Cyber Alert: Massive Locky Ransomware and Trickbot E-mail Campaign Exploiting Microsoft DDE

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) has detected a recent and dramatic increase in unsolicited e-mails attempting to deliver either the “Asasin" version of the Locky ransomware variant or the Trickbot banking trojan to state government e-mail addresses. Further analysis revealed that this is linked to a global ransomware campaign that appears to be using the Necurs botnet to distribute the malicious emails. These emails originate from various random domains and the subject line contains the words “Your Invoice” followed by a string of five or six digits. Attached to the e-mail is a Microsoft Word document named “Invoice_file_[random digits]. doc.” This document attempts to abuse Microsoft’s Dynamic Data Exchange (DDE) feature and downloads either Locky or Trickbot if the recipient opens the attachment and clicks “Yes” on the associated prompt.

Examples are provided below: