ShareFile®

CITRIX®

4 Ways to Reduce the Risk of Ransomware

Secure solutions and best practices to protect your organization and safeguard your most sensitive data

Recent years have seen the Internet swarmed with more than 50 variants of ransomware with names like Locky, KeRanger, Cryptolocker, CryptoWall and TeslaCrypt.

Initially targeting consumers, these scripts increasingly target victims with highly sensitive, high-value data such as healthcare, banking, legal and finance organizations. Once activated by an unwitting user, the ransomware calls home to a command-and-control server to acquire a unique, randomly created AES encryption key, then applies it to critical files found on local, network and cloud-connected drives. At that point, this data is entirely under the control of the hacker, who demands the prompt payment of a ransom to recover it or prevent its disclosure. This amount may range from hundreds of dollars for individual consumers to many thousands for a business. Payments are often demanded in Bitcoin, further complicating a business response.

As an illicit business model, ransomware is as effective as it is simple, reportedly earning hundreds of millions of dollars for the Cryptowall script alone. For the victim organization, recovering access to data and systems can literally be a matter of life and death, as in the case of a hospital where electronic medical records (EMR) as well as the systems responsible for CT scans, documentation, lab work and pharmacy functions have been rendered unavailable. Targeted companies in every industry, including education, utilities, retail, finance and government, face dire consequences as well, including losing access to core business functions such as email and payroll; the customer information to deliver services; and the production data on which operations depend. Even without the countdown timer displayed by most ransomware, the urgency of a response is all too clear.

Paying the ransom, typically in Bitcoin through a self-service process, is an unappealing prospect; doing so incurs a cost, rewards criminal activity and strengthens the incentive for such attacks throughout the industry. Still, at least the victim can be reasonably confident that they will be given the needed decryption key—or will they? Reports have begun to surface of "boneidleware," malware that emulates ransomware and elicits payment, but deletes data rather than encrypting it, leaving paid-up victims empty-handed. Refusing to pay can be even worse. IT must respond quickly by shutting off systems and networks to prevent ransomware from spreading—a considerable disruption—and restoring encrypted data from the most recent backup. Even then, the encrypted data still remains in the hands of the hacker, who will doubtless punish the uncooperative victim and aim to monetize the attack another way through its sale or leak.

The traditional approach for mitigating ransomware revolves around user education, antimalware, frequent backups—and keeping a supply of Bitcoin on hand just in case. These are sensible measures, but they're not nearly enough, as proven by numerous spectacular failures. What's needed is a more robust, systems-level approach designed to keep data out of harm's way entirely.

Here are four ways to kidnap-proof your data

TABLE OF CONTENTS

1

Publish virtualized, sandboxed and hardened browsers

Browsers serve as the front end for modern applications across web, cloud, mobile and embedded platforms, making them a prime attack vector. A user's computer can become infected simply by visiting a site that hosts malware disguised as a download or plugin update, coded in active content, or even silently embedded in an image or video. Browser virtualization provides an abstracted architecture to insulate business data and corporate networks from web-based malware such as ransomware. By using a provider to run a hosted browser, IT can introduce a layer between the corporate environment and the Internet to shield the trusted computer and its data from attack. The virtualized browser also keeps sensitive data off the endpoint.

As a further step, IT can isolate the browser through containerization or sandboxing. All web usage, including hyperlinks in emails and social media apps, are redirected to open in a one-time-use virtual browser within the container or sandbox. This browser instance does not have access to other applications, the endpoint, file shares or other sensitive resources, limiting the reach of ransomware to the current browser session. As a result, no data beyond the current browser session is vulnerable to third-party encryption, and the malware used to deliver the attack will not penetrate the rest of the enterprise environment or persist beyond the current session. Content inspection, whitelisting and other security measures can also be integrated with the isolated browser to reduce the risk of ransomware and other forms of malware.

Use case-specific browsers allow further hardening against infection, reducing the attack surface for illicit software. By configuring a separate virtual browser for each application and use case, IT can disable extraneous settings, unnecessary active content and other capabilities not currently required, such as Flash, Silverlight or Java. As an added benefit, multiple browsers such as Internet Explorer and Chrome can be published, and multiple versions can be maintained as needed by specific applications.

2

Publish a virtualized, sandboxed, and hardened email client

Similar to the publication of hosted browsers, IT can use a secure service provider to deliver a virtual email client to protect against infection via email links and attachments. This can be either a traditional native client such as Microsoft Outlook, or web-based email including Google Gmail and Microsoft Office 365. Publishing the email client ensures that all required security settings are configured and consistent for all users and specific to use cases. Antivirus, DLP (data leakage protection), whitelisting and other technologies are integrated with the published email application and are therefore not endpoint-dependent or limited. Only the pixels representing the email app are sent to the endpoint, not actual messages, attachments or other data, ensuring that ransomware does not infect the user's computer and thus gain a foothold within the enterprise environment for further penetration and attack.

3

Protect mobile devices against attack with containerization

As mobile devices become ubiquitous in the enterprise, they also become a prime attack vector for ransomware and other malware—especially when both personal and business apps are used on the same device. To prevent infection, IT can use an enterprise mobility management (EMM) solution to create a separate container on the smartphone or tablet for business data and corporate apps, making it possible to centralize management, security and control for apps as well as data and settings without interfering with any personal content on the device. For example, IT can define contextual security policies that provide access only in approved scenarios to reduce exposure to malware. Whitelists and blacklists can prevent the installation of known malicious apps on the device, including those known to deliver ransomware.

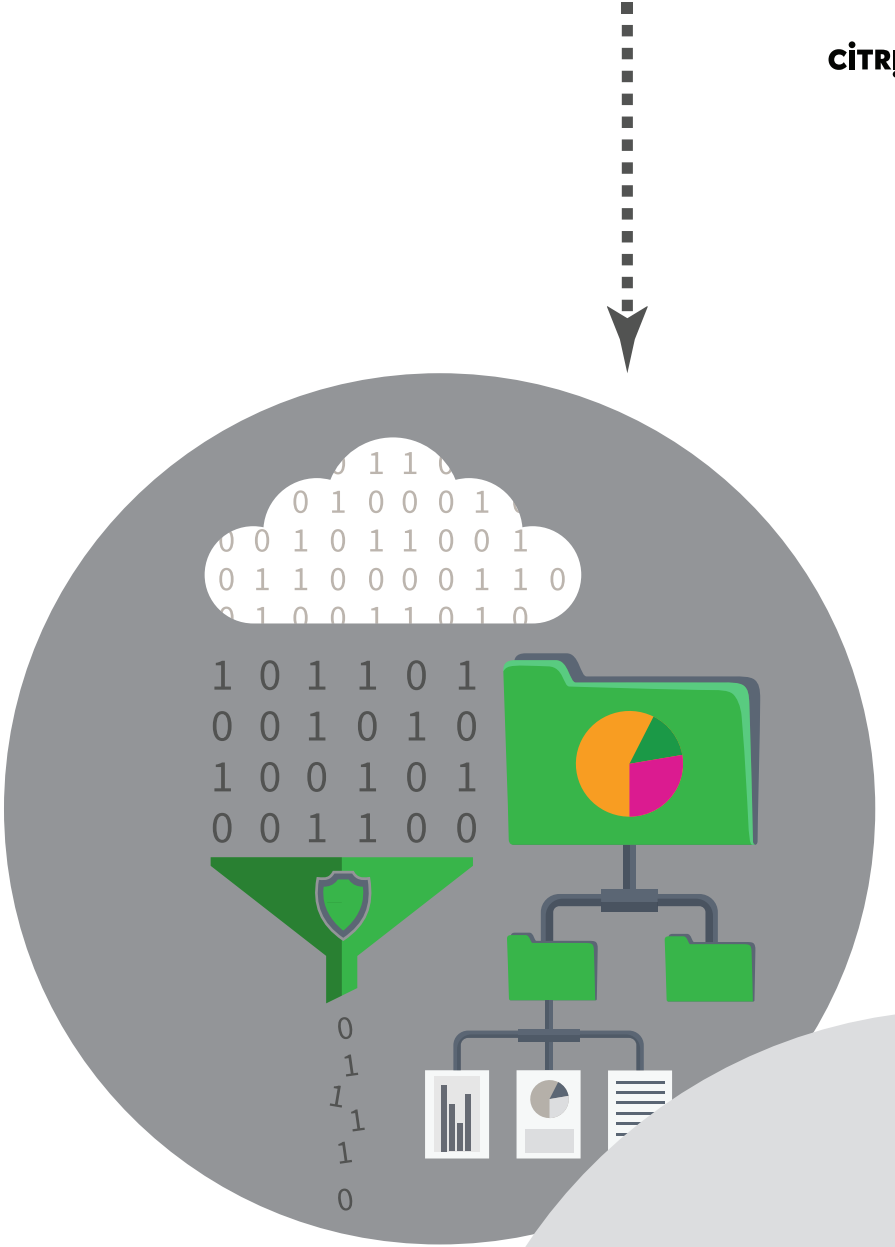
Similarly, certain EMM solutions check to ensure that the device has not been jailbroken or rooted to allow the installation of pirated or non-validated apps, a common vector for malware designed to acquire super admin status. Non-compliant devices are blocked prior to enrollment, ensuring that any ransomware or other malware they may contain will not enter the corporate network.

To keep pace with constantly changing malware definitions and security trends, and protect devices proactively against any ransomware, malicious app or profile, seek out an EMM solution that natively integrates with security vendors such as Skycure, Palo Alto Networks and Zimperium.

4

Provide a secure and robust enterprise data sync and sharing service

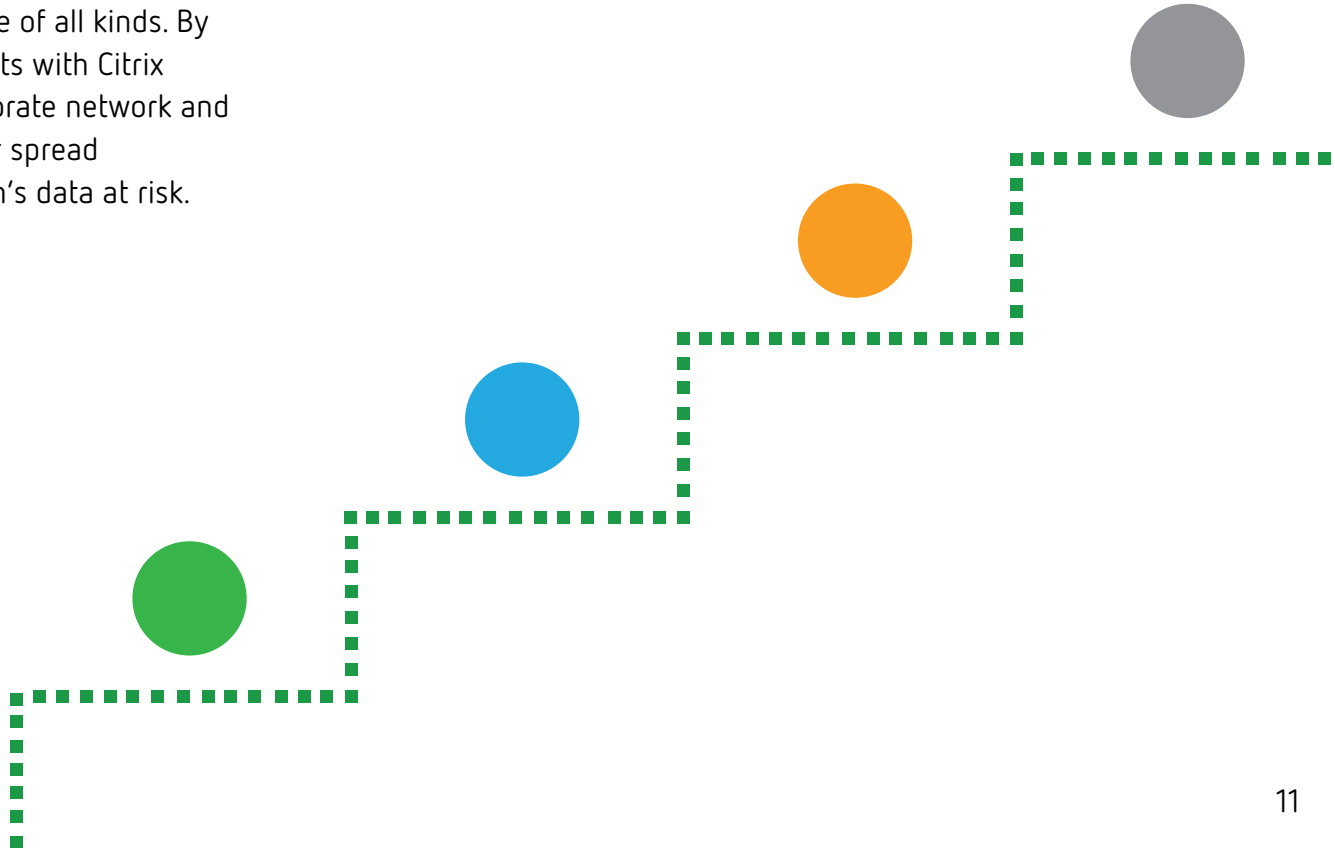
The rise of ransomware is a stark reminder of the critical importance of data. An enterprise file sync and sharing (EFSS) service can help keep data out of reach of ransomware without impeding productivity. Data can be stored, managed, secured and accessed elsewhere—while still appearing as if it resides locally from the user's perspective for optimal convenience and ease of use. Best-in-class EFSS solutions should include versioning functionality that retain multiple versions of each file. In the event a file is encrypted by ransomware, IT can revert to the most recent uncompromised version, eliminating the need for a hacker's decryption key.



Next Steps

Ransomware is one of the most serious security threats organizations face today, and calls for an equally robust response—well beyond simply cautioning users abou suspi-cious links. Citrix recommends a multilayered approach designed to reduce exposure to ransomware attacks, as well as to recover encrypted data more quickly and effectively. Citrix supports this approach through Citrix Workspace solutions, providing an integrated and flexible framework to secure apps, data and the network from infection by malware of all kinds. By publishing virtual web browsers and email clients with Citrix XenApp, IT can isolate endpoints from the corporate network and ensure that infected hosts are unable to further spread ransomware and place more of the organization's data at risk.

Citrix XenMobile enables secure mobility through containerization to protect data on smartphones and tablets. Citrix ShareFile captures versions of files in real time to ensure that a clean version is always available to replace a file that has been encrypted by ransomware. In this way, IT can protect the business and its data, minimize disruptions and avoid rewarding hackers for their illicit activity.



Citrix customers are already using these methods to avoid the damage and disruption of ransomware. To learn how your organization can use Citrix secure digital solutions to reduce the threat of ransomware, visit citrix.com/sharefile.

© 2017 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).