(U) LOCKY Ransomware resurfaces with new tactics

(U/FOUO) The latest release of the LOCKY malware uses a delayed trigger making it more dangerous than ever and even more difficult for security professionals. This new version of ransomware uses a malicious Microsoft Word document that carries payload instructions to only download and run LOCKY, then triggers when the user closes the document. This payload methodology circumvents "sandbox" detection methods and makes it very difficult to detect using traditional malware prevention methods.

(U) LOCKY is notorious for its effectiveness and profitability. Over the past two years, LOCKY has been used to extort more than $7.8 million in payments from victims, according to a recent study by Google, Chainalysis, UC San Diego, and the NYU Tandon School of Engineering.

(U) The first release of the LOCKY ransomware operated on the premise of an unreadable attachment. As the reader tries to open the attachment, they receive a message that the “file is unreadable”, and the user will have to “Enable Macros”. Once macros are enabled, the binary files ran the downloaded encrypted Trojan.

(U) The release of the second variant utilizes a botnet of zombie computers coordinated to launch phishing attacks appearing to come from a targeted recipient’s trusted business-class multifunction printer. This campaign created an email using a popular printer model in the subject line to trick users into thinking the messages were legitimate. One such message read, “Scanned image from MX-2600N”. MX-2600N is the model of a leading enterprise-class Sharp multifunction printer.

(U) The latest LOCKY variant no longer requires any type of user action, other than to open and close the message in order to trigger the payload, underscoring the sophistication of the latest release.

(U) More than 54,048 IP addresses were used in the “scanned image” campaign – 27 percent of those were also used in the original attack that began on August 9, according to an analysis of the botnet used in the attacks. The top source countries behind the “zombie computer” botnet are Vietnam, Turkey, India and Mexico. Targeted countries included European and Southern Asia-based countries with minimal targeting of the United States and Russia.

(U/FOUO) The Cal-CSIC strongly recommends organizations implement an awareness campaign to ensure users are aware of these new variations of the LOCKY ransomware.

(U/FOUO) Information security professionals should notify the Cal-CSIC immediately at CalCSIC@CalOES.CA.Gov or (833)REPORT1 for further information.