

# Malware-Traffic-Analysis.net - 2017-05-16 - More examples of Jaff ransomware

Archived: 2026-04-05 14:19:56 UTC

## NOTICE:

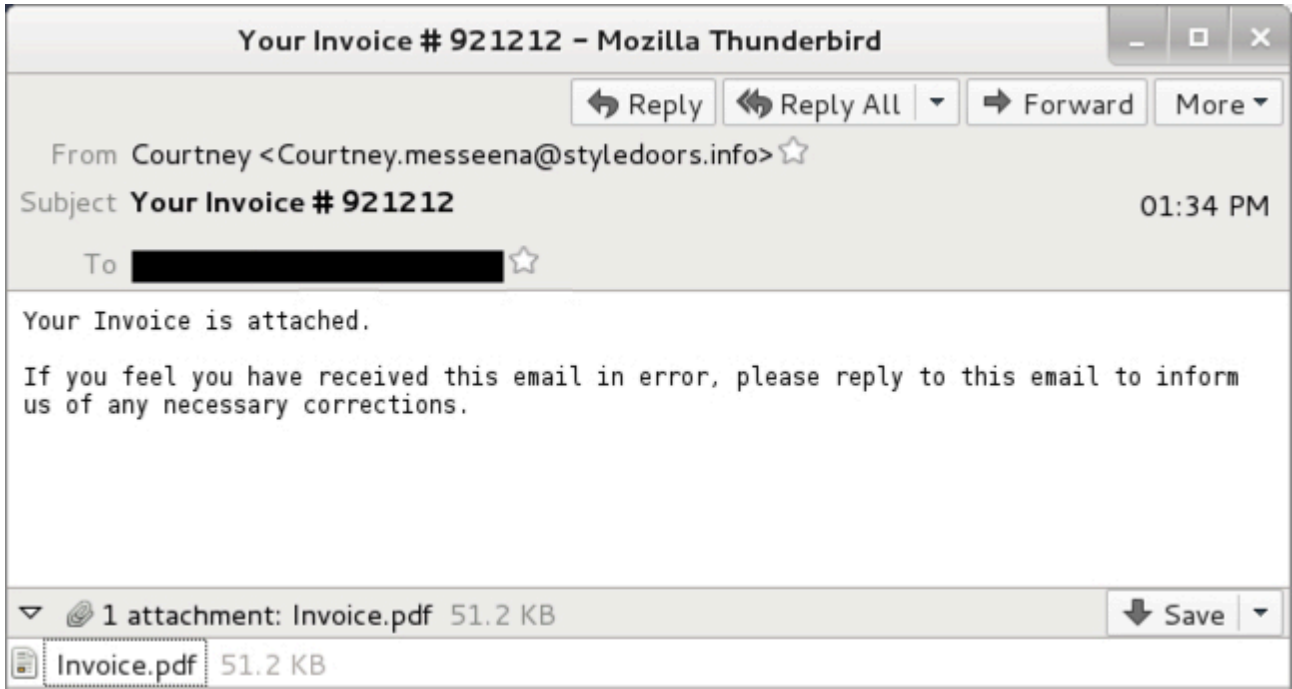
- The zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

## ASSOCIATED FILES:

- [2017-05-16-Jaff-ransomware-traffic.pcap.zip](#) 92.3 kB (92,253 bytes)
  - 2017-05-16-Jaff-ransomware-malspam-traffic.pcap (97,799 bytes)
- [2017-05-16-Jaff-ransomware-malspam-tracker.csv.zip](#) 1.1 kB (1090 bytes)
  - 2017-05-16-Jaff-ransomware-malspam-tracker.csv (3,024 bytes)
- [2017-05-16-Jaff-ransomware-emails-and-malware.zip](#) 1.2 MB (1,195,959 bytes)
  - 2017-05-16-133459-UTC-Invoice.pdf (52,399 bytes)
  - 2017-05-16-141909-UTC-Invoice.pdf (52,239 bytes)
  - 2017-05-16-142344-UTC-Invoice.pdf (52,322 bytes)
  - 2017-05-16-142529-UTC-Invoice.pdf (52,322 bytes)
  - 2017-05-16-142819-UTC-Invoice.pdf (52,322 bytes)
  - 2017-05-16-143514-UTC-Invoice.pdf (52,322 bytes)
  - 2017-05-16-144044-UTC-Invoice.pdf (52,322 bytes)
  - 2017-05-16-145739-UTC-Invoice.pdf (52,464 bytes)
  - 2017-05-16-150804-UTC-Invoice.pdf (52,439 bytes)
  - 2017-05-16-155014-UTC-Invoice.pdf (52,214 bytes)
  - 2017-05-16-173344-UTC-Invoice.pdf (52,185 bytes)
  - 2017-05-16-182134-UTC-Invoice.pdf (51,875 bytes)
  - 2017-05-16-Jaff-Decryptor-index.css (2,661 bytes)
  - 2017-05-16-Jaff-Decryptor.html (5,090 bytes)
  - 2017-05-16-Jaff-ransomware-ReadMe.bmp (3,145,782 bytes)
  - 2017-05-16-Jaff-ransomware-ReadMe.html (1,431 bytes)
  - 2017-05-16-Jaff-ransomware-ReadMe.txt (482 bytes)
  - 2017-05-16-Jaff-ransomware-galaperidol8.exe (147456 bytes)
  - 2017-05-16-jaff-malspam-133459-UTC.eml (71,787 bytes)
  - GUMHSZUM.docm (55,176 bytes)
  - HBTEJ.docm (55,154 bytes)

- HSOTN2JI.docm (55,170 bytes)
- LNJ9DNIJ.docm (55,187 bytes)
- U4HKZVPRL.docm (55,175 bytes)
- UCER2Q.docm (55,134 bytes)
- UTTNNVW6V.docm (55,166 bytes)
- VEZLGKVC.docm (55,155 bytes)

## EMAIL



Shown above: An example of the emails.

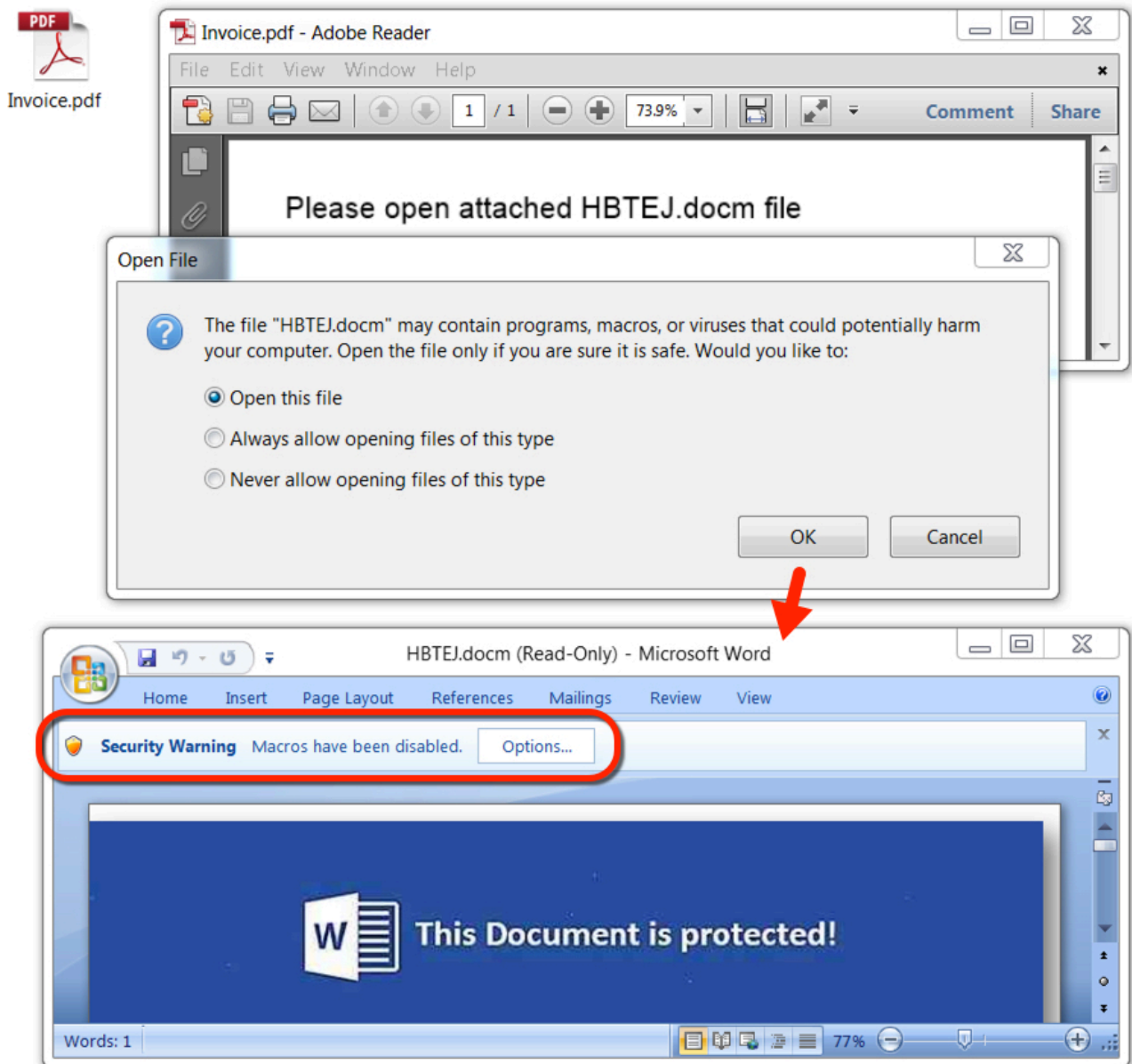
### 12 EMAIL EXAMPLES:

READ: DATE/TIME -- SUBJECT -- ATTACHMENT NAME -- SENDING ADDRESS (SPOOFED)

- 2017-05-16 13:34:59 UTC -- Your Invoice # 921212 -- Invoice.pdf -- "Courtney" <Courtney.messeena@styledoors[.]info>
- 2017-05-16 14:19:09 UTC -- Your Invoice # 878923 -- Invoice.pdf -- "Jeremiah" <Jeremiah.cogguns@ledomassage[.]nl>
- 2017-05-16 14:23:44 UTC -- Your Invoice # 654270 -- Invoice.pdf -- "Shelly" <Shelly.hullson@ariakarasana[.]com>
- 2017-05-16 14:25:29 UTC -- Your Invoice # 87871 -- Invoice.pdf -- "Jodie" <Jodie.work@pisorial[.]com>
- 2017-05-16 14:28:19 UTC -- Your Invoice # 850914 -- Invoice.pdf -- "Blake" <Blake.sykes@vivacerveja[.]com[.]br>
- 2017-05-16 14:35:14 UTC -- Your Invoice # 62287 -- Invoice.pdf -- "Adrienne" <Adrienne.haddock@k2news[.]net>
- 2017-05-16 14:40:44 UTC -- Your Invoice # 24559 -- Invoice.pdf -- "Virgie" <Virgie.burke@spi[.]com[.]ar>

- 2017-05-16 14:57:39 UTC -- Your Invoice # 852594 -- Invoice.pdf -- "Krystal" <Krystal.doole@papa-ganda[.]net>
- 2017-05-16 15:08:04 UTC -- Your Invoice # 99499 -- Invoice.pdf -- "Laurie" <Laurie.devell@coveredwagon[.]ca>
- 2017-05-16 15:50:14 UTC -- Your Invoice # 08175 -- Invoice.pdf -- "Kristy" <Kristy.oglethorp@maloufimo[.]com>
- 2017-05-16 17:33:44 UTC -- Your Invoice # 927414 -- Invoice.pdf -- "Marlene" <Marlene.balmer@seniorsmarketplacene[.]com>
- 2017-05-16 18:21:34 UTC -- Your Invoice # 376427 -- Invoice.pdf -- "Earlene" <Earlene.wyatville@gradinitamagica[.]ro>

## MALWARE



Shown above: As usual, the PDF attachment contains an embedded Word document with malicious macros.

## SHA256 HASHES FOR THE ATTACHMENTS:

- 279bd153041b64966147eb7d036f570199e2d068c92746eb3e571d49fd7e3805 - Invoice.pdf
- 5b10d2ae464ec1b3c5d62d70d452d205419c0892fa2d21892767f8f30a6b8e98 - Invoice.pdf
- 5da7c8bf86dc71531b2cd34e565385dae7b080cde104e5abe29577ed03787a71 - Invoice.pdf
- 66c406bbe06a7804508e39eb3822b0a4f27b14a9d4c5dff970d559bcd88d6abc - Invoice.pdf
- 728174eddaf20492bfc3d85df3148aad3ff2677c88c901d727272c0f1aa4a0dd - Invoice.pdf
- 85640107aec9c21f6fdcf62ef79046aa57c18da35d29795febb7ac634165f93c - Invoice.pdf
- bd5cc7c63481cb6f54b8ddd3b459976021839119f2f57a2f60e52159ac0c184d - Invoice.pdf
- ebcdc058e4d7d7e2d9bcf59042c50814c335e3aa18b59f76a9eccc9918c78bb7 - Invoice.pdf

## SHA256 HASHES FOR THE EMBEDDED WORD DOCUMENTS:

- 1bc1196f611d2c6e5bd904160354fe1374c39b907411a5a15592bbc80bd4c4c4 - VEZLGKVC.docm
- 349365e97bba0377c960894ddcdb9939e386b55e764b7d3f8257aa538866167d - LNJ9DNIJ.docm
- 4da60d4278f4996163f5ffa28196919369d4ca365245ce8c60dc46bd9d816667 - HSOTN2JI.docm
- 4ff07b88668dfc828f18859b84805aae9c06b485594d029e42c1b0c9255988e6 - U4HKZVPR.L.docm
- 9c9e0e6900b82b14816ccd7dd3f3269c44bb752a63c63afe652feaf090c551c2 - UCER2Q.docm
- a7810d1b9d50e78157ee43d2c6f34ddd70f11bc0c76311a0e223fbd9ee20165 - HBTEJ.docm
- b8ddb998befb348bbc242ed66757b8024f4fceec1f5b5b145f8aac5874d9e81f - GUMHSZUM.docm
- d30b4f0c787794a838b3cf34bdae77bc95f42fe84bef67c5283033ee4265111 - UTTNNVW6V.docm

## JAFF RANSOMWARE SAMPLE:

- SHA256 hash: 387812ee2820cbf49812b1b229b7d8721ee37296f7b6018332a56e30a99e1092  
File size: 147,456 bytes  
File location: C:\Users\[username]\AppData\Local\Temp\galaperidol8.exe

## TRAFFIC

### URLS FROM THE WORD MACROS TO DOWNLOAD JAFF RANSOMWARE:

- 34.209.214[.]237 port 80 - **herrossoidffr6644qa[.]top** - GET /af/Nbiyure3
- 194.58.119[.]16 port 80 - **jsplast[.]ru** - GET /Nbiyure3
- 80.150.6[.]143 port 80 - **juvarent[.]de** - GET /Nbiyure3
- 120.76.230[.]145 port 80 - **opearl[.]net** - GET /Nbiyure3
- 103.63.135[.]197 port 80 - **playmindltd[.]com** - GET /Nbiyure3
- 34.209.214[.]237 port 80 - **sjffonrvcik45bd[.]info** - GET /af/Nbiyure3
- 107.180.26[.]179 port 80 - **tidytrend[.]com** - GET /Nbiyure3
- 101.0.99[.]38 port 80 - **titanmachinery[.]com[.]au** - GET /Nbiyure3
- 92.245.188[.]95 port 80 - **tomcarservice[.]lit** - GET /Nbiyure3
- 176.223.209[.]15 port 80 - **ventrust[.]ro** - GET /Nbiyure3
- 188.65.115[.]35 port 80 - **vipan-photography[.]com** - GET /Nbiyure3
- 107.180.48[.]250 port 80 - **wizbam[.]com** - GET /Nbiyure3

JAFF RANSOMWARE POST-INFECTION TRAFFIC:

- 47.91.107[.]213 port 80 **eesiiuroffde445[.]com** - GET /a5/
- **rktazuzi7hbln7sy[.]onion** - Tor domain for Jaff Decryptor (same as the last few times)

Date/Time	Dst	port	Host	Info
2017-05-16 14:37:01	101.0.99.38	80	titanmachinery.com.au	GET /Nbiyure3 HTTP/1.1
2017-05-16 14:37:26	47.91.107.213	80	eesiiuroffde445.com	GET /a5/ HTTP/1.1

Traffic from the infection filtered in Wireshark.

Date/Time	Dst	port	Host	Info
2017-05-16 14:37:01	101.0.99.38	80	titanmachinery.com.au	GET /Nbiyure3 HTTP/1.1

**Follow TCP Stream (tcp.stream eq 0)**

Stream Content

```
GET /Nbiyure3 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: titanmachinery.com.au
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 16 May 2017 14:37:01 GMT
Server: Apache
Last-Modified: Tue, 16 May 2017 12:49:24 GMT
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Expires: Wed, 16 May 2018 14:37:01 GMT
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain

1faa
.....W\].6H/
J/.;(!....".."F...&.NH@...J..*b.i.F ..DE...! .(D.....7.....w'..u...
{..uN.q...qaD;4....G#m\p8.*<.M.y.B...Q.=..
[.#0..i.....w.....<.W....4U.348.].....S.....5x..ub.....,}
4q>.....}.xw..8..{.....;(\.a...x.r.....G[G..G.....XU.}'. '.....0.
$ ll ox WD4 a O D A ? - I 99 C Y4< 00 12
```

HTTP request for the Jaff ransomware.

Date/Time	Dst	port	Host	Info
2017-05-16 14:37:26	47.91.107.213	80	eesiuroffde445.com	GET /a5/ HTTP/1.1

**Follow TCP Stream (tcp.stream eq 1)**

Stream Content

```
GET /a5/ HTTP/1.1
Host: eesiuroffde445.com

HTTP/1.1 201 Created
Server: nginx
Date: Tue, 16 May 2017 14:37:26 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 7
Connection: keep-alive
ETag: W/"7-rM9AyJuqT6iOan/xHh+Aw+7K/T8"

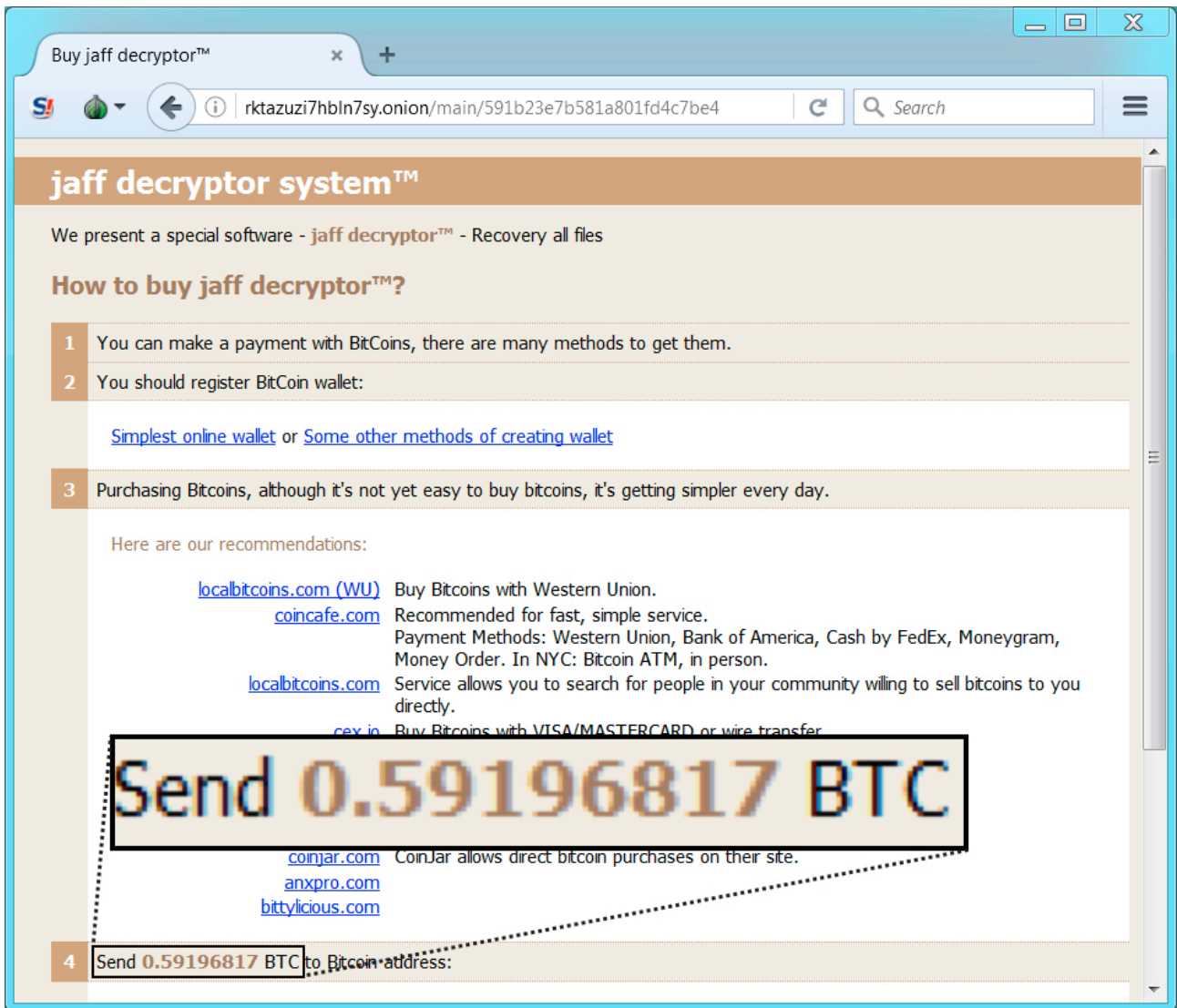
Created
```

Post-infection traffic from the infected Windows host.

## IMAGES



Shown above: Desktop of an infected Windows host.



Shown above: Going to the Jaff Decryptor.

## FINAL NOTES

[Click here](#) to return to the main page.

---

Source: <http://malware-traffic-analysis.net/2017/05/16/index.html>