Mailto (NetWalker) Ransomware Targets Enterprise Networks

bleepingcomputer.com/news/security/mailto-netwalker-ransomware-targets-enterprise-networks/

Lawrence Abrams

By
Lawrence Abrams

- February 5, 2020
- 04:08 PM
- 5

With the high ransom prices and big payouts of enterprise-targeting ransomware, we now have another ransomware known as Mailto or Netwalker that is compromising enterprise networks and encrypting all of the Windows devices connected to it.

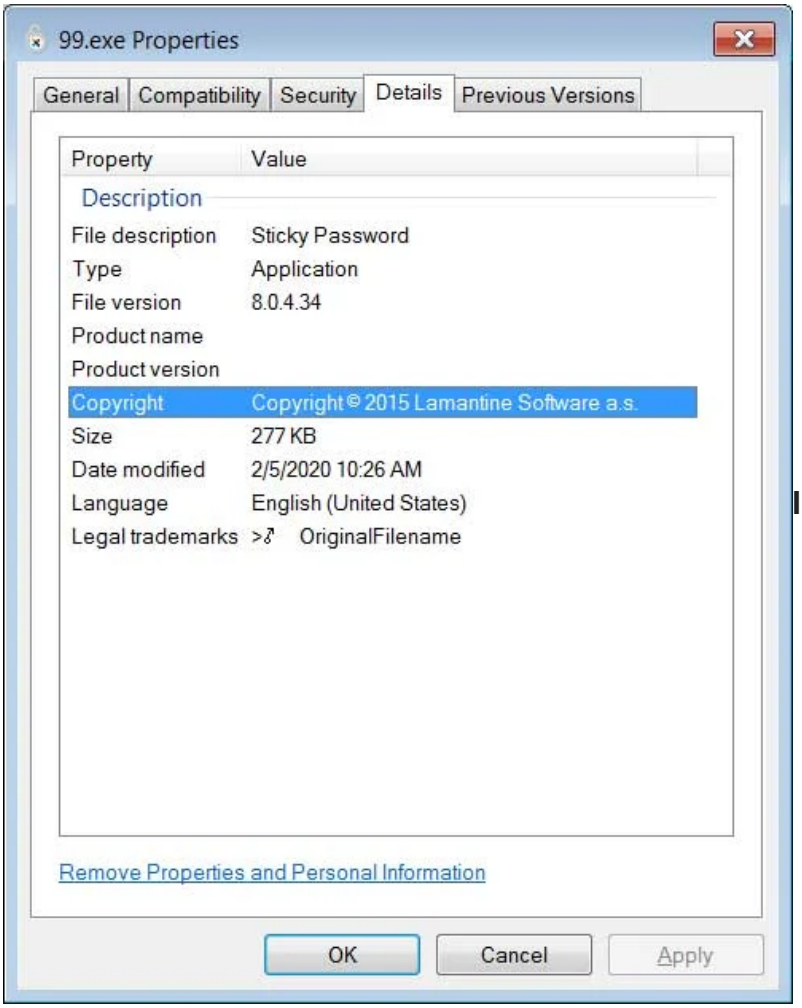
In August 2019 a new ransomware was spotted in ID Ransomware that was named Mailto based on the extension that was appended to encrypted files.

It was not known until today when the Australian Toll Group disclosed that their network was attacked by the Mailto ransomware, that we discovered that this ransomware is targeting the enterprise.

It should be noted that the ransomware has been commonly called the Mailto Ransomware due to the appended extension, but analysis of one of its decryptors indicates that it is named Netwalker. We will discuss this later in the article.

The Mailto / Netwalker ransomware

In a recent sample of the Mailto ransomware shared with BleepingComputer by MalwareHunterTeam, the executable attempts to impersonate the 'Sticky Password' software.



Impersonating Sticky Password

When executed, the ransomware uses an embedded config that includes the ransom note template, ransom note file names, length of id/extension, whitelisted files, folders, and extensions, and various other configuration options.

According to Head of SentinelLabs Vitali Kremez who also analyzed the ransomware, the configuration is quite sophisticated and detailed compared to other ransomware infections.

"The ransomware and its group have one of the more granular and more sophisticated configurations observed," Kremez told BleepingComputer.

The configuration that was embedded in the analyzed sample can be found here.

```
{
 "mpk :"EXgCIpycIJzspm07Loi9L5uOcxC+VZ/NjxWfOn7UqVE=",
 "mode :0,
 "thr :1500,
 "spsz :16384,
 "namesz :6,
 "idsz :5,
 "crmask :".mailto[{mail1}].{id}",
 "mail :["sevenoneone@cock.li" ,"kavariusing@tutanota.com"],
 "lfile :"{ID}-Readme.txt",
 "lend
 :"SGkhDQpZb3VyIGZpbGVzIGFyZSBlbmNyeXB0ZWQuDQpBbGwgZW5jcnlwdGVkIGZpbGVzIGZvciB0aGlzIGNvbXB1dGVyIGhhcyBleHRlb
 nNpb246IC57aWR9DQoNCi0tDQoNCklmIGZvciBzb21lIHJlYXNvbiB5b3UgcmVhZCB0aGlzIHRleHQgYmVmb3JlIHRoZSBlbmNyeXB0aW9u
 IGVuZGVkLA0KdGhpcyBjYW4gYmUgdW5kZXJzdG9vZCBieSB0aGUgZmFjdCB0aGF0IHRoZSBjb21wdXRlciBzbG93cyBkb3duLCANCmFuZCB
 5b3VyIGhlYXJ0IHJhdGUgaGFzIGluY3JlYXNlZCBkdWUgdG8gdGhlIGFiaWxpdHkgdG8gdHVybiBpdCBvZmYsDQp0aGVuIHdlIHJlY29tbW
 VuZCB0aGF0IHlvdSBtb3ZlIGF3YXkgZnJvbSB0aGUgY29tcHV0ZXIgYW5kIGFjY2VwdCB0aGF0IHlvdSBoYXZlIGJlZW4gY29tcHJvbWlzZ
 WQsDQpyZWJvb3Rpbmcvc2h1dGRvd24gd2lsbCBjYXVzZSB5b3UgdG8gbG9zZSBmaWxlcyB3aXRob3V0IHRoZSBwb3NzaWJpbGl0eSBvZiBy
 ZWNvdmVyeSBhbmQgZXZlbiBnb2Qgd2lsbCBub3QgYmUgYWJsZSB0byBoZWxwIHlvdSwNCml0IGNvdWxkIGJlIGZpbGVzIG9uIHRoZSBuZXR
 3b3JrIGJlbG9uZ2luZyB0byBvdGhlciB1c2Vycywgc3VyZSB5b3Ugd2FudCB0byB0YWtlIHRoYXQgcmVzcG9uc2liaWxpdHk/DQoNCi0tDQ
 oNCk91ciBlbmNyeXB0aW9uIGFsZ29yaXRobXMgYXJlIHZlcnkgc3Ryb25nIGFuZCB5b3VyIGZpbGVzIGFyZSB2ZXJ5IHdlbGwgcHJvdGVjd
 GVkLCB5b3UgY2FuJ3QgaG9wZSB0byByZWNvdmVyIHRoZW0gd2l0aG91dCBvdXIgaGVscC4NClRoZSBvbmx5IHdheSB0byBnZXQgeW91ciBm
 aWxlcyBiYWNrIGlzIHRvIGNvb3BlcmF0ZSB3aXRoIHVzIGFuZCBnZXQgdGhlIGRlY3J5cHRlciBwcm9ncmFtLg0KRG8gbm90IHRyeSB0byB
 yZWNvdmVyIHlvdXIgZmlsZXMgd2l0aG91dCBhIGRlY3J5cHQgcHJvZ3JhbSwgeW91IG1heSBkYW1hZ2UgdGhlbSBhbmQgdGhlbiB0aGV5IH
 dpbGwgYmUgaW1wb3NzaWJsZSB0byByZWNvdmVyLg0KDQpXZSBhZHZpc2UgeW91IHRvIGNvbnRhY3QgdXMgYXMgc29vbiBhcyBwb3NzaWJsZ
 Swgb3RoZXJ3aXNlIHRoZXJlIGlzIGEgcG9zc2liaWxpdHkgdGhhdCB5b3VyIGZpbGVzIHdpbGwgbmV2ZXIgYmUgcmV0dXJuZWQuDQpGb3Ig
 dXMgdGhpcyBpcyBqdXN0IGJ1c2luZXNzIGFuZCB0byBwcm92ZSB0byB5b3Ugb3VyIHNlcmlvdXNuZXNzLCB3ZSB3aWxsIGRlY3J5cHQgeW9
 1IHNvbWUgZmlsZXMgZm9yIGZyZWUsIA0KYnV0IHdlIHdpbGwgbm90IHdhaXQgZm9yIHlvdXIgbGV0dGVyIGZvciBhIGxvbmcgdGltZSwgbW
 FpbCBjYW4gYmUgYWJ1c2VkLCB3ZSBhcmUgbW92aW5nIG9uLCBodXJyeSB1cCB3aXRoIHRoZSBkZWNpc2lvbi4NCg0K0KFvbnRhY3QgdXM6D
 QoxLnttYWlsMX0NCjIue21haWwyfQ0KDQpEb24ndCBmb3JnZXQgdG8gaW5jbHVkZSB5b3VyIGNvZGUgaW4gdGhlIGVtYWlsOg0Ke2NvZGV9
 ",
 "white :{
    "path :["*system volume
    information","*windows.old","*:\users\*\*temp","*msocache","*:\winnt","*$windows.~ws","*perflogs","*boot
    ","*:\windows","*:\program file*","\vmware","\\*\users\*\*temp","\\*\winnt
    nt","\\*\windows","*\program
    file*\vmwaree","*appdata*microsoft","*appdata*packages","*microsoft\provisioning","*dvd
    maker","*Internet Explorer","*Mozilla","*Old Firefox data","*\program file*\windows media*","*\program
    file*\windows portable*","*windows defender","*\program file*\windows nt","*\program file*\windows
```

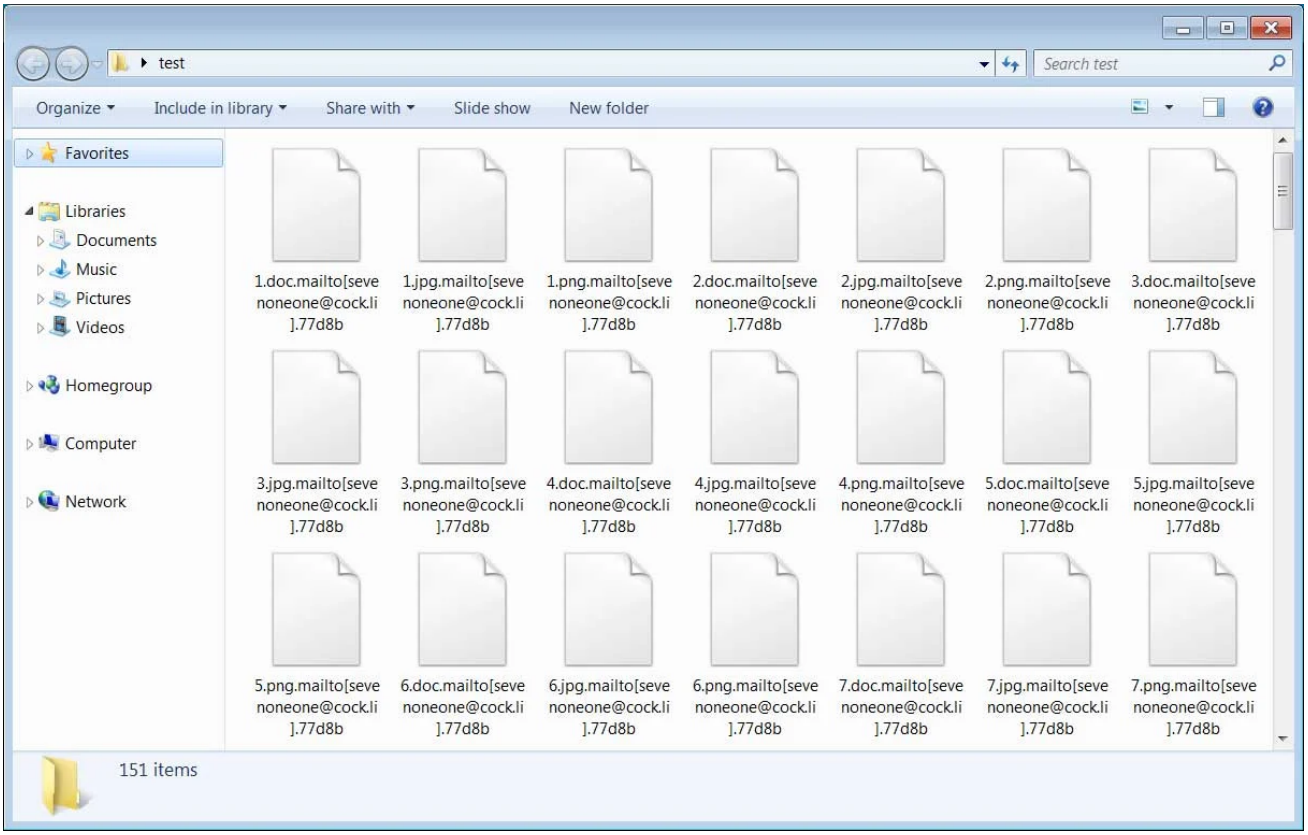

Ransomware config

While almost all current ransomware infections utilize a whitelist of folders, files, and extensions that will be skipped, Mailto utilizes a much longer list of whitelisted folders and files than we normally see.

For example, below is the list of folders that will be skipped from being encrypted.

```
*system volume information
*windows.old
*:\users\*\*temp
*msocache
*:\winnt
*$windows.~ws
*perflogs
*boot
*:\windows
*:\program file*
\vmware
\\*\users\*\*temp
\\*\winnt nt
\\*\windows
*\program file*\vmwaree
*appdata*microsoft
*appdata*packages
*microsoft\provisioning
*dvd maker
*Internet Explorer
*Mozilla
*Old Firefox data
*\program file*\windows media*
*\program file*\windows portable*
*windows defender
*\program file*\windows nt
*\program file*\windows photo*
*\program file*\windows side*
*\program file*\windowspowershell
*\program file*\cuas*
*\program file*\microsoft games
*\program file*\common files\system em
*\program file*\common files\*shared
*\program file*\common files\reference ass*
*\windows\cache*
*temporary internet*
*media player
*:\users\*\appdata\*\microsoft
\\*\users\*\appdata\*\microsoft
```

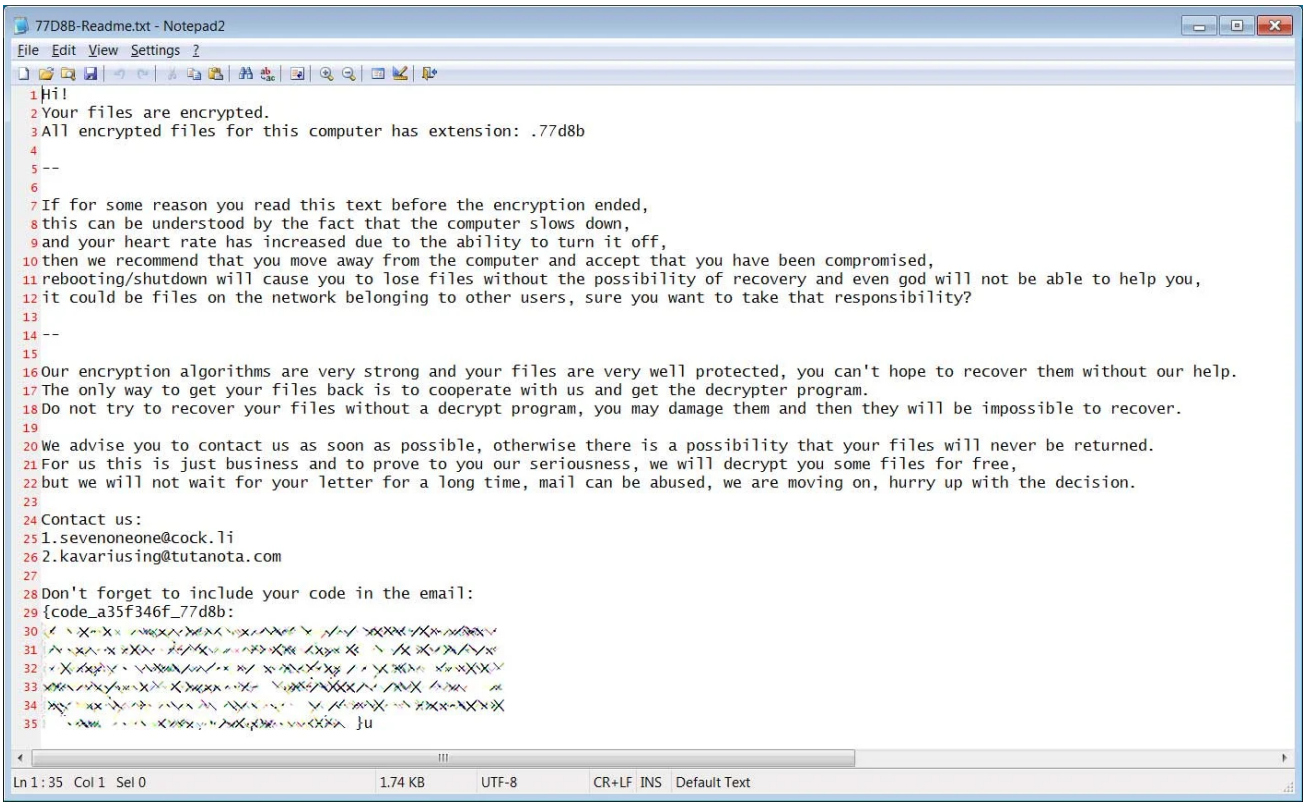
When encrypting files, the Mailto ransomware will append an extension using the format .mailto[{mail1}].{id}. For example, a file named 1.doc will be encrypted and renamed to 1.doc.mailto[sevenoneone@cock.li].77d8b as seen below.



Encrypted Files

The ransomware will also create ransom notes named using the file name format of {ID}-Readme.txt. For example, in our test run the ransom note was named 77D8B-Readme.txt.

This ransom note will contain information on what happened to the computer and two email addresses that can be used to get the payment amount and instructions.



Mailto / Netwalker Ransom Note

This ransomware is still being analyzed and it is not known if there are any weaknesses in the encryption algorithm that can be used to decrypt files for free. If anything is discovered, we will be sure to let everyone know.

For now, those who are infected can discuss this ransomware and receive support in our dedicated Mailto / Netwalker Ransomware Support & Help Topic.

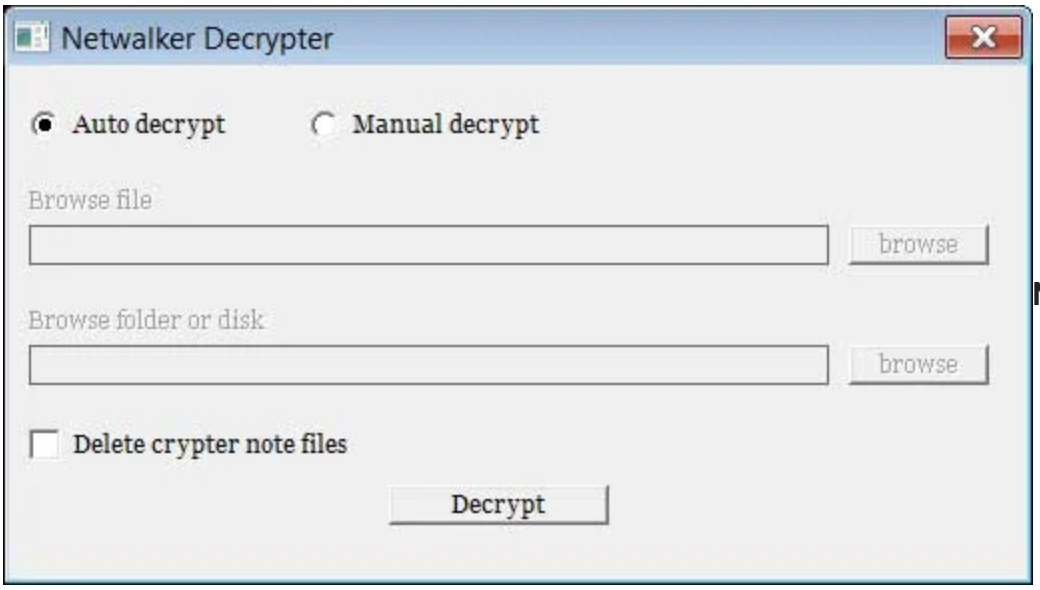
Is it named Mailto or Netwalker?

When new ransomware infections are found, the discoverer or researchers will typically look for some indication as to the name given to it by the ransomware developer.

When a ransomware does not provide any clues as to its name, in many cases the ransomware will be named after the extension appended to encrypted files.

As the Mailto ransomware did not have any underlying hints as to its real name, at the time of discovery it was just called Mailto based on the extension.

Soon after, Coveware discovered a decryptor for the ransomware that indicated that the developer's name for the infection is 'Netwalker'.



Netwalker Decrypter

In situations like this, it is difficult to decide what name we should continue to call the ransomware.

On one hand, we clearly know its name is Netwalker, but on the other hand, the victims know it as Mailto and most of the helpful information out there utilizes that name.

To make it easier for victims, we decided to continue to refer to this ransomware as Mailto, but the names can be used interchangeably

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:

```
416556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443e8e
```

Associated files:

```
{ID}-Readme.txt
```

Mailto email addresses:

sevenoneone@cock.li
kavariusing@tutanota.com

Ransom note text:

```
Hi!
Your files are encrypted.
All encrypted files for this computer has extension: .{id}

--

If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been
compromised,
rebooting/shutdown will cause you to lose files without the possibility of recovery
and even god will not be able to help you,
it could be files on the network belonging to other users, sure you want to take
that responsibility?

--

Our encryption algorithms are very strong and your files are very well protected,
you can't hope to recover them without our help.
The only way to get your files back is to cooperate with us and get the decrypter
program.
Do not try to recover your files without a decrypt program, you may damage them and
then they will be impossible to recover.

We advise you to contact us as soon as possible, otherwise there is a possibility
that your files will never be returned.
For us this is just business and to prove to you our seriousness, we will decrypt
you some files for free,
but we will not wait for your letter for a long time, mail can be abused, we are
moving on, hurry up with the decision.

Contact us:
1.{mail1}
2.{mail2}

Don't forget to include your code in the email:
{code}
```

- Enterprise
- Mailto
- Netwalker
- Ransomware

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

- 

  Amigo-A - 2 years ago

  -
  -

  """As the Mailto ransomware did not have any underlying hints as to its real name, at the time of discovery it was just called Mailto based on the extension."""

  It is not right info. A screenshot of the decrypter that “proves” today the name was published 3 days after the first publication. That is September 9, 2019. Here are tweets by date. Look.
  https://twitter.com/GrujaRS/status/1169354031791300608
  https://twitter.com/demonslay335/status/1169623711785336832
  https://twitter.com/coveware/status/1171073312170139649

- 
  Lawrence Abrams - 2 years ago
  -
  -
  Thanks. Wasn't aware of the previous discovery. Fixed attribution.
- 
  Rangergroup - 2 years ago
  -
  -
  what other companies have been affected by Mailto other than Toll Australia?

- 

  npeep - 2 years ago

  -
  -

  Mine :\ For us it was through a "200.exe" that they pushed with psexec from a server that had an RDP vulnerability. 200.exe had "Glary Utilities" as it's name under its properties.

  Our .mailto email addresses were also different.
  1.johprohnpo@cock.li
  2.cancandecan@tutanota.com

  We are still very much in the middle of recovering. If anyone learns anything new about decrypting these, hit me up and lets talk.

- 

  All_Is_Lost - 2 years ago

  -
  -

  Virus ran on Saturday and the mailto email addresses are:

  1.johprohnpo@cock.li
  2.cancandecan@tutanota.com

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: