

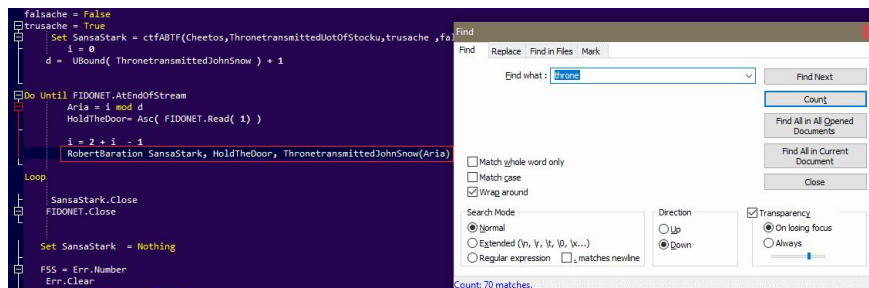
The owner of extortionist Lockey is a big fan of Game of Thrones

This is a group of fans that George RR Martin might not want to be in the line of kingship - a group of ransomware Locky authors.

According to what researchers at PhishMe recently discovered, the hacker group behind malicious code Locky is a fan of HBO's hit series, so much so that they include script names of movie characters and lots of information. other.

The researchers found this information in Visual Basic scripts, part of a ZIP or RAR file attached to a spam email. When the user opens the mail, download the file and run this script, the file will download and install Locky.

Names related to Game of Thrones can be found in VB scripts such as Aria, SansaStark, RobertBaration, JohnSnow and HoldTheDoor (or Hodor). The word Throne is also used 70 times.



Many names related to Game of Throne can be found in the script of malicious code

The runtime environment of this script does not matter how variable names are. The variable name would be fine, although it was a random combination of letters and numbers, 'said researcher Victor Cornell at PhishMe. 'The people behind this malicious code choose their own themes for their variables, thus revealing their interests'.

According to an independent researcher at MalwareHunter, this scenario has been exploited for several weeks. Below is IOC information.

File name: SCNMSG00001018.vbs

MD5: 170ae05fb405e9f2b2a4474739b75a66

SHA256: fc89d30e245a8b166af2e17b2d7b6835ff15999d746b91214edcfdc7b9c5db35

You finished reading the article "**The owner of extortionist Lockey is a big fan of Game of Thrones**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can

search for similar articles on tips and guides. Thank you for reading and for following us regularly.
