Jaff - New Ransomware From the Actors Behind the Distribution of Dridex, Locky, and Bart

proofpoint.com/us/threat-insight/post/jaff-new-ransomware-from-actors-behind-distribution-of-dridex-locky-bart

May 11, 2017

Blog
Threat Insight
Jaff - New Ransomware From the Actors Behind the Distribution of Dridex, Locky, and Bart

May 11, 2017 Proofpoint Staff

After a two-week break in campaign activity, the actors behind the distribution of Locky Affid=3 and Dridex 220/7200/7500 have introduced a new ransomware called “Jaff”. The group has introduced new ransomware before in similar fashion, specifically the Bart ransomware. While Bart was only seen several times in email, and then spread via exploit kit (EK) campaigns, it remains to be seen how Jaff will be used.

Analysis

On May 11, Proofpoint researchers detected a large campaign involving tens of millions of messages with .pdf attachments containing embedded Microsoft Word documents with macros that, if enabled, download Jaff ransomware. The messages in this campaign purported to be:

- From "Joan <joan.1234@[random domain]>" (random name, digits) with subject "Receipt to print" and attachment "Sheet_321.pdf" (random digits; also "Document" and "Receipt")
- From "John <john.doe123@[random domain]>" (random name, digits) with subject "Document_1234567" (random digits; also "Copy", "File", "PDF", "Scan") and attachment "nm.pdf"

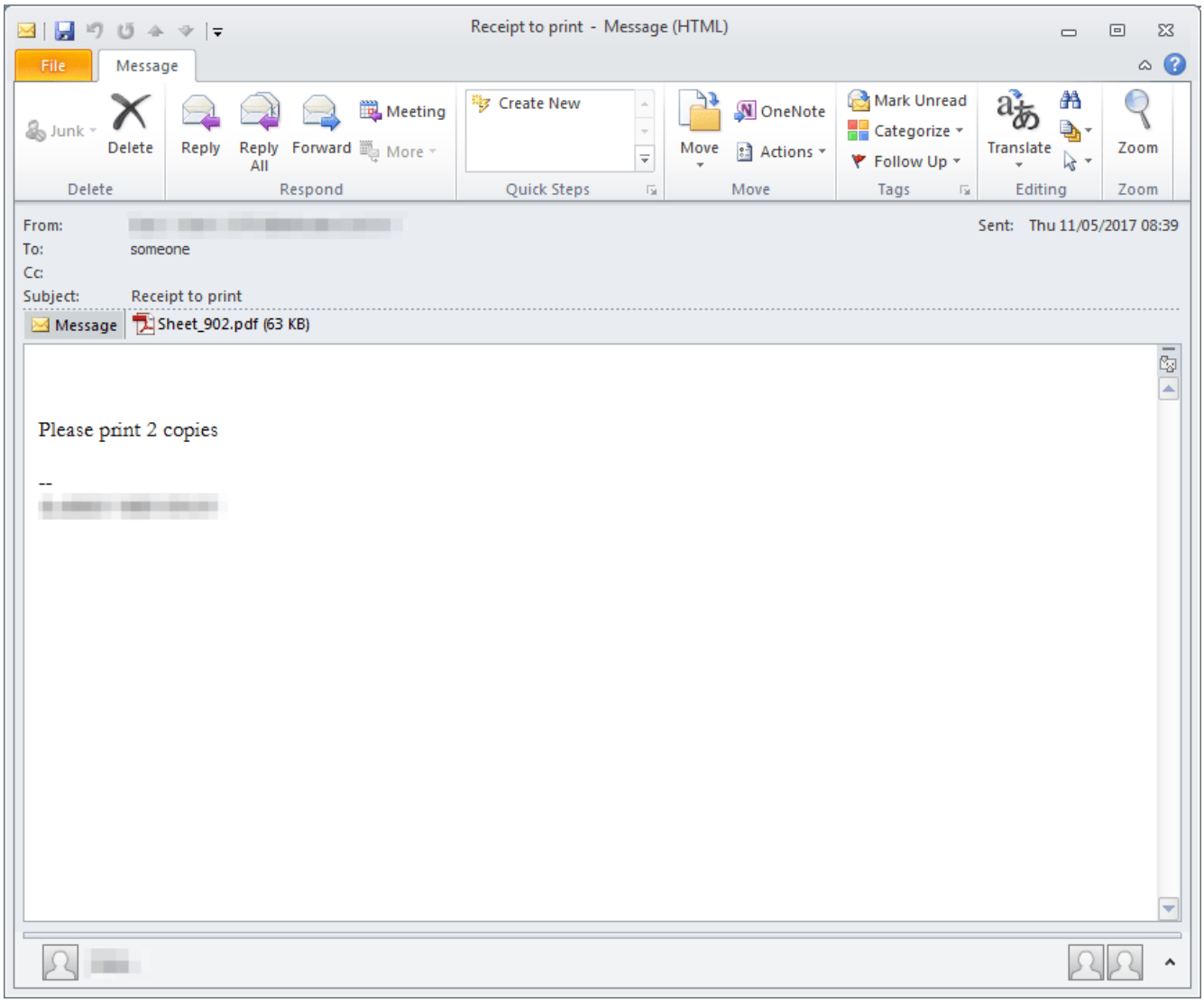

Figure 1: Email delivering the PDF distributing Jaff ransomware

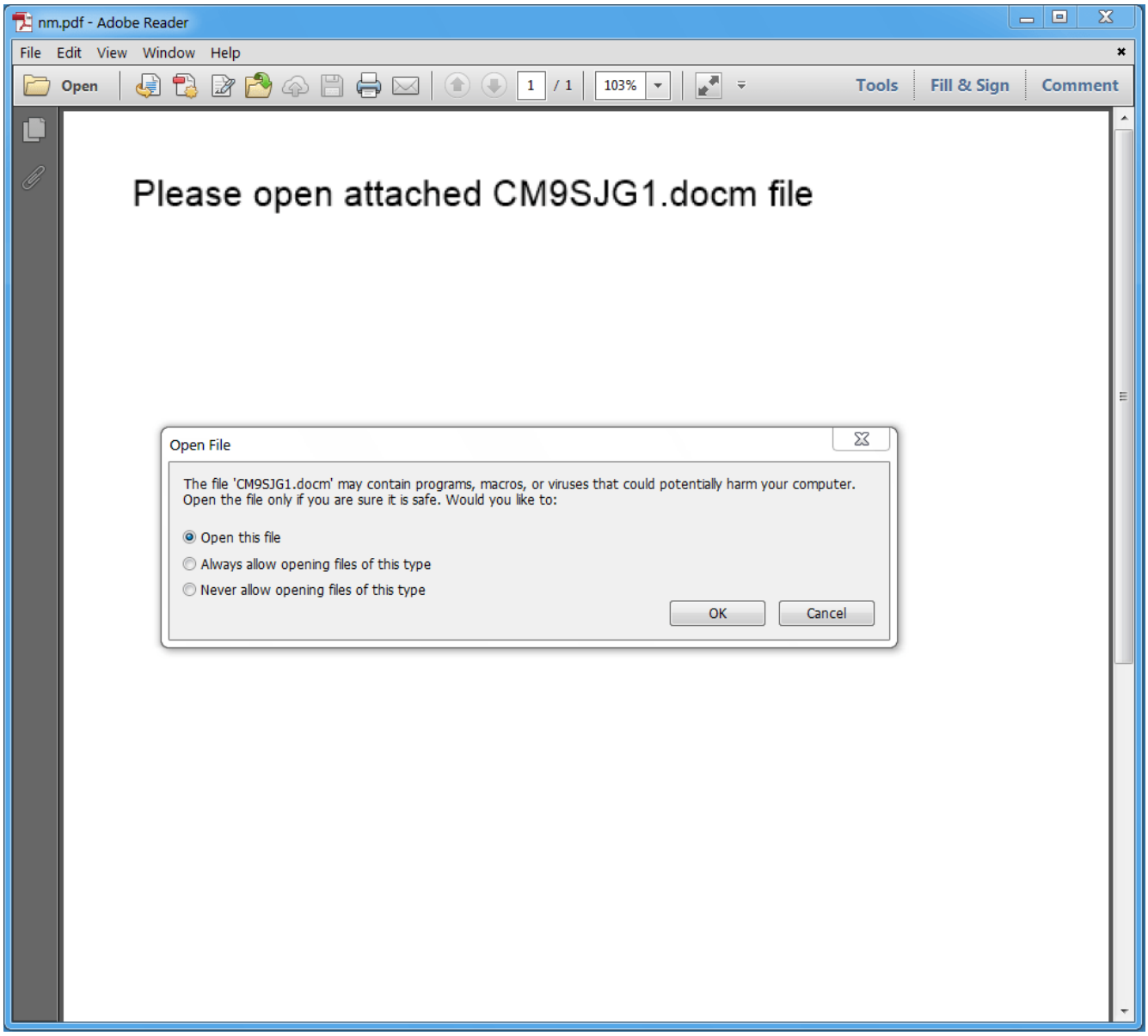

Figure 2: The PDF file delivered by malicious email messages

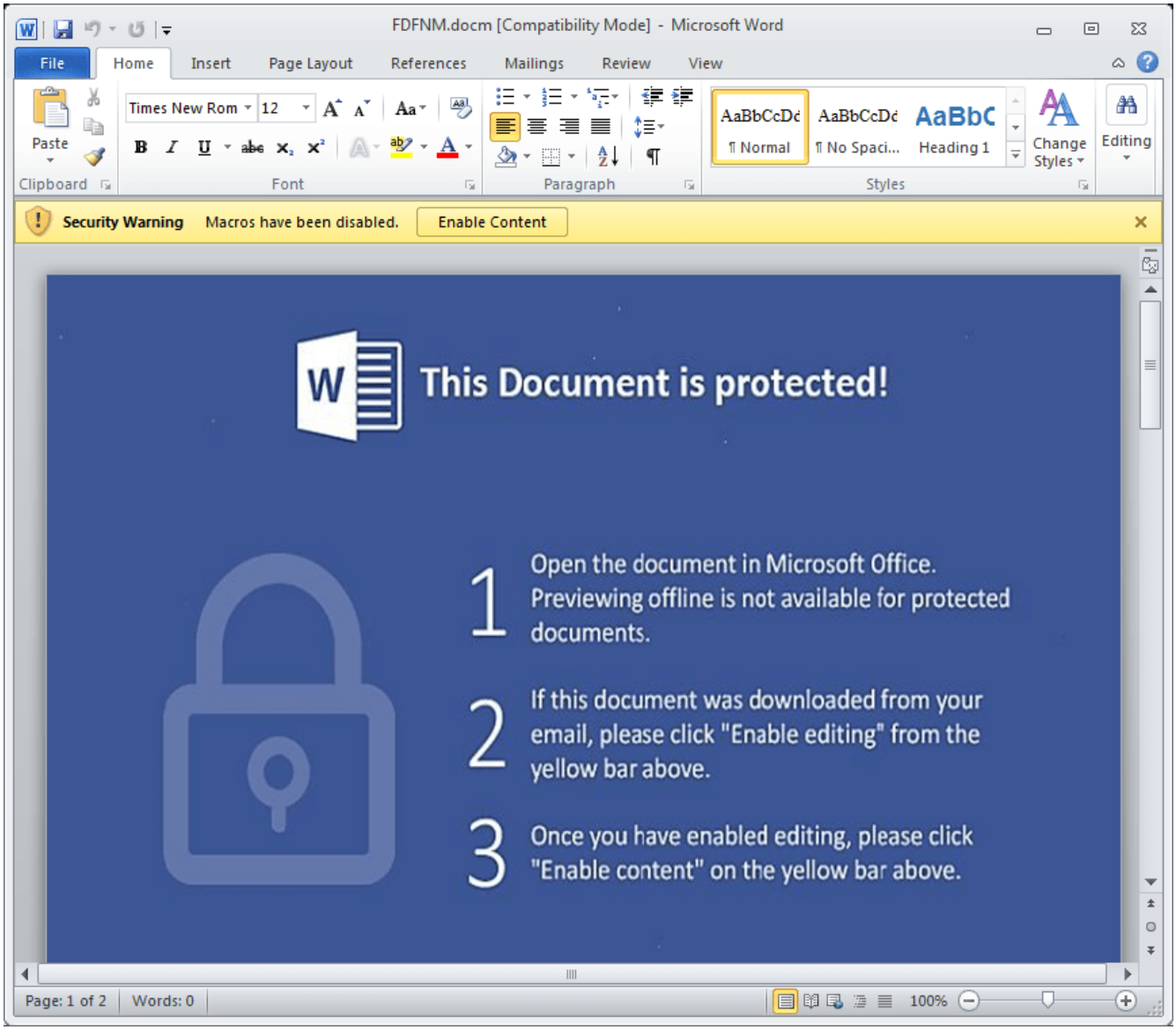

Figure 3: The Microsoft Word document embedded inside the PDF

To alert the victim that they are infected and that their files are encrypted, this ransomware creates two types of files, similar to many other types of ransomware. Specifically, it drops a ReadMe.bmp and ReadMe.html as shown in the following figures.

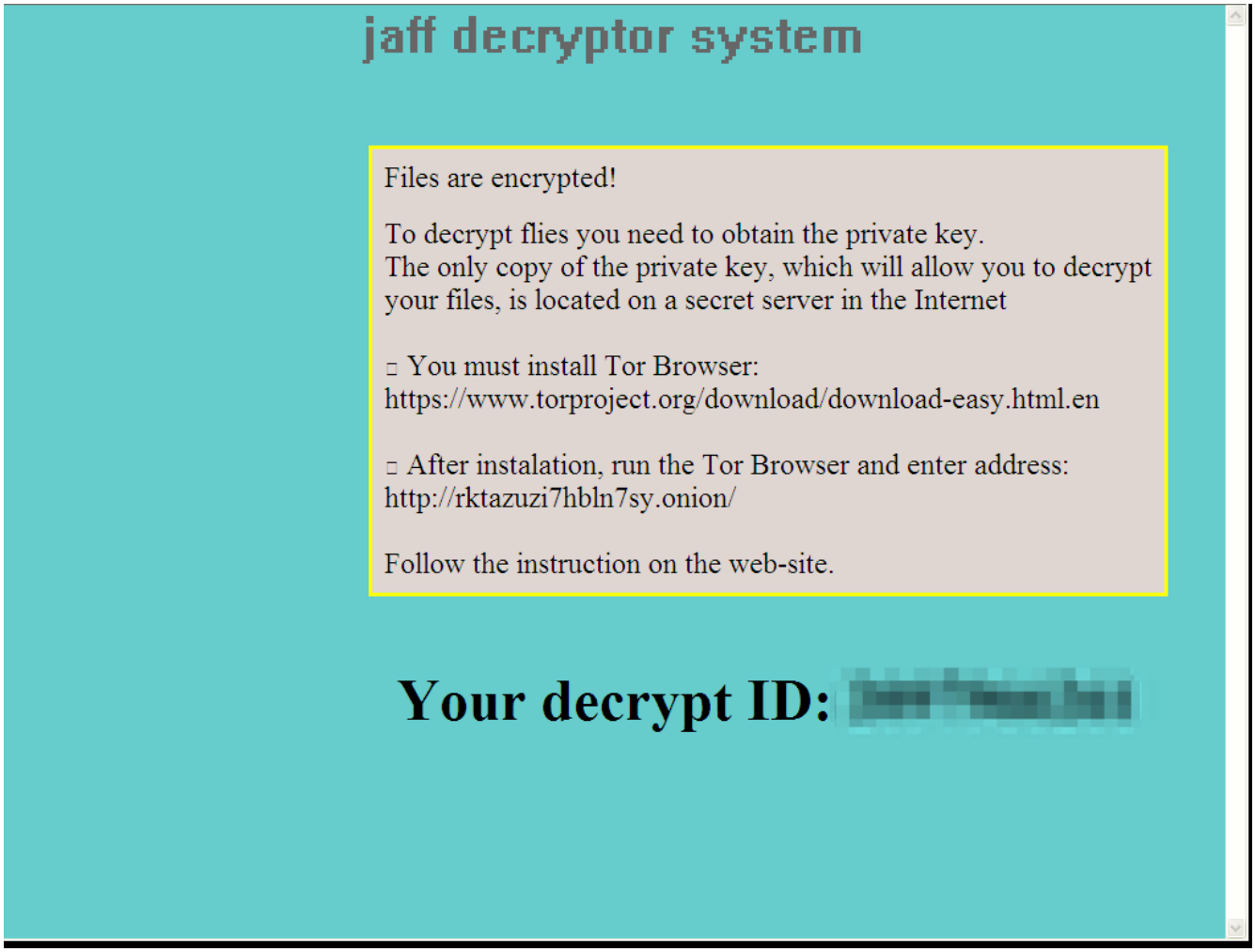

Figure 4: Readme.bmp ransom message

Figure 5: Readme.html ransom message

After encryption, a ".jaff" extension is appended to the encrypted files. The list of file extensions that Jaff encrypts includes:

.xlsx | .acd | .pdf | .pfx | .crt | .der | .cad | .dwg | .MPEG | .rar | .veg | .zip | .txt | .jpg | .doc | .wbk | .mdb | .vcf | .docx | .ics | .vsc | .mdf | .dsr | .mdi | .msg | .xls | .ppt | .pps | .obd | .mpd | .dot | .xlt | .pot | .obt | .htm | .html | .mix | .pub | .vsd | .png | .ico | .rtf | .odt | .3dm | .3ds | .dxf | .max | .obj | .7z | .cbr | .deb | .gz | .rpm | .sitx | .tar | .tar.gz | .zipx | .aif | .iff | .m3u | .m4a | .mid | .key | .vib | .stl | .psd | .ova | .xmod | .wda | .prn | .zpf | .swm | .xml | .xlsm | .par | .tib | .waw | .001 | .002 | 003. | .004 | .005 | .006 | .007 | .008 | .009 | .010 | .contact | .dbx | .jnt | .mapimail | .oab | .ods | .ppsm | .pptm | .prf | .pst | .wab | .1cd | .3g2 | .7ZIP | .accdb | .aoi | .asf | .asp. | aspx | .asx | .avi | .bak | .cer | .cfg | .class | .config | .css | .csv | .db | .dds | .fif | .flv | .idx | .js | .kwm | .laccdb | .idf | .lit | .mbx | .md | .mlb | .mov | .mp3 | .mp4 | .mpg | .pages | .php | .pwm | .rm | .safe | .sav | .save | .sql | .srt | .swf | .thm | .vob | .wav | .wma | .wmv | .xlsb | .aac | .ai | .arw | .c | .cdr | .cls | .cpi | .cpp | .cs | .db3 | .docm | .dotm | .dotx | .drw | .dxb | .eps | .fla | .flac | .fxg | .java | .m | .m4v | .pcd | .pct | .pl | .potm | .potx | .ppam | .ppsx | .ps | .pspimage | .r3d | .rw2 | .sldm | .sldx | .svg | .tga | .wps | .xla | .xlam | .xlm | .xltm | .xltx | .xlw | .act | .adp | .al | .bkp | .blend | .cdf | .cdx | .cgm | .cr2 | .dac | .dbf | .dcr | .ddd | .design | .dtd | .fdb | .fff | .fpx | .h | .iif | .indd | .jpeg | .mos | .nd | .nsd | .nsf | .nsg | .nsh | .odc | .odp | .oil | .pas | .pat | .pef | .ptx | .qbb | .qbm | .sas7bdat | .say | .st4 | .st6 | .stc | .sxc | .sxw | .tlg | .wad | .xlk | .aiff | .bin | .bmp | .cmt | .dat | .dit | .edb | .flvv | .gif | .groups | .hdd | .hpp | .log | .m2ts | .m4p | .mkv | .ndf | .nvram | .ogg | .ost | .pab | .pdb | .pif | .qed | .qcow | .qcow2 | .rvt | .st7 | .stm | .vbox | .vdi | .vhd | .vhdx | .vmdk | .vmsd | .vmx | .vmxf | .3fr | .3pr | .ab4 | .accde | .accdt | .ach | .acr | .adb | .srw | .st5 | .st8 | .std | .sti | .stw | .stx | .sxd | .sxg | .sxi | .sxm | .tex | .wallet | .wb2 | .wpd | .x11 | .x3f | .xis | .ycbcra | .qbw | .qbx | .qby | .raf | .rat | .raw | .rdb | rwl | .rwz | .s3db | .sd0 | .sda | .sdf | .sqlite | .sqlite3 | .sqlitedb | .sr | .srf | .oth | .otp | .ots | .ott | .p12 | .p7b | .p7c | .pdd | .pem | .plus_muhd | .plc | .pptx | .psafe3 | .py | .qba | .qbr.myd | .ndd | .nef | .nk | .nop | .nrw | .ns2 | .ns3 | .ns4 | .nwb | .nx2 | .nxl | .nyf | .odb | .odf | .odg | .odm | .ord | .otg | .ibz | .iiq | .incpas | .jpe | .kc2 | .kdbx | .kdc | .kpdx | .lua | .mdc | .mef | .mfw | .mmw | .mny | .moneywell | .mrw.des | .dgc | .djvu | .dng |

.drf | .dxg | .eml | .erbsql | .erd | .exf | .ffd | .fh | .fhd | .gray | .grey | .gry | .hbk | .ibank | .ibd | .cdr4 | .cdr5 | .cdr6 | .cdrw | .ce1 | .ce2 | .cib | .craw | .crw | .csh | .csl | .db_journal | .dc2 | .dcs | .ddoc | .ddrw | .ads | .agdl | .ait | .apj | .asm | .awg | .back | .backup | .backupdb | .bank | .bay | .bdb | .bgt | .bik | .bpw | .cdr3 | .as4 | .tif | .asp | .hdr

The ransom note urges the user to visit a payment portal located on a Tor site in order to pay 1.79 bitcoins (over $3300 USD at current exchange rates). The payment portal, shown in the figures below, is similar to the one used by Locky and Bart. Visually, the primary changes involve titles and headings: for example, “How to buy Decryptor Bart?” was changed to “How to buy jaff decryptor?”. While the payment portals look visually identical, the ransomware code remains to be analyzed and there are reports that it is different.

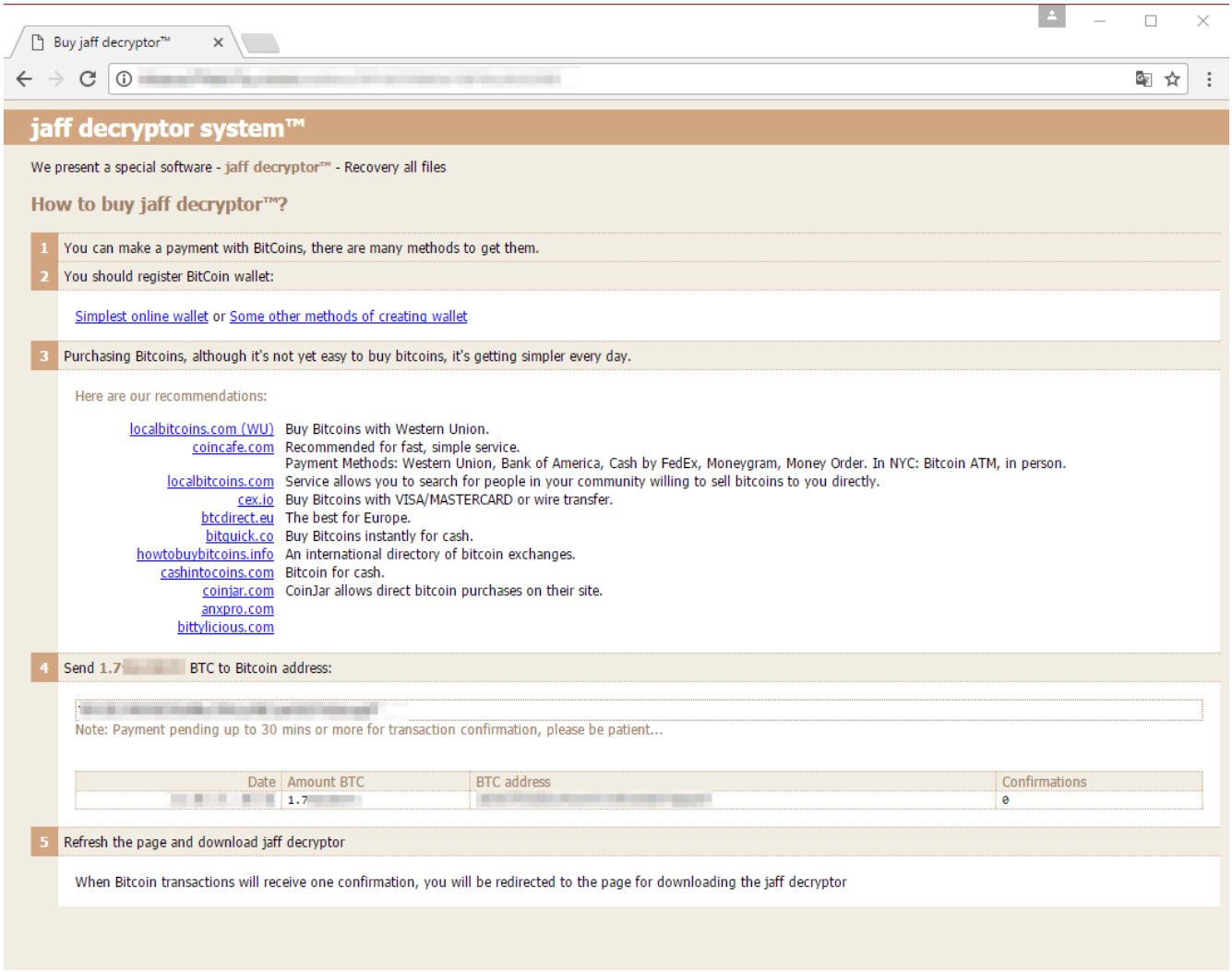

Figure 6: Ransomware payment portal

Conclusion

The actors behind the distribution of Dridex and Locky regularly try new document types, lures, exploits, and more to deliver their payloads more effectively. Similarly, after months of distributing Dridex in high-volume campaigns, they introduced Locky ransomware, which ultimately became the primary payload in the largest campaigns we have ever observed. Within months, they also brought Bart ransomware to the scene. While Bart never gained significant traction, the appearance of Jaff ransomware from the same group bears watching. We will be looking more closely at Jaff samples in the weeks to come and will continue to monitor its use in email campaigns and elsewhere.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
5bd8352171880485bf06d2d089e39d4112e8540f28d0f84bb045ab58737ad6bf	SHA256	nm.pdf email attachment
f41b4b6de5d7680b554b177ab6ebad01b5248a7b54044d64bf0593f383166eec	SHA256	CM9SJG1.docm embedded in nm.pdf
hxxp://5hdnnd74fffrottd[.]com/af/f87346b	URL	Payload URL
hxxp://babil117[.]com/f87346b	URL	Payload URL
hxxp://boaevents[.]com/f87346b	URL	Payload URL
hxxp://byydei74fg43ff4f[.]net/af/f87346b	URL	Payload URL
hxxp://easysupport[.]us/f87346b	URL	Payload URL
hxxp://edluke[.]com/f87346b	URL	Payload URL
hxxp://julian-g[.]ro/f87346b	URL	Payload URL
hxxp://phinamco[.]com/f87346b	URL	Payload URL
hxxp://takanashi[.]jp/f87346b	URL	Payload URL
hxxp://techno-kar[.]ru/f87346b	URL	Payload URL
hxxp://tending[.]info/f87346b	URL	Payload URL
hxxp://tiskr[.]com/f87346b	URL	Payload URL
hxxp://trans-atm[.]com/f87346b	URL	Payload URL
hxxp://trialinsider[.]com/f87346b	URL	Payload URL
hxxp://vscard[.]net/f87346b	URL	Payload URL
hxxp://wipersdirect[.]com/f87346b	URL	Payload URL
hxxp://fkksjobnn43[.]org/a5/	URL	Jaff C&C
hxxp://rktazuzi7hbln7sy[.]onion/	URL	Payment URL