THE WALL STREET JOURNAL.

http://www.wsj.com/articles/hackers-trick-email-systems-into-wiring-them-large-sums-1438209816

BUSINESS | SMALL BUSINESS

Hackers Trick Email Systems Into Wiring Them Large Sums

Scrap processor thought it paid $100,000 to its vendor: 'We in fact had sent a wire to who knows where'

By **RUTH SIMON**
July 29, 2015 6:43 p.m. ET

Cybercriminals are exploiting publicly available information and weaknesses in corporate email systems to trick small businesses into transferring large sums of money into fraudulent bank accounts, in schemes known as "corporate account takeover" or "business email fraud."

Companies across the globe lost more than $1 billion from October 2013 through June 2015 as a result of such schemes, according to the Federal Bureau of Investigation. The estimates include complaints from businesses in 64 countries, though most come from U.S. firms. Both "organized crime groups from overseas and domestic-based actors" are typical perpetrators, said Patrick Fallon, a section chief in the FBI's Criminal Investigative Division.

Their targets are businesses such as Mega Metals Inc., a 30-year-old scrap processor. In April, the company wired $100,000 to a German vendor to pay for a 40,000-pound container load of titanium shavings. Mega Metals typically buys three to four loads of titanium a week from suppliers in Europe and Asia, for anywhere from $50,000 to $5 million or more per transaction. Mega Metals crushes and washes the titanium scrap before selling it to mills that remelt the scrap into new products.

But following the recent transaction, the vendor complained that it hadn't received payment. A third party had infected the email account used by a broker working for Mega Metals, the company said. "We got tricked," said David Megdal, vice president of the family-owned business in Phoenix, which has 30 employees. "We, in fact, had sent a

wire to who knows where."

George Kurtz, chief executive of CrowdStrike Inc., an Irvine, Calif., cybersecurity firm that investigated the loss, said it appears that malicious software implanted on the broker's computer allowed the crooks to collect passwords that provided access to the broker's email system, and then to falsify wire-transfer instructions for a legitimate purchase. "Given that the money has been moved out several times, there is no hope of recovering it," said Mr. Kurtz.

'We got tricked,' said David Megdal, vice president of Mega Metals. 'We in fact had sent a wire to who knows where.'
PHOTO: MARK PETERMAN FOR THE WALL STREET JOURNAL

Mr. Megdal of Mega Metals said that he reported the incident to his bank, Comerica Inc. "We investigate reported instances of potential fraud," said a Comerica spokesman, adding that it is bank policy not to comment on its "internal fraud policies or procedures or on matters involving a current or former customer claim."

In a recent advisory, the FBI said its Dallas office had identified six Nigerians, possibly working as a group, who had targeted roughly 25 Dallas companies, "with an attempted loss of over $100 million." The emails appeared to be from high-level executives in the company being targeted, the FBI said in the advisory. But in fact, the emails were sent from a domain that was similar, not identical, to the target's actual domain name.

In other instances, cybercrooks have used malware to insert themselves into a company's email system. After monitoring email traffic, they tinker with a legitimate message, altering wire transfer or Automated Clearing House orders so that the payment is diverted to a bank account they control.

A spokeswoman for Nacha, the industry-run group overseeing ACH transactions, says the group "strongly advocates" that businesses "work together with their financial institutions to understand and use sound business practices to prevent and mitigate the risk of corporate account takeover."

In the last year, some insurers began offering "social engineering fraud" coverage as an add-on to their standard crime policies, reimbursing companies for losses when employees are intentionally misled into sending money or diverting a payment based on fraudulent information provided via email, fax, phone call or other means.

Mega Metals now verifies emailed wire-transfer instructions with a phone call to the company getting the payment, using a number received from a source other than the emailed instructions. *PHOTO: MARK PETERMAN FOR THE WALL STREET JOURNAL*

The problem is "really quite new in its frequency and severity," said Steven Balmer, social engineering product manager with Travelers Cos. "Larger companies have some belief that they are better protected because of their internal procedures and controls, but there is strong interest in the coverage from midsize and smaller businesses once they are made aware of the exposure."

"It is very likely that the hacker was able to get into our electronic mails, changing the information for his own benefit," said Giampiero D'Angelo, owner of Co.se.tra Sri, in Naples, Italy, the broker that acted as the middleman between Mega Metals and the vendor. His company has added new verification procedures in an effort to prevent future problems, Mr. D'Angelo said.

Companies of all sizes have lost money as a result of such schemes, but "small businesses are probably one of the biggest targets because they don't have the same

budgets for security and investigations," said Brian Hussey, global director of incident response for cybersecurity firm Trustwave Holdings Inc.

In February, the chief financial officer for Infront Consulting Group Inc., based in Toronto and Las Vegas, received an email that appeared to come from the company's chief executive, instructing her to "Process a payment of $169,705.00 USD." Attached wire transfer instructions, reviewed by The Wall Street Journal, directed that payment be made via Northern Trust Co. to "Cat Financial Power Investment" in Naples, Fla.

The scheme unraveled when Infront CEO Rory McCaw, by coincidence, called the CFO as she was reviewing the request. When she asked what the money was for, Mr. McCaw said he knew nothing about it. Further scrutiny revealed that the email was sent from an address similar to the company's, but that lacked the letter "I" in "consulting."

"We could have missed it," said Mr. McCaw, whose 38-person firm helps companies implement Microsoft software. "We were somewhat lucky that we caught it when we did."

Mr. McCaw said he reported the incident to the police in Lexington, Mass., because the domain was registered at a store in that location.

"The Lexington Police Department decided not to pursue the investigation since no money was lost, it was difficult to determine jurisdiction to investigate, and because bank security was in a better position to track the interstate fraud attempt," said Lexington Police Chief Mark Corr. "These types of banking/security fraud cases are difficult for a small police department to solve."

A Northern Trust spokeswoman said the bank has "robust procedures for detecting and reporting on potentially fraudulent transactions. Upon receiving Mr. McCaw's information," she added, "we promptly followed those procedures." A search of Florida State Division of Corporations records shows no registration for a Cat Financial Power Investment.

Fraudulent transfer schemes are proliferating because "everything is online these days," said Steven Bullitt, an assistant special agent in charge of the Secret Service's Dallas Field Office. By monitoring social media, a company's website and other sources, crooks can gather intelligence needed to craft a legitimate-seeming request, security experts say.

Banks can sometimes "claw back" or recover some or all of the funds by notifying the

receiving bank that the wire was the result of a fraudulent transaction, said Bill Nelson president of the Financial Services Information Sharing and Analysis Center, a nonprofit focusing on cybersecurity issues whose members include banks and other financial institutions.

The window for recovering missing funds can be hours, or at best, a few days. “Once you reach beyond the 72-hour mark, it’s extremely difficult,” said Mr. Fallon of the FBI.

Mega Metals now verifies emailed wire-transfer instructions with a phone call to the company receiving the payment, using a number received from a source other than the emailed instructions, such as the vendor’s website, or via fax.

“We are always trying to make our process more ironclad,” Mr. Megdal said. Losing the $100,000 “was an expensive learning lesson,” he added, “but at least it wasn’t a career-ending lesson.”

Write to Ruth Simon at ruth.simon@wsj.com