Hot Clicks: FBI Hacks to Track Down Finance Cybercriminals

The agency created a fake website and rigged document to try to obtain an IP address.

Amanda Ziadeh

Mon, 11/26/2018 - 17:21

Photo Credit: South_agency/iStock

The FBI usually uses these techniques for child pornography and bomb threat cases, but recently, is using hacking to find financially-driven cybercriminals, according to court documents discovered by Motherboard. In one case, the FBI set up a fake FedEx website and created a Word document trap, both designed to get the IP address of scamming cybercriminals. The FedEx website was created to help a cranes manufacturing company in New York. Cybercriminals used an official looking email to pose as the company's CEO, emailing the accounts team asking for

payments for a new vendor, and the finance department mailed a check for more than $82,000. But the company noticed it was fraudulent, and when they got another email from their fake CEO, the FBI was ready.

The fake FedEx site was sent to the target to capture the scammer's IP address, but it didn't work, so the FBI used a network investigation technique (NIT). This is a term the FBI uses for a variety of hacking techniques, and in this case, meant the FBI used a Word document containing an image, a screenshot of a FedEx tracking portal for a send payment, that would connect to the FBI server and show the criminal's IP address. It's unknown yet if this was successful. Motherboard

First CRISPR Babies Cause Controversy

Chinese researcher He Jiankui says he created the first gene-edited babies, twin girls Lula and Nana. This came out after MIT Technology Review reported on a secretive Chinese project to produce children with modified genomes making them HIV-resistant. In a video statement, Jiankui said the twins were conceived using IVF and his team added some protein and "information" to the fertilized eggs. MIT says that's a reference to the ingredients of CRISPR, the gene-editing technology used to delete a gene called CCR5 (HIV can use this gene to enter and infect host cells). But this experiment has set off criticism in China and from experts around the world due to the unknown risks and medical uses, and Jiankui faces investigation over whether it breaks Chinese laws. MIT Technology Review

You Can Pay Taxes in Bitcoin in Ohio

It's a first in the country: Ohio is allowing businesses to pay their taxes in cryptocurrency, and all interested companies have to do is go to OhioCrypto.com and register for the program. And this includes everything, like cigarette sales tax and employee withholding taxes, and the plan is to extend this crypto capability to individual filers, too. In order to convert bitcoin to dollars, Ohio is working with the cryptocurrency payment startup BitPay. This bitcoin program is part of the state's goal to become more tech-friendly, as it has its own tech hub developing in Columbus. TechCrunch

Success: NASA’s InSight Lander Made it to Mars

There’s a new robot on Mars, and it landed safely on Nov. 26 -- the first to do so since the Curiosity rover in August 2012. Signals confirming InSight’s landing got to the Jet Propulsion Laboratory managing the mission, easing the anticipation and breaking the silence of eager NASA members. Minutes later, JPL received the confirmation from InSight’s radio that it was functioning correctly after landing. But NASA isn’t in the clear yet, as team members won’t know if InSight successfully deployed its solar panels until the evening of Nov. 27, which is when NASA’s MArs Odyssey orbiter will be in the right place to relay that deployment confirmation. If those arrays don’t extend, the lander won’t survive or probe Mars’ interior — InSights main goal. Plus, NASA’s Mars Odyssey won’t be able to relay that deployment confirmation Space.com

USPS Had — and Fixed — a Data Leak

The U.S. Postal Service fixed a security vulnerability on its website that let anyone see the personal account information, like username, email and street address, usps.com users. The vulnerability included all 60 million account users, and was caused by an authentication weakness in the application programming interface that let anyone get into a USPS database meant for businesses and advertisers to track user data and packages. The API is supposed to verify if an account has permission to access that data, but those controls weren’t in place. The flaw was identified a year ago by an independent researcher but USPS did patch it until November when it was flagged by a journalist. USPS said it’s still investigating to make sure data wasn’t inappropriately used. The Verge

View PDF
news roundup
space
Mars
FBI
China
NASA
cryptocurrency
bitcoin