WILMINGTON TRUST

MEMBER OF THE M&T FAMILY

Avoid Becoming a Victim of Ransomware Attacks

Whether securing your business or yourself, the first step is to understand how cybercriminals work

Key points

- Ransomware is a type of malicious software that encrypts files so they can no longer be accessed
- Cybercriminals hold the files hostage until the owner pays a ransom for their return
- Business owners and individuals can take proactive steps to identify cyber risks and employ best practices to protect data

Ransomware has become one of the top threats to data stored on company networks and personal computers. For those still unfamiliar with ransomware, it is a type of malicious software (also known as malware) that, when downloaded to a computer, encrypts files so they can no longer be accessed—or it locks down the operating system entirely so the user can no longer access anything.*

Cybercriminals will hold the user's files hostage until the owner pays a ransom—usually several hundred dollars—and often in a secure e-currency, such as bitcoin. In short, ransomware is an easy way for cybercriminals to make money by stealing yours.

Every industry and every individual can be at risk of falling victim to a ransomware attack. Tactics used by cybercriminals are increasingly sophisticated and tend to mimic legitimate emails and documents, fooling users into clicking on malicious links or opening malware-laden attachments.

Cybercriminals take advantage of users who may not be aware of these types of risks or who don't follow security best practices. When it comes to disarming cybercriminals and lowering the ransomware threat, security training and education can go a long way.

As a business owner or an individual, your basic security education should include how to recognize the tricks cybercriminals use to con you into downloading malware and how to take a proactive approach to preventing data loss.

* Source: https://www.blackfog.com/the-state-of-ransomware-in-2020/.

Continued

Some of the most common ransomware tactics

Social engineering is a popular tactic used to spread ransomware. It focuses on user behaviors and habits, anticipating that they will give in to curiosity. Cybercriminals send links or add attachments that may look legitimate, but are really malware that is then loaded onto the user's computer. Popular social engineering tactics include the following:

Phishing

A study* found that 97% of phishing emails contain ransomware. Recognizing how to tell a phishing email from a legitimate email is one of the best defenses in protecting computer systems from a potential ransomware attack. However, that's easier said than done—phishing emails are becoming more targeted and harder to detect. There are still the generic and random phishing scams to watch for—threatening letters from the "IRS" is one popular example but on the whole, users are becoming better at avoiding generic phishing traps. Spearphishing (an email that appears to be from a known or trusted person or business, often directly addressed to a specific user) and whaling (spearphishing emails that target high-profile and/or high-level persons) are typically more difficult to discern.

One of the best defenses against phishing scams is to always verify the authenticity of the email before opening an attachment or clicking a link. Some telltale signs that an email is not authentic include the use of ".exe" in the attachment or link, or odd misspellings and grammatical mistakes. Regardless, verify that the email sender is who he or she claims to be. Do so by sending a new email communication, and not in the form of a reply, for additional security.

Clickbait

Clickbait uses attention-grabbing headlines to get the reader to click on the link. We've all likely seen them—articles with headlines such as "Father feeds child and you won't believe what happens next!" Readers are naturally curious and more inclined to click on these types of articles. Cybercriminals know the power of the clickbait headline and tend to use these articles to hide malware. To avoid potential ransomware delivered by clickbait, don't be tempted to click on these links, or, if possible, block sponsored ads on social media so they don't appear on any feeds.

Social media

While cybercriminals do use social media as a way to spread ransomware, what they really get from social media is a treasure trove of personal information that can help them develop those targeted, socially engineered attacks. Thanks to user "oversharing" and lax privacy settings, cybercriminals learn critical personal information, such as birthdates, likes and dislikes, vacation habits, favorite sports teams and television shows, and so on—and can then use all of that information to entice users to fall for a targeted attack. The best way to protect yourself on social media is to put security settings on the highest levels and to proactively limit personal details shared.

Fake "patches" and software updates

Cybercriminals also use drive-by malware—when malware code is downloaded from a legitimate website without the user's knowledge—to spread ransomware. What tends to happen is that the user will get a notice that software, a browser, or an operating system needs to be patched, and when the user allows the "patch," ransomware is downloaded instead.

It's tough to know when a legitimate website has been loaded with malware, but to prevent damage from a drive-by ransomware attack, users should ensure their antivirus/anti-malware software is up to date. There are also ways to check whether a patch is legitimate or malicious. For example, you can go to the browser or software help site to check for reports of a new patch, do a quick Internet search for news about an update, or set up applications to automatically download patches and updates.

Geo-targeting

This is a relatively new tactic used by cybercriminals. Each device has an address, which also reveals the device location. This allows hackers to design their attacks based on where the user lives, works, and plays. Cybercriminals use geo-targeting to ensure that their ransomware delivery method (phishing, website, etc.) is translated to the user's language or uses information that would be known to the user's country or state. Using IRS phishing emails is a type of geo-targeting, as it focuses on U.S. residents and is usually sent around tax time. To avoid an attack via geo-targeting, users should practice the same caution advised for phishing and fake update tactics: verify, patch, and use updated security software tools.

* Source: Cofense 2016 Q3 Malware Review.

Continued

Even when users recognize the tactics used by cybercriminals and have adopted some of the security practices referenced, ransomware may end up on the system. If this happens, the FBI advises against paying the ransom because it doesn't guarantee the information will actually be returned. Instead, the best step against losing important files is to back up everything to the cloud or an external drive, so that if your computer files are encrypted, nothing is lost.

Ransomware may continue to be a top security concern in the coming years because of its ease of use and high profitability. By keeping informed of the latest cybercrime tactics and doing all you can to protect your systems and your personal information, you can do your part to avoid becoming a victim.

48462 201016 VF