WBM Technology Services Community Briefing

MAY 13, 2016 End User Alert

RANSOMWARE ATTACKS

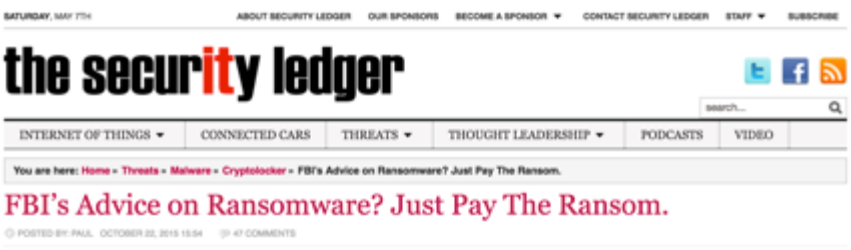
WBM has now met numerous organizations in recent weeks who have been victims of ransomware attacks across western Canada and have required assistance to bring their businesses back and be protected moving forward. We have also seen an extreme rise in ransomware attempts across our customer community, and this is consistent with the explosive growth in attacks throughout North America as ransomware is now clearly the single fastest growing security threat to business.

Attacks in recent days have forced high profile state of emergency at Hollywood Presbyterian Hospital, downed a Michigan Electricity provider, and the new forms of the virus are so sophisticated that some FBI officials have advised infected businesses to **"just pay the ransom,"** despite there being no guarantee that the data will be decrypted, and payments only incenting growth in this crime.

Michigan electricity utility downed by ransomware attack
The Register - May 4, 2016
A water and electricity authority in the US State of Michigan has needed a week to recover from a **ransomware attack** that fortunately only hit its ...

Electric company hit by ransomware
Komando - May 3, 2016

Explore in depth (7 more articles)



what is ransomware?

Ransomware locks down files and freezes your ability to operate by planting infection, usually in the form of emailed word, pdf, or zip attachments, but more and more often taking on much more difficult to detect exploit kits.

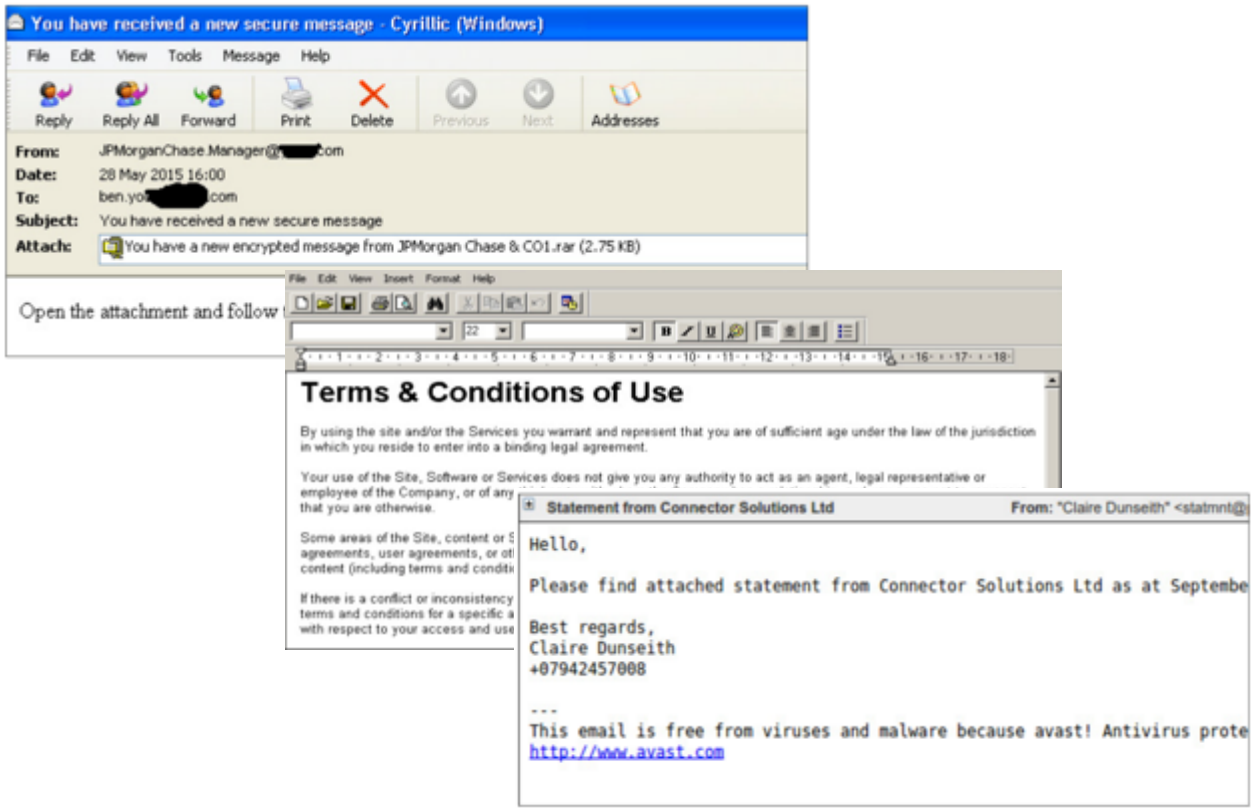
Once infected, your files will be locked, and screens will direct you to pay a ransom, usually in Bitcoin. The ransom will often increase as more time passes.

Ransomware first appeared in 2013 as the infamous Crypto-locker. The ransomware infections we are now seeing are much more sophisticated and must be protected against rather than fixed after the fact.

It is of critical business importance that end users exercise caution with regard to opening unknown attachments (in particular any files with a .exe extension), accepting suspicious terms of use while browsing the internet, or inserting usb or external devices from unknown origin.

In the event of an infection alert, your WBM Managed Services team may disable your device in an attempt to prevent spread throughout the network.

RECENT SCREEN SHOTS OF ATTACK FORMS (CRYPTOWALL, TESLACRYPT, CTB LOCKER)



Your organization does have protection measures in place, but they can never provide 100% assurance of safety. Excising caution is a best practice that applies to both your work, and your home computing experience.

If you have any questions, please feel free to contact your administrator or WBM directly, either online at www.wbm.ca, by phone at 1.888.ASK4WBM, or by speaking with your WBM Account Manager.