SERVICE BRIEF

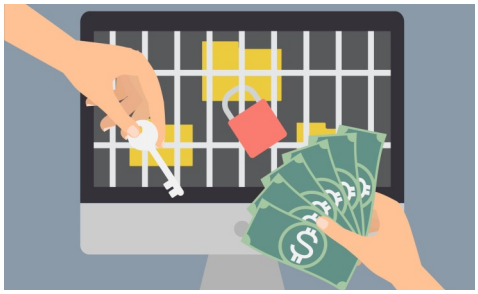
Understanding Ransomware

What you need to know about the malware that hits your data, then your wallet.

Why Does It Seem Like Ransomware Is Popular Among Online Actors With Ill Intent?

Ransomware is on the rise, and not by accident.

Recently, it seems that more and more cyber criminals select ransomware as their weapon of choice. Knowing what ransomware is, and how to avoid falling victim to it, is critical to a business' survival. Fortunately, this particular malware has a few distinct characteristics that make it relatively simple to identify and describe.



How To Recognize Ransomware

Knowing the warning signs is crucial for every business.

This malware classification follows a simple, but devious, method of attack: the program will encrypt files on the host system and demand that the user pay to regain access to their files, typically asking to be paid in some form of cryptocurrency. To add a sense of urgency to this demand, the extortionist will include a time limit within their demands, threatening to either delete the files or double the amount demanded if the stated deadline passes.

There are some targets that tend to be assaulted more than others. A cyber criminal's motivation for utilizing ransomware is financial, so they will be more apt to attack targets with more capital and higher liquidity. This means that businesses are much more likely to be targeted than a private user, although the latter is not unheard of.

How Is Ransomware Spread?

Understanding how you could be infected is the first step to avoiding infection.

A favorite tactic of malware distributors is the use of email phishing—sending out deceptive emails to fool the recipient into allowing the malware to access their system. The malware is sent as an attachment that executes when opened, bypassing the system's defenses through the user's permission. This tendency for malware to spread via phishing provides two more reasons that businesses are so frequently targeted: camouflage and points of access.

Business users tend to get lots of emails, leading to email management on autopilot. If a corrupted email looks legitimate, what cause would an employee have to worry? These assumptions are precisely what cyber criminals rely on to infiltrate their victim's systems.

As they grow, businesses will usually need to take on more employees to support their operations. An unfortunate side effect of this is that as a company grows in potential value to a cyber criminal, it also increases the number of potential access points for a cyber criminal.

Ransomwares to Recognize

- CryptoLocker
- Zepto
- Cerber3
- Fairware
- Petya
- WildFire
- LeakerLocker
- WannaCry
- Locky

Avoiding Ransomware

- Don't click on links or open attachments in unexpected emails from unfamiliar sources.
- If the email was unexpected, confirm its legitimacy through another channel.
- Do not respond directly to suspected ransomware attempts.