Necurs Recurs | Trustwave | SpiderLabs

trustwave.com/Resources/SpiderLabs-Blog/Necurs-Recurs/

The Necurs botnet, which was responsible for millions of malicious spam messages last year, has recently been extremely active again. For the past three weeks it has spammed emails with a malicious PDF attachment that drops a word document with a macro that, in turn, downloads rebranded ransomware. The chart below, which is data from our Spam Research Database, shows the daily spam received from the previous weeks to present. In typical Necurs fashion, you can see the short high volume bursts.

The campaign uses various subjects in the spammed emails.

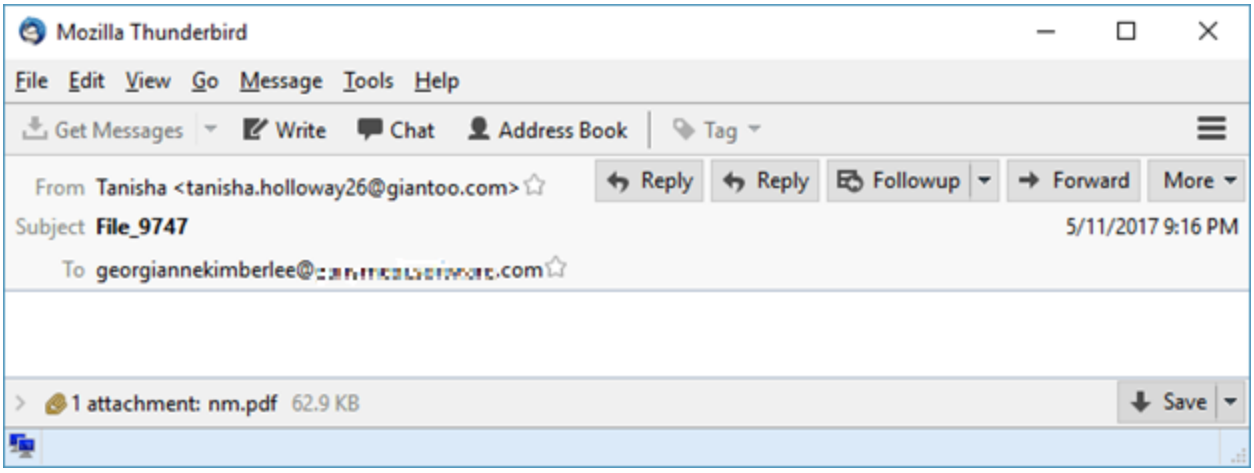
Week 1 (May 11-12)

Scanned image Receipt to print File_ {random numbers} Copy_{random numbers} Document_{random numbers} PDF_{random numbers} Scan_{random numbers}
Week 2 (May 15 -17)
Your Invoice # {random numbers} XX_Invoice_XXXX Emailing: {random numbers}.pdf Invoice {random numbers} {mm/dd/yyy}
Week 3 (May 22-25)
Invoice(XX-XXXX) Copy of Invoice {random numbers} IMG_XXXX.pdf Payment Receipt XXX Payment Receipt#XXX Payment Receipt_XXX Payment XXX Payment#XXX Payment_XXX Payment-XXX Receipt XXX Receipt#XXX Receipt_XXX Receipt-XXX

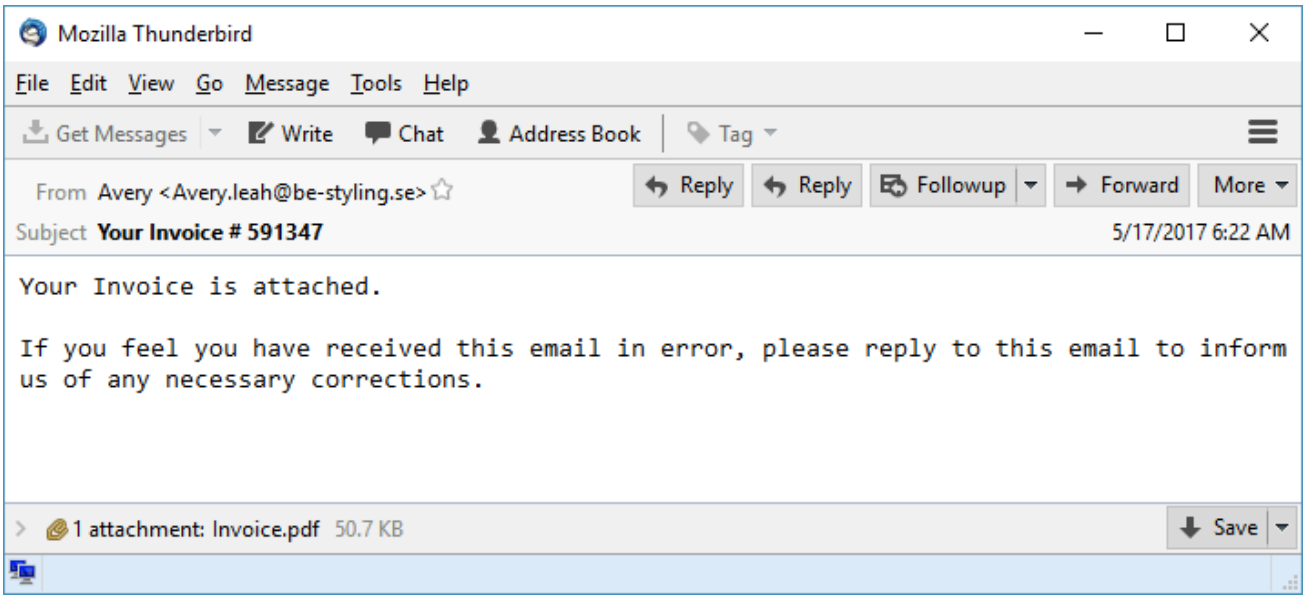
****Note that X is any random number*

Sample emails:

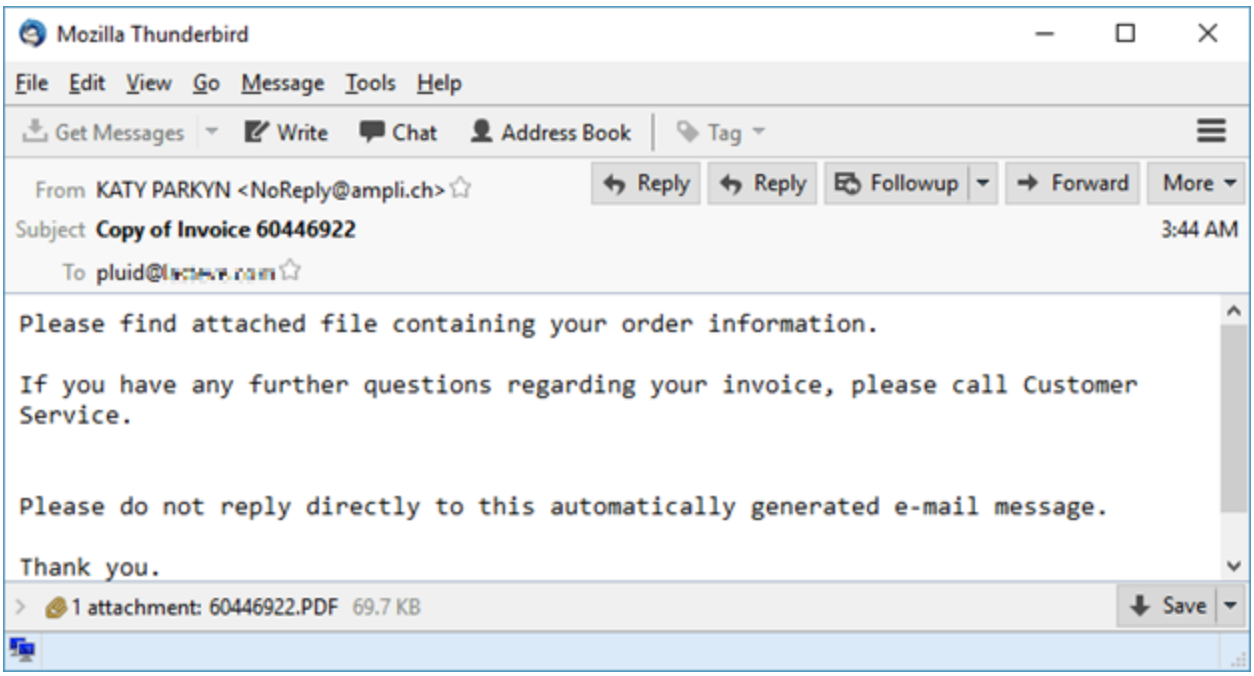
1st week



2nd week

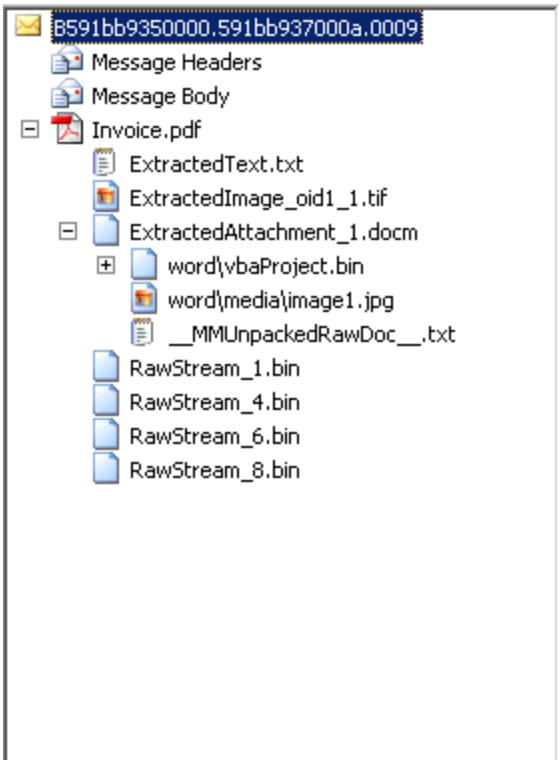


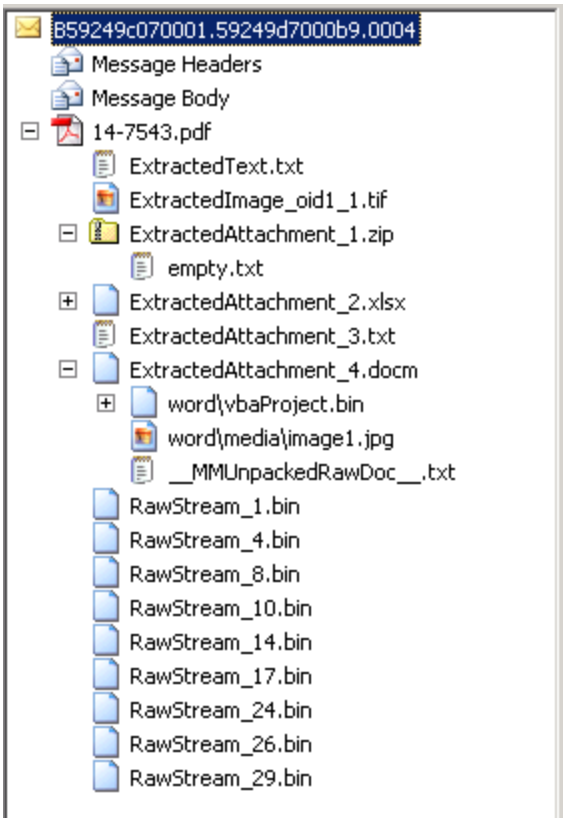
3rd week



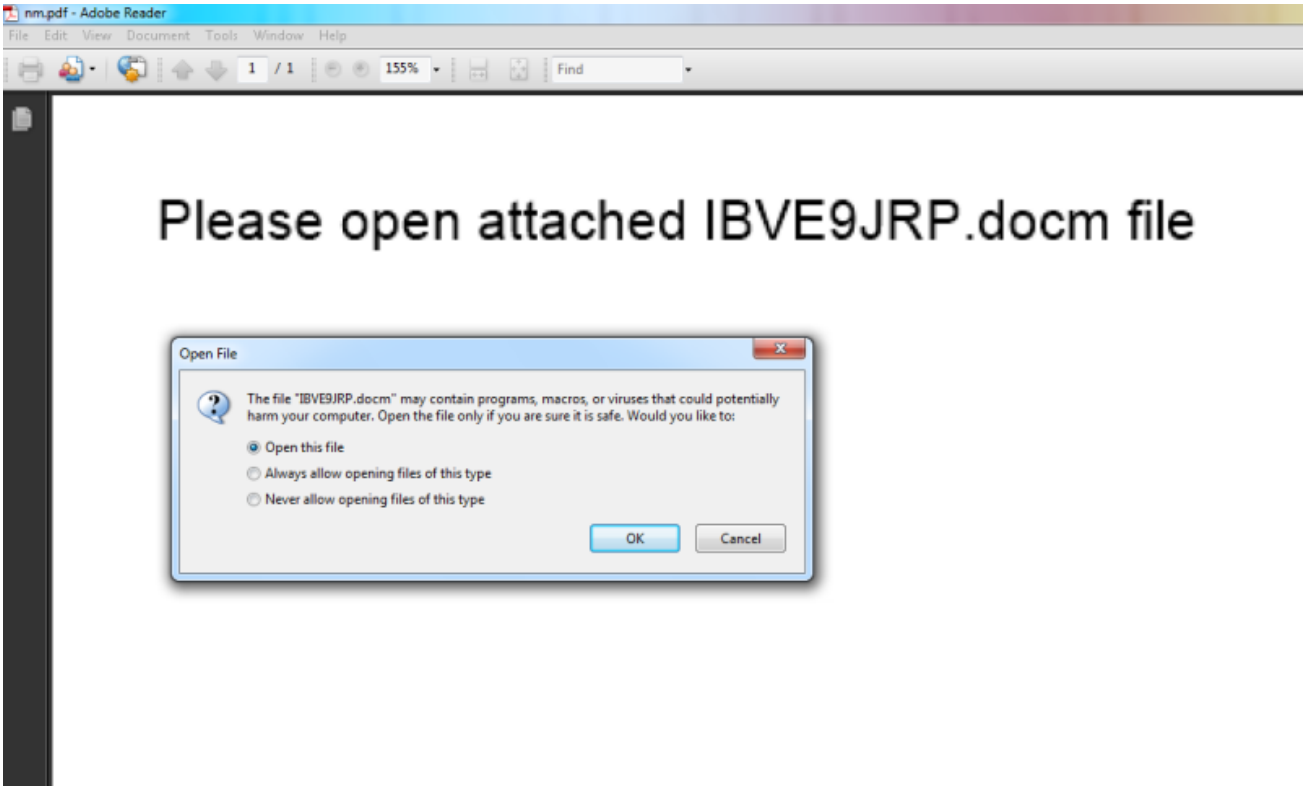
The PDF campaigns have been evolving, almost daily. Recent documents have a larger number of embedded files inside the pdf. These additional files do nothing, and are probably just decoys. But the main.docm file, with its malicious macro, still acts as the malware downloader. Below you can see how the Trustwave Secure Email Gateway sees these messages. Note the docm file with its vbaProject macro component.

1st and 2nd Week	3rd Week

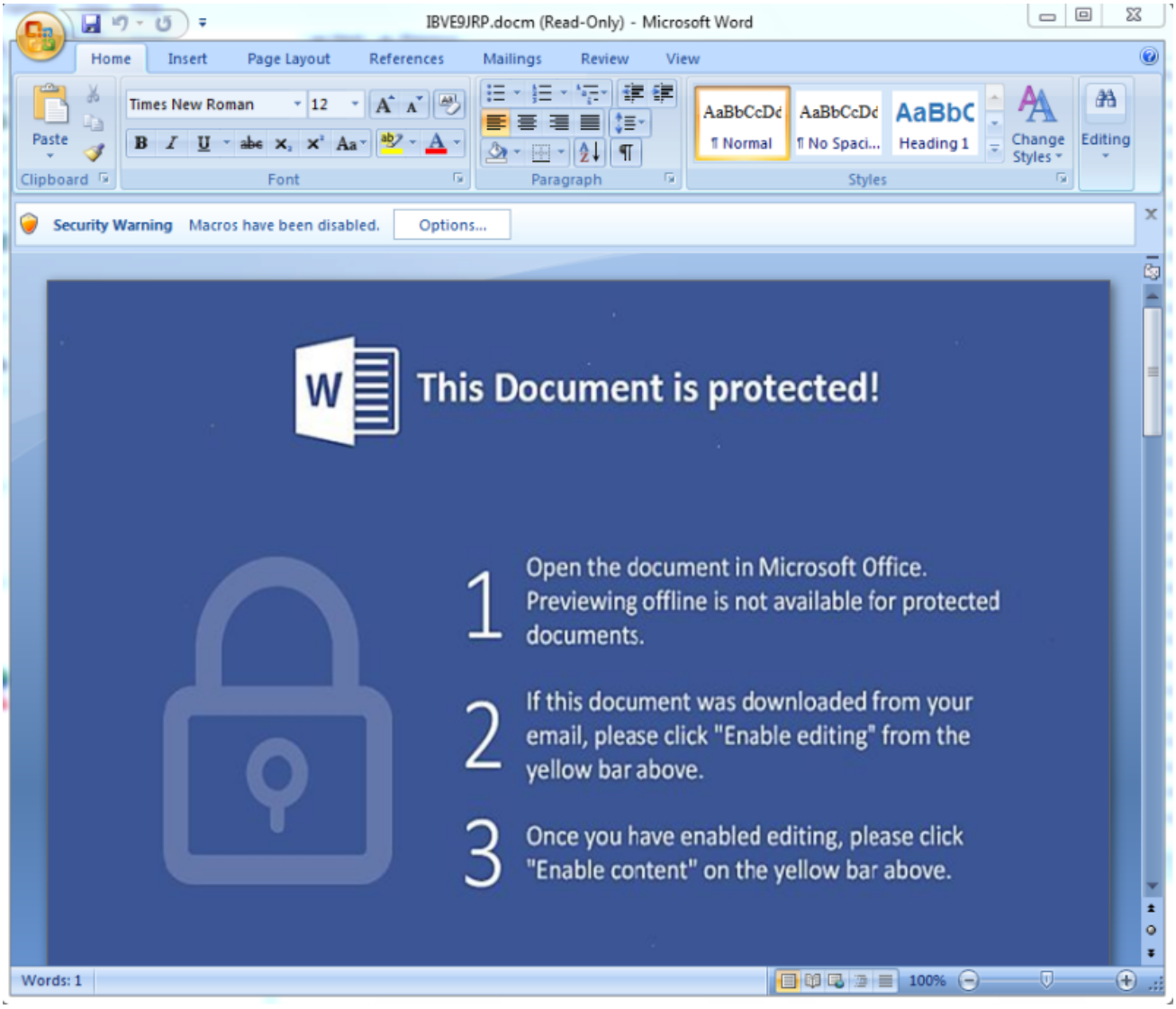




Saving and opening the PDF attachment, as shown below, has an exportDataObject Launch instruction to open the embedded .docm file



The PDF File will drop and launch the embedded .docm file



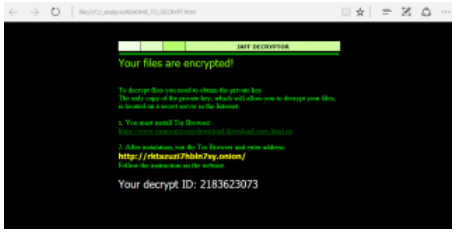
If the macro is enabled, it will start to download a malicious file from URL which is the Jaff Ransomware. The table below shows differences from variants from week to week:

1st and 2nd Week	3rd Week
Dropped ransom notes on every folder that it encrypted files in it, the image file was also used as a desktop wallpaper once ransomware done encrypting your files.	

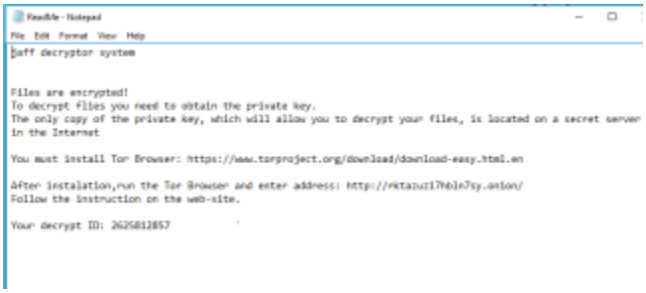
Readme.bmp

README_TO_DECRYPTI.bmp

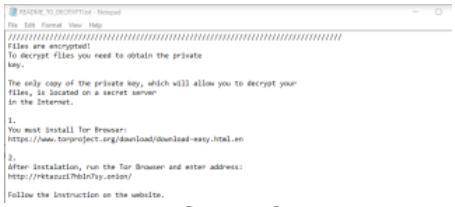
ReadMe.html



ReadMe.html



ReadMe.txt



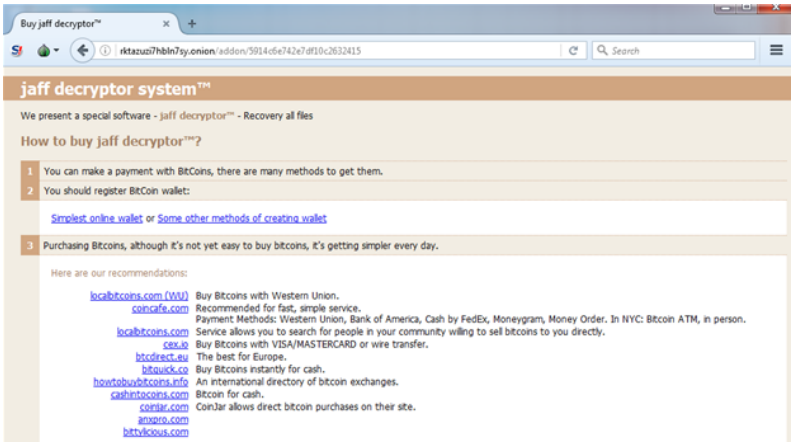
README_TO_DECRYPTI.txt

Encrypted files will have an appended file extension

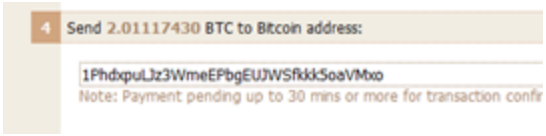
{Original FileName}.**jaff**

{Original FileName}.**wlu**

Even though the appearance is different, both variants have the same URL where you are able to recover your encrypted files.



Earlier versions asks for 2.01 BTC and later versions it only asks for 0.31 BTC



To conclude Necurs is a large botnet and when active it distributes massive volumes of malicious spam. As observed, it tends to take breaks on weekends and it currently has an ongoing campaign using malicious PDFs to download Jaff ransomware. These malicious PDFs are continuously evolving by adding more layers of embedded files and obfuscation.

The Trustwave Secure Email Gateway can recognize and block this threat.

MD5 hashes of the malware:

PDF Droppers
d364eb043e01f61822c9d2906a36ad2f902c60d7
8e4f36e0710aee26f125acc69b14cac44467238f
2001971c7ddaa9b2550d1b870f5e377c56f15f70

DOC Downloaders
ee4fef6b870d0baa3a503aa8594dc16920f7b8a3
f66680aac290ad5febd6bc5b40efe16817bd6850
5045d532a951af205d0e0d91805b2bc38ee6aedd

Jaff Ransomware 1
03b17da93cf91f61c9dbb4d25182016cefec0659

Jaff Ransomware 2
551f953db4ba48452a4f7de9f5f7149c98ddf52f