NEWS BRIEF

U.S. Aftermath of WannaCry Ransomware Yet to be Seen

The WannaCry ransomware that has spread across 150 countries since Friday has appeared to slow down, but employees starting the workweek should be careful, as the effects in the United States are yet to be determined.

WannaCry locks users out of their computers by exploiting a vulnerability in outdated versions of Microsoft Windows. It then demands money from users who want to regain control of their data. The ransomware initially requests around $300, and if no payment is made, threatens to double the amount after three days and delete files within seven days. Once it infects one computer, it can spread to every computer in that network within seconds.

According to Elliptic—a London startup that helps law enforcement agencies track criminals—around $50,000 worth of bitcoin payments have been made to the hackers as of Monday morning.

Countries Affected in First Few Hours of Cyber Attack

- United States – FedEx
- United Kingdom – The National Health Service
- Russia – The Ministry of Internal Affairs
- France – Renault
- Spain – Telefonica
- China – Universities and gas stations
- Japan – Hitachi

Nobody knows who is behind the attack, but Europol is working on a decrypting tool. Many firms hired experts over the weekend to prevent new infections, which seems to have worked in Europe, so far.

After the initial discovery of the WannaCry ransomware, Microsoft issued a warning to the U.S. government concerning its data-storing practices. Microsoft claimed that the tool used in the WannaCry cyber attack was developed by the U.S. National Security Agency and was stolen by hackers. Microsoft released a Windows security update in March to tackle the problem exposed by the latest attack, but many users haven't run the update yet.

Precautions

Some experts recommend that you should not pay the ransomware if you've been hacked. Even if there is a way to determine if you've paid the ransom, there is no guarantee that the hackers will return the files to you unharmed, if returned at all. Experts also recommend you take the following precautions:

- Update your network if you haven't yet.
- Turn on auto-updaters, if available.
- Don't click on links that you don't recognize.
- Don't download files from people you don't know.
- Back up your documents regularly.

Huckaby & Associates will continue to monitor the situation. Contact us if you have any further questions regarding how you can avoid disruptive business interruptions from cyber attacks.

HUCKABY & ASSOCIATES
H&A
1976
EST
INSURANCE

The content of this News Brief is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and should not be relied upon as such. © 2017 Zywave, Inc. All rights reserved.