NOT RECOMMENDED FOR FULL-TEXT PUBLICATION
File Name: 15a0710n.06

Case No. 14-5718

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

FILED
Oct 22, 2015
DEBORAH S. HUNT, Clerk

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff-Appellee,	)	
	)	ON APPEAL FROM THE UNITED
v.	)	STATES DISTRICT COURT FOR
	)	THE EASTERN DISTRICT OF
IBRAHIMSHAH SHAHULHAMEED,	)	KENTUCKY
	)	
Defendant-Appellant.	)	
	)	
	)	

BEFORE: BOGGS, SUTTON, and STRANCH, Circuit Judges.

BOGGS, Circuit Judge. On the evening of August 23, 2012, Ibrahimshah Shahulhameed was fired from his job at GlobalSource IT as a contractor for Toyota Motors. A few hours later, Toyota experienced a cyberattack that rendered several of its computer servers inoperable. Toyota's investigation revealed that the attack came from Shahulhameed's Toyota-owned laptop and Shahulhameed's user account. An independent investigator and the FBI corroborated Toyota's findings.

Shahulhameed was arrested and charged with "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer," resulting in at least $5,000 of damage in a one-year period, in violation of 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i). After a five-day trial,

a jury returned a guilty verdict. Shahulhameed appeals on the ground that there was insufficient evidence to support the conviction. After carefully considering the evidence, we affirm Shahulhameed's conviction.

I

In reviewing the sufficiency of the evidence, we must affirm the conviction if "after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." United States v. Warshak, 631 F.3d 266, 308 (6th Cir. 2010) (quoting Jackson v. Virginia, 443 U.S. 307, 319 (1979)).

II

A

A reasonable jury could have found that Shahulhameed knowingly transmitted computer codes and commands to a protected computer. Dennis James Seibert, Jr., a specialist in Toyota's information security department, testified that Shahulhameed's password-protected user account ("ishah") logged in to Toyota's remote-access system on the following occasions:

	Login	Logout
Access #1	August 23, 2012 11:56:04 PM	August 24, 2012 1:55:26 AM
Access #2	August 24, 2012 3:10:10 AM	August 24, 2012 4:20:07 AM
Access #3	August 24, 2012 4:40:45 AM	August 24, 2012 6:13:48 AM
Access #4	August 24, 2012 6:26:07 AM	August 24, 2012 6:55:09 AM

The IP address associated with these log ins, 10.235.0.150, matched the IP address of the Toyota-owned laptop issued to Shahulhameed for work. Logging in to the remote-access system

from a Toyota-owned laptop using an assigned user name and password is the only way to access Toyota's servers from outside of Toyota's facilities.

That night, during those remote log-in sessions, Shahulhameed's laptop accessed Toyota's computer servers and transmitted codes and commands to them. Shahulhameed's laptop made changes to the configuration files for the ToyotaSupplier.com website, the eKanban system, the Long Lead Time Parts system, and the Oracle Business Intelligence system. A search of the Internet browsing history on Shahulhameed's laptop confirmed that his laptop accessed the servers. Because these changes came from Shahulhameed's laptop and his password-protected user account, a reasonable jury could have found that Shahulhameed was behind them.

In addition, Toyota's computer systems were "protected." A "protected computer" is a computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). Tom Cantrell, assistant manager at Toyota's information systems technology department, testified that approximately 700 suppliers across the United States interact with Toyota through ToyotaSupplier.com, and that the above-mentioned computer systems are used by Toyota employees in states across the country. Based on the foregoing evidence, a reasonable jury could have found that Shahulhameed knowingly transmitted computer codes and commands to Toyota's protected computer systems.

B

The evidence also shows that Shahulhameed acted without authorization. Authorization requires approval or sanction. See WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012). Andrew Sell, a technical recruiter for GlobalSource IT, testified that he received a call on August 23, 2012, from Adi Gimpaunu, a GlobalSource contractor working for Toyota,

stating that Shahulhameed had harassed Gimpaunu by demanding that Gimpaunu pay Shahulhameed a "finder's fee," or something to that effect. Managers at Toyota heard about the incident and called GlobalSource that evening, stating that one of the two contractors had to be removed. Sell called Shahulhameed on the evening of August 23, 2012, and "told him that the decision has been made that your project has been terminated, that you should have no contact with anyone at Toyota, [and] that you should not report to Toyota tomorrow morning, the next day." Sell asked if Shahulhameed understood, and Shahulhameed said, "yes, okay." Sell also sent Shahulhameed an e-mail that same evening clarifying that he should not report to work the next day and that he should not have contact with anyone at Toyota. Shahulhameed testified that he received the e-mail and replied to it.

Shahulhameed argues that his access was authorized because Toyota did not disable his user account until at least eight hours after his conversation with Andrew Sell. But Toyota's failure to disable his account does not mean that his access was authorized; the phone call and e-mail from Sell are sufficient to establish a lack of authorization. Given the late hour—Sell e-mailed Shahulhameed around midnight—it is not surprising that Toyota waited until the next business day to disable his account. A reasonable jury could have found that Shahulhameed was not authorized to access Toyota's computer systems.

C

Shahulhameed intentionally caused damage to Toyota's computer systems. Dennis Seibert testified that the configuration changes traced to Shahulhameed's laptop on the morning of August 24, 2012, included: (1) disabling load balancing between ToyotaSupplier.com servers, which prevented users from accessing the systems; (2) changing letters in connector names, which made it impossible for servers to communicate with each other, effectively shutting the

servers down; and (3) adding unknown password requirements for access to administrative consoles, which made it impossible to use the consoles. Based on this evidence, a reasonable jury could discredit Shahulhameed's claim of only trying to help Toyota close his projects or transition them to others.

The destructive nature of these changes betrays an intention to cause damage. Seibert testified that in his opinion, the changes were not consistent with a business purpose. Some of the changes were minute and difficult to detect without a specialized tool. In one instance, the letter "S" was changed from uppercase to lowercase, and in another, the letter "O" was switched with the number "0." Adam Keown, a special agent with the FBI, testified that making these subtle changes, without coordinating with colleagues, was harmful and inconsistent with a legitimate business purpose.

The attacker also used a touch command, which changes the timestamp for when the file was last modified. Agent Keown testified that the touch command is commonly used by cyber-attackers in an attempt to hide their changes. Justin Hall, an outside forensic investigator with Cincinnati Bell Technology Solutions, testified that the attacker removed history files and modified files in a way that "you wouldn't do unless you were trying to hide something."

Shahulhameed contends that it would be irrational for him, an experienced professional with family obligations, to commit such an easily-detectable crime intentionally. But emotions can lead to rash decisions, and Shahulhameed's attempts at hiding his tracks suggest that he may well have thought that he could escape detection. A reasonable jury could have concluded that Shahulhameed intentionally damaged Toyota's computer systems.

D

Finally, the evidence shows that Shahulhameed's conduct resulted in at least $5,000 of damage in a one-year period. Agent Keown investigated the costs that Toyota incurred as a result of the cyberattack. Toyota provided Keown with documentation showing that Toyota employees spent 2,133 hours responding to the cyberattack between August 24 and October 30, 2012, with an estimated value of $152,070. Toyota also paid Cincinnati Bell Technology Solutions for 200 hours of labor at $175 per hour between August 24 and September 30, 2012, totaling $35,000. These figures were not challenged at trial. Contrary to Shahulhameed's argument, the prosecution demonstrated exactly how it calculated the damage that Toyota suffered. Based on this evidence, a reasonable jury could have found that Shahulhameed caused at least $5,000 of damage.

III

Shahulhameed cites United States v. White for the proposition that "evidence which requires a leap of faith in order to support a conviction" is insufficient. 932 F.2d 588, 590 (6th Cir. 1991) (per curiam). White held that the defendant's mere awareness of a marijuana patch growing behind his house was insufficient to establish possession or intent to distribute when: (1) the marijuana patch was not on his property; (2) there was no testimony that he was ever seen in the patch; (3) there was no path connecting his trailer home to the patch; (4) there was overgrowth between his trailer and the patch; (5) the fertilizer in the patch did not match the fertilizer in his trailer; (6) the police found no seeds, scales, or drug paraphernalia when they searched his trailer; and (7) his physical disability suggested that he lacked the physical capacity to grow a twenty foot by thirty foot marijuana patch. Ibid. Here, no leap of faith is required. The cyber-attack came from a laptop assigned to Shahulhameed and in Shahulhameed's

possession. It was launched from his password-protected account, just hours after he was fired. The nature and extent of the damage and Shahulhamed's attempts to cover his tracks could lead a reasonable jury to believe that he intended to cause damage.

A rational trier of fact could have found beyond a reasonable doubt that Shahulhameed knowingly transmitted codes and commands that intentionally caused damage to Toyota's protected computers without authorization, resulting in at least $5,000 of damage in a one-year period. Shahulhameed's conviction is AFFIRMED.