COMMVAULT®

Win the War Against Ransomware

6 TIPS TO FEND OFF SECURITY THREATS WITHOUT PAYING A KING'S RANSOM

The threat of ransomware is only just beginning. In fact, nearly 50% of organizations have suffered at least one ransomware attack in the past 12 months,[1] and estimates predict this will continue to increase at an exponential rate. While healthcare and financial services are the most targeted industries, no organization is immune. And the cost? Nothing short of exorbitant.

Ransomware is indeed big business. But to win the war against this cyber threat, without paying a king's ransom, you need a strong defense. Rather than arming yourself with catapults and battering rams, consider these six tips to protect against the threat of ransomware and take control of your enterprise's kingdom for good.

1 Osterman Research, "Understanding the Depth of the Global Ransomware Problem," August 2016

THE GROWING MALWARE THREAT

The truth is, Ransomware isn't new. It's been around, in one form or another, for more than 20 years. Traditionally there are two forms of ransomware: "blockers" which simply block the user's ability to access files and "encryptors" that encrypt the users' files, usually irreversibly. Both hold the victim "ransom" forcing them to pay for continued access to data.

It's been the penetration of crypto ransomware that has driven the most recent influx of ransomware incidents. According to Security Week,[2] CryptoWall accounted for nearly 59% of incidents between 2014 and 2015. But, between 2015 and 2016, TeslaCrypt replaced CryptoWall and was the culprit behind nearly 49% of all ransomware incidents. While CryptoWall and TeslaCrypt have received the most press attention, there's in fact been a 600% growth in new ransomware families since December 2015.[3]

This rapid growth of new ransomware, in addition to the alarming speed at which TeslaCrypt overtook CryptoWall, is particularly concerning. It has led many experts to think there is a true criminal-to-criminal infrastructure behind ransomware development with potentially off-the-shelf malware that can be used to speed new ransomware development. The result? New families of ransomware will be storming in faster and more furious than ever.

RANSOMWARE: A BIG AND LUCRATIVE BUSINESS

What's driving this dark business of ransomware? It's distressingly lucrative. According to the Federal Bureau of Investigation, ransomware attackers collected more than $209 million from victims during the first three months of 2016 alone.[4] This total is up from $24 million for all of 2015, or as much as $10,000 per infection.

The attackers know that they have a high rate of success too. In fact, globally nearly 40% of ransomware victims paid the ransom. That's potentially because the cybercriminals target that data which we hold most dear by targeting those employees with the highest profile data access, which is showcased by the fact that nearly 80% of organizations breached have had high-value data held for ransom and 68% percent of U.S. companies' middle managers and above were ransomware targets.[5]

What's the most common way ransomware breaks in? Email. As many as 31% of ransomware breaches entered the organization via an email link, 28% broke in via an email attachment, while 24% entered through a website or web application other than email or social media.[6]

But the truth is, no matter how the ransomware breaks in, data is at risk everywhere it's stored. And whether it's on-premises or in the cloud, data must be protected and managed with decisive processes to ensure that it won't be compromised by a cybersecurity intrusion.

"Ensure backups are not connected permanently to the computers and networks they are backing up. Examples are security backups in the cloud or physically storing backups offline... Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data."

"HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE,"
A U.S. Government Interagency Technical Guide

2 Security Week, "History and Statistics of Ransomware," June 24, 2016
3 Proofpoint, "Quarterly Threat Summary," June 2016
4 Wall Street Journal, "In the Bitcoin Era, Ransomware Attack Surge," August 19, 2016
5 Osterman Research, "Understanding the Depth of the Global Ransomware Problem," August 2016
6 ibid

6 TIPS TO BUILD YOUR BEST DEFENSE

If you're ready to protect your data from the increasing risk of ransomware, consider these six tips. They just may ensure your organization can achieve business continuity in the face of the unexpected malware attack.

1 **Protect Data, Regardless of Where It's Stored.** It's important to do a complete assessment of your data assets and to know precisely where all of your most valuable data is stored. Map out the data's location (including data centers, remote facilities, cloud, and service provider datasets) and understand the data flow between each. Pay specific attention to those systems that store, process or transmit sensitive data and understand which systems could present the highest risk for your operations. Then select, apply and manage security controls based on risk.

2 **Integrate Your Data Protection Strategy.** Select solutions that give you a complete, integrated view into all of your stored data. This will ready you for rapid response in the event of a breach, while also simplifying day-to-day management and control. The most powerful solutions will protect everything from file servers and storage arrays to third-party file sharing apps in the cloud, all from a single solution. They will also monitor, alert and identify the rate of file change across your enterprise so that suspicious activity can be quickly discovered and investigated before potential malware hops and infects other systems.

3 **Employ a Dual Backup Configuration.** For assured protection, best practices state that it's vital to have a dual backup configuration, where only one system is connected at a time. In fact, this is a core recommendation of the Center for Internet Security (CIS) Critical Security Control (CSC) for ransomware protection. The standard states:

"Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations."

This can be a powerful protection against ransomware. If the hackers can't find an access path to online backup sets, they can't break through to delete the attached backup pool. Further, if you use a secure, centralized and searchable virtual repository, you can also protect cold storage by using a protective "gap" that will prevent stored data from being corrupted while still ensuring its active use for business insights.

4 **Keep a "Gold" Image of Systems and Configurations.** Should a ransomware attack penetrate and infect one of your systems, eliminate the need to pay the "ransom" by having a "gold" image at the ready. This fundamental element of your data management policy could eliminate the risk of ransomware altogether. If a system is infected, you can easily clone the infected system with your master image. However, it's vital to have intense security and protection around your gold images to ensure attacks can never infect them.

4 Ways to Protect and Recover from Ransomware Attacks

Learn best practices from healthcare organizations as they effectively protect and recover from a ransomware attack.

READ NOW

http://bit.ly/2ajAvGy

Ransomware attackers collected more than $209 million from victims during the first three months of 2016 alone.

FEDERAL BUREAU OF INVESTIGATION

5 **Protect Vulnerable Endpoints.** Laptops and desktops are easy targets for ransomware, especially if they are not sufficiently protected. Be sure to deploy web browser URL reputation plug-in solutions that will display the reputation of the websites users access. Restrict software to corporate-approved applications and deploy two-step authentication on any website or application that offers it. Finally, employ comprehensive endpoint backup solutions that will ensure that you can rapidly recover a user's system in the event of an infection – so you can prevent further contamination throughout the enterprise.

6 **Train, and Retrain Your Users.** The best security from ransomware is to prevent it from entering your infrastructure in the first place. Because the majority of attacks enter via email, you need to train, train, and retrain your users. Every user should be educated on the risk of email attachments and know not to open anything that isn't from a known sender or trusted source. They should also be informed not to execute software that has been downloaded from the internet, unless it's first been scanned for malware. They should also be extra cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends. Finally, encourage employees to sound the alarm if they see anything suspicious or fear they've become infected. The more quickly you are altered, the easier infections will be to contain.

Don't let the risk or cost of ransomware storm your organization's castle. It will wreak havoc on your valuable data and impact business continuity. Instead, employ a multi-layer security strategy that not only includes anti-malware, firewall, and hard disk and file encryption, but also data loss prevention technology and standards-based data protection. Each are critical to mitigate cybersecurity risks and protect vital information so you can avoid business disruption without ever paying a king's ransom.

59% of ransomware breaches entered the organization via email.

OSTERMAN RESEARCH

COMMVAULT

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM