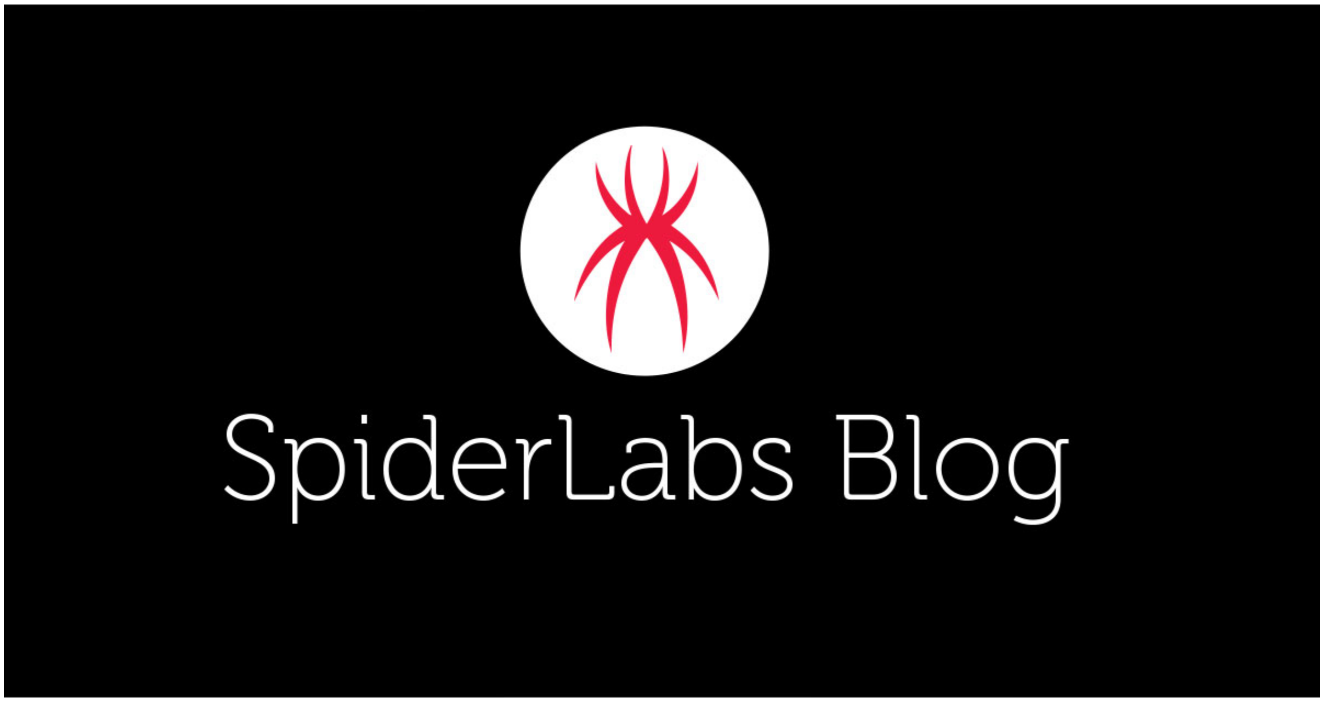
An In-depth Look at MailTo Ransomware, Part Three of Three

trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-three-of-three/



Overview

In Part One of this series, we discussed how MailTo ransomware installs and configures itself on the victim's system and in Part Two we discussed how the malware, executes and injects itself into the system. In this post, we take a look at what makes ransomware different than other malware and gives it its deadly bite, encryption.

Encryption

Just before the encryption routine begins, the MailTo ransomware performs the following tasks:

- Adjusts token privileges to give itself “SeDebugPrivilege” and “SeImpersonatePrivilege”.
- Collects tokens of logged on users for use of impersonation
- Scan system handle information for later use with removing processes/services from holding files from the ransomware.

We found that the ransomware uses this implementation of curve25519:

https://github.com/agl/curve25519-donna/blob/master/curve25519-donna.c

This is implemented to create a key to be used with a ChaCha stream cipher to encrypt files. It is not possible to decrypt any encrypted files without the private key of the ransomware owners.

MailTo encrypts the following locations using a ChaCha stream cipher:

- Local Disk Drives
- Network Shares
- Hidden Network Shares (IPC$, Admin$)

The MailTo ransomware has three main threads that kick off the encryption, each thread having its own purpose. One of these threads is aimed at encrypting the local drive while the other two are targeted towards encrypting shared network locations.

Encryption Thread 1

The first thread created for the encryption process serves the roll of encrypting the local disk drives via the API function "GetLogicalDriveStringsW". This function will return a list of drives and shared network locations. This routine will begin creating threads for every file and directory to encrypt on the found drives. It attempts to connect with the network locations using the current user's access token and via the API functions "WNetUseConntectionW" and "WNetAddConnection2W".

Encryption Thread 2

The second thread created will again perform "GetLogicalDriveStringsW" to get a list of drives as well as shared network locations. In this thread, the drives are filtered for only network drives. Before connecting to the network locations, the ransomware call "ImpersonateLoggedOnUser" in order to attempt to gain access to the network locations using different access tokens collected from logged-in users.

Encryption Thread 3

The third thread will act similar to the second created thread in terms of impersonating all currently logged on users but will collect shared network drives in a different manor. "GetNetShares" and "WNetEnumResourceW" are used to iterate over shared network drives and paths. "GetNetShares" will also pick up hidden network shares such as "IPC$" and "Admin$".

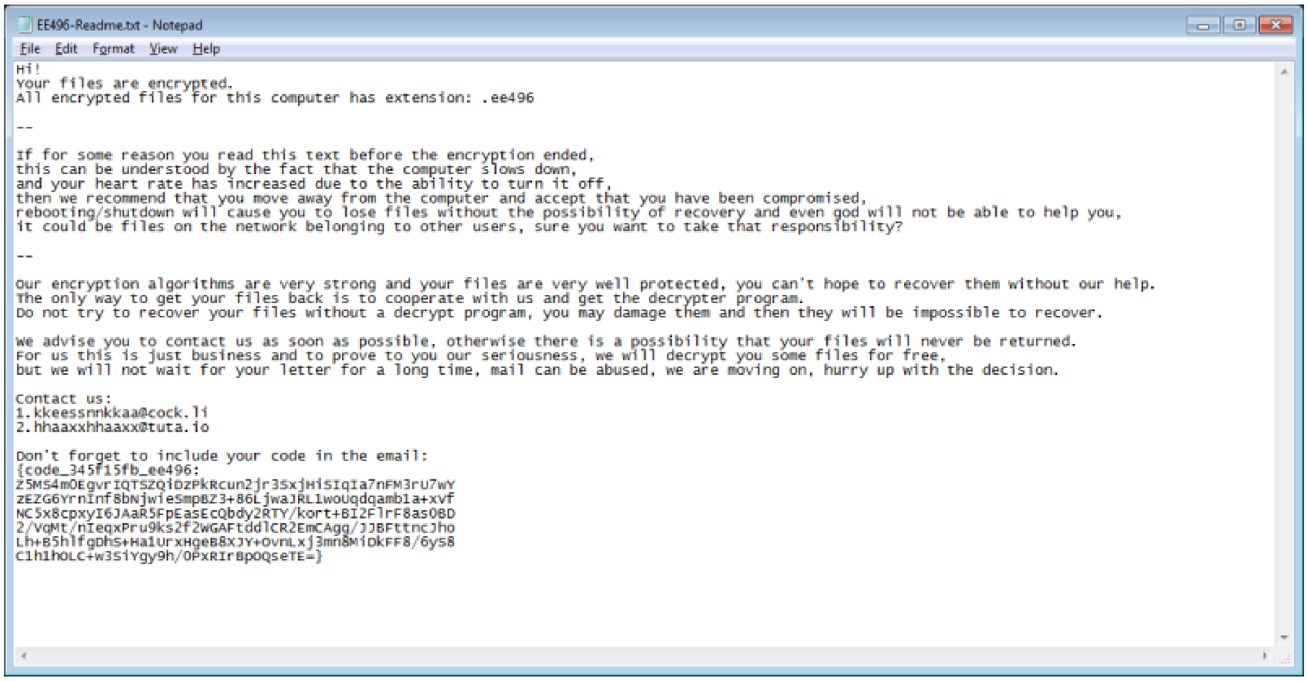
File Encryption

When it comes to encrypting an individual file, the ransomware is quite robust in ensuring that it will encrypt that file. When we say this, we mean if a process or service has a hold on a file that the ransomware wants to encrypt, the ransomware will kill that process or service in order to do so. If the ransomware does not have access to a file or network path, it will iterate all duplicated access tokens of users logged onto the machine and use that token in an attempt to encrypt the file. If the ransomware was shut down and only partially encrypted a file, but later executed again, it will check the last four bytes of the file for a CRC32 hash of their public ECC key. If the four bytes match the CRC32 hash of their public key, the ransomware will know that the file was fully and successfully encrypted.

Finalization

Ransomware Note

When the MailTo ransomware has finished encrypting, it will open notepad with a ransomware note.



```
Hi!
Your files are encrypted.
All encrypted files for this computer has extension: .ee496

--

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.kkeessnnkkaa@cock.li
2.hhaaxxhhaaxx@tuta.io

Don't forget to include your code in the email:
{code_345f15fb_ee496:
Z5MS4mOEgvrIQTSZQiDzPkRcun2jr3SxjHiSIqIa7nFM3rU7wY
zEZG6YrnInf8bNjwieSmpBZ3+86LjwaJRL1wOUqdqamb1a+xVf
NC5x8cpxyI6JAaR5FpEasEcQbdy2RTY/kort+BI2FlrF8asOBD
2/VqMt/nIeqxPru9ks2f2WGAFtddlCR2EmCAgg/JJBFttncJho
Lh+B5hlfgDhS+Ha1UrxHgeB8XJY+OvnLxj3mn8MiDkFF8/6yS8
C1h1hOLC+w3SiYgy9h/OPxRIrBpOQseTE=}
```

Figure 1 – Ransomware Note

Uninstallation

After the ransomware note has been displayed, MailTo deletes the following entries from the system if they exist:

- Files
  - Program Files (x86)/<uniqueName>/< uniqueName.exe>
  - Program Files/< uniqueName >/< uniqueName.exe>
  - C:\Users\<username>\AppData\Roaming\<uniqueName>\<uniqueName.exe>

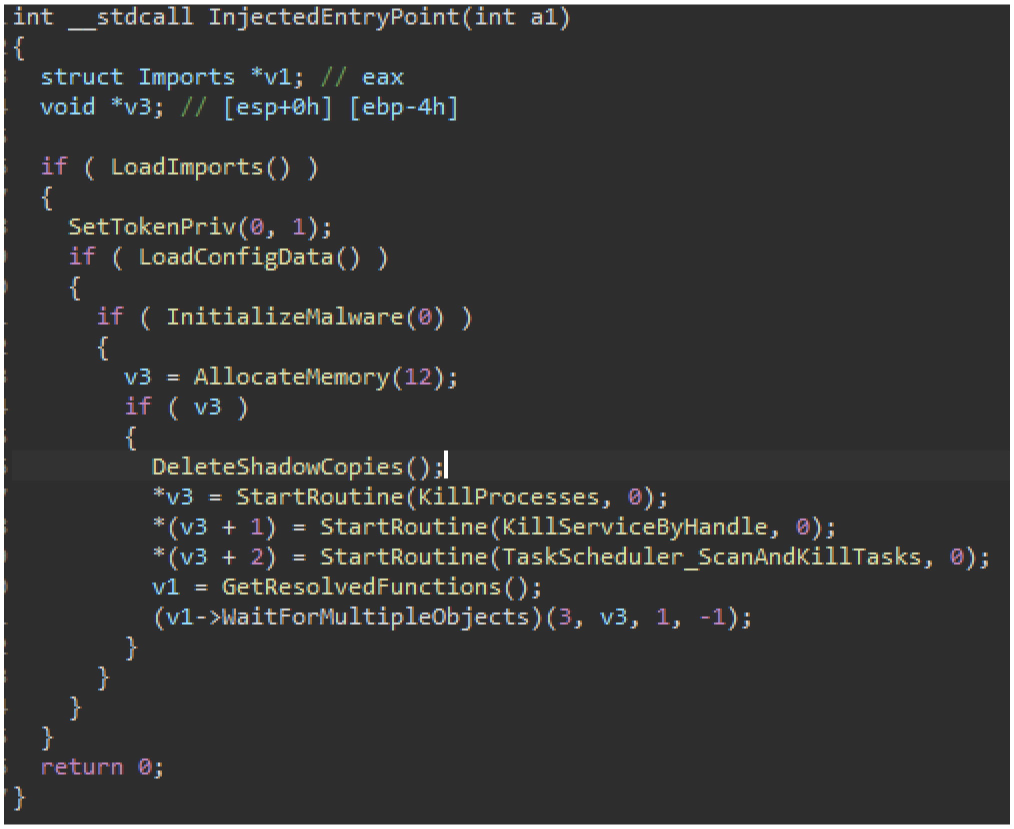
- Registry Keys
    - HKEY_LOCAL_MACHINE\SOFTWARE\Mircrosoft\Windows\CurrentVersion\Run
    - HKEY_CURRENT_USER \SOFTWARE\Mircrosoft\Windows\CurrentVersion\Run

Shadow Copy Deletion

Shadow copy deletion occurs after MailTo uninstalls itself from the system. “vssadmin.exe” is used with the following command for shadow copy deletion:

“vssadmin.exe delete shadows /all /quiet”

Shadow copy deletion using this simple *vssadmin* command is typical of many ransomware. Interestingly, shadow copy deletion also occurs one additional time during the execution of the injected entry point of Explorer.exe (2).



```
int __stdcall InjectedEntryPoint(int a1)
{
  struct Imports *v1; // eax
  void *v3; // [esp+0h] [ebp-4h]

  if ( LoadImports() )
  {
    SetTokenPriv(0, 1);
    if ( LoadConfigData() )
    {
      if ( InitializeMalware(0) )
      {
        v3 = AllocateMemory(12);
        if ( v3 )
        {
          DeleteShadowCopies();
          *v3 = StartRoutine(KillProcesses, 0);
          *(v3 + 1) = StartRoutine(KillServiceByHandle, 0);
          *(v3 + 2) = StartRoutine(TaskScheduler_ScanAndKillTasks, 0);
          v1 = GetResolvedFunctions();
          (v1->WaitForMultipleObjects)(3, v3, 1, -1);
        }
      }
    }
  }
  return 0;
}
```

Figure 26 – DeleteShadowCopies() call inside of Explorer.exe (2)

Conclusion

The MailTo ransomware is complex ransomware which effectively does its job of encrypting files. What makes MailTo tricky is its ability to leave no stone unturned when it comes to encrypting files. The ransomware has been designed in a careful way to ensure that its privileges are exhausted to the fullest extent by enumerating every logical drive and network share through impersonated user accounts. The ransomware also makes sure that it destroys any handles to files that are not its own. Even if a service or process is making changes to a file, the ransomware will eliminate that process/service and encrypt the file. The ransomware also sets up a persistent registry key and only removes it once the encryption has been complete.

MailTo does its best to minimize its detection vectors by deleting itself, hiding its imports, and injecting into processes using stealthy techniques. MailTo avoids the use of suspicious Windows APIs as much as it can by using the undocumented windows functions and keeping away from the Windows crypto API. Even though MailTo has its flaws such as with service termination, this ransomware will successfully encrypt files on a system and mapped network drives without the possibility of decrypting them without the ransomware private key.

MailTo is getting more and more popular, so stay safe and keep offline or unconnected backups of your important data.

Full Series

An In-depth Look at MailTo Ransomware, Part One
An In-depth Look at MailTo Ransomware, Part Two

IOC

MailTo Sample SHA256:
58e923ff158fb5aecd293b7a0e0d305296110b83c6e270786edcc4fea1c8404c