Hot Clicks: Did China Hack U.S. Companies with a Tiny Microchip?

If so, the attack impacted 30 companies, including Amazon and Apple.

Amanda Ziadeh

Tue, 10/09/2018 - 13:54

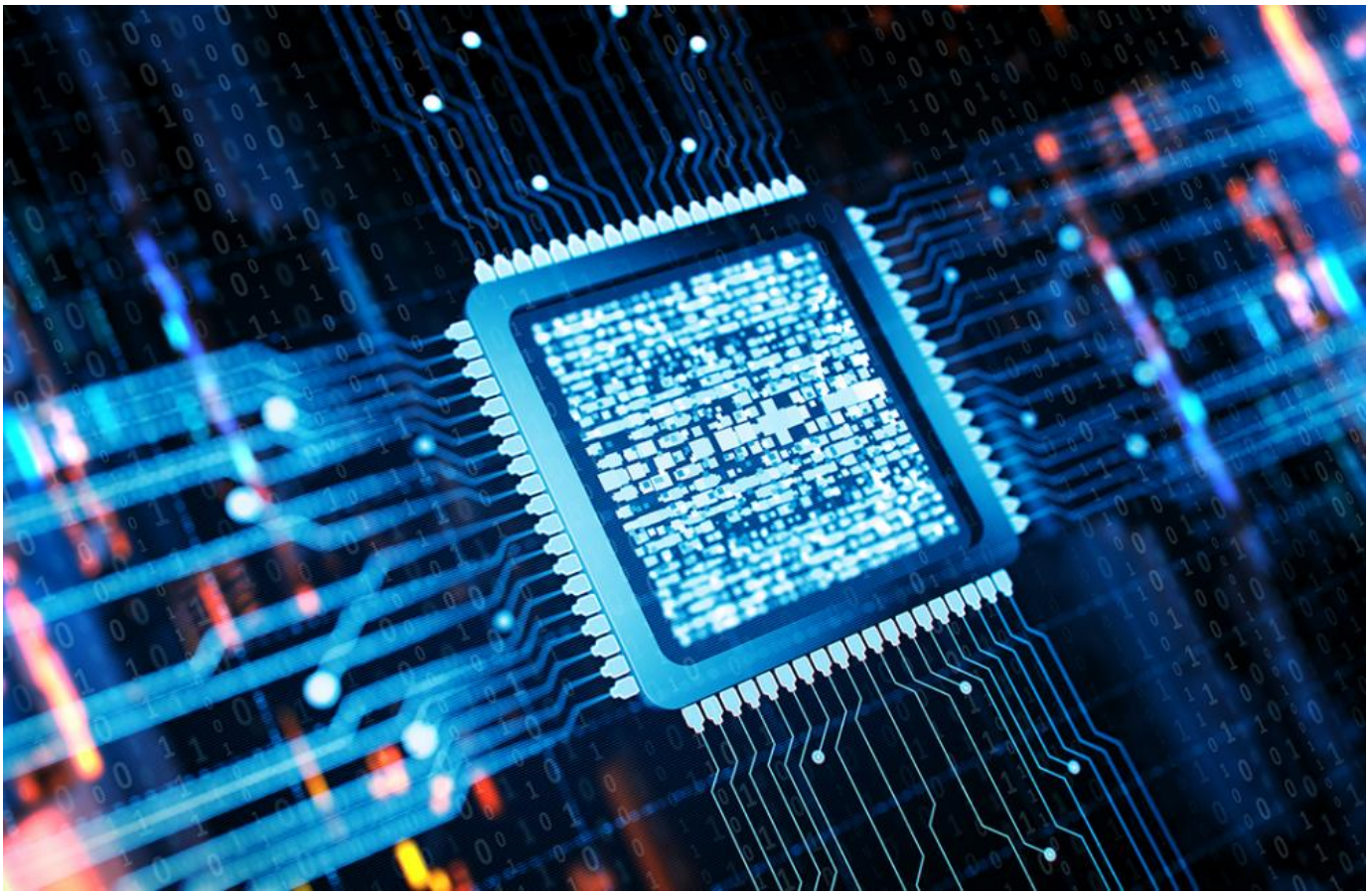

Photo Credit: MF3d/iStock

The hack started when Amazon.com Inc. looked into a startup called Elemental Technologies to help with its Amazon Prime video streaming services in 2015. Elemental made software for compressing big video files. Amazon Web Services was also overseeing possible acquisition to use the software in its government business, and hired a third-party company to vet Elemental's security. This led to a closer look at the servers assembled for Elemental by Super Micro Computer Inc., one of the world’s biggest suppliers of server motherboards.

It was in the motherboards that a third-party security company testing the

equipment found a tiny microchip, which wasn't part of the boards' original design. A secret U.S. investigation began and discovered that the chips allow attackers to create a doorway into any network connected to the altered machines, and they were inserted during manufacturing at factories run by subcontractors in China.

Elemental's servers are found in Defense Department data centers, in the CIA's drone operations, onboard networks of Navy warships, and an official said this attack impacted 30 companies including Apple Inc. Apple has since denied that its systems were compromised by China in a letter to Congress, but questions remain over the validity and severity of this ongoing investigation. Bloomberg

Deep Learning Algorithms are Teaching Prosthetic Limbs

Infinite Biomedical Technologies, a Baltimore startup company, is using deep learning algorithms to identify signals in the upper arm of an amputee that relate to different hand movements. The amputee is Andrew Rubin, a 49-year-old college professor from Washington, D.C., who wears a special device on his upper arm. The electrodes in his arm connect to a box that records the patterns of his nerve signals going off, so he's training the prosthetic limb to act like a real hand (and even open his beers). When he thinks of closing a hand, muscles in the forearm naturally contract. "The software recognizes the patterns created when I flex or extend a hand that I do not have," he told Wired. There are prosthetic devices that can recognize limited signals, but Infinite is using better signal processing, pattern recognition software and advances in engineering to build new prosthetic controllers that are even more like real limbs, by allowing the prosthetic to receive more data. Wired

Google Plus is Shutting Down After Users' Data Exposed

Google announced that it's getting rid of Google+, its attempt at a social networking site, after a security vulnerability exposed the private data of 500,000 users. The company actually discovered the security issue in March, but says it didn't tell users because it didn't seem as if anyone gained access to user information. So, Google's Privacy & Data Protection Office said it wasn't legally

required to report it. Still, 400 applications made by outside developers could have gained access to the vulnerability via APIs, and access to user names, email addresses, occupation, gender and age. Google says the vulnerability did not allow access to other Google accounts, however, and outside developers weren't even aware of it. The New York Times

Can AI Detect Fake News Yet?

Apparently it is not being done well enough, according to a new study. Researchers from MIT, Qatar Computing Research Institute and Sofia University in Bulgaria tested more than 900 variables for predicting the trustworthiness of a media outlet by training a machine-learning model on the different combination of those variables to see what would give the most accurate results. At best, the model correctly labeled news outlets with “low,” “medium,” or “high” factuality 65 percent of the time. What this really tells us is what it actually takes to have a machine fact-check for us, and it’s challenging. The method comes from one of four approaches to detecting fake news: measuring the reliability of news sources, because this gets closest to the origin of fake information. So, to identify fake news sources in close-to-real-time, the team trained the system using variables that could be organized without human fact-checkers, like sentence structure of headlines, word diversity, website traffic, and so on. But there just isn’t enough training data yet to get to the truth, because labeling media outlets with high or low factuality requires professional journalists to follow “rigorous methodologies,” and this takes time. MIT Technology Review

DotGov Rolls Out Two-Step Verification

The General Services Administration’s DotGov is the registrar that manages .gov domains for the U.S. government, and it began putting new security protections in place on Oct. 1 for government sites to prevent domain name system takeover attacks. If an attacker phishes their way into a .gov domain, they can change the DNS entries for the domain and redirect users to malicious sites, so DotGov is rolling out Google Authenticator 2-step verification mechanism to protect .gov accounts. So from now till Feb. 13, DotGov will ask all .gov domain owners to start setting up 2SV for their accounts. This will take a while, and government domain owners will need to install the Google Authenticator app on their mobile devices and after logging in with their credentials, scan a barcode with the app to generate a

one-time code they can use for phase two of the login process. All, of course, in the name of security. ZDNet

View printer friendly version
news roundup
Apple
Amazon
GSA
AI
Google
hacking