Cybersecurity Tip of The Week- 10/30/17

The U.S. government has issued a warning about a new ransomware attack that spread through Russia and Ukraine and into other countries around the world.

Cybersecurity experts said the ransomware, which posed as an Adobe update before locking down computers and demanding money for people to get their files back, targeted Russian media companies and Ukrainian transportation systems. It has also been detected in other countries including the U.S., Germany and Japan.   The U.S. Computer Emergency Readiness Team said late last Tuesday it "has received multiple reports of ransomware infections ... in many countries around the world."

Dubbed "Bad Rabbit," the virus is the latest example of cybercriminals using ransomware to try to extort money from victims across the globe. Two major international attacks earlier this year caused widespread disruption affecting businesses, government institutions and hospitals. When Bad Rabbit infects a computer, it seizes files and demands a ransom. Experts and government agencies advise victims not to pay up, warning that there's no guarantee they will get their files back.

This virus uses a popular malware trick. The Bad Rabbit ransomware infiltrated computers by posing as an Adobe Flash installer on compromised news and media websites. It serves as a reminder that people should never download apps or software from pop-up advertisements or websites that don't belong to the software company. ESET says once the ransomware infected a machine, it scanned the network for shared folders with common names and attempted to steal and exploit user credentials to get on other computers.

According to malware researcher James Emery-Callcott, the ransomware campaign is slowly dying down. "As far as I can see, the attacker's server is no longer live and most of the infected sites hosting the script that gives the Flash update prompt" have fixed the issue, he said. "Fake Flash updates are an incredibly popular method of distributing malware these days. Hopefully people will start to realize that when you get an unsolicited Flash update, it's generally going to be bad."

THINK BEFORE YOU CLICK