FEDERAL BUREAU OF INVESTIGATION

Private Sector Advisory

July 5, 2013

(U) Nigerian Cyber Criminals Using "Man-in-the-E-Mail" Fraud Scheme to Interfere with Business-to-Business Communications

(U) Nigerian Cyber Criminals (NCCs)[1] are diverting large sums of wire payments through access to, and interference with, small business–to-business communications using a "man-in-the-e-mail"[2] technique. We assess, however, that this activity is more prevalent than current reporting indicates. This advisory will inform the reader how the scheme works, provide options on mitigating the threat, and advise how to report incidents to law enforcement.

(U) How the Scheme Works

(U) Step 1

(U) The perpetrator, believed to be an NCC based in Nigeria, compromises a business e-mail account, typically of a Chinese-based manufacturer. The e-mail intrusion is likely accomplished using malware[3] sent via spear phishing[4] to the Chinese supplier; with a subsequent compromise of a US company's e-mail account being optional.[5]

UNCLASSIFIED

(U) E-mail Account Spoofing Techniques

- **(U) Adding/removing characters**: widgets@freemail.com to widget@freemail.com.
- **(U) Rearranging characters**: acme868@freemail.com to acme686@freemail.com.
- **(U) Replacing characters**: In a sans serif font frequently used in e-mail, e.g., Arial, different characters appear to be the same/similar: sa**l**es@freemail.com to sa**l**es@freemail.com; sa**l**es@freemail.com to sa**l**es@freemail.com.

[1](U) The term "Nigerian Cyber Criminal" in this context encompasses both the fraud and hacker methodologies.
[2](U) The term "man-in-the-e-mail" technique is a reference to accessing and interfering with e-mail communications between two victims, distinguishing it from other "man-in-the-middle"-type attacks, which is a form of active ease dropping in which the attacker makes independent connections with the victims and relays messages between them making the victims believe they are talking directly to each other over a private connection.
[3](U) Malware: Malicious software written intentionally to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs, so that users are induced into activating them. Malware include Trojan horses, computer viruses, and worms.
[4](U) Spear Phishing: A type of phishing attack that focuses on a single user or department within an organization to criminally and/or fraudulently acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity.
[5](U) There is a pattern of compromising Chinese companies first and then targeting their US clients. Actual intrusions into US companies' e-mail accounts are not necessary, and the frequency of same is unknown.

(U) Step 2

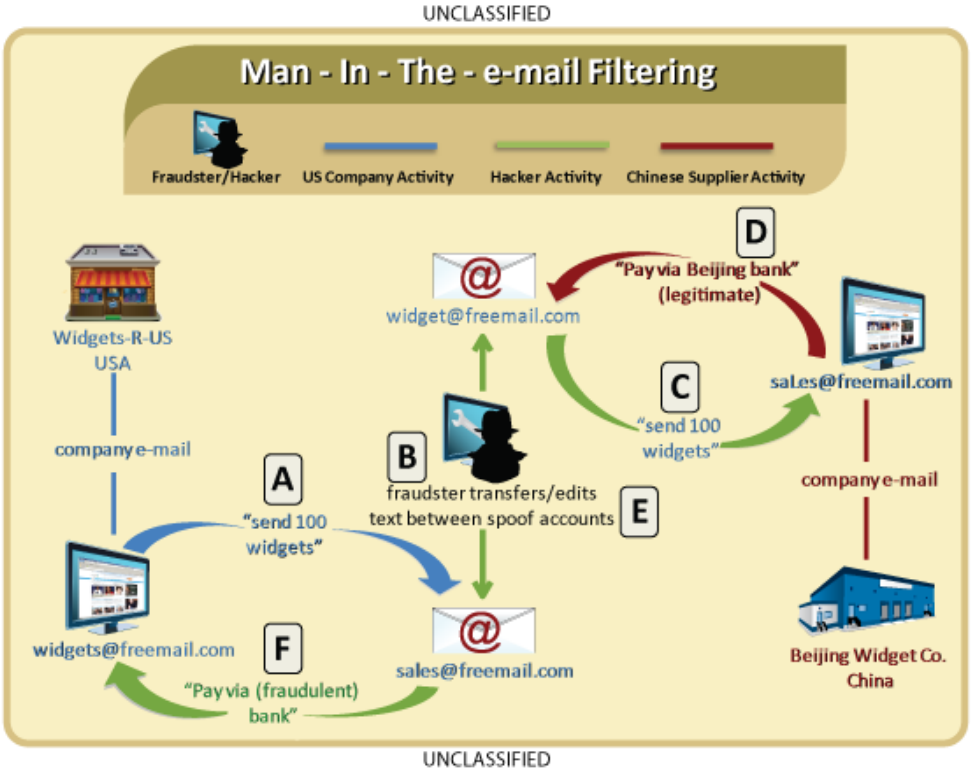
(U) The NCC creates two spoofed e-mail accounts designed to look like the legitimate company e-mail addresses of the US business and Chinese supplier. The fraudster uses different methods to successfully spoof e-mail addresses, such as adding or removing characters, rearranging characters, or replacing characters with similar-looking characters.

(U) Step 3

(U) The NCC, using the new spoofed e-mail addresses, impersonates the Chinese supplier and US business, thus inserting himself as the "man-in-the-e-mail" filter between the two businesses. This is done by either responding to e-mail messages or passing them on to the intended recipient. The NCC monitors the business-to-business communications and transactions until an opportunity to commit a large-scale fraud is identified.

(U) Step 4

(U) The US business subsequently orders a shipment of goods from the Chinese supplier as part of its normal commercial activity. The NCC accesses the communications and relevant documents, such as purchase orders and invoices. The NCC, posing as the Chinese supplier, uses the spoofed supplier's e-mail account to contact the US business with an altered invoice. The fraudulent invoice and accompanying e-mail instructs the US business to pay for the shipment by wire transfer to a new Chinese bank. Unbeknownst to either business, the new bank account was opened and controlled by the NCC.



(U) Step 5

(U) The Chinese supplier ships the goods to the United States. The US business wires payment to the new, NCC controlled bank account, and the NCC removes the funds from the account. The Chinese and US businesses do not realize a fraud has occurred until weeks later, when the US business is unable to claim the goods and/or the Chinese business realizes it had not received the invoice payment.

UNCLASSIFIED

(U) Original Spoofing Still in Use

(U) The original e-mail spoofing technique, distinct from the "man-in-the-e-mail" technique, is less complex and is still being used. Historically, e-mail spoofing involved editing the e-mail header information so the recipient saw the spoofed address, instead of the hacker's actual e-mail address, in the "From" line. Fortunately, this technique can be instantly thwarted if the recipient uses the "Reply" button and notices that the hacker's actual e-mail address is automatically placed in the "To" line. Or, if the hacker also uses the spoofed address in the "Reply to" field, the real user of the real account will get the response and realize a fraud is being attempted.

(U) Incidents in the United States

(U) In most cases, the supplier and/or US small business used free, web-based e-mail accounts. The suspected NCC typically did not use a proxy or virtual private network (VPN)[6] servers, and the spoofed e-mail headers showed Nigeria-based internet protocol (IP) addresses.

- (U) A US business was defrauded out of more than $390,000 in 2012 after it placed an order from its usual suppliers in China. The unidentified NCC failed at a second attempt to commit the same fraud in 2013 for more than $800,000, using the same Hong Kong bank account for both attempts.

- (U) A US business regularly purchased products from its supplier in China when it was defrauded out of more than $270,000 via two different Hong Kong banks.

- (U) A US business bought products from its regular Chinese manufacturer when it was tricked into wiring a payment of more than $150,000 to a fraudster's account in a bank not used by the Chinese business.

- (U) A US-based business was defrauded out of $140,000 by a suspected NCC in 2013. The business negotiated a deal with a Chinese company and paid approximately $20,000 for the initial fees. After the initial fee was paid, a NCC was able to hack into the Chinese companies' account and instruct the US business to make the final payment to an NCC-controlled Hong Kong bank account.

[6] (U) A virtual private network extends a private network across a public network(s), like the Internet, while maintaining functionality and security.

(U) Mitigation to Counter "Man-in-the-e-Mail" Fraud

(U) Mitigation steps for consideration in countering "man-in-the-e-mail" fraud include:

- **(U) Out of Band Communication:** Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
- **(U) Digital Signatures:** Both entities on either side of transactions should use digital signatures. However, this will not work with web-based e-mail accounts. Additionally some countries ban or limit the use of encryption.
- **(U) Avoid Free Web-Based E-mail:** Establish a company web site domain and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- **(U) Forward vs. Reply:** Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct e-mail address or select it from the e-mail address book to ensure the real e-mail address is used.
- **(U) Delete Spam:** Immediately delete unsolicited e-mail (spam) from unknown parties. Do not open spam e-mail, click on links in the e-mail, or open attachments.
- **(U) Significant Changes:** Beware of sudden changes in business practices. For example, if suddenly asked to contact a representative at their personal e-mail address when all previous official correspondence has been on a company e-mail, verify via other channels that you are still communicating with your legitimate business partner.

(U) Reporting the Crime

(U) The FBI encourages victims of "man-in-the-e-mail" fraud schemes to report the crimes as follows:

1. (U) Report the scheme to the Internet Crime Complaint Center (IC3) at www.ic3.gov and record the unique complaint ID number.
2. (U) Report the scheme to your local FBI office http://www.fbi.gov/contact/fo/fo.htm and include the IC3 complaint number. You will also be asked to provide following information:

    - (U) Header information from e-mail messages;
    - (U) Identifiers for the perpetrators, e.g., name, Web site, bank account, e-mail addresses;
    - (U) Details on how, why, and when you believe you were defrauded;
    - (U) Actual and attempted loss amounts;
    - (U) Other relevant information you believe is necessary to support your complaint; and
    - (U) Reference "man-in-the-e-mail" attack. If known, reference any ties to Nigeria, e.g., IP addresses.