Technical analysis of a new variant of Zepto Ransomware

The Infiltration

Just like the previous variant, the new version of Zepto is also targeting victims through malspam.

In most cases, the victim receives an email that seems to be from a legitimate source and has an attachment. The spam campaigns are getting more sophisticated with time by pretending to address the victim based on the email ID itself.

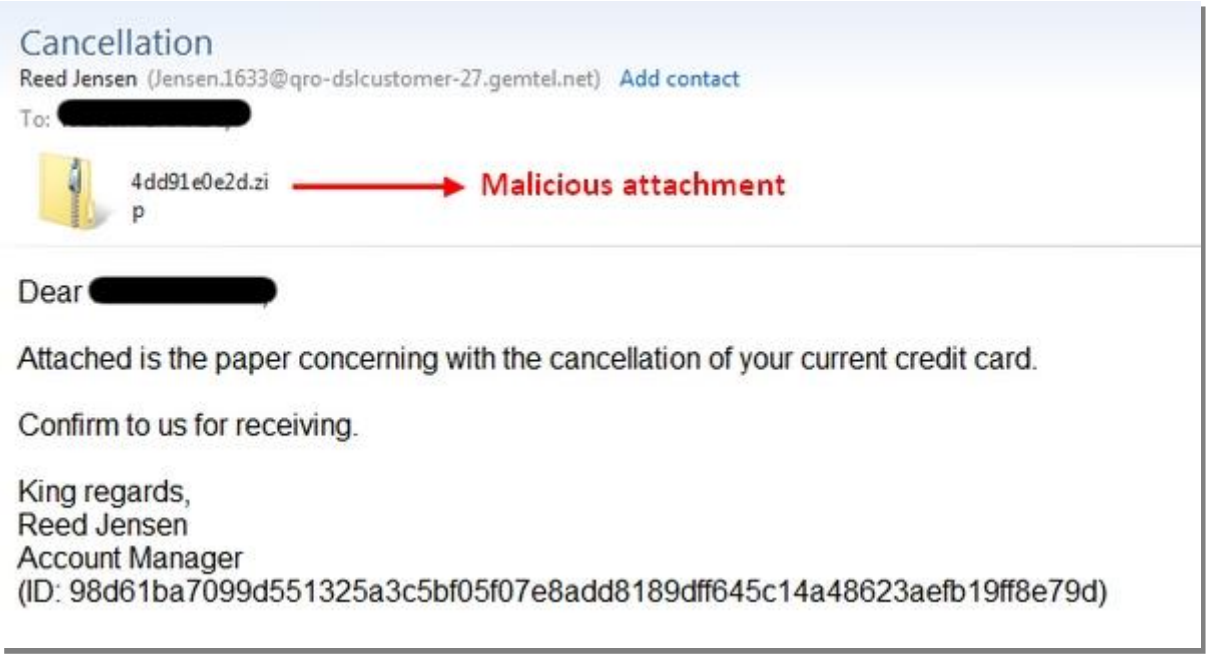


Fig 1. The subject and content of the mail is designed to lure the victim into opening it.

The attachment contains a malicious script file which is usually a JS or WSF file type.

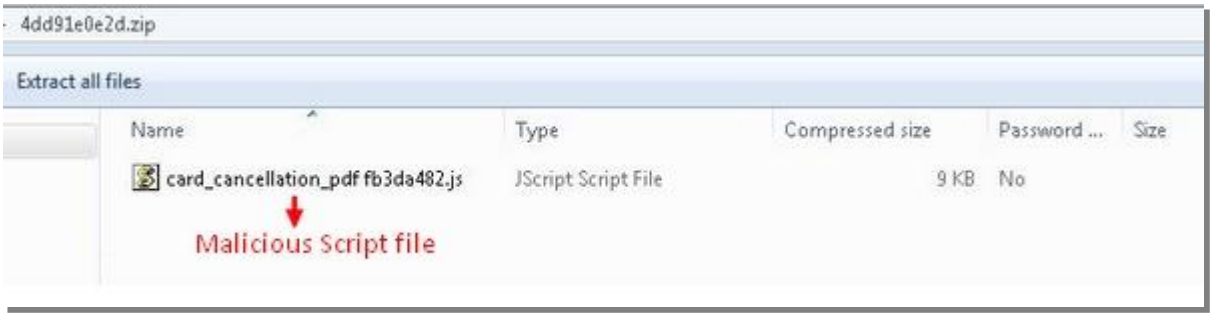


Fig 2. Here, we see a JS file which is poorly disguised as a PDF file.

The unsuspecting user double clicks on the script file which releases the malicious code hidden inside it. The execution is done by the Windows Script Host (wscript.exe) which is an integrated application to run scripts on Windows Operating System.

The encryption

Upon execution of the script files, wscript tries connecting to a few malicious links for downloading the ransomware payload which is an encoded extension-less file. The encoded file is then decoded into the DLL file by Windows Script Host which is still running the malicious script.

Fig 3. The downloaded encoded file and the respective DLL file obtained after decoding.

As mentioned earlier, the new variant uses DLL files unlike its previous variant and unlike exe files, DLL files cannot be executed on their own. Hence the wscript calls forth rundll32.exe which is another Windows OS file used to run DLL libraries.

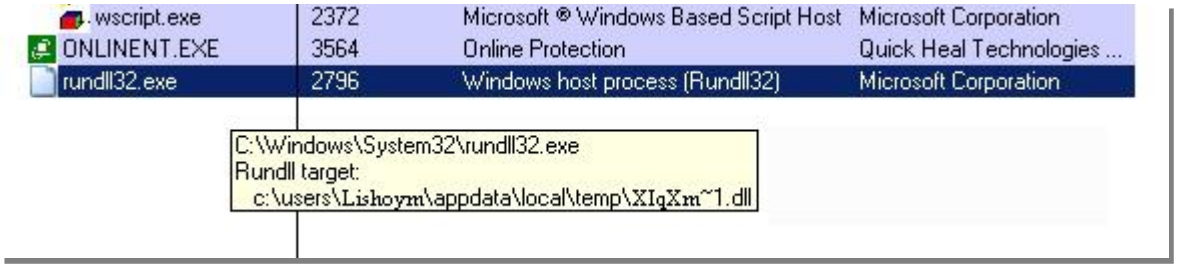


Fig 4. The payload being run by Windows rundll32.

Thereafter, the encrypting begins targeting specific file types based on their extensions. The affected files can be recognized by the new unique ID and appended '.zepto' extension.

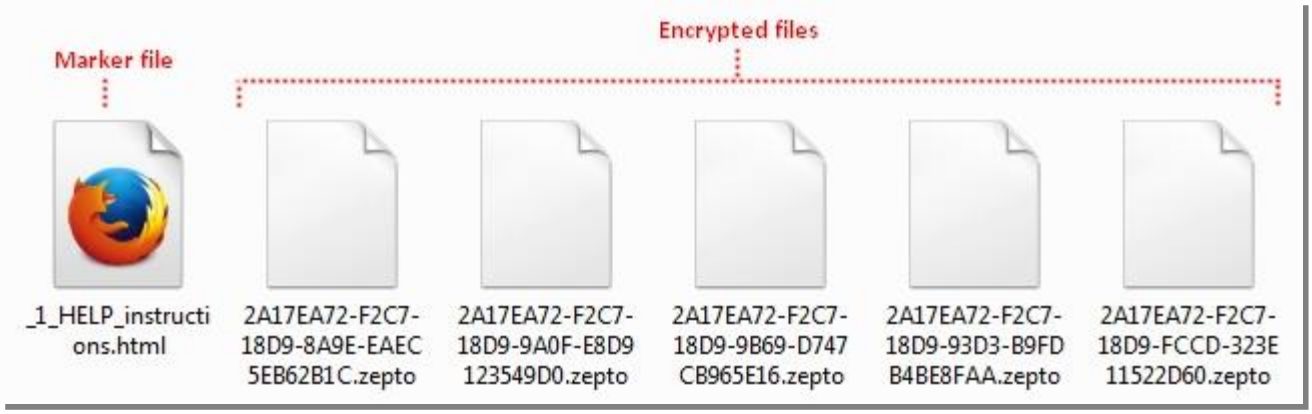
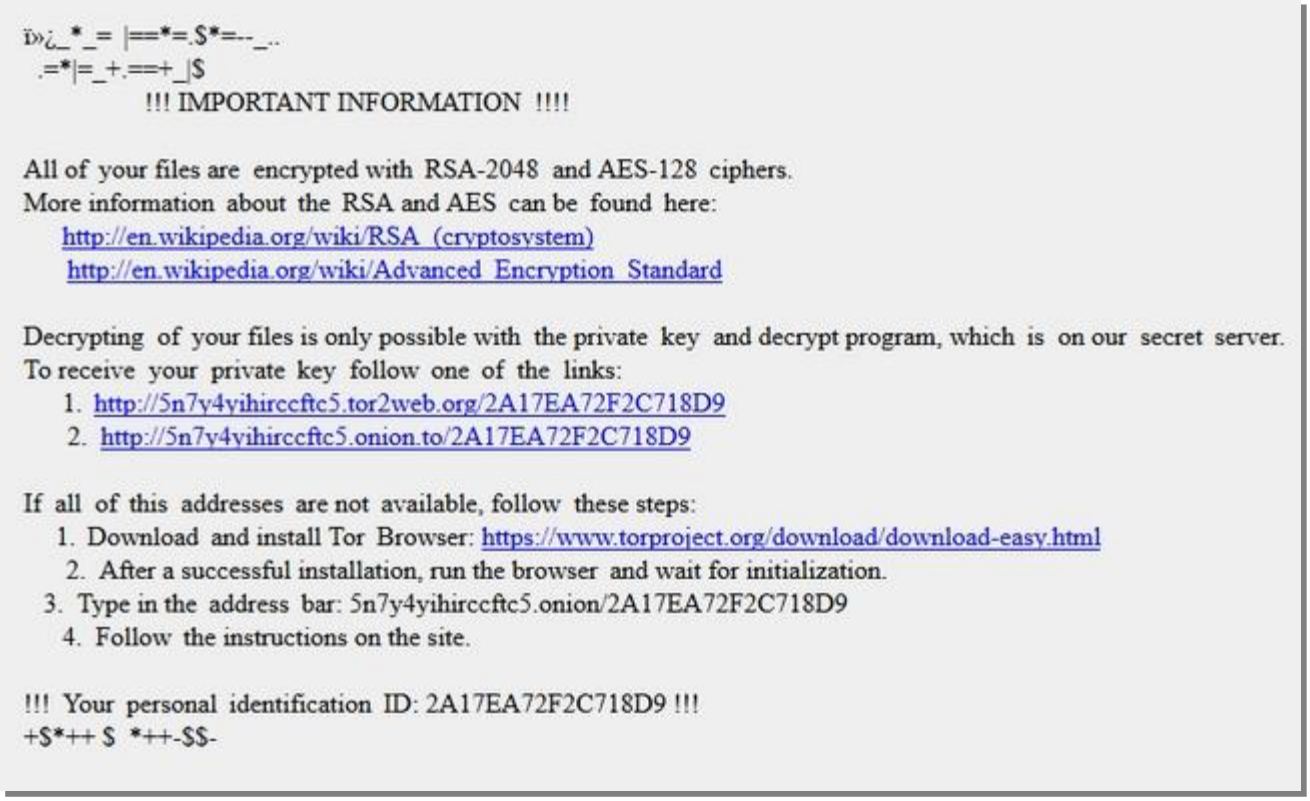


Fig 5. The dropped marker file and the encrypted files with .zepto extension.

After the encryption is completed, the ransomware changes the desktop wallpaper and opens up the dropped marker file. The marker file contains details of the encryption and how to recover the files by paying the ransom.



ï»¿_*_= |==*=.$*=--_..
.=*|=_+.==+_|$

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://5n7y4yihirccftc5.tor2web.org/2A17EA72F2C718D9
2. http://5n7y4yihirccftc5.onion.to/2A17EA72F2C718D9

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 5n7y4yihirccftc5.onion/2A17EA72F2C718D9
4. Follow the instructions on the site.

!!! Your personal identification ID: 2A17EA72F2C718D9 !!!
+$*++ $ *++-$$-

Fig 6. The information page which opens up after encryption is completed.

Finally, the ransomware's finishing move is deleting itself to evade security analysts.