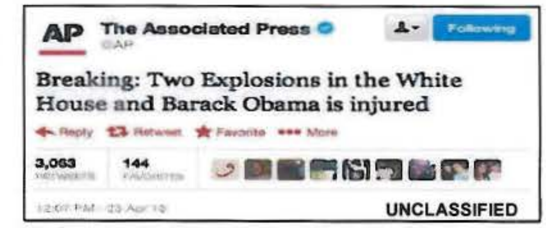
ROLL CALL RELEASE

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

30 August 2013

(U) Compromises of Official Social Media Accounts Spread Disinformation

(U//FOUO) Malicious cyber actors have used compromised social media accounts to spread disinformation about alleged emergencies and attacks, most prominently through Twitter^{USPER}. Because it is difficult to determine the authenticity of a tweet, we anticipate malicious cyber actors will continue to seek to exploit Twitter and other social media platforms used by news organizations and public safety agencies to propagate disinformation.



The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

3,063 RETWEETS
144 FAVORITES

12:07 PM - 23 Apr 13

UNCLASSIFIED

(U) Screenshot of SEA's 23 April AP Twitter disinformation post.

- (U) Syrian Electronic Army (SEA) cyber actors on 23 April 2013 claimed that they had posted disinformation on the Associated Press^{USPER} (AP) Twitter account indicating that two explosions had occurred at the White House and that President Obama had been injured. Within minutes of the posting, the Dow Jones Industrial Average dropped 145 points (nearly 1 percent), but it quickly recovered after the AP removed the false posting.

- (U) A group calling itself the "Script Kiddies" on 4 July 2011 claimed responsibility for hacking a Fox News^{USPER} Twitter account and posting six tweets indicating that the President of the United States had been fatally shot. An administrator deleted the false postings 10 hours later. The false postings, however, attracted considerable attention.

(U) First responders are encouraged to secure and monitor all official social media accounts and verify reports of events posted to social media to ensure that they are legitimate. The below security practices are intended to prevent compromises of social media accounts.

(U) Recommended Practices for Securing and Monitoring Social Media Accounts

(U) Security Principle	(U) Recommended Practice
(U) Prevent account compromises	(U) Use two-factor authentication for logins to social media accounts.
	(U) Change passwords regularly for e-mail and social media accounts.
	(U) Use complex, 12-character passwords that include numbers, letters, and symbols.
	(U) Monitor organization's social media account activity for non-authorized access.
(U) Maintain situational awareness	(U) Monitor organization's social media pages for malicious posts and quickly delete misinformation.
	(U) Verify claimed emergencies with additional, non-social media sources.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0198-13

(U) Prepared by the Office of Intelligence and Analysis, Cyber Intelligence Analysis Division and the National Protection and Programs Directorate, US Computer Emergency Readiness Team and the Federal Bureau of Investigation, Directorate of Intelligence. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label ^{USPER} and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at IA.PM@hq.dhs.gov, IA.PM@dhs.sgov.gov, or IA.PM@dhs.ic.gov.

*(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.*

[redacted]