The New York Times | https://nyti.ms/2qkOeoV

PERSONAL TECH

How to Protect Yourself From Ransomware Attacks

Tech Fix

By BRIAN X. CHEN MAY 15, 2017

A decade-old form of malicious software known as ransomware has been making headlines after cybercriminals hijacked hundreds of thousands of computers worldwide.

Ransomware, which is often transmitted by email or web pop-ups, involves locking up people's data and threatening to destroy it if a ransom is not paid. The global cyberattack has affected 200,000 Windows computers in more than 150 countries, including China, Japan, South Korea, Germany and Britain.

The cybercriminals have generally targeted hospitals, academic institutions, blue-chip companies and businesses like movie theater chains. The attacks highlight the challenges that organizations face with consistently applying security safeguards on a large scale.

"Not only individuals, but even governments and big companies with so much to lose fail to secure their systems and train their employees about necessary security practices," said Marty P. Kamden, a marketing executive for the private network service provider NordVPN. “Cautious online behavior would probably have prevented the malware from infecting the network in the first place.”

What can businesses and individuals do to protect themselves from ransomware? Here are some tips from security experts.

Update your software

Security experts believe the malware that spurred this global attack, called WannaCry, may have initially infected machines by getting people to download it through email. After that, the malicious code was able to easily travel to a broader network of computers that were linked together through the Windows file-sharing system. (Users of Macs or other non-Windows computers were not affected.)

The most disheartening revelation from the cyberattack was that there was a fix available for the ransomware before the attack. Microsoft, which makes Windows, released a patch for the WannaCry vulnerability eight weeks ago, said Chris Wysopal, the chief technology officer of Veracode, an application security company.

In other words, if people had simply stayed on top of security updates, their machines would not have been infected. “People kind of got complacent and not vigilant about updating their machines,” Mr. Wysopal said.

Consumers can remedy this by configuring their Windows machines to automatically install the latest software updates.

Even though WannaCry specifically targeted Windows machines, that does not mean Mac or Linux users are off the hook in the future. Other breeds of malware may infect various operating systems, so no matter which device you are using, you should regularly update your software to install the latest security enhancements.

Install antivirus software

In addition to keeping Windows up-to-date with the latest security enhancements, antivirus software can prevent malware from infecting your computer. Mr. Kamden of NordVPN said 30 percent of popular antivirus systems were capable of detecting and neutralizing the ransomware.

Of course, with antivirus software, the same principle applies: Make sure to keep the antivirus app up-to-date, too, so it blocks the latest emerging malware. Also, download antivirus apps only from reputable vendors like Kaspersky Lab, Bitdefender or Malwarebytes, Mr. Kamden said.

Be wary of suspicious emails and pop-ups

Security experts believe WannaCry may have initially infected machines via email attachments. The lesson: Avoid clicking links inside dubious emails, Mr. Kamden said.

How do you spot a fishy email? Look carefully at the email address of the sender to see if it is coming from a legitimate address. Also, look for obvious typos and grammatical errors in the body. Hover over hyperlinks (without clicking on them) inside emails to see whether they direct you to suspicious web pages. If an email appears to have come from your bank, credit card company or internet service provider, keep in mind that they will never ask for sensitive information like your password or social security number.

In addition, ransomware developers often use pop-up windows that advertise software products that remove malware. Do not click on anything through these pop-ups, then safely close the windows.

Create backups of your data

In the event that a hacker successfully hijacks your computer, you could rescue yourself with a backup of your data stored somewhere, like on a physical hard drive. That way, if a hacker locked down your computer, you could simply erase all the data from the machine and restore it from the backup.

In general, you should be creating a copy of your data in the first place, in case your computer fails or is lost. To be extra safe from hackers, after backing up your data onto an external drive, unplug the drive from the computer and put it away.

Create a security plan for your business

For larger businesses with hundreds or thousands of employees, applying security updates organizationwide can be difficult. If one employee's machine lacks the latest security software, it can infect other machines across the company network.

Mr. Wysopal said businesses could learn from how WannaCry spread through the Windows file-sharing system by developing a strict schedule for when computers companywide should automatically install the latest software updates. Businesses should determine the best time to apply these security updates to office computers without interrupting productivity, he added.

Information technology professionals should also regularly educate and test employees on spotting suspicious emails, said Matt Ahrens, vice president of Crypsis, a cybersecurity firm.

What to do if already infected

If you are already a victim of ransomware, the first thing to do is disconnect your computer from the internet so it does not infect other machines. Then report the crime to law enforcement and seek help from a technology professional who specializes in data recovery to see what your options might be. If there are none, don't lose hope: There may be new security tools to unlock your files in the future.

In some extreme cases, it might make sense to pay a ransom if you have no backups and the encrypted files are valuable, Mr. Wysopal said. But he added that with WannaCry, people definitely should not pay the ransom. That's because the hackers are apparently overloaded with requests from victims asking for their data to be released — and many who have paid the ransom are not hearing back.

Twitter: @bxchen.