IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DAVIS LU, Defendant.	)	INDICTMENT JUDGE BARKER CASE NO. 1:21CR226 Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i)

GENERAL ALLEGATIONS

At all times material herein:

1. From on or about August 4, 2019 through on or about September 5, 2019, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant DAVIS LU accessed and attempted to access protected computers without permission.

2. Defendant was a resident of Pittsburgh, Pennsylvania. Defendant was an employee of Company 1 from on or about November 1, 2007 through on or about October 4, 2019.

3. Company 1 was an Ohio corporation with its principal place of business in Cleveland, Ohio, in the Northern District of Ohio, Eastern Division.

4. Software 1 was an application in use at Company 1 at all times material herein where data was maintained and which supported multiple branches of Company 1.

5. From on or about May 2017 through on or about July 2019, Defendant was employed by Company 1 as a Software 1 Senior Developer and tasked to work with Emerging Technology.

6. On or about August 1, 2019, Defendant was reassigned to the Development Team for Software 1.

7. On or about August 3, 2019, for the first time after Defendant's re-assignment, updates were made to Software 1 without Defendant's involvement in code deployment to the production server.

8. On or about August 4, 2019, Company 1 experienced a disruption which crashed the user-facing Java Virtual Machines operating on the production servers and prevented Company 1 employees based in the Northern District of Ohio and elsewhere from accessing those servers.

9. Company 1 investigated the source of the disruption and discovered code on a development server located in Kentucky that was causing a production server to enter an infinite loop and crash.

10. Company 1 discovered that the code that caused the disruption was executed by Defendant's user id operating on a computer located in Kentucky.

11. Defendant was the only Software 1 developer at Company 1 with access to the development server where the program was running.

12. The code that caused the crashes had no beneficial purpose, and Company 1 did not request that the code be developed.

13. Company 1 found additional code on the development server that, when executed, deleted files associated with user profiles, denying those users access to Software 1.

14. Company 1 found additional code that queried whether Defendant's account was active or not, and if it was inactive, prevented other users from accessing the system.

15. Company 1 requested Defendant return his company-issued computer. Shortly before returning the computer, Defendant deleted encrypted volumes, attempted to delete the Linux directories, and attempted to delete two projects.

16. Company 1 discovered that Defendant conducted internet searches querying how to escalate privileges, hide processes, and delete large folders and/or files.

17. On or about October 7, 2019, Defendant admitted to investigators that he created the code described in paragraphs 9-10 above.

COUNT 1
(Intentionally Damaging Protected Computer(s), 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i))

The Grand Jury charges:

18. The factual allegations of paragraphs 1 through 17 of this Indictment are hereby repeated, re-alleged, and incorporated by reference as if fully set forth herein.

19. From on or about August 4, 2019 through on or about September 5, 2019, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant DAVIS LU did knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused damage affecting ten (10) or more protected computers during a one (1)-year period, and the offense caused loss to persons during a one (1)-year period from Defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i).

FORFEITURE

The Grand Jury further charges:

20. For the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), the allegation of Count 1 is incorporated herein by reference. As a result of the foregoing offense, Defendant DAVIS LU shall forfeit to the United States any property constituting or derived from proceeds obtained directly or indirectly as a result of the violation charged in Count 1; and any property real or personal that was used or intended to be used to commit or to facilitate the commission of the violation charged in Count 1.

SUBSTITUTE ASSETS

If, as a result of any act or omission of the Defendant, any property subject to forfeiture:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been comingled with other property which cannot be subdivided without difficulty;

the United States intends, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any property of Defendant up to the value of any property described above.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.