MBU TIMES

VOLUME
12
ISSUE
3
March
2017

MONTHLY NEWSLETTER OF
MEDICAL BILLING UNLIMTED, INC

Backup Your Data

A report by McAfee Labs published in December revealed that the number of new ransomware samples totaled 3,860,603 in the third quarter, which is an 80% increase from the beginning of the year. With a huge jump in the number of ransomware attacks coupled with significant technical advances in this area, the company predicted that “2016 may be remembered as ‘the year of ransomware’. These malicious software programs encrypt files on an infected computer and then require payment from the victim to recover them, often in bitcoin (one bitcoin = $1,250.00). Even if you are attacked and decide to pay the ransom, the FBI warned in September that there is no guarantee you will regain access to your files. The agency revealed:

Get Educated and Trust No One!!

The best practice is to employ preventative measures to defend your network from getting infected with ransomware. The first line of defense is education. Users can educate themselves to “scrutinize links contained in e-mails and do not open attachments included in unsolicited e-mails,” the FBI recommended. In addition, software should only be downloaded from trusted sites. “When possible, verify the integrity of the software through a digital signature prior to execution,” the agency noted. “Trust no one. Literally,” advised an initiative of the National High Tech Crime Unit of the Netherlands’ police, Europol’s European Cybercrime Centre, Kaspersky Lab and Intel Security called “No More Ransom!” The project’s website warned that:

Various tricks and tools exist to help users spot malicious files such as enabling the ‘Show file extensions’ option in the Windows settings on your computer. “Stay away from file extensions like ‘.exe’, ‘.vbs’ and ‘.scr’,” No More Ransom! wrote. “Scammers can use several extensions to disguise a malicious file as a video, photo, or document (like hot-chics.avi.exe or doc.scr).”

Off-site Backups

The last line of defense from ransomware attacks is backups which can be software based, hardware based, or both. Knowbe4.com suggested that in addition to regularly backing up files, the restore procedure should also be routinely tested. “Test the data integrity of physical backups and ease-of-recovery for online/software based backups,” Knowbe4 advised. Once your data is backed up, make sure it is not easily accessible by other computers such as keeping it off-site. If your backups are easily accessible by a computer infected with ransomware, they too could be encrypted.

No More Ransom! recommended “It’s best to create two back-up copies,” suggesting storing one in the cloud and one physically such as portable hard drive, thumb drive, or extra laptop. However, the FBI noted that “some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization.”

While preventative measures can help a long way towards avoiding ransomware infections, it is not a complete safeguard. Not More Ransom! Noted that:

If you discover a rogue or unknown process on your machine, disconnect it immediately from the internet or other network connections (such as home Wi-Fi) — this will prevent the infection from spreading.

1. bitcoin.com