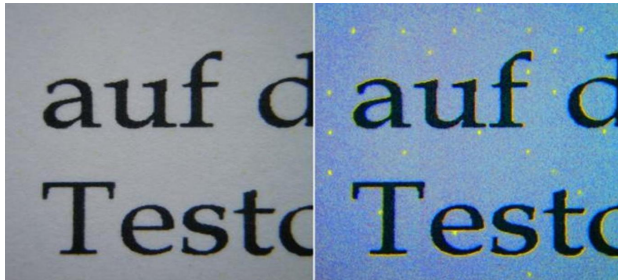


Tu impresora te delata

Algunas marcas de impresoras de chorro de tinta dejan rastros con información del usuario

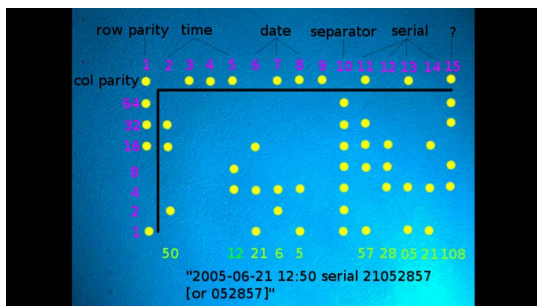


El 3 de junio varios agentes del FBI irrumpieron en la casa de la contratista del gobierno Reality Leigh Winner en Augusta, Georgia. Habían estado los dos últimos días investigando un documento confidencial secreto que, supuestamente, fue filtrado a la prensa.

Para poder localizar a Winner, los agentes dijeron que analizaron cuidadosamente copias de un documento impreso y "trasladado a mano a un lugar seguro".

Efectivamente, el FBI dijo que Winner admitió haber impreso el informe de la Agencia de Seguridad Nacional.

Los expertos comenzaron a analizar el documento más en profundidad y descubrieron algo muy interesante: puntos amarillos en un patrón rectangular que se repetían a lo largo de la página. Eran prácticamente invisibles para el ojo humano, pero formaban un mensaje cifrado.



Tras varios análisis rápidos, descubrieron que los puntos parecían revelar la fecha y día exacto en el que las páginas habían sido impresas: las 6:20am del 9 de mayo de 2017 (al menos, esa era la hora en el reloj interno de la impresora en ese momento).

Instagram de Britney Spears: Hackers rusos utilizaban los comentarios para comunicarse



Hay que aceptar que los hackers cada vez se vuelven más creativos, ya que han sabido aprovechar nuevas herramientas que están al alcance de todos, como las redes sociales. Tal es el caso de la cuenta de Instagram de Britney Spears, que se convirtió en una plataforma perfecta de comunicación entre hackers sin que nadie se diera cuenta.

La firma de seguridad ESET ha publicado un informe donde detalla cómo hackers rusos han usado el perfil de Instagram de la cantante a través de los comentarios en cada una de sus fotos, lo que lo vuelve una misión imposible de rastrear debido a la gran cantidad de comentarios que recibe diariamente. Es que Britney tiene más de 17 millones de seguidores, y sus fotos contabilizan miles de comentarios.

ESET descubrió que entre esos miles de comentarios, aparentemente inofensivos, se encuentran algunos con instrucciones encubiertas para la difusión de malware. Dichos comentarios suelen pasar como SPAM ya que contienen varios hashtags sin sentido aparente, pero en realidad contienen detalles de una dirección web.

En el comentario que ESET pone de ejemplo se ve un hashtag central que sirve para localizar el comentario, y una vez allí se coloca una cadena de caracteres que servirán para crear una dirección web dentro de un enlace 'bit.ly'. En este caso todo apuntaba a '2kdhuHX', que servía para conectarse con el servidor de mando y control del malware.

