MORETON & COMPANY

CLIENT | ALERT

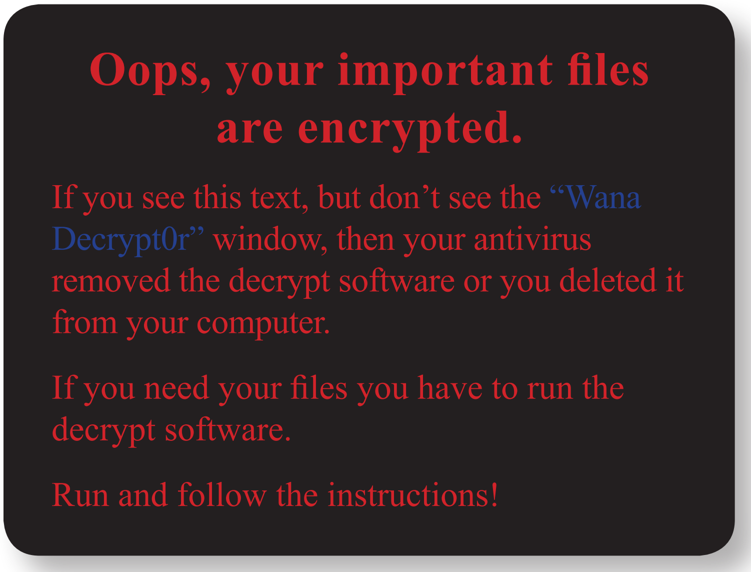
May 15, 2017

WannaCry Ransomware Attack

Ransomware attacks made headlines in 2016, and did so again over the weekend as the trend continues into 2017. WannaCry (WanaCrypt0r.20) has effected an estimated 200,000+ devices in over 150 countries as of May 15, 2017. That numbers is expected to increase as the work week begins, and the virus seems to have hit Asian and European businesses the hardest. Similar to attacks in 2016, healthcare was targeted and prevented hospitals from providing care to patients.

Ransomware is a special type of virus that encrypts your data and makes it unusable unless the attacker is paid a ransom. There is usually a screen that appears providing payment information and a warning that your data is inaccessible until they are paid.

Over the last several days, many businesses and employees were stunned to see the following message (or something similar) on their work screens:



Oops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Run and follow the instructions!

The United States Computer Emergency Readiness Team (US-CERT) provided the following as it relates to the WannaCry ransomware threat. Users should:

- Be careful when clicking directly on links in emails, even if the sender appears to be known; attempt to verify web addresses independently (e.g., contact your organization's helpdesk or search the Internet for the main website of the organization or topic mentioned in the email).
- Exercise caution when opening email attachments. Be particularly wary of compressed or ZIP file attachments.
- Follow best practices for Server Message Block (SMB) and update to the latest version immediately. (See US-CERT's SMBv1 Current Activity for more information)

Additional details and best practices can be found at:
https://www.us-cert.gov/security-publications/Ransomware

In addition to the above best practices, a cyber liability insurance policy can be a critical component in protecting your business and data. Each cyber policy varies in coverage but may extend to a ransomware attack or other cyber extortion claim. We at Moreton & Company have experienced these types of claims and know how to respond and react in the event of a ransomware attack. Ransomware demands may be low, but it is critical to have a plan before a security incident occurs, along with experts at your side to respond to such an event. A cyber liability insurance policy along with a trusted insurance brokerage partner may be your best line of defense.

Please contact your Moreton & Company representative for further details.

Please visit http://www.moreton.com/news-events/ for more information and to view other client alerts. This Client Alert was written by Charles Kikumoto of Moreton & Company. For additional questions, please contact your Moreton & Company representative.

This Client Alert is intended to alert recipients to recent legal developments. It does not constitute the rendering of legal advice or recommendations and is provided for your general information only. If you need legal advice upon which you can rely, you must seek an opinion from your attorney.