e-Newsletter

April 2016

Ransomware 'Locky' Update

We share information internally at Agility. It's a perk to being on a team. A common theme around the water cooler is the ransomware virus 'Locky'. Agility Consultants have shared their brushes with 'Locky' and we've put together a few updates on the virus and simple ways to avoid this one.

What is 'Locky'?

Locky is ransomware distributed via malicious .doc files attached to spam email messages. Each word document contains scrambled text, which appear to be macros. When users enables macro settings in the Word program, an executable file (the ransomware) is downloaded. Various files are then encrypted.

What does 'Locky' do?

Locky scrambles any files in any directory on any mounted drive that it can access, including removable drives that are plugged in at the time, or network shares that are accessible, including servers and other people's computers, whether they are running Windows, OS X or Linux.

What you can do to avoid Locky -

- Backup regularly and keep a recent backup copy off-site. There are dozens of ways other than ransomware that files can suddenly vanish, such as fire, flood, theft, a dropped laptop or even an accidental delete. Encrypt your backup and you won't have to worry about the backup device falling into the wrong hands.
- Don't enable macros in document attachments received via email. Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of malware infections rely on persuading you to turn macros back on, so don't do it!
- Be cautious about unsolicited attachments. The crooks are relying on the dilemma that you shouldn't open a document until you are sure it's one you want, but you can't tell if it's one you want until you open it. If in doubt, leave it out.
- Don't give yourself more login power than you need. Most importantly, don't stay logged in as an administrator any longer than is strictly necessary, and avoid browsing, opening documents or other "regular work" activities while you have administrator rights. If you are logged in as a domain administrator and you get hit by ransomware, you could do very widespread damage indeed.
- Consider installing the Microsoft Office viewers. These viewer applications let you see what documents look like without opening them in Word or Excel itself. In particular, the viewer software doesn't support macros at all, so you can't enable macros by mistake!

- Patch early, patch often. Malware that doesn't come in via document macros often relies on security bugs in popular applications, including Office, your browser, Flash and more. The sooner you patch, the fewer open holes remain for the crooks to exploit.

References

Here is an abbreviated list of articles that further explain the Locky virus;

"Locky" ransomware – what you need to know – Naked Security

Virus Bulletin :: Locky Strike: Smoking the Locky Ransomware Code

"Locky" crypto-ransomware rides in on malicious Word document macro

---