

Russian malware link hid in a comment on Britney Spears' Instagram

 engadget.com/2017/06/07/russian-malware-hidden-britney-spears-instagram/

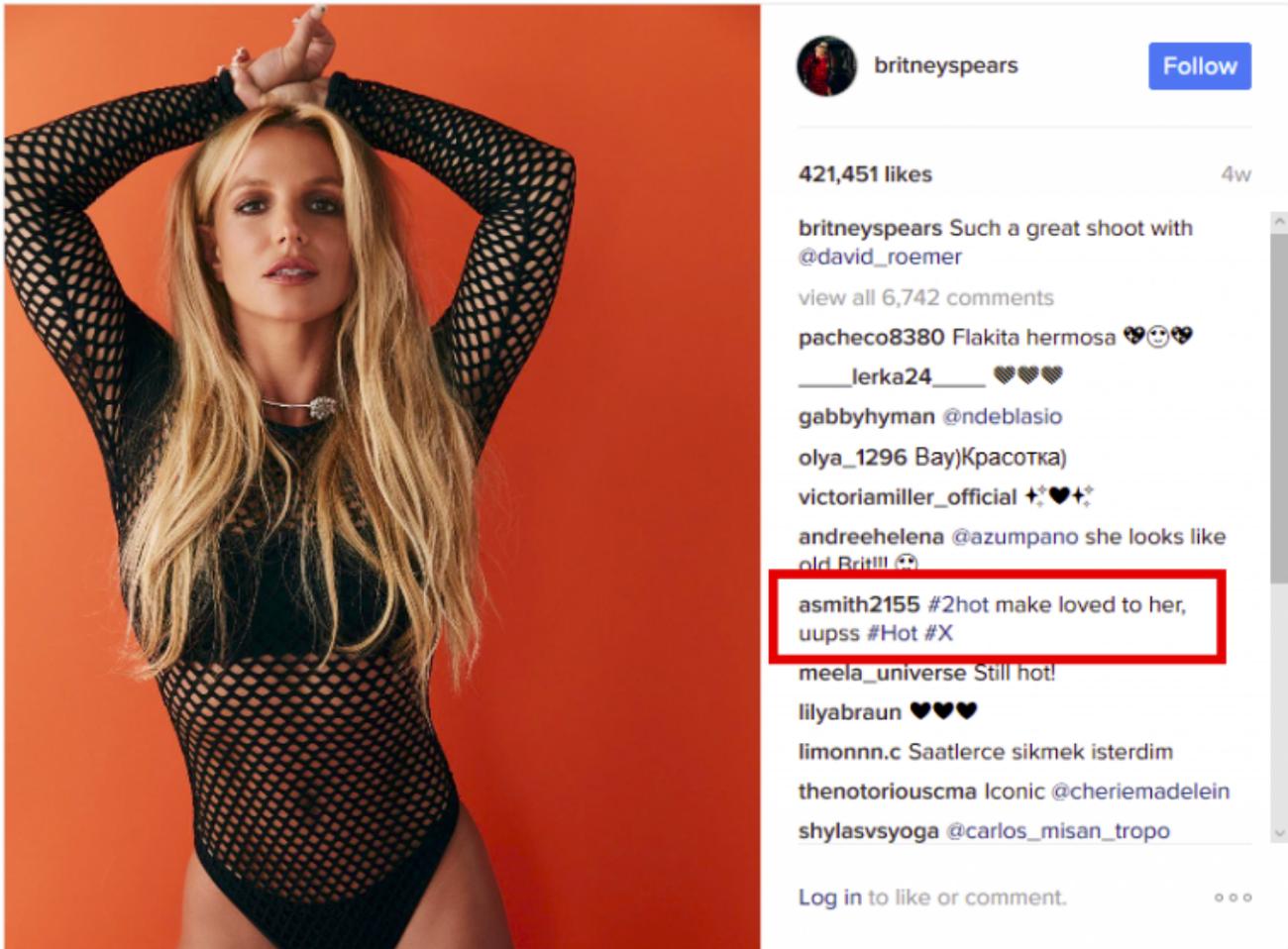
Mallory Locklear



Radio Disney via Getty Images

Instagram is on its way to hitting a billion users this year and with that kind of popularity comes a lot of traffic. But lurking among all of many, many harmless comments that get posted each day, there's also the occasional post instructing Russian malware how to get in touch with its controllers. Because of course there is.

The Slovak IT security company ESET Security released a report yesterday detailing a cleverly hidden example of such a post. And its hideout? A Britney Spears photo. Among the nearly 7,000 comments written on the performer's post (shown below) was one that could easily pass as spam.



The malware was situated in a Firefox browser extension pretending to be a security feature and it would search for hidden links in order to connect back to its control server. And the comment, now deleted, was actually a web address that required a fairly complicated, multi-step process to decipher.

In this case, the malware went through all of the comments on Spears' Instagram photo and computed a number, or a "hash," for each one, while it looked for a specific hash. When it found the comment with the right hash, it would check it out for particular characters, grab the letters that came after those characters and turn them into a [link](#). That link would then let the malware connect to its controllers. Such a method allows the controllers to change where it meets up with the malware without having to change the malware itself.

ESET Security said they thought this particular post was just a test and linked the malware scheme to a group called Turla, a cyber espionage group that the company says has targeted governments, government officials and diplomats for some time.

So, while that weird comment on your latest selfie might look like junk, it could actually be a conduit for some Russian malware and the subject of some upcoming breaking news. Happy posting.

All products recommended by Engadget are selected by our editorial team, independent of our parent company. Some of our stories include affiliate links. If you buy something through one of these links, we may earn an affiliate commission.