

1 DAVID L. ANDERSON (CABN 149604)
United States Attorney

2 HALLIE HOFFMAN (CABN 210020)
3 Chief, Criminal Division

4 SUSAN KNIGHT (CABN 209013)
Assistant United States Attorney

5 150 Almaden Boulevard, Suite 900
6 San Jose, California 95113
7 Telephone: (408) 535-5056
8 FAX: (408) 535-5066
Email: Susan.Knight@usdoj.gov

Attorneys for United States of America

9 UNITED STATES DISTRICT COURT
10 NORTHERN DISTRICT OF CALIFORNIA
11 SAN JOSE DIVISION
12

13 UNITED STATES OF AMERICA,) CASE NO. CR 20-00289 LHK
14 Plaintiff,)
15 v.) UNITED STATES' SENTENCING
16 SUDHISH KASABA RAMESH,) MEMORANDUM
17 Defendant.) Date: December 9, 2020
Time: 9:15 a.m.
Court: Honorable Lucy H. Koh
18)

19 INTRODUCTION

20 The defendant, Sudhish Kasaba Ramesh, stands before the Court to be sentenced following his
21 guilty plea to Intentionally Accessing a Protected Computer and Recklessly Causing Damage, in
22 violation of 18 U.S.C. § 1030(a)(5)(B) and (c)(4)(A)(i)(I). The Probation Office has calculated the
23 defendant's adjusted offense level to be 21, which includes a two-point enhancement for use of special
24 skill pursuant to United States Sentencing Guideline ("U.S.S.G.") Section 3B1.3. The plea agreement
25 did not include this enhancement, and the government stands by its agreement to recommend an
26 adjusted offense level of 19. As discussed below, given the egregiousness of the conduct in this case
27 and the need to deter similar conduct in the future, the government respectfully recommends a low-end
28 Guidelines sentence of 30 months in prison.

DISCUSSION

A. The Offense Conduct

The Presentence Report (“PSR”) accurately recounts the defendant’s conduct. PSR ¶¶ 6-14. The defendant worked for Cisco Systems, Inc. from August 2016 to April 2018. He was part of the platform team at the company and focused on automation, access to data, and logging metric and learning. PSR ¶ 11. 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. PSR ¶ 11. WebEx Teams is a virtual meeting platform that allows its users to, among other things, conduct group video meetings and share documents.

On September 24, 2018, at approximately 4:33 p.m., the defendant 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. PSR ¶ 6. The shutdown affected 16,000 customers and some customers had to wait up to two weeks to have their accounts restored. PSR ¶ 8. Furthermore, Cisco spent approximately \$1,400,000 in employee time to restore the damage to WebEx Teams, and issued \$1,000,000 in refunds to their customers. PSR ¶ 15.

The FBI identified the defendant 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 address from which the attack was launched resolved to the defendant’s work computer and took place while he was present at work. PSR ¶¶ 7, 9, 14.

B. Objection to the Presentence Report

Over the parties’ objection, the Probation Officer has included a two-point enhancement for use of a special skill pursuant to U.S.S.G. § 3B1.3 in his Guidelines calculation. PSR ¶ 23, Addendum to PSR. The government has reviewed the Probation Officer’s comments and his points are well-taken. Nevertheless, the government stands by its agreement with the defendant to recommend the Guidelines calculation contained in the Plea Agreement.

//

1 Furthermore, the government wishes to correct a typographical error that was included in its
2 objection letter to the Probation Officer. Undersigned counsel mistakenly stated that the defendant used
3 a proxy IP address to hide his connections. The sentence should have stated that he *did not* use
4 encrypted IP addresses to hide his identity.

5 **C. Sentencing Recommendation**

6 There is no doubt that the defendant's conduct had a catastrophic effect on Cisco. Their 16,000
7 customers were unable to use the WebEx Teams applications for nearly two weeks, and Cisco spent
8 \$1,400,000 in employee time to remedy the damage. The company also had to issue \$1,000,000 in
9 refunds.¹

10 Balanced against the aggravated nature of the defendant's conduct is his personal characteristics.
11 He has no criminal history, has a Master of Science in Electrical and Computer Engineering from the
12 University of California at Santa Barbara, a Bachelor of Technology in Electronics and Communication
13 Engineering from VIT University in India, has several computer-related certifications, is fluent in
14 English, Hindi, and Kannada, and has the ability to converse in Tamil and German. PSR ¶¶ 32, 53-56.
15 He has an impressive job history and worked for numerous technology companies, including
16 Qualcomm, Oracle, WePay, and Stitch Fix. PSR ¶¶ 58-62. The government is perplexed on how the
17 defendant - a highly intelligent individual - could have left a trail of bread crumbs that lead the FBI to
18 determine that he was responsible for the deletion of Cisco's servers on AWS. He did not use a proxy
19 internet service to hide his identity, registered his Google Cloud Platform account with his email address
20 and American Express card, and launched the attack from his work computer. In fact, when the FBI
21 searched his work computer, the case agent found numerous Google searches for information on AWS
22 servers and how to delete servers. The government surmises that the defendant possibly did not realize
23 that he was accessing a live production environment.

24 Taking in to account the Guidelines calculation and the defendant's history and characteristics,
25 the government respectfully requests that the Court impose a low-end sentence of 30 months
26

27 ¹ Counsel for Cisco informed undersigned counsel that the company will not submit a victim-
28 impact statement nor make a statement at the sentencing hearing. However, a representative from Cisco
will observe the sentencing hearing.

1 imprisonment, and three years of supervised release. Cisco is not seeking restitution, and therefore, the
2 government believes that a \$15,000 fine is appropriate. PSR ¶ 15.

3 **CONCLUSION**

4 With full consideration of the Sentencing Guidelines and the factors set forth in 18 U.S.C. §
5 3553(a), the government respectfully requests that the Court sentence the defendant to 30 months of
6 imprisonment; 3 years of supervised release (with conditions to be fixed by the Court and the special
7 suspicionless search condition agreed upon); the \$15,000 fine recommended by Probation; and a \$100
8 mandatory special assessment.

9 DATED: 12/2/20

Respectfully submitted,

10 DAVID L. ANDERSON
11 United States Attorney

12 */s/ Susan Knight*

13 _____
14 SUSAN KNIGHT
Assistant United States Attorney