decrypt the file

```
"OTQvpF2egoNQWEfV0nx2fvJborhsuPYhCMBkr-FySQQ=.xtbl"
```

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

```
>shadedecrypt.exe -k F7AB2CA6D04AC4DA110C.txt -f
OTQvpF2egoNQWEfV0nx2fvJborhsuPYhCMBkr-FySQQ=.xtbl
```

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. If the contents of the file were successfully decrypted but the file name was not, then a new file will be created with a ".decrypted" extension.