Cyber Intel Advisory:
Malicious Actors Using Syrian Crisis as Basis for Spam Campaigns

11 September 2013

Integrated Intelligence Center
Multi-State Information Sharing and Analysis Center
William F. Pelgrin, President and CEO

The Risk: It is likely that the Syrian crisis will become a source of malicious spam over the next several days, in light of the recent attention focused on the Syrian crisis, including media interviews with US President Barack Obama$^{\text{US and}}$ Syrian President Bashar al-Assad. The Center for Internet Security (CIS) recommends that users exhibit caution when responding to requests for donations or viewing unsolicited emails or websites purporting to contain information regarding the Syrian crisis. Malicious spam taking advantage of a major new event is a common occurrence.

The Threats: Cyber security experts from Symantec$^{\text{US Business}}$ and others have already identified spam taking advantage of the escalating crisis in Syria.

- Malicious actors are sending phishing emails containing malware. One email links to a falsified CNN$^{\text{US business}}$ article with the title "The United States Began Bombing!" If a user clicks on the link, the Blackhole exploit kit will be executed. The Blackhole exploit kit is used to discover vulnerabilities on a system and deliver malware. Another email containing an attachment referencing the chemical attack in Syria exploits a publicized vulnerability to install a backdoor. Clicking links or opening attachments can infect a victim's computer, furthering other malicious activity such as keystroke logging.
- Malicious actors are sending spam emails calling for donations to the Red Cross and Red Crescent organizations. The emails link to the British Red Cross site, but request that donations above a certain value be sent via money transfer to an email address impersonating the British Red Cross.

The Action: Internet users need to apply a critical eye and conduct due diligence before clicking links and visiting websites. Users should employ good cyber practices when accessing information about news events, including news associated with the US reaction to the Syrian crisis, such as:

- Users and organizations should automatically update systems and applications with patches. Malware frequently exploits vulnerabilities for which a software patch was released.
- Users and organizations employ anti-virus/anti-malware software and implement a system for scanning and blocking all email attachments that contain malicious code. Popular malware, like the Blackhole exploit kit, are identified by many anti-malware programs' signatures.
- Users should understand basic cyber security awareness procedures. Organizations should perform regular exercises to test employees' response to targeted malicious emails employing social engineering. Spam often exploits victim's emotions via social engineering to generate a response.
- Never send sensitive information or conduct financial transactions over the Internet before confirming the identity of the recipient. Always conduct transactions through a trusted site and be wary of requests for transactions to be conducted through a third party or outside of the standard procedure.

The information provided above is intended to increase the security awareness of an organization's users and to encourage more secure behavior. Organizations have permission and are encouraged to brand and redistribute this advisory in whole for educational, non-commercial purposes. For more information regarding cyber threats please visit the Center for Internet Security website at CISecurity.org.