Malicious Email Delivering Emotet

Date: December 4, 2019

Summary:

On November 15th, an email supposedly coming from a GE.com email address was observed delivering a malicious Microsoft Word document as a first stage for the Emotet malware. This was not caught by the security perimeter but was not detonated by any users.

Background:

The GE Gas Power Cybersecurity team has verified that the email was not sent from a compromised email account within GE, and was sent by an outside address spoofing a GE email address. Further, we have observed 9 emails blocked by Proofpoint containing the same malicious attachment also sent in mid-November. There is no evidence of the Emotet variant delivered by these attachments being installed on any GE machines.

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.