Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

August 28, 2008

HIT MAN E-MAIL RETURNS

The IC3 continues to receive thousands of reports concerning the hit man e-mail scheme. E-mail content has evolved since late 2006; however, the messages remain similar in nature, claiming the sender has been hired to kill the recipient.

Two new versions of the scheme began appearing in July 2008. One instructed the recipient to contact a telephone number contained in the e-mail and the other claimed the recipient or a "loved one" was going to be kidnapped unless a ransom was paid. Recipients of the kidnapping threat were told to respond via e-mail within 48 hours. The sender was to provide the location of the wire transfer five minutes before the deadline and threatened bodily harm if the ransom was not received within 30 minutes of the time frame given. The recipients' personally identifiable information (PII) was included in the e-mail to promote the appearance that the sender actually knew the recipient and their location.

Perpetrators of Internet crimes often use fictitious names, addresses, telephone numbers, and threats/warnings regarding the failure to comply to further their schemes.

In some instances, the use of names, titles, addresses, and telephone numbers of government officials, business executives and/or victims' PII are used in an attempt to make the fraud appear more authentic.

Below are links for the two previous PSAs published by the IC3 concerning the hit man scheme:

https://www.ic3.gov/media/2007/070109.aspx

https://www.ic3.gov/media/2006/061207.aspx

Consumers always need to be alert to unsolicited e-mails. Do not open unsolicited e-mails or click on any embedded links, as they may contain viruses or malware. Providing your PII will compromise your identity!

Individuals who receive e-mails containing threats of violence and their PII are encouraged to contact law enforcement as well as file a complaint at www.IC3.gov.