UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
CENTRAL DIVISION
AT LEXINGTON

UNITED STATES OF AMERICA, **Plaintiff,** **V.** **IBRAHIMSHAH SHAHULHAMEED,** **Defendant.**	**CRIMINAL ACTION NO. 5:12-118-KKC** **OPINION & ORDER**

*** *** ***

This matter is before the Court on the defendant's motion for acquittal, or in the alternative, motion for a new trial (DE 102). For the following reasons, the Court will deny the defendant's motion.

Defendant Ibrahimshah Shahulhameed was found guilty of violating 18 U.S.C. § 1030(a)(5)(A), which makes it unlawful to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer. During a trial that lasted approximately one week, the United States presented evidence that the defendant was terminated from his position at Toyota Engineering & Manufacturing North America—where he worked as a subcontractor—on August 23, 2012. Following his termination, the defendant used his remote access to Toyota's computer system to make a series of programming changes to Toyota's servers that caused extensive damage. The defendant now moves for acquittal pursuant to Rule 29 of the Federal Rules of Criminal Procedure, arguing that the evidence

was insufficient for a rational trier of fact to have found him guilty under 28 U.S.C. § 1030(a)(5)(A).

I.

When addressing a motion for judgment of acquittal, the Court must view the evidence in the light most favorable to the prosecution and determine whether there was sufficient evidence offered at trial to convince a rational trier of fact beyond a reasonable doubt that all of the elements of the charged crimes have been established. *United States v. Graham*, 622 F.3d 445, 448 (6th Cir. 2010). The Court is precluded from weighing the evidence, considering witness credibility, or substituting its judgment for that of the jury. *United States v. Chavis*, 296 F.3d 450, 455 (6th Cir. 2002). The court gives the government "the benefit of all inferences which can reasonably be drawn from the evidence, even if the evidence is circumstantial." *United States v. Carter*, 355 F.3d 920, 925 (6th Cir. 2004).

The defendant can be found guilty of violating 18 U.S.C. § 1030(a)(5)(A) only if the following facts are proved beyond a reasonable doubt:

(1) the defendant knowingly caused the transmission of a program, information, code, or command to a protected computer;

(2) the defendant, as a result of such conduct, intentionally caused damage to a protected computer without authorization; and

(3) the damage resulted in losses of more than $5,000 during a one-year period.

In view of these elements, the defendant presents three reasons as to why he is entitled to acquittal under Rule 29: First, he contends that insufficient evidence was presented to prove that the defendant's actions caused more than $5,000 in damage. Second, the defendant argues that the evidence does not support a finding that he was "without authorization" at the time the programming changes occurred. Third, the defendant argues

that the evidence did not establish beyond a reasonable doubt that he was the individual who issued the programming changes that caused the damage. All three of these arguments are without merit and the defendant's motion will be denied.

A. Evidence of Damage

The United States must prove that the damage caused by the defendant resulted in losses of $5,000 or more within a one-year period. Under 18 U.S.C. § 1030(a)(5)(A), a "loss" includes "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." 18 U.S.C. § 1030(e)(11). Losses can include the cost of time spent by a salaried employee of the victim in responding to the damage. *See United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006). Thus, the cost of Toyota's remedial efforts in responding to the defendant's cyber-attack is properly considered a loss under § 1030(a)(5)(A).

To prove that the defendant caused at least $5,000 in damage to the affected computers, the United States relied on the testimony and reports by a number of witnesses. Deva Veerasamy, an information systems employee at Toyota, testified that he spent a significant amount of hours diagnosing and repairing the problems caused by the defendant's actions. Tom Cantrell, a supervisor at Toyota, testified to the hundreds of hours that employees within his department worked to repair the damage. Although these witnesses did not quantify the exact cost of the many hours of labor expended, the United States introduced Exhibit 6 to make such a quantification. Exhibit 6 provided a summary of the hours and costs incurred by Cincinnati Bell Technology Solutions (CBTS) and Toyota. It did so by displaying the number of hours employees spent working on the problems alongside of each employee's hourly rate. According to this exhibit, the damage caused to Toyota between August 24, 2012 and October 30, 2012 was at least $187,070, far greater

than the $5,000 minimum requirement. Moreover, testimony by Toyota employees during trial indicated that Toyota continued to incur costs after October 30, though quantification of these costs was unnecessary given the amount of damage already established at trial.

The defendant contends that this evidence is insufficient for a rational trier of fact to conclude that the $5,000 threshold was met. He points to the fact that the government failed to introduce "certified business records" and the fact that Exhibit 6 did "not show what was supposedly worked on, the damage that existed, how said damage was fixed, any description of the work performed or any other illuminating information." (DE 102, at 2). While it might be true that the government could have provided even more evidence to establish the damage at issue, the evidence presented at trial is sufficient on its own for a rational trier of fact to find that the losses exceeded $5,000. Considering the testimony of the various witnesses in conjunction with the summary exhibit of Toyota's costs, and viewing it all in the light most favorable to the government, the evidence was more than sufficient to establish the minimum amount of damage required.

B. Evidence Established the Defendant Was "Without Authorization"

The defendant argues that the evidence does not support a finding that he was "without authorization" when the programming changes were made because witnesses for the United States testified that his access to Toyota's computer system was revoked sometime between 6:32 a.m. and 7:00 a.m. the morning after the cyber-attack. That is to say, the defendant contends that he could not have been "without authorization" if his access had not yet been revoked.

To begin, the defendant glosses over the testimony by Andrew Sell, the defendant's supervisor at the employment agency for whom he worked. Sell testified that the defendant was terminated from his position at Toyota on the evening of August 23, 2012 at

approximately 11:00 p.m. The cyber-attack did not take place until after that termination occurred. The defendant dismisses Sell's testimony, calling it "sketchy at best," but offers no reason to doubt it. Moreover, the defendant's supervisor at Toyota testified that none of the programming changes made by Shahulhameed were authorized, so even if he retained his access and had not been terminated, the changes he made were "without authorization."

As the United States correctly explains, the defendant's argument improperly conflates "*access* itself with the authorization to *use* access to transmit information, codes, and commands." (DE 103, at 4). In doing so, the defendant relies on several cases that analyze different provisions of § 1030 that make it unlawful to access a computer without authorization. But Shahulhameed was not charged with unauthorized *access*. Rather, the defendant was charged under § 1030(a)(5)(A), which makes it unlawful to "cause[] damage without authorization." 18 U.S.C. § 1030(a)(5)(A). "No one claimed at trial that the Defendant lacked the ability to access Toyota's computer systems after his termination." (DE 103, at 5). Instead, and in accordance with the crime charged, evidence was presented to demonstrate that the defendant used his access to make unauthorized programming changes that damaged Toyota's computers. Support for this lack of authorization came in several forms, including Sell's testimony that he had been terminated from his position at Toyota and the defendant's former supervisor who testified that the changes made by Shahulhameed were not authorized. The evidence here undoubtedly supports a finding by a rational trier of fact that the defendant caused damage without authorization.

C. Evidence Supports Finding Defendant Issued the Damaging Commands

Finally, the defendant argues that he is entitled to acquittal because the evidence did not sufficiently establish he was the one issuing the commands that caused damage to Toyota's computers. This argument is, essentially, the same put forth at trial that was

rejected by the jury. At trial, the defendant repeatedly questioned how the government's witnesses could know that the defendant issued the damaging commands when the command logs lacked timestamps, no evidence was presented regarding other individuals who might have been accessing the server at the same time, the server logs relied on by Toyota *could* be manipulated, and thus no trier of fact could find beyond a reasonable doubt that it was Shahulhameed who engaged in the cyber-attack. The defendant's claim that the evidence is insufficient to establish his guilt on this issue is wholly without merit.

The United States presented evidence through a number of witnesses who testified it was Shahulhameed who issued the damaging commands. Jaime Seibert and Justin Hall, forensic investigators for Toyota and CBTS, testified that the four user accounts used to access the servers and issue the programming changes all traced back to the defendant. Seibert examined the defendant's laptop and testified that its internet history indicated that Shahulhameed accessed the web interface through which one could make the changes. The government also introduced a number of exhibits demonstrating that the defendant, using the four user accounts associated with the commands, accessed these servers during the relevant periods. Although the defendant repeats his argument at trial that these logs could *in theory* be manipulated, no evidence was presented to prove any such manipulation occurred and the jury clearly rejected this argument. Such a finding by the jury is certainly reasonable. Finally, the forensic investigators and Agent Keown all testified that the configuration changes made to the servers were sufficient to disable the computer systems.

The defendant also relies on the fact that the command history logs do not contain timestamps indicating when each change to the server files was made. While this is true, the United States presented significant amounts of evidence that the defendant, using his laptop and user account, made the programming changes that caused the damage. In fact,

during his testimony the defendant himself admitted that he made some of these programming changes. The fact that others might have been logged into Toyota's server at the same time does not call into question the jury's reasonableness in determining—based on the testimony of several witnesses—that the defendant was behind the attack. Ample evidence presented at trial indicated that the defendant was the *only* individual who could be traced to as having issued the damaging commands. Although the defendant might question this conclusion, the jury clearly did not.

Viewing all of the evidence in the light most favorable to the government, including the testimony by the private forensic investigators and Agent Keown, along with the server logs and the defendant's own testimony that he issued some of the programming commands, a rational trier of fact could reasonably determine that it was Shahulhameed who made these programming changes, which then caused damage to the Toyota servers. The evidence is therefore sufficient to sustain the guilty verdict and the defendant's motion for acquittal will be denied.

II.

The defendant styles his motion as seeking a new trial in the alternative to his motion for acquittal. The motion, however, does not present arguments for a new trial. The Court will therefore construe his motion as arguing for a new trial on the same grounds as for acquittal: that being the manifest weight of the evidence does not support the jury's verdict.

The standard for a new trial does not parallel that for acquittal. When examining a defendant's motion for a new trial, the court "may vacate any judgment and grant a new trial if the interest of justice so requires." Fed. R. Crim. P. 33(a). "The decision whether to grant a new trial is left to the sound discretion of the district court." *United States v. Pierce*, 62 F.3d 818, 823 (6th Cir. 1995). "A district judge, in considering the weight of the evidence

for purposes of adjudicating a motion for new trial, may act as a thirteenth juror, assessing the credibility of witnesses and the weight of the evidence." *United States v. Hughes*, 505 F.3d 578, 593 (6th Cir. 2007) (citing *United States v. Lutz*, 154 F.3d 581, 589 (6th Cir. 1998)). Moreover, "it is widely agreed that Rule 33's 'interest of justice' standard allows the grant of a new trial where substantial legal error has occurred." *United States v. Munoz*, 605 F.3d 359, 373 (6th Cir. 2010).

In construing the defendant's arguments for acquittal as also supporting a motion for a new trial, the Court finds them without merit. Although the Court is permitted to act as the thirteenth juror and weigh the evidence in order to determine whether a new trial is necessary, the reasons stated above all support the same conclusion in this alternative motion. The evidence overwhelmingly supports the findings that the losses totaled more than $5,000, that Shahulhameed was without authorization in causing the damage, and that he was the individual behind the cyber-attack. For all of the reasons stated above, the defendant's alternative motion for a new trial will be denied.

* * *

Accordingly, **IT IS ORDERED** that the defendant's motion for acquittal, and in the alternative, motion for a new trial (DE 102) is **DENIED**.

Dated his 16th day of April, 2014.

Karen K. Caldwell

KAREN K. CALDWELL, CHIEF JUDGE
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY