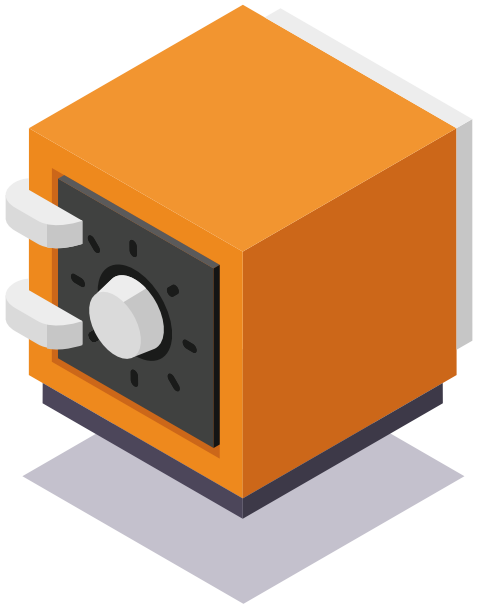
KeepItSafe®



RANSOMWARE ATTACK: WHAT'S YOUR DATA RECOVERY PLAN?

Learn more about how KeepItSafe can help to reduce costs, save time, and provide compliance for online backup, disaster recovery-as-a-Service, mobile data protection, and cloud SaaS backup — contact us today.

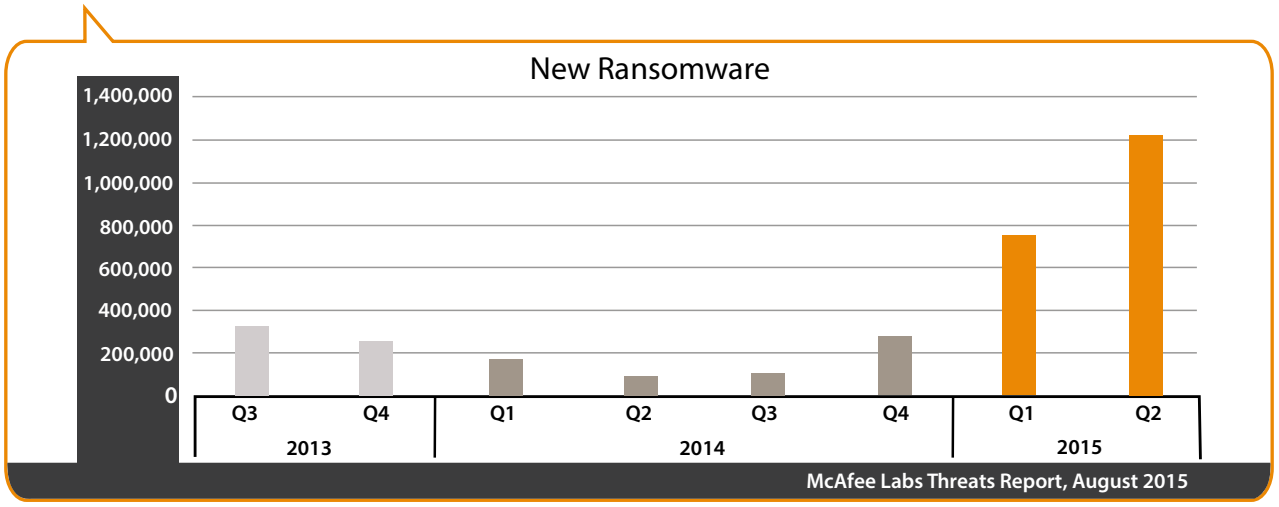
888 965 9988

www.keepitsafe.com

sales@keepitsafe.com

TABLE OF CONTENTS

WHAT IS RANSOMWARE AND WHY IS IT ON THE RISE?



Imagine sitting down at your office computer, logging in to your corporate network, and being greeted by the following onscreen message:

"We have locked you out of access to all of your company's systems, files and other data. To have access restored, please deposit $100,000 in the following bitcoin account."

This is "ransomware," one of the most prevalent forms of malicious cyber attacks facing businesses today.

With a ransomware attack, a cyber hacker infects your network or device with malicious software, usually through code attached to an email or contained within seemingly legitimate software you download from a website. Once the malicious software propagates through your systems, the hacker can then encrypt your data — and contact you with an offer to pay a ransom to get the data back.

If this sounds to you like a rare occurrence, or simply the stuff of thriller movies, we have bad news. Malicious cyber attacks, including ransomware, are sharply on the rise against businesses. In fact, according to a 2016 report by the Financial Times, malicious attacks now represent the leading cause of all corporate data loss — surpassing the previous leader, employee error. [1]

Even more concerning, experts predict that ransomware attacks are about to skyrocket. According to the insurance company Beazley, which tracks and reports on data security vulnerabilities in its Beazley Breach Insights report, it is estimated that ransomware attacks are on track to increase 250% in 2016. [2]

Why is ransomware becoming so prevalent? One reason is that it has proven effective. A quick story will illustrate why:

The Hollywood Presbyterian Medical Center in Los Angeles had its computer network hacked in early 2016, leaving all of the hospital's data encrypted and inaccessible. Shortly after, hospital administrators received a ransom message from the hackers — reportedly demanding $3.4 million for the decryption key.

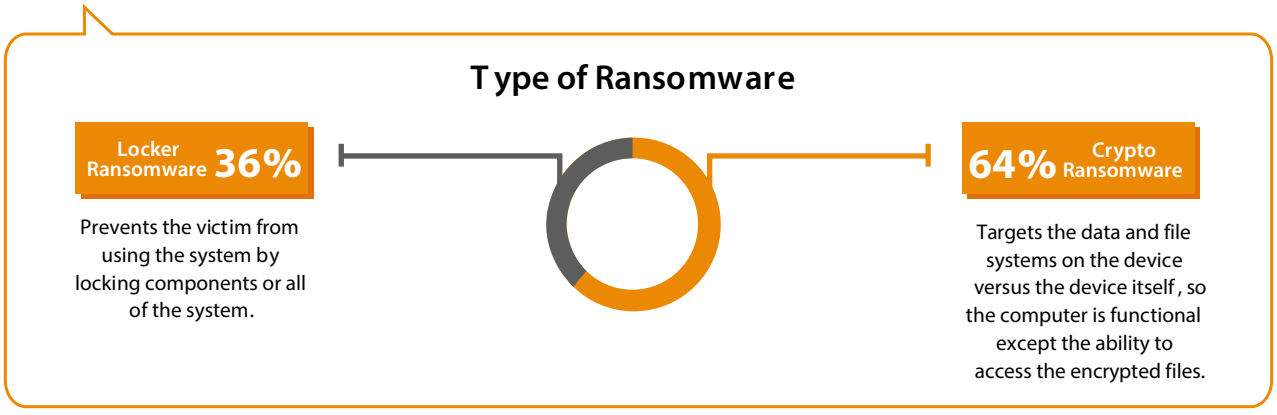
For a healthcare company such an attack can be devastating almost immediately. Business stops. Care stops. In this case, it meant that hospital staff were unable to access vital patient data records and save new information digitally, slowing operations to a crawl as they resorted to paper systems, impeding access to key historical and real time data needed to make the most accurate diagnostic care and business decisions. After a few days with their systems offline, the hospital agreed to pay the attackers $17,000.

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," the hospital's president explained in a press release. "In the best interest of restoring normal operations, we did this." [3]

With ransomware repeatedly proving a successful strategy for extorting money from businesses, we can expect this threat to increase with time. Furthermore, ransomware can inflict lasting damage in that even if hackers are paid off and the data is released, they may still have a backdoor to an organization's website or network from which to target users. Of course, like many cyber enabled threats, the existence of ransomware kits expands the threat even further as criminals who might generally not have the computer skills to create such threats can execute attacks prepared by others.

We have prepared this white paper to help educate IT teams on how ransomware works — how to prevent it from happening to their businesses.

THE MOST COMMON TYPES OF RANSOMWARE AND ITS MOST POPULAR TARGETS



Ransomware attacks are broadly broken into two categories: locker and crypto.

Locker ransomware is a simpler form of attack where the malicious code disables some or all of your computer systems' functionality. For example, you won't be able to access any of the applications or data folders on your desktop but you will still be able to use your keyboard and mouse to communicate with the hackers.

The locker malware typically does not encrypt your files, but merely locks you out of access to them.

Crypto ransomware is a more sophisticated form of attack wherein the hackers encrypt your mission-critical data, and then present a ransom demand, perhaps with a countdown threat— *"Deposit this amount in our account by this time, or we will destroy all of your data."*

Although a crypto attack is often a signal of a more advanced cyber criminal than the simpler locker attack, both forms of ransomware can pose a significant threat to a business's intellectual property, reputation, regulatory compliance and ability to continue normal business operations. Businesses, therefore, need to be ready to defend against both forms of attack.

Ransomware Attackers' Favorite Targets

Business Server Software

Corporate IT teams need to stay vigilant against malicious attacks such as ransomware because the cyber hackers themselves are always looking for new ways to penetrate corporate systems — and often finding them.

One example of the rapidly evolving vehicles for ransomware attacks is through unpatched business server software. As PCWorld reported in 2016, attackers are exploiting vulnerabilities in server software that allows them to implant ransomware code directly onto business servers, rather than through the more indirect methods of sending spam emails with malicious attachments or by infecting legitimate software downloads with the ransomware code. The "Samsam" ransomware that spreads through unpatched JBoss application servers is one recent example. [4]

The critical challenge for corporate IT departments is that ransomware attackers are continually growing more sophisticated and creative in their methods and thus the IT teams defending corporate data must continually educate themselves on new threats.

Healthcare Data

Among ransomware attackers' favorite target industries is healthcare, primarily for two reasons:

First, these cybercriminals know how vital — life and death in some cases — access to patient data can be for a healthcare organization. This means that medical organizations will be among the most likely to pay a ransom for the fast return of their data.

Second, cyber hackers also know how heavily regulated the medical industry is and therefore how vulnerable to running afoul of regulators if they leave their electronic protected health information — ePHI — exposed to theft or attack. A major data breach could cost a healthcare organization enormous fines for compliance violations, and even lead regulators to shut the company down completely.

Because of the regulatory angle, you can also assume that any business in an industry whose data is subject to strict privacy regulations will also be a tempting target for ransomware attacks — financial services, legal, real estate, business consulting firms, any publicly traded corporation, to name a few.

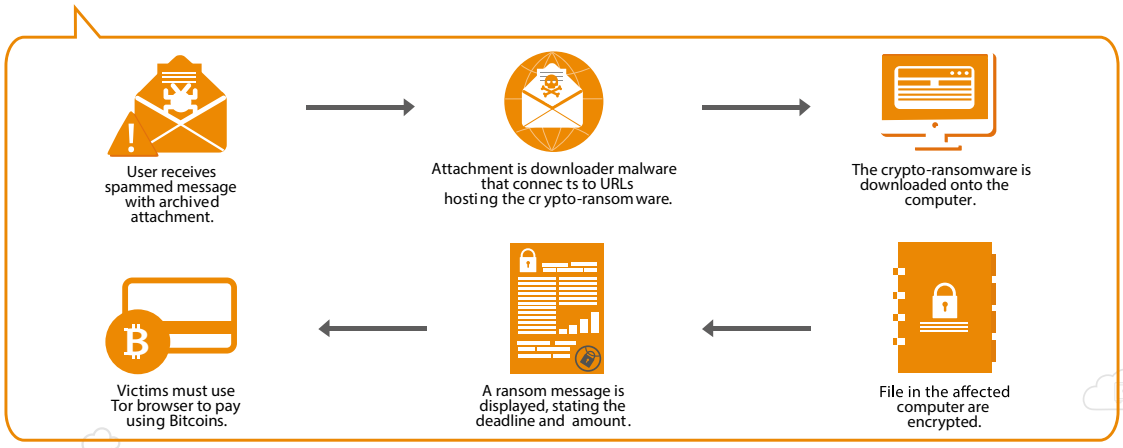
Mobile Devices

As BankInfoSecurity.com has reported, mobile devices represent another treasure trove of possible ransomware victims.[5]

With mobile ransomware attacks, cybercriminals are able to exploit two trends: the current security weaknesses among apps on smartphones and other consumer-grade mobile devices, and the increasing use of mobile devices for accessing corporate networks.

Malicious criminals can infect legitimate apps with ransomware, wait for users to download those apps to the devices, and lastly bring those devices into their office environments.

HOW RANSOMWARE SPREADS



We've covered what ransomware attackers will do to extort their victims for money after they've successfully taken control of their data — either through a simple locker attack or a more advanced crypto attack. We've also discussed broadly the types of companies most likely to be targeted by a ransomware attack.

Now let's take a step back and explore how the ransomware attacker gains control over a business's data in the first place. What are their methods of getting their malicious code into your corporate systems? What do you and your team need to be on the lookout for?

Spam Email Messages

This is the most common method of infecting a system with ransomware code. Taking advantage of social engineering techniques the attacker sends an innocent-looking email with the malicious software either embedded in an attachment that the message asks the reader to open or on a site whose link the message tricks the reader to click.

Cybercriminals are becoming increasingly sophisticated in disguising these spam messages. Some appear to come from a friend in the recipient's address book, others appear to come from an online service provider the recipient does business with — such as Amazon.com or FedEx — asking for an update to profile information or warning of a breach of their account. (Cyber hackers have a sense of irony.)

The malware gets run when the user opens the attached ZIP file, by entering the password included in the message, and attempts to open the PDF it allegedly contains. CryptoLocker, by example, takes advantage of Windows' default behavior of hiding the extension from file names to disguise the real *.exe extension of the malicious file.

As soon as the user takes the required step (downloading the attached file; clicking on the link), the ransomware goes to work embedding itself into the now compromised computer system and then propagating itself across the network.

Downloads and Botnets

With this method of attack the cybercriminals will initially infect your systems with malware through the methods noted above. However the code will not take action immediately - the hackers' code might sit on your network or severs, undetected, for some time before the hackers are ready to launch the ransomware attack.

When the time comes, this malicious code will communicate, via the malware's botnet, with the hackers. This usually happens through the launching of an apparently innocent "upgrade" or other click enticing request to the user that enables execution of the malware, gives access to the hackers allowing the remote encryption of your data (the crypto method) – cumulating in the delivery of the ransomware message.

This method of ransomware attack has become so prevalent that in mid-2016 the United States Senate introduced a bill called the Botnet Prevention Act.[6]

Operating Systems or Software Exploits

With this approach, the hackers are able to exploit a security vulnerability in either an application running on your systems or network, or directly in the operating system of one of your computers or servers.

This type of ransomware attack can be even more difficult to defend against than the previous two mentioned —spam emails and malicious downloads — because it does not require any proactive action taken by anyone in your organization. Such an attack can be launched merely by exploiting the presence of a vulnerability you do not know exists.

Executable Files

A variant on the downloadable ransomware attack is by infiltrating a *.exe (executable) file into a computer or server via an apparently innocent delivery and then configuring that file to launch upon system startup — thereby propagating its malicious code across the system and network.

There are many variants of these ransomware approaches, and hackers are testing new and more sophisticated approaches regularly.

For a useful and up-to-date resource to help your team keep up with the ever-evolving ransomware variants, visit the website of the United States Computer Emergency Readiness Team (US-CERT) and search "ransomware variants."[7]

WHAT YOU CAN DO: 10 STEPS TO DEFENDING AGAINST RANSOMWARE

Following are 10 steps, all proven best practices, that your business can take to protect against the ever-present threat of a ransomware attack.

1. Implement a Comprehensive Data Backup and Recovery Plan

Implement a program to whitelist applications that will require active approval by your team or authorized administrators to grant permissions for those apps or programs to run on any networked devices. The result is that unanticipated, and thus not whitelisted, applications will need inspection. The whitelist might be available from a trusted source.

This is a smart way to place one more obstacle, and a trained set of eyes, on any new piece of software to check for malicious code such as ransomware — before allowing it access to your corporate network.

2. Implement a Plan to Regularly Scan and Test All Networked Devices

Another key component to ransomware prevention is ensuring that, at all times, all of your company-issued devices or personal devices that interact with your network are up to date with the latest anti-virus software or other tools to prevent the introduction of malicious code. Given the trend of using executable files to launch malware, it's very important that your process include scanning all local drives and devices before executing a launch.

Ideally, your data backup and recovery solution will also include an endpoint protection component thereby empowering your IT team with centralized visibility into and control over all devices that interact with your network or other systems — including mobile devices. As a minimum, the ability to force an offending device off the network.

Deploying such an endpoint protection system will make it far easier to have visibility into any devices that might pose a threat, and to remotely prevent them from gaining access to your network.

3. Keep Your Operating Systems and Software Up-to-Date With New Patches

When it comes to introducing malware into a system, including ransomware, one of the easiest points of entry for cyber hackers is through an application or operating system that is out of date or that has a security vulnerability. Keep up with the latest security patches for all apps and operating systems your company uses.

4. Isolate Infected Devices Quickly

The damage a ransomware attack can do to your data is directly related to how fast, far and wide the malicious code can propagate itself across your network, servers, and systems.

So part of your process should be that as soon as you identify a device that might be infected with any malware, you will disconnect that device from your network.

5. Filter for .exe Attachments in Email

To be proactive in protecting against the dreaded CryptoLocker code and similar threats which launch themselves through an executable file embedded into one of your systems, include in your process for preventing malware a filter for executable files attached to inbound email traffic to your users.

You can then choose to scan the *.exe or macros in those email attachments, in an isolated environment, on a case-by-case basis, to help your users — but filtering for such attachment first will reduce the likelihood of a crypto ransomware attack sneaking onto your network.

6. Disable Files Running from AppData Folders

Another common trick of the CryptoLocker code is to run its executable from the AppData or Local AppData folders. So you can limit the chance of such an attack by creating rules within Windows or with Intrusion Prevention Software to default to disallowing any executable to run from these folders.

If you have legitimate software that you know is set to run not from the usual Program Files area but rather from the AppData area, you can exclude it from this rule or override it.

7. Disable Remote Desktop Protocol (RDP)

The CryptoLocker/Filecoder malware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely.

If you do not require the use of RDP, you can disable RDP to protect your machine from Filecoder and other RDP exploits.

8. Protect Your Operating Systems and Apps

It's important to understand that even a simple, unsophisticated ransomware attack can include the locking and encrypting everything across your network — including your applications and operating systems — not merely your files.

This means your system protection process should also include steps to secure your apps and systems as well as your files and folders.

9. Train Your Staff and Test Readiness for an Attack

Another necessary component in any cybersecurity process is to make sure your staff across the organization is trained in preventing cyber hacks, and knows what to do if one occurs.

So document cybersecurity processes — one for your IT team, and another for the employees across your company. Train staff on the malware-prevention steps outline above, such as not opening suspicious emails or downloading apps or files from websites unless they are certain of their legitimacy. Social Engineering, the human user, is often one of the weakest links in the security chain.

Train your staff also to isolate a device should they discover it has been infected with malware, ensuring the damage is minimized and not letting the malicious code replicate itself across your network.

Lastly, run drills, performing regular tests to help your employees learn how to react to a cyber-attack so that their response, should one occur, is smooth, thorough, and most importantly, immediate.

10. Implement a Comprehensive Data Backup and Recovery Plan

Finally, roll out a company-wide solution for backing up all corporate data, on all systems and devices, as well as a disaster recovery and business continuity program. Your backup solution will ideally be cloud-based, with a trusted provider that maintains all of your data securely in the cloud and across multiple, geographically distinct locations — with immediate failover, should one of these locations suffer an outage or natural disaster.

A cloud backup solution is preferable to limiting your business to onsite backup for several reasons — such as the risks of human error (e.g., forgetting to replace a backup tape), employee theft or natural disasters. But another reason to consider outsourcing backup and recovery to the cloud is that with the right provider, you can ensure your critical backups stand isolated from your onsite systems, so an infected machine on your premises cannot also propagate its malicious code across your other networked devices onsite.

HOW KEEPITSAFE HELPS COMBAT RANSOMWARE

For the data backup and recovery component of your organization's cybersecurity process, the most proven and comprehensive solution comes from KeepItSafe®.

KeepItSafe's suite of offsite data backup, disaster recovery and business continuity solutions include:

- ✓ Fully managed and monitored global data backup in the cloud
- ✓ Protection of your company's data at rest with AES 256-bit encryption
- ✓ 24/7 support by phone or email from a trained team of data-protection support engineers
- ✓ Backup and recovery solutions are certified to ISO-27001 and SSAE-16

References

1. "Malicious Attacks Now Account for Bulk of Data Loss"
http://www.ft.com/intl/cms/s/0/7dec0636-e541-11e5-bc31-138df2ae9ee6.html#axzz49sNB5CrD

2. "Beazley Breach Insights 2016 Show Sharp Increase in Hacking and Malware"
https://globenewswire.com/news-release/2016/03/08/817850/10160778/en/Beazley-Breach-Insights-2016-shows-sharp-increase-in-hacking-and-malware.html

3. "Hollywood Hospital Pays $17,000 to Ransom Hackers"
http://www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack/#:e8I-tLVDZ6CtXA

4. "Server Software Poses Soft Target for Ransomware"
http://www.pcworld.com/article/3052556/server-software-poses-soft-target-for-ransomware.html

5. "Why Fraud is Shifting to Mobile Devices"
http://www.bankinfosecurity.com/interviews/fraud-shifting-to-mobile-devices-i-2569

6. With Ransomware on the Rise, Senate Botnet Bill Gets Another Shot"
https://fcw.com/articles/2016/05/19/botnet-whitehouse-bill.aspx

7. Ransomware Variants from the US Computer Emergency Readiness Team
https://www.us-cert.gov/ncas/alerts/TA16-091A

18037 — ©2018 KeepItSafe, Inc. All rights reserved. KeepItSafe is a trademark of KeepItSafe, Inc. or its affiliates and is registered in the United States and other countries. All other trademarks cited herein are the property of their respective owners.