New ransomware detection not only encrypts files but also helps 'clean up' the system

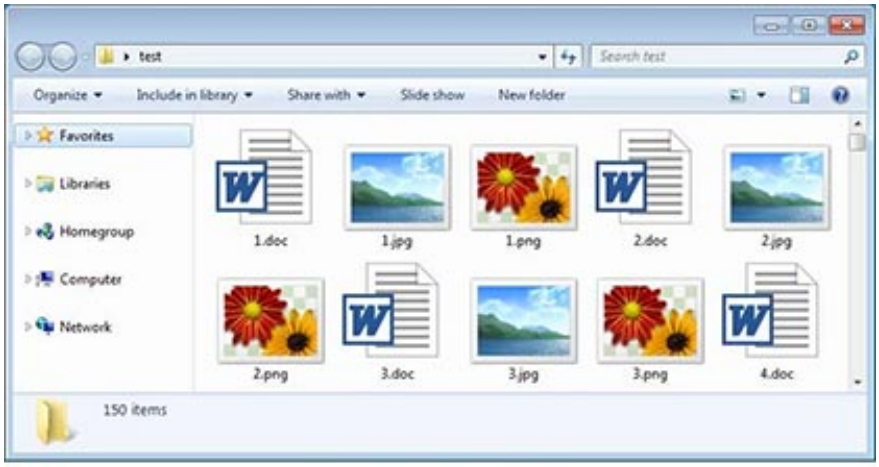
Rxomware vxCrypter is the first ransomware in the world that not only encrypts the victim's data but also helps clean up their computers by deleting duplicate files on the system.

Rxomware vxCrypter is probably the first ransomware in the world that not only encrypts the victim's data but also helps clean up their computers by deleting duplicate files on the system.

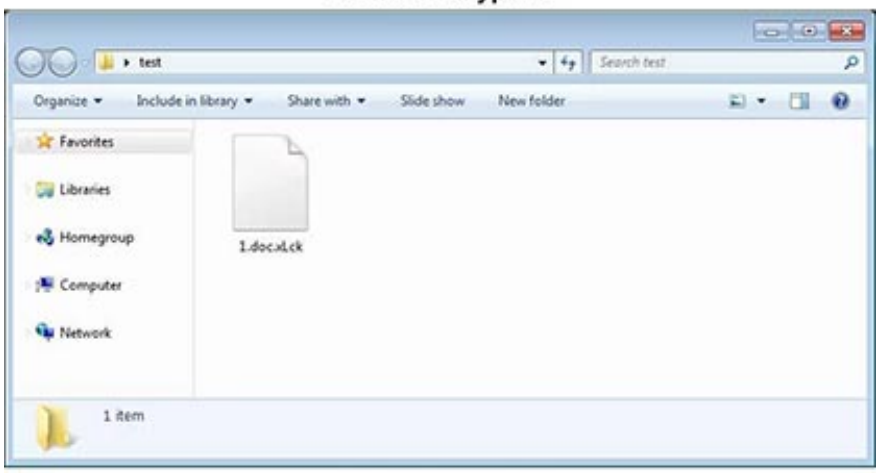
Last week, security researchers at BleepingComputer discovered a new ransomware called vxCrypter is currently being developed and spread globally. This is a ransomware .NET and is based on an old ransomware that has never been distributed, called vxLock.

The list of nearly 600 MAC addresses was targeted in the recent hacking of millions of ASUS computer users

When first experimenting with this ransomware software, the researchers found that in addition to encrypting system data like the usual way that extortion codes often do, it also deletes all files. duplicate in the directory and leave only one file, as illustrated in the images below. According to experts, it is likely that this is just an error in the encryption process because as mentioned, this ransomware software is still in the development stage, so if something goes wrong It is understandable.



Before Encryption



After Encryption

1. The alarming increase in the number of attacks targeted at IoT devices

After conducting some necessary tests, security researcher Michael Gillespie said that deleting the file is intentional because ransomware is actually deleting duplicate files and not deleting them. Moreover, this is also the first ransomware software in the world to be recorded with this strange behavior.

When analyzing ransomware, Michael Gillespie noticed that it would track the SHA256 hash functions of each encrypted file. Because ransomware has encrypted many different files on the system, so if it encounters the same SHA256 hash function (duplicate), it will delete the file immediately instead of decoding.

```
public void EncryptFile(string filePath)
{
    byte[] encryptedBytes = new byte[1];
    EncryptedFileStruct encryptedFileStruct = new EncryptedFileStruct();
    FileHeader fileHeader = new FileHeader();
    HashAndKeygenClass.FileHashClass fileHashClass = new HashAndKeygenClass.FileHashClass();
    RijndaelManaged rijndaelManaged = new RijndaelManaged();
    rijndaelManaged.KeySize = 256;
    rijndaelManaged.BlockSize = 128;
    rijndaelManaged.Mode = CipherMode.CBC;
    rijndaelManaged.IV = Encoding.ASCII.GetBytes(this.HashinInstance.SecureKeygen(16));
    rijndaelManaged.Key = Encoding.ASCII.GetBytes(this.HashinInstance.SecureKeygen(32));
    int num = rijndaelManaged.KeySize / 8 + rijndaelManaged.BlockSize / 8;
    byte[] array = new byte[num];
    Array.Copy(rijndaelManaged.Key, 0, array, 0, 32);
    Array.Copy(rijndaelManaged.IV, 0, array, 32, 16);
    if (File.Exists(filePath))
    {
        fileHeader.EncryptedKeyAndIV = this.rsacryptoServiceProvider_0.Encrypt(array, true);
        fileHeader.FileSHA256 = Encoding.ASCII.GetBytes(fileHashClass.SHA256File(filePath));
        fileHeader.ushort_0 = 3788;
        if (this.Sha256InEncryptedList(Encoding.ASCII.GetString(fileHeader.FileSHA256)))
        {
            try
            {
                File.Delete(filePath);
                return;
            }
            catch (Exception)
            {
                return;
            }
        }
        byte[] array2 = new byte[1];
```

1. Endpoint Detection and Response threats, an emerging security technology

It should be noted, however, that this ransomware only deletes duplicate files that have tail extensions that were originally targeted for encryption, including:

.txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .sqlite, .odt, .jpg, .jpeg, .bmp, .gif, .png, .csv, .sql, .mdb , .sln, .php, .asp, .aspx, .html, .xml, .psd, .xsd, .cpp, .c, .h, .hpp, .htm, .py, .reg, .rb,. pl, .zip, .rar, .tgz, .key, .jsp, .db, .sqlite3, .sqlitedb, .bat, .bak, .7z, .avi, .fla, .flv, .java, .mpeg, .pem, .wmv, .tar, .tgz, .tiff, .tif

For files in a format other than the above list, such as .exe or .dll, the duplicate file will still be preserved.

Now researchers have not been able to confirm exactly why ransomware vxCrypter does this, the most reasonable assumption now is that deleting duplicate files is one way to help malicious code speed up the data encryption. system. Besides, vxCrypter's behavior is also a warning that we must be really wary in the context that attackers continue to develop malware that contains many different behaviors to increase performance. causing damage to malicious code.