Cyber Advisory

Boston Marathon Bombing Used to Disseminate Malware and Conduct Fraud

April 18, 2013

(U//FOUO) New Jersey Regional Operations Intelligence Center (NJ ROIC) Intelligence & Analysis Threat Unit ~ IAU201304-722[1]

Summary

(U//FOUO) Websites and emails referencing the Boston Marathon bombing should be viewed with caution, as malicious actors are using the incident to disseminate malware and conduct fraud. While other agencies investigate the frauds, the NJ ROIC provides this information for situational awareness.

Tactics, Techniques & Procedures

(U//FOUO) Cyber security experts have identified multiple fake websites and charity efforts taking advantage of the Boston Marathon bombing. Based on previous incidents, more scams will follow.

- Within the hours of the bombings, actors with unknown intentions registered more than 125 domain names using a combination of “Boston,” “Marathon,” “2013,” “bomb,” “explosions,” “attack,” “victims,” and “donate” and should be viewed with caution. More domains are likely to follow.
- Malicious actors are using social networking sites to spread hoaxes, including information regarding the purported death of several child runners (children are not allowed to participate in the Boston Marathon), and injured runners purportedly running for a variety of charities and causes.
- Phishing emails may provide links to malicious websites purporting to contain information, pictures, and video, or may contain attachments with embedded malware. Clicking on the links or opening the attachments can infect the victim’s computer to further malicious activity.
- Multiple fake charities were created on social networking websites within minutes of the explosions, purporting to collect funds for victims. Traditionally, these websites are scams.

(U//FOUO) In addition, numerous spam emails referencing the bombing have been distributed. Some of the subject lines include:

- “2 Explosions at Boston Marathon”
- "BREAKING - Boston Marathon Explosion"
- 2 Explosions at Boston Marathon
- Boston Explosion Caught on Video
- Explosion at the Boston Marathon
- Opinion: Boston Marathon Explosions made by radical Gays? Really? - CNN.com
- Opinion: FBI knew about bombs 3 days before Boston Marathon - Why and Who Benefits? - CNN.com
- “Aftermath to explosion at Boston Marathon”
- "Video of Explosion at the Boston Marathon 2013"
- Aftermath to explosion at Boston Marathon
- BREAKING - Boston Marathon Explosion
- Explosions at Boston Marathon
- Opinion: Boston Marathon Explosions - Romney Benefits? - CNN.com
- Opinion: Osama Bin Laden video about Boston Marathon Explosions - bad news for all the world. - CNN.com
- “Boston Explosion Caught on Video"
- "Runner captures. Marathon Explosion"
- Arbitron. Dial Global. Boston Bombings
- Explosion at Boston Marathon
- Explosions at the Boston Marathon
- Opinion: Boston Marathon Worse Sensation - Osama bin Laden still alive!? - CNN.com

[1] The NJ ROIC produced this advisory in conjunction with the Center for Internet Security (CISecurity.org).

Recommendations

Internet users should conduct due diligence before clicking links, visiting sites, or making donations.

- Be cautious of emails/websites that claim to provide information because they may contain viruses.
- Do not open unsolicited emails, or click on the links/attachments contained in those messages.
- Never reveal personal or financial information in email.
- Do not go to unfamiliar websites to view the event or information regarding it.
- Never send sensitive information over the Internet before checking a site's security and confirming its legitimacy. Malicious websites often look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- Search email systems for the subject lines noted above and delete them from inboxes.

Suspicious Activity Reporting

(U//FOUO) Suspicious activity should be reported immediately, per existing protocols. Activity can also be reported 24 hours a day to the NJ ROIC Counter Terrorism Watch at (866) 4-SAFE-NJ (866-472-3365) or tips@njhomelandsecurity.gov.

Contact Information

(U//FOUO) Any agency with further information regarding this tactic should contact the NJ ROIC at (609) 963-6900, option 1, or roic@gw.njsp.org. Questions about this product should be directed to the NJ ROIC at (609) 963-6900, ext. 6253, or njroicanalysis@gw.njsp.org.