Issued 11/10/17

Locky Ransomware Used to Target Hospitals

Hospitals rely on electronic records to look after their patients properly and schedule everything from appointments to operations, and faced with a long backup process and catastrophic disruption, the hospital gave in and paid $17,000 in Bitcoin for a decryption key. Accord ing to new research released by Cylance, a relatively new Locky variant, dubbed Diablo6, includes a few tweaks which are making detection of the ransomware more difficult for traditional antivirus solutions as well as end users. In a blog post, the team sa id Diablo6 performs an attack in two stages.

The first is a typical attack vector for ransomware -- a spear phishing email which contains a .zip archive, but something new for the Locky variant. While masquerading as a legitimate email and attachment, the file actually contains a VBS file which, when decompressed and opened, attempts to connect to Locky's command - and - control (C&C) server for instructions. If the connection is a success, the VBS script then downloads the ransomware. However, should this stag e fail, there is a backup C&C server which the script will attempt to download its payload from. At the same time, the VBS script uses a string to split and load the real instructions. The payload is then downloaded and stored in a temporary folder before executing and encrypting files.

The Locky Diablo6 ransomware targets all kinds of files in its encryption quest, including images, videos, backups, and zipped files. Once encryption is complete, a ransom note is issued on the home screen and then the encry ption script deletes itself. Domains connected to a mail.com email address have been connected to Locky, and in total, 333 domains were registered in 2016 and as recently as October this year.

The researchers are using the registrant to keep an eye e domains, which have been linked to serving other kinds of ransomware. "In some cases, authors can make small changes in their code to keep their malware as dangerous to the end user as it was the day they released it," Cylance says. "This appears to be t he case the case with the Locky ransomware. This old malware didn't need to have anything new, the authors behind Locky just had to tweak the only part of the process that can never be fixed -- the end user." This month, ProofPoint researcher Matthew Mesa also uncovered a new strain of ransomware. Dubbed GIBON, the new strain uses macros embedded in malicious documents spread through phishing campaigns to lock PCs. However, as the ransomware is so new, little is known about its demands, target demographics, or origin.