NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0015-NCCIC –120020110826

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

(U) PHYSICAL EVENTS (NATURAL AND/OR MAN-MADE) PROVIDE MALICIOUS USERS WITH TOPICS FOR SOCIAL ENGINEERING CAMPAIGNS

EXECUTIVE SUMMARY

(U) Malicious users seeking to exploit interest related to physical events such as earthquakes and hurricanes will likely use subject lines and attachment titles related to the incidents in phishing[1] e-mails. Network administrators and general users should be aware of these attempts and avoid opening messages with attachments and/or subject lines related to physical events.

BACKGROUND

(U) This NCCIC Bulletin is being provided for your situational awareness because of the malicious cyber activity that is commonly associated and that follows highly publicized physical events such as hurricanes and earthquakes. Recent examples of topics that may be used in these e-mails include but are not limited to the 23 August 2011 earthquake in Virginia, and the impending landfall of Hurricane Irene in the southeast US.

(U) Both government agencies and private organizations could possibly become recipients of malicious activity, most commonly in the form of socially engineered spear-phishing emails. These emails may appear to originate from a reputable source, with the email subject closely aligned to the event and usually of interest to the recipient. The email in most cases will contain a malicious attachment with a subject name relevant to the event alluring the recipient to open. The attachment when opened will launch malware into the users system in most cases in the form of a key logger or remote access tools.

DHS/NCCIC ACTIONS

(U) The NCCIC will continue to monitor reporting from multiple public and private sources, and generate additional products if new information becomes available.

[1] Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques.

(U) DHS/US-CERT is collecting phishing email messages and web site locations so that we can help people avoid becoming victims of phishing scams. You can report phishing to US-CERT by sending email to phishing-report@us-cert.gov.

POINTS OF CONTACT

(U) Please direct all questions to the NCCIC Duty Officer (NDO). NCCIC will continue to coordinate with the appropriate component organizations listed below:

NCCIC Duty Officer	**US-CERT**	**NCS/NCC**	**ICS-CERT**
NCCIC@HQ.dhs.gov	SOC@US-CERT.gov	NCS@HQ.dhs.gov	ICS-CERT-SOC@dhs.gov
(703) 235-8831	(888) 282-0870	(703) 235-5080	(877) 776-7585