Fillezilla is used in many organizations for proper file transfers. For example purposes, this writeup is for a PoC of how easy it is to obtain filezilla credentials on a user machine.

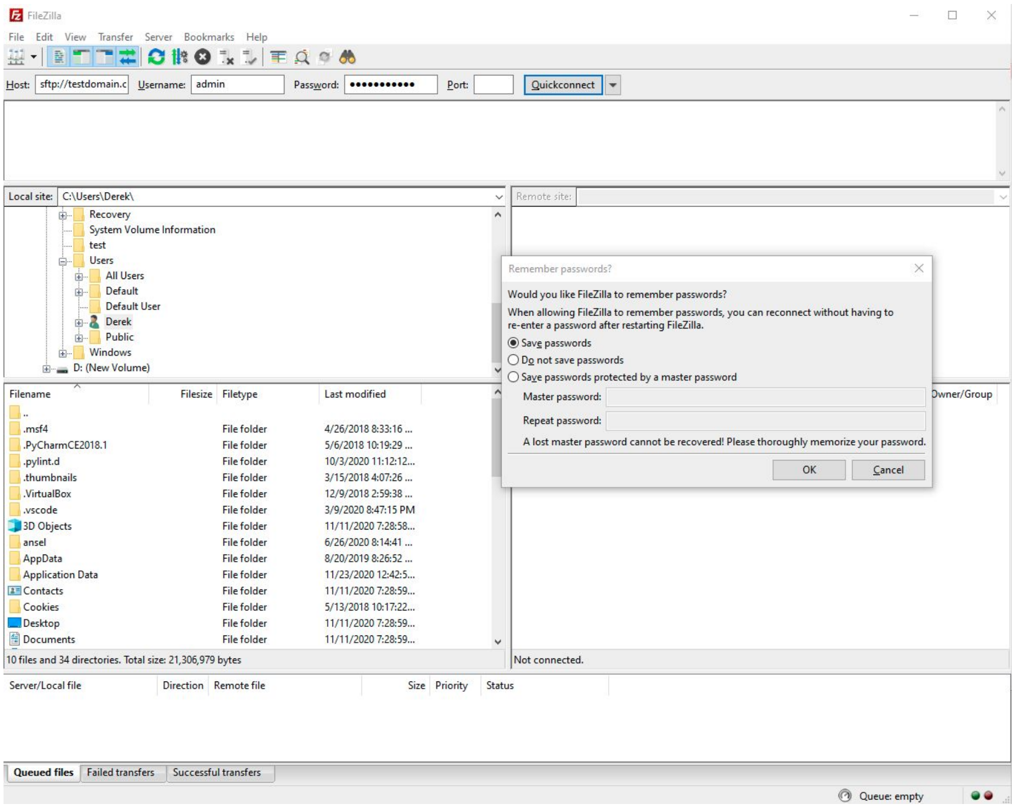
I am connecting to the following ftp servers:

Domain: testdomain.com
Username: admin
Password: password123
Port: 21

AND

Domain: Ftp.dlptest.com
Username: dlpuser@dlptest.com
Password: eUj8GeW55SvYaswqUyDSm5v6N
Port: 21
Source: https://dlptest.com/ftp-test/

In the latest version of filezilla, users are prompted to save passwords. Most will do so for easy access. Recently, Filezilla has added an option to create a master password, but we will not explore that here yet. Let's assume we are saving passwords without setting a master password.



Host: sftp://testdomain.c Username: admin Password: ●●●●●●●●●●● Port:

Local site: C:\Users\Derek\

Remote site:

Remember passwords?

Would you like FileZilla to remember passwords?

When allowing FileZilla to remember passwords, you can reconnect without having to re-enter a password after restarting FileZilla.

● Save passwords
○ Do not save passwords
○ Save passwords protected by a master password

Master password:
Repeat password:

A lost master password cannot be recovered! Please thoroughly memorize your password.

OK Cancel

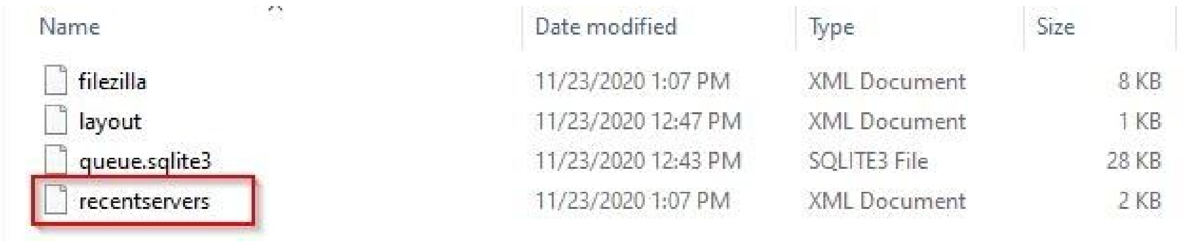
Filename	Filesize	Filetype	Last modified
..			
.msf4		File folder	4/26/2018 8:33:16 ...
.PyCharmCE2018.1		File folder	5/6/2018 10:19:29 ...
.pylint.d		File folder	10/3/2020 11:12:12...
.thumbnails		File folder	3/15/2018 4:07:26 ...
.VirtualBox		File folder	12/9/2018 2:59:38 ...
.vscode		File folder	3/9/2020 8:47:15 PM
3D Objects		File folder	11/11/2020 7:28:58...
ansel		File folder	6/26/2020 8:14:41 ...
AppData		File folder	8/20/2019 8:26:52 ...
Application Data		File folder	11/23/2020 12:42:5...
Contacts		File folder	11/11/2020 7:28:59...
Cookies		File folder	5/13/2018 10:17:22...
Desktop		File folder	11/11/2020 7:28:59...
Documents		File folder	11/11/2020 7:28:59...

10 files and 34 directories. Total size: 21,306,979 bytes

Not connected.

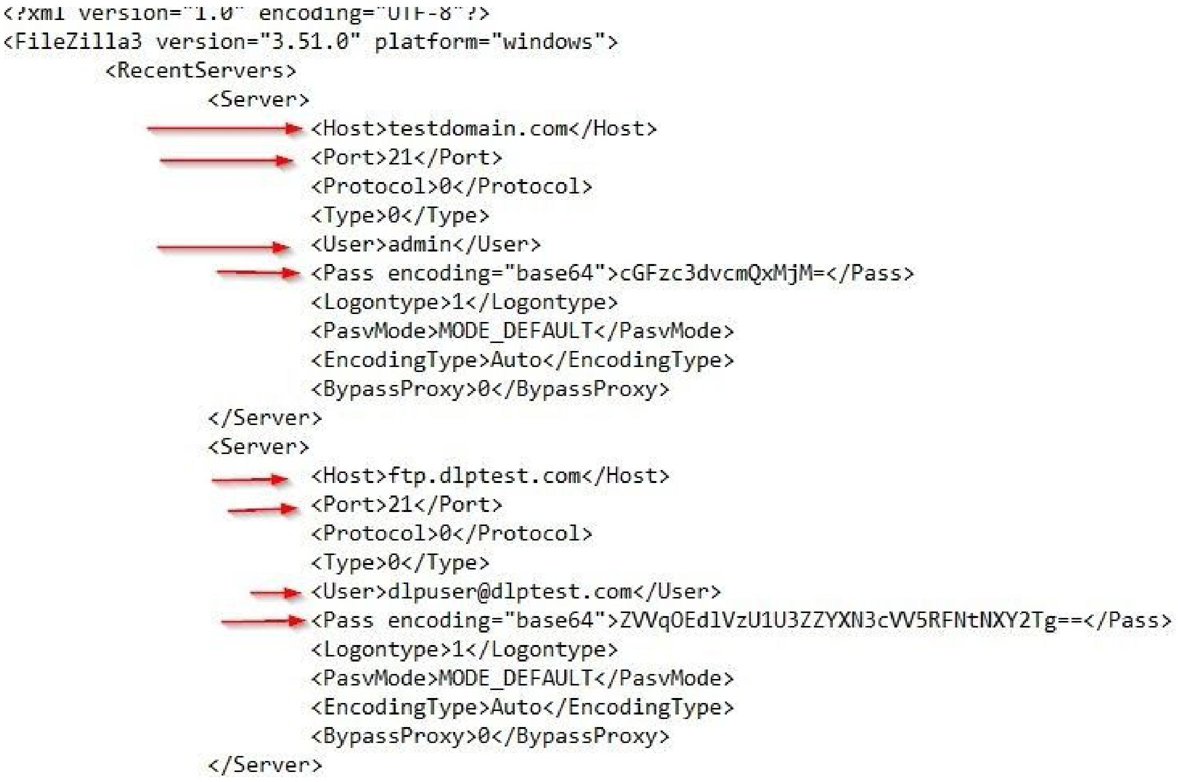
Server/Local file	Direction	Remote file	Size	Priority	Status

Once you connect to an ftp server, the credential information is stored in an XML file locally. The directory is **C:\Users\<current user>\AppData\Roaming\FileZilla\** and the file is **recentservers.xml**



Name	Date modified	Type	Size
filezilla	11/23/2020 1:07 PM	XML Document	8 KB
layout	11/23/2020 12:47 PM	XML Document	1 KB
queue.sqlite3	11/23/2020 12:43 PM	SQLITE3 File	28 KB
recentservers	11/23/2020 1:07 PM	XML Document	2 KB

Once you open the xml file in Notepad, the following is shown:



```
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.51.0" platform="windows">
        <RecentServers>
                <Server>
                        <Host>testdomain.com</Host>
                        <Port>21</Port>
                        <Protocol>0</Protocol>
                        <Type>0</Type>
                        <User>admin</User>
                        <Pass encoding="base64">cGFzc3dvcmQxMjM=</Pass>
                        <Logontype>1</Logontype>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <EncodingType>Auto</EncodingType>
                        <BypassProxy>0</BypassProxy>
                </Server>
                <Server>
                        <Host>ftp.dlptest.com</Host>
                        <Port>21</Port>
                        <Protocol>0</Protocol>
                        <Type>0</Type>
                        <User>dlpuser@dlptest.com</User>
                        <Pass encoding="base64">ZVVqOEdlVzU1U3ZZYXN3cVV5RFNtNXY2Tg==</Pass>
                        <Logontype>1</Logontype>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <EncodingType>Auto</EncodingType>
                        <BypassProxy>0</BypassProxy>
                </Server>
```

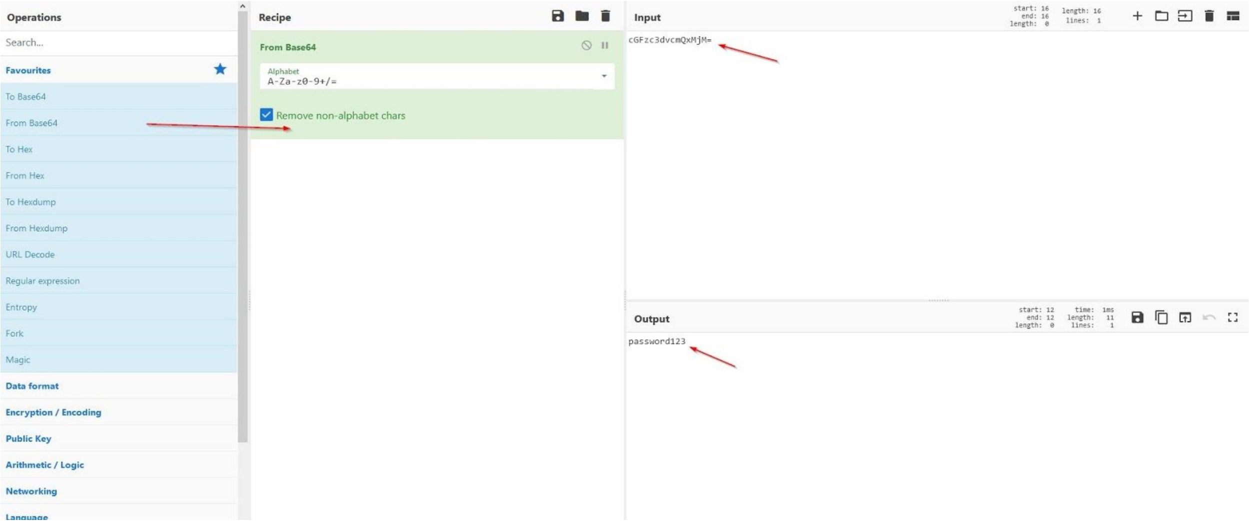
The Host, Username, and port used are all in plaintext. The following passwords are encoded in base64:

Testdomain.com = cGFzc3dvcmQxMjM=
Ftp.dlptest.com = ZVVqOEdlVzU1U3ZZYXN3cVV5RFNtNXY2Tg==

You might be saying: “Big deal, you cannot read these passwords anyway”. Let’s view how we can read them.

Cyberchef (http://icyberchef.com/):

My favorite tool for something like this Cyberchef. Simply search for the “From Base64” recipe on the far left, drag it to the middle column, and place the base64 in the input box! Below is the base64 output for testdomain.com and ftp.dlptest.com respectively:



From Base64

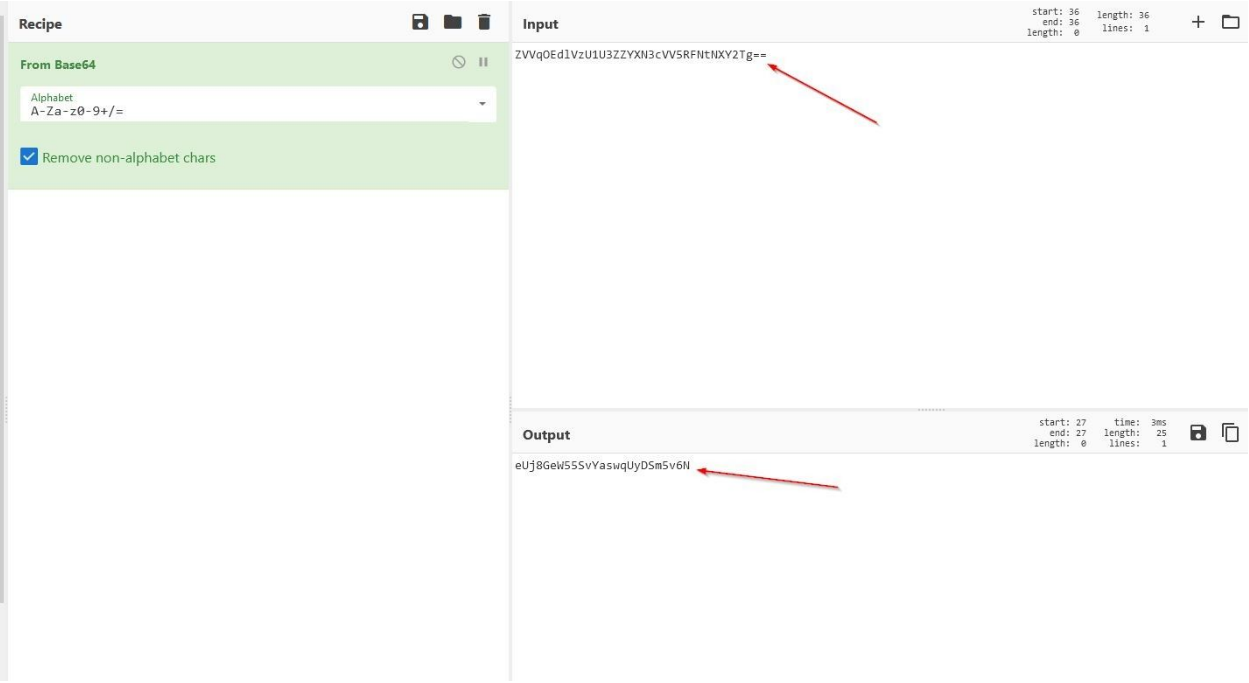
Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

```
cGFzc3dvcmQxMjM=
```

```
password123
```

Ftp.dlptest.com:



From Base64

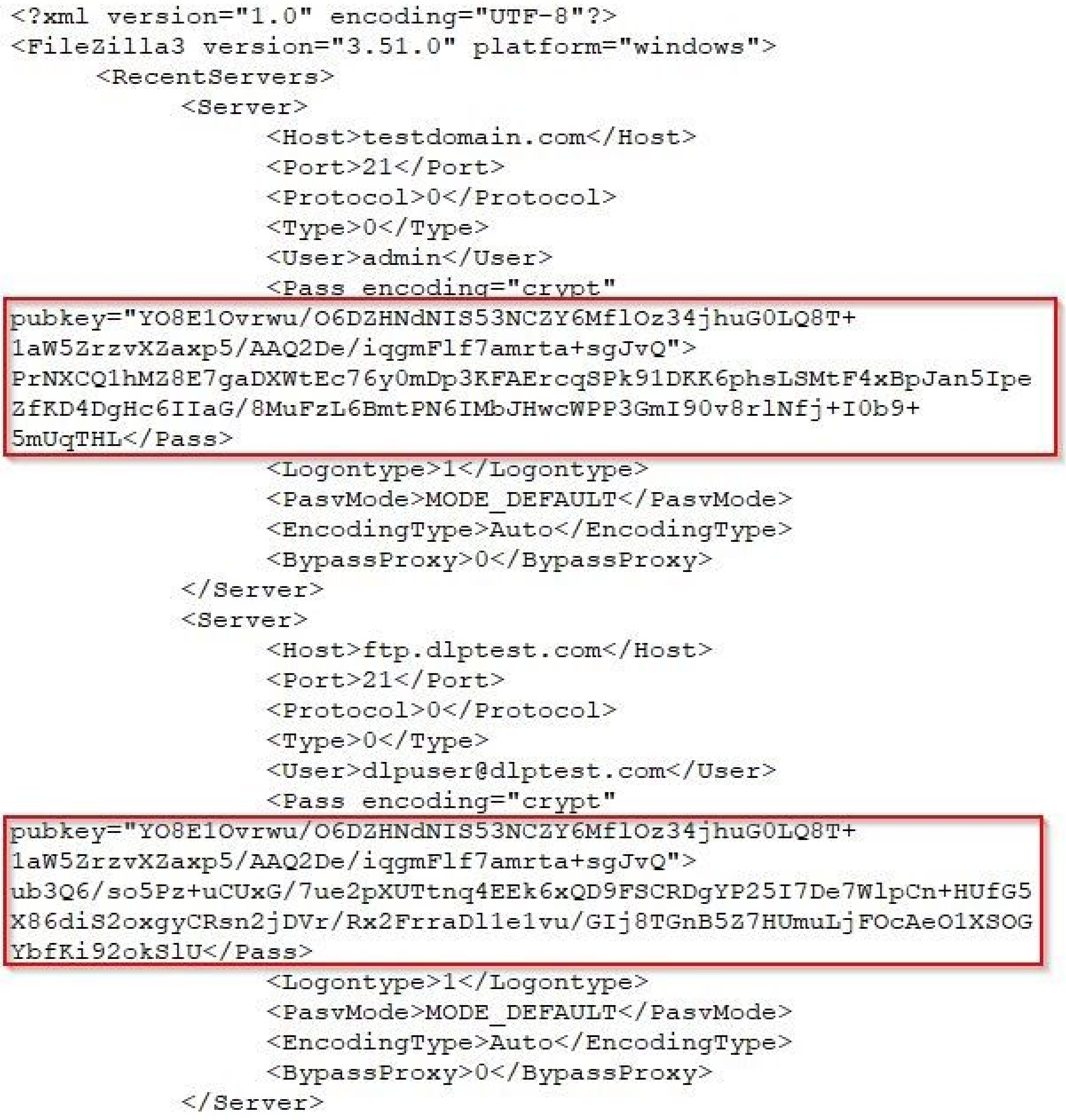
Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

```
ZVVqOEdlVzU1U3ZZYXN3cVV5RFNtNXY2Tg==
```

```
eUj8GeW55SvYaswqUyDSm5v6N
```

Filezilla is a great tool, but installed without oversight can lead to pivoting and eventually information disclosure for malicious users inside the network if not managed properly inside an organization. As I said earlier in the review, Filezilla now has a master password option. This stores the passwords in a much secure way shown below:



```
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.51.0" platform="windows">
      <RecentServers>
            <Server>
                  <Host>testdomain.com</Host>
                  <Port>21</Port>
                  <Protocol>0</Protocol>
                  <Type>0</Type>
                  <User>admin</User>
                  <Pass encoding="crypt"
pubkey="YO8E1Ovrwu/O6DZHNdNIS53NCZY6Mf1Oz34jhuG0LQ8T+
1aW5ZrzvXZaxp5/AAQ2De/iqgmFlf7amrta+sgJvQ">
PrNXCQ1hMZ8E7gaDXWtEc76y0mDp3KFAErcqSPk91DKK6phsLSMtF4xBpJan5Ipe
ZfKD4DgHc6IIaG/8MuFzL6BmtPN6IMbJHwcWPP3GmI90v8rlNfj+I0b9+
5mUqTHL</Pass>
                  <Logontype>1</Logontype>
                  <PasvMode>MODE_DEFAULT</PasvMode>
                  <EncodingType>Auto</EncodingType>
                  <BypassProxy>0</BypassProxy>
            </Server>
            <Server>
                  <Host>ftp.dlptest.com</Host>
                  <Port>21</Port>
                  <Protocol>0</Protocol>
                  <Type>0</Type>
                  <User>dlpuser@dlptest.com</User>
                  <Pass encoding="crypt"
pubkey="YO8E1Ovrwu/O6DZHNdNIS53NCZY6Mf1Oz34jhuG0LQ8T+
1aW5ZrzvXZaxp5/AAQ2De/iqgmFlf7amrta+sgJvQ">
ub3Q6/so5Pz+uCUxG/7ue2pXUTtnq4EEk6xQD9FSCRDgYP25I7De7WlpCn+HUfG5
X86diS2oxgyCRsn2jDVr/Rx2FrraDl1e1vu/GIj8TGnB5Z7HUmuLjFOcAeO1XSOG
YbfKi92okSlU</Pass>
                  <Logontype>1</Logontype>
                  <PasvMode>MODE_DEFAULT</PasvMode>
                  <EncodingType>Auto</EncodingType>
                  <BypassProxy>0</BypassProxy>
            </Server>
```

The best suggestion to mitigate this risk would be to set this Master password setting, use a complex password as the master password, and store the password in a password manager. This will ensure all ftp and sftp credentials multiple layers of protection.