Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 01, 2016

Alert Number
I-060116-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Offices:
www.fbi.gov/contact-us/field

Extortion E-mail Schemes Tied to Recent High-Profile Data Breaches

The Internet Crime Complaint Center (IC3) continues to receive reports from individuals who have received extortion attempts via e-mail related to recent high-profile data thefts. The recipients are told that personal information, such as their name, phone number, address, credit card information, and other personal details, will be released to the recipient's social media contacts, family, and friends if a ransom is not paid. The recipient is instructed to pay in Bitcoin, a virtual currency that provides a high degree of anonymity to the transactions. The recipients are typically given a short deadline. The ransom amount ranges from 2 to 5 bitcoins or approximately $250 to $1,200.

The following are some examples of the extortion e-mails:

"***Unfortunately your data was leaked in a recent corporate hack and I now have your information. I have also used your user profile to find your social media accounts. Using this I can now message all of your friends and family members."***

"If you would like to prevent me from sharing this information with your friends and family members (and perhaps even your employers too) then you need to send the specified bitcoin payment to the following address."

"If you think this amount is too high, consider how expensive a divorce lawyer is. If you are already divorced then I suggest you think about how this information may impact any ongoing court proceedings. If you are no longer in a committed relationship then think about how this information may affect your social standing amongst family and friends."

"We have access to your Facebook page as well. If you would like to prevent me from sharing this dirt with all of your friends, family members, and spouse, then you need to send exactly 5 bitcoins to the following address."

"We have some bad news and good news for you. First, the bad news, we have prepared a letter to be mailed to the following address that details all of your activities including your profile information, your login activity, and credit card transactions. Now for the good news, You can easily stop this letter from being mailed by sending 2 bitcoins to the following address."

Fraudsters quickly use the news release of a high-profile data breach to initiate an extortion campaign. The FBI suspects multiple individuals are involved in these

extortion campaigns based on variations in the extortion emails.

If you believe you have been a victim of this scam, you should reach out to your local FBI field office, and file a complaint with the IC3 at www.ic3.gov. Please include the keyword "Extortion E-mail Scheme" in your complaint, and provide any relevant information in your complaint, including the extortion e-mail with header information and Bitcoin address[1] if available.

TIPS TO PROTECT YOURSELF:

- Do not open e-mail or attachments from unknown individuals.
- Do not communicate with the subject.
- Do not store sensitive or embarrassing photos of yourself online or on your mobile devices.
- Use strong passwords and do not use the same password for multiple websites.
- Ensure security settings for social media accounts are turned on and set at the highest level of protection.
- When providing personally identifiable information, credit card information, or other sensitive information to a website, ensure the transmission is secure by verifying the URL prefix includes https, or the status bar displays a "lock" icon.

The FBI does not condone the payment of extortion demands as the funds will facilitate continued criminal activity, including potential organized crime activity and associated violent crimes.

[1] A Bitcoin payment destination containing 26 to 35 alphanumeric characters beginning with the number 1 or 3.