Intelligence Note

Prepared by the

Internet Crime Complaint Center (IC3)

Middle East Cyber Intelligence Unit (MECIU)

April 18, 2013

BEWARE OF POSSIBLE FRAUD ASSOCIATED WITH THE BOSTON MARATHON EXPLOSIONS

On 04/15/2013, two explosions occurred near the finish line of the Boston Marathon causing death and injury to spectators, as well as participants of the marathon. While Americans feel the need to assist or contribute to those affected by this tragedy; criminals see it as way to exploit contributor's kindness. History has shown criminals utilize disasters to take advantage of those wanting to assist.

Individuals need to be aware of emerging fraud online associated with the explosions and how to take necessary precautions when using e-mail and social networking Web sites. As of 17 April 2013, the FBI has received indications that individuals may be using social media and e-mail to facilitate fraudulent activities online.

There have been reports of a Spam E-mail being circulated to lure potential victims to malware and exploits. The subject of the spam e-mail in one version is "Boston Marathon Explosion". The e-mail contains links that could infect your computer. Clicking on the link opens up a compromised Web page that shows a series of videos of the attack site. There is an unloaded video at the bottom of the Web page that leads to the Red Exploit Kit, which exploits various vulnerabilities on the user's computer. Once an exploit has been successful, the user sees a popup asking them to download a file at which time malware is downloaded.

Social Media is another avenue criminals use to solicit donations. According to various reports, a Twitter account was created soon after the explosions that resembled a legitimate Boston Marathon account. Allegedly, for every tweet received to the account a dollar would be donated to the Boston Marathon victims. Though the account was suspended by Twitter, it is likely others may use this same method to commit fraud. The FBI was made aware of at least 125 questionable domains registered within hours of the Boston Marathon Explosions. Though the intentions of the registrants are unknown, domains have emerged following other disasters for fraudulent purposes.

Individuals should be vigilant when using email and social networking Web sites following the Boston Marathon explosions. Based on previous disasters, cyber criminals may use this event as a means to further illegal activity to gain personally identifiable information (PII).

Individuals can limit exposure to cyber criminals by taking the following preventative actions when using email and social networking Web sites.

- Messages may contain pictures, videos, and other attachments designed to infect your computer with malware. Do not agree to download software to view content.
- Links appearing as legitimate sites (example: fbi.gov), could be hyperlinked to direct victims to another Web site when clicked. These sites may be designed to infect your computer with malware or solicit personal information. Do not follow a link to a Web site; go directly to the Web site by entering the legitimate site's URL.

Individuals can also limit exposure to cyber criminals by taking the following preventative actions when receiving solicitations from, or donating to, charitable organizations online.

- Verify the existence and legitimacy of organizations by conducting research and visiting official Web sites. Be skeptical of charity names similar to but not exactly

the same as reputable charities.

- Do not allow others to make the donation on your behalf. Donation-themed messages may also contain links to Web sites designed to solicit personal information, which is routed to a cyber criminal.
- Make donations securely by using debit/credit card or write a check made out to the specific charity. Be skeptical of making donations via money transfer services as legitimate charities do not normally solicit donations using this method of payment.

If you believe you have been the victim of fraud by someone soliciting funds on behalf of disaster victims or want to report suspicious e-mail solicitations or fraudulent Web sites please file a complaint with the FBI's Internet Crime Complaint Center at http://www.ic3.gov/