Direct Deposit Scam

FBI Denver Cyber Squad advises citizens to be aware of a new phishing campaign. The FBI Denver Cyber Squad advised citizens of a new spear phishing campaign involving personal and business bank accounts, financial institutions, money mules, and jewelry stores. The campaign involves a variant of the "Zeus" malware called "Gameover." The campaign features e-mails claiming to be from the National Automated Clearing House Association (NACHA), and advising the user of a problem with an ACH transaction at their bank that was not processed. Users that click on the link are infected with the Zeus or Gameover malware, which can key log as well as steal online banking credentials, defeating several forms of two-factor authentication. After accounts are compromised, the perpetrators conduct a Distributed Denial of Service (DDoS) attack on the financial institution. The belief is the DDoS is used to deflect attention from the wire transfers as well to prevent a reversal of the transactions (if found). A portion of the wire transfers is being transmitted directly to high-end jewelry stores, wherein the money mule comes to the actual store to pick up his $100,000 in jewels (or whatever dollar amount was wired). An investigation has shown the perpetrators contact the high-end jeweler requesting to purchase precious stones and high-end watches. The perpetrators advise they will wire the money to the jeweler's account and someone will come pick up the merchandise. The next day, a money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as "pending" and releases the merchandise to the mule. Later on, the transaction is reversed or cancelled (if the financial institution caught the fraud in time), and the jeweler is out whatever jewels the money mule was able to obtain. Source: http://www.fbi.gov/denver/press-releases/2011/fbi-denver-cyber-squadadvises-citizens-to-be-aware-of-a-new-phishing-campaign?utm_campaign=email-Immediate&utm_medium=email&utm_source=denver-pressreleases&utm_content=51037

Re: Your Direct Deposit disallowance

noreply@direct.nacha.org

You replied on 11/28/2011 9:45 AM.
This message was sent with Low importance.

Sent: Wed 11/23/2011 8:49 AM
To: [redacted]

Attn: Accounting Department

We are sorry to inform you, that your most recent Direct Deposit via ACH payment (ID846212726012) was cancelled, because your current Direct Deposit software version was out of date. Please use the link below to enter the secure section of our web site and see the details::

http://www.viprowebtech.com/f8c26c/index.html

Please consult with your financial institution to obtain your updated version of the software needed.

Best regards,

ACH Network Rules Department
NACHA | The Electronic Payments Association

13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171
Phone: 703-561-1100 Fax: 703-787-0996