FILED
OCT 04 2016
CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY ____________
DEPUTY

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Western District of Texas

United States of America
v.
Joe Vito Venzor

Defendant(s)

Case No. EP:16-M-03836-LS

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of September 1, 2016 in the county of El Paso in the Western District of Texas, the defendant(s) violated:

Code Section	*Offense Description*
Title 18, United States Code Section 1030 (a) (5) (A)	on September 1, 2016 Joe Vito Venzor knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer.

This criminal complaint is based on these facts:

See attached Probable Cause Statement.

☑ Continued on the attached sheet.

Complainant's signature

John Bohovic, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: October 4, 2016

Judge's signature

City and state: EL PASO, TEXAS

LEON SCHYDLOWER
US MAGISTRATE

Printed name and title

PROBABLE CAUSE STATEMENT

1. I, John Bohovic, hereinafter referred to as Complainant, am a Special Agent (SA) of the Federal Bureau of Investigation (FBI), and conduct investigations of violations of Federal Criminal Law, including unauthorized intrusion upon protected computers.

2. On September 1, 2016, at approximately 10:30a.m., Joe Vito Venzor was terminated from the IT department of Lucchese Bootmaker, 40 Walter Jones Blvd, El Paso, in the Western District of Texas. Venzor was called into the office of IT director and told the circumstances of his termination. Venzor became volitile and it took almost an hour to get him out of the building. As a consequence of the termination, Venzor's computer access was revoked and his account was disabled immediately after his termination.

3. On the same day, at approximately 11:30a.m., a network account with administrator rights named "elplaser" accessed the Lucchese network and shutdown the company's email server. Shortly after this, the same account shut down the company's application server and deleted critical system files so that the server could not be rebooted. The application server controlled the company's production line, warehouse, distribution center, and their ability to take orders. The elplaser account also accessed online services which were used by Lucchese and changed passwords and closed service accounts.

4. During the course of the intrusion the Lucchese IT director discovered a document which Venzor had sent from his work email to his personal email address. According to employee records Venzor had listed this address as his personal email. The document contained a list of account usernames and passwords for network systems and services used by Lucchese. The IT director noticed that the intrusion followed the same order the as the accounts listed in the document. After noticing this, the IT staff was able to get ahead of the intrusion by changing the admin passwords and locking out the elplaser account. The intrusion lasted approximately 45 minutes.

5. On or about September 14, 2016, the IT department discovered that several weeks prior to the intrusion, the elplaser account had been logged into from Venzor's work computer. Venzor was the only one with access to his work computer because it was password protected. The elplaser account was named such to appear innocuous, like a laser printer, and look like any other service account. Lucchese uses service accounts in production and gives these accounts only basic network privileges, not full administrative access. Elplaser had no legitimate purpose on the network but instead was created as a backdoor, giving the attacker full administrative access to the Lucchese network.

6. As a result of this unauthorized intrusion, 300 employees in the factory could not work for nearly three hours and eventually had to be sent home because the system could not be fixed. The Lucchese distribution center could not ship any products and they were unable to accept any new orders for half that day. The application server could not be restored and the company had to set up a new application server from scratch and had to pay addition IT professionals to assist. The company estimates they lost approximately $100,000 of sales in addition to the lost production time and the extra IT expenses.

7. Based upon the above information, the Complainant has probable cause to believe that on September 1, 2016, Joe Vita Venzor committed the offense of knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer. This offense is in violation of Title 18 United States Code Section 1030 (a) (5) (A).