BALOUGH LAW OFFICES, LLC

McAfee Sees Dramatic Increase In Ransomware Attacks

Ransomware attacks spiked in 2015’s first quarter as new “families” of the malware have appeared. The new ransomwares have more evasive techniques to avoid detection and now also are targeting mobile platforms, McAfee Labs reports in its latest Threats Report.

Ransomware programs are malicious software that encrypts data on a computer and prevent the owner from accessing the data until a ransom payment is made using Bitcoins and a key to unlock the files is sent. Ransomware campaigns target victims in relatively rich countries because of their perceived ability to pay.

McAfee has seen a 165 percent rise in ransomware in the first quarter of 2015. The attacks targeted desktop and laptop computers, Android mobile devices, mass storage devices, and servers.

Ransomware is spread when users open email attachments. “The phishing email topics that lead to infestation by ransomware are very specific. The email template and attachment names appear not only in the local language but also pretend to be coming from real companies in the targeted countries,” McAfee said.

The most successful ransomware is known as CTB-Locker, which “uses clever, evasive techniques to get around security software. Second, the phishing emails used in CTB-Locker campaigns are more ‘believable’ that in other ransomware campaigns. For example, the malware uses local businesses and location-relevant filenames.”

“CTB-Locker is distributed in many ways, including Internet Relay Chat, peer-to-peer networks, newsgroup postings, email spam, and more,” McAfee warned.

The security software provider said the most frequently asked question about ransomware is “‘Can we recover the encrypted data?’ The answer is generally ‘No’—unless you pay the ransom and the thieves provide the private key.”

To avoid being a victim of ransomware, the Threats Report recommends:

- Back up data. “Although this seems obvious, far too often there is no backup available or the backup process was never tested and didn’t work. Removable storage is widely available, inexpensive, and simple to use. Home users should create a backup, disconnect the device, and store it in a safe place.”
- Perform user-awareness education. “Because most ransomware attacks begin with phishing emails, user awareness is critically important and necessary. For every ten emails sent by attackers, statistics have shown that at least one will be successful. Don’t open emails or attachments from unverified or unknown senders.”
- Keep system patches up to date. “Many vulnerabilities commonly abused by ransomware can be patched.”
- Employ antispam. “Most ransomware campaigns start with a phishing email that contains a link or a certain type of attachment.”

Balough Law Offices, LLC, is a Chicago-based law firm which focuses on cyberspace, business, and intellectual property law. Our homepage is balough.com.