Issued 2/9/17

Macro Malware Comes to MacOS

Macro-based malware has crossed the divide between the Windows and Mac platforms. Following the same script as similar Windows-based attacks, the attached documents have a luring subject line, in this case: “U.S. Allies and Rivals Digest Trump’s Victory – Carnegie Endowment for International Peace.docm.” Once a user tries to open the attachment, they’re presented with a familiar dialogue box instructing them that macros must be enabled to view the document. If the macro is enabled, it executes its payload which then tries to download more code from the attacker’s site.

Never open an attached document with verifying from the sender it is legit!