

FBI



FLASH

FBI LIAISON ALERT SYSTEM

#E-000037-PH

(U) The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

SUMMARY

(U) The FBI is providing the following information with HIGH confidence. Through FBI investigation we have reason to believe members of the US Senate, State Senates, and other elected legislative officials may have been or will be targeted, in the near term, by a spear phish campaign. FBI has observed unattributed cyber actors, suspected to be state sponsored, performing research on members of the US Senate as well as members of the State Senates. This activity is typically a precursor to a spear phish attack.

TECHNICAL DETAILS

(U) Through the course of our investigation, there are indications Senate members may be targeted by an advanced threat. These actors perform spear phishing campaigns against professional and personal email accounts. For professional accounts, spear phishing emails typically containing attachments such as Word, Excel, or PDF files. Links are sometimes used which direct the user to malicious domains which compromise their computer. For personal email accounts, such as Yahoo or Gmail, the actors send a spear phishing email purporting themselves to be the Email Provider, asking for a password reset. If the user clicks the button to reset the password, a malicious webpage is displayed which looks very similar to the legitimate password reset page. The user would provide their email account, current password, and a new password which when submitted, gets emailed to an operational email account. Users often use the same password for multiple accounts. If the actors obtain a personal email account password which is the same as the official Senate account, they would potentially have access to both accounts. These actors are known to target the social media accounts as well such as Facebook, Twitter, and LinkedIn. FBI has reason to believe, as of 13 August 2014, some of the spear phish emails to State Senators have already been sent. Victims will be notified as soon as their identities are ascertained. No further information is available at this time however; as soon as additional information is available this FLASH will be updated.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or
FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937