Ransomeware Prevention

How to prevent ransomware as a sysadmin. How to avoid ransomware as an end-user.

Ransomware Prevention for Users

Everyone knows about ransomware right? Its a form of malware that's been around for about 3 years now that encrypts all of your files and demands ransom to get them back. Gone are the days where malware simply slows down your computer. Now it costs money. Generally in Bitcoin and to the tune of at least $300 USD and up.

Ok so its obviously scary, but how do you avoid it?

Tip 1

- Use an adblocker.

Ransomware generally ends up on your system one of two ways. Either a fake download/popup/ad or a malicious email (we'll cover email tips later in this post).

The function of an adblocker blocks every ad on a webpage. This speeds up your browsing experience, enhances your privacy, and blocks malicious ads (that attempt to deliver malware and ransomware) from being accessed by your computer.

-Adblocking suggestions:

Brave - Brave is a web browser based on google chrome with a built-in adblocker. It can

be enabled or disabled by pressing the lion icon in the screenshot below and turning the "shields" on or off. It works for windows/linux/mac/android/iOS and is the simplest way to block ads.

Ublock Origin - Ublock is an adblocker available for ***Chrome*** and ***Firefox***. It has a similar on/off feature like brave. It is not easily installed for mobile so my recommendation would be to use Brave on your mobile device.

Tip 2

- Be more wary of your emails.

Emails are the main way ransomware gets into your system. Its usually a .ZIP file with an "invoice" or "resume" inside. The .ZIP in this case is used to hide these malicious files from your spam filter and antivirus applications.

Additionally you may get emails appearing to be a bill/invoice/resume with a real word/pdf attachment, but when opened you are prompted to "enable" a feature to view the contents or the document claims to be defective. This is ransomeware almost 100% of the time.

Lastly the email may contain similar features to the above, but have a shortened or spoofed link. You can hover over each link in your email to reveal its true destination. If the link and its revealed destination do not match, be sure you do not click in. In the case of shortened links you can scan it with a web service like ***VirusTotal*** to reveal and scan its destination.

Its important to be wary of the type of emails listed above even if it is from someone you know or appears to be from a reputable source. When in doubt you can upload the attatchments or links to ***VirusTotal*** for free to further ensure you aren't getting yourself

into trouble.

Tip 3

-When your computer tells you it has updates, install them.

Imagine you are trying to get some work done and your tells you that it has updates ready to install and ignore it for weeks because you don't feel like not having to wait for Microsoft's blue spinning wheel to take time away from ~~facebook~~ work. DO NOT DO THIS. If your computer says it has updates, install them TODAY or better yet NOW. Updates generally fix problems or contain security fixes that keep your computer safe from ranswomare and other threats. In the case of the "WannaCry" ransomware that was in the news in May of 2017... those 300,000+ systems that were infected were only infected because they did not have their updates installed. The update that would've prevented this was release a full MONTH earlier in April. So as inconvenient as it can be, its worth the time to do it.

Summary

So the TL;DR. The quick take away here is the following:

-USE AN ADBLOCKER
-BE SUSPICIOUS OF YOUR EMAILS
-UPDATE YOUR COMPUTER

Thanks for reading!