CASE STUDY

Sabotage

Sudhish Kasaba Ramesh

- Age 31 at time of conviction
- Software Engineer
- Fluent in English, Hindi, and Kannada and has the ability to converse in Tamil and German.

WHAT HAPPENED

Employed by Cisco Systems, Inc. from August 2016 to April 2018, Sudhish Kasaba Ramesh was part of a platform team at Cisco, which focused on automation, access to data, and logging metric and learning. As a member of the platform team, he possessed the access key for Cisco's WebEx Teams application that was maintained on servers hosted by Amazon Web Services (AWS). Ramesh would leave employment at Cisco Systems, Inc. and later join the workforce of Stich Fix, an online personal styling service that utilizes recommendation algorithms and data science to personalize clothing items.

After Ramesh's departure, Cisco failed to change the AWS password. Consequently, on September 24, 2018, Ramesh used his AWS key to access Cisco's AWS account that maintained the servers for WebEx through his Google Cloud Platform account. He then issued commands over the course of two hours that deleted approximately 456 servers, resulting in the complete shutdown of the WebEx Teams application.

The FBI identified Ramesh as the responsible party because the Google Cloud Platform account was registered in his name as well as in the name of his alias, Ramya Ravichandran, and paid for using his American Express card. In addition, the Internet Protocol (IP) address from which the attack was launched was the defendant's work computer and took place while he was present at work.

On July 13, 2020, Ramesh was charged with one count of intentionally accessing a protected computer without authorization and recklessly causing damage. The maximum penalty for this charge is five years imprisonment and a fine of $250,000.

According to the plea agreement, Ramesh admitted to intentionally accessing the Cisco Systems and that during his unauthorized access he deployed a code from his Google Cloud Project account that resulted in the deletion of the virtual machines for Cisco's WebEx Teams application.

On December 9, 2020, Ramesh was sentenced to 24 months in prison, followed by one year of supervised release and a fine of $15,000.

INDICATORS

Access Attributes:

- As a member of the Cisco platform team, Ramesh possessed the access key for Cisco's WebEx Teams application that was maintained on servers hosted by Amazon Web Services.

Technical Activity:

- Ramesh used his AWS key to access Cisco's AWS account and delete over 450 servers, resulting in the complete shutdown of the WebEx Teams application.

CDSE

Center for Development of Security Excellence

IMPACT

- As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers.
- Ramesh is a non-US citizen working in the United States with an H-1B visa. This visa means he possesses highly specialized knowledge or skills and education to work in specialty occupations. This classification of visas are generally good for three years. Both the court and his employer, Stich Fix, acknowledged his guilty plea may have immigration consequences, up to and including deportation.
- At one point, Stitch Fix was willing to work with Ramesh regarding the possibility of his remaining in the country and continuing to work for the company. If Mr. Ramesh is deported, he could serve any period of supervised release or probation in his native country of India while continuing to work either for his current employer or another employer.

ADDITIONAL INFO

- Ramesh has a Master of Science in Electrical and Computer Engineering from the University of California at Santa Barbara, a Bachelor of Technology in Electronics and Communication Engineering from Vellore Institute of Technology in India, and has several computer-related certifications.
- Ramesh's job history connects him to numerous technology companies, including Qualcomm, Oracle, and WePay.
- Though it cost them 2.4 million in restoration and refunds, Cisco did not request any restitution for the damages caused by Ramesh.
- Ramesh's motivation for his actions remains unknown.
- No customer data was compromised as a result of the defendant's conduct.

Resources for further exploration:

- Insider Threat Indicators Job Aid:
  https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf?ver=_HedcDtQk9sSEZItNMLQzA==
- Privileged User Cybersecurity Responsibilities, DS-IA112.06:
  https://public.cyber.mil/training/privileged-user-cybersecurity-responsibilities/l
- DHS - U.S. CERT "Combating the Insider Threat":
  https://www.us-cert.gov/security-publications/Combating-Insider-Threat

IF YOU SEE SOMETHING, SAY SOMETHING!

Contact the appropriate POC to report any observed potential risk indicators:

Name: _____ Agency/Department: _____
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager