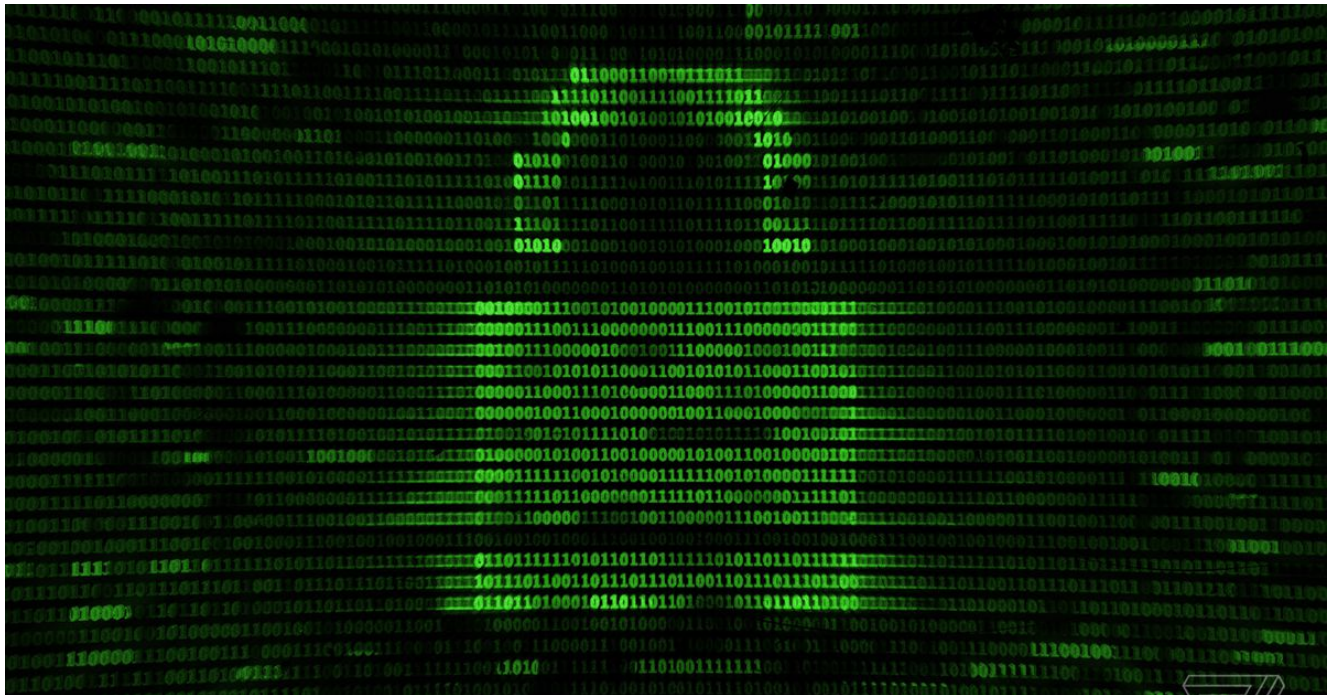


Ubiquiti hack may have been an inside job, federal charges suggest



An indictment from the Department of Justice suggests that the Ubiquiti hack reported in January, and subsequent whistleblower claims of a cover-up, were the work of someone who was then an employee of the company. The DOJ alleges that Nickolas Sharp, 36, was arrested on Wednesday on accusations that he used his employee credentials to download confidential data and sent anonymous demands to the company he worked for pretending to be a hacker in an attempt to get a ransom of 50 Bitcoin. You can read the full indictment below.

The indictment doesn't specifically name Ubiquiti, only referring to a "Company-1." However, all the details line up. In January, Ubiquiti sent an email to users saying an unauthorized party had accessed its "information technology systems hosted by a third party cloud provider." In March, someone claiming to be a whistleblower represented the incident as "catastrophic," alleging that the company couldn't

tell the full extent of the attack because it wasn't keeping logs and that the attacker had access to Ubiquiti's Amazon Web Services (AWS) servers.

The indictment says the scheme fell apart because of a 'fleeting' VPN hiccup

The indictment says the company is based in New York, which Ubiquiti is, and says that the company's stock price fell by around 20 percent between March 30th and March 31st after news broke of the incident. According to Yahoo Finance, Ubiquiti's stock was worth \$376.78 on March 29th and fell to \$298.30 by March 31st.

Perhaps most notable is the allegation that Sharp posed as a whistleblower to media outlets in late March 2021 – the same time a whistleblower accused Ubiquiti of covering up the data breach's severity, despite the company's denial that user data was targeted. We also viewed a LinkedIn profile that appears to belong to Sharp and shows him working for Ubiquiti during the timespan listed in the indictment.

The DOJ alleges that Sharp accessed the company's Amazon Web Services and Github accounts after applying for a job at another company in December 2020. The indictment says that another employee discovered the breach days after Sharp downloaded "gigabytes" of confidential data and applied AWS policies to limit logging. Sharp was allegedly assigned to the response team meant to assess the incident, and the DOJ says he used this position to try and avoid suspicion.

Sharp allegedly contacted media outlets after the FBI searched his house

According to the indictment, Sharp sent an anonymous ransom email that promised not to publish the data and help the company patch a backdoor if he was paid 50 Bitcoin by January 10th, 2021. The DOJ alleges that Sharp released some of the stolen data when the company didn't pay the ransom.

The DOJ says that it was able to track down Sharp because of

one tiny technical glitch – Sharp allegedly used SurfShark VPN to mask his identity while taking data and sending emails, but “in one fleeting instance,” his real IP was identified and logged as connecting to the company’s GitHub. According to the DOJ, this happened when Sharp’s home internet went down, and then reconnected.

According to the indictment, this eventually led to the FBI carrying out a search warrant on Sharp’s house, where he denied using SurfShark and said that someone else used his PayPal account to purchase the subscription. In a final twist, the indictment says that Sharp contacted media outlets posing as a whistleblower *after* the FBI searched his home and seized electronic devices.

If Sharp is found guilty and the DOJ can prove that the incident unfolded as laid out in the indictment, it’ll certainly cast a new light on the reports of the Ubiquiti hack. The indictment alleges that Sharp started the attack using credentials he had been given to do his job. In March, Ubiquiti held fast to its statement that attackers didn’t access customer data, which doesn’t appear to be contradicted by the information revealed today.

<https://www.theverge.com/2021/12/1/22812761/ubiquiti-data-breach-aws-doj-indictment-inside-job>