How to Protect Your Business from Ransomware Attacks

What You Need to Know and Do to Keep Your Business Secure

Meridian PC Solutions
1446 Pottstown Pike
West Chester, PA 19380

t: 484-753-7200
e: info@meridianpcsolutions.com
w: www.meridianpcsolutions.com

About This White Paper

Headlines such as "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating"[1] and "The CryptoJoker Ransomware Is Nothing to Laugh About"[2] are common. They are indicators of a much larger problem: The number of ransomware attacks is increasing at an alarming rate, making ransomware the biggest cyber threat that businesses are facing today.

The situation is so serious that the United States and Canada issued a joint cyber alert about the dangers and prevalence of ransomware attacks. The alert recommends that businesses take preventive measures to protect their computers from ransomware infections.

Toward that end, this white paper covers:

- What ransomware is
- How ransomware is spread
- How to protect your business from ransomware attacks

[1] *Los Angeles Times*, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating"

[2] Bleeping Computer, "The CryptoJoker Ransomware Is Nothing to Laugh About"

The number of ransomware attacks is increasing at an alarming rate, making ransomware the biggest cyber threat that businesses are facing today. To see this disturbing trend, you only have to turn back the clock to the beginning of 2016. There was a 30 percent increase in the number of ransomware attacks in the first quarter of 2016 compared to the fourth quarter of 2015.[3]

The situation is so serious that the United States and Canada issued a joint cyber alert in March 2016 about the dangers and prevalence of ransomware attacks.[4] The alert recommends that businesses take preventive measures to protect their computers from ransomware infections.

> Some small business leaders believe that a ransomware attack will never happen to them because their businesses are too small to be noticed by cybercriminals.
>
> This is wishful thinking.

It is important for all businesses — including small ones — to take measures to protect themselves from the growing ransomware threat. While some small business leaders believe that a ransomware attack will never happen to them because their businesses are too small to be noticed by cybercriminals, the fact is that this is wishful thinking. The number of cyberattacks targeting businesses with fewer than 250 employees has been steadily increasing over the last five years, according to Symantec's "2016 Internet Security Threat Report."[5] In 2015, 43 percent of all reported cyberattacks were against small businesses — a 9 percent increase over the number reported in 2014.

So, no matter the size of your business, you need to protect it against ransomware. To do this, you first need to learn what ransomware is and how it is spread. Armed with this knowledge, you can take measures to secure the points at which ransomware might enter your business. You also need to prepare for the worst-case scenario — a ransomware infection occurs, despite your best efforts to prevent it.

What Ransomware Is

Ransomware is a type of malware that cybercriminals use to extort money from businesses and individuals. It usually encrypts files, but it also might lock computer systems. The cybercriminals then demand a ransom for the private key needed to decrypt the files.

Locky provides a good example of how ransomware works. It was used to infect Windows computers worldwide in February 2016.[6]

---

[3] Kaspersky Lab, "IT Threat Evolution in Q1 2016"

[4] U.S. Computer Emergency Readiness Team, "Alert (TA16-091A): Ransomware and Recent Variants"

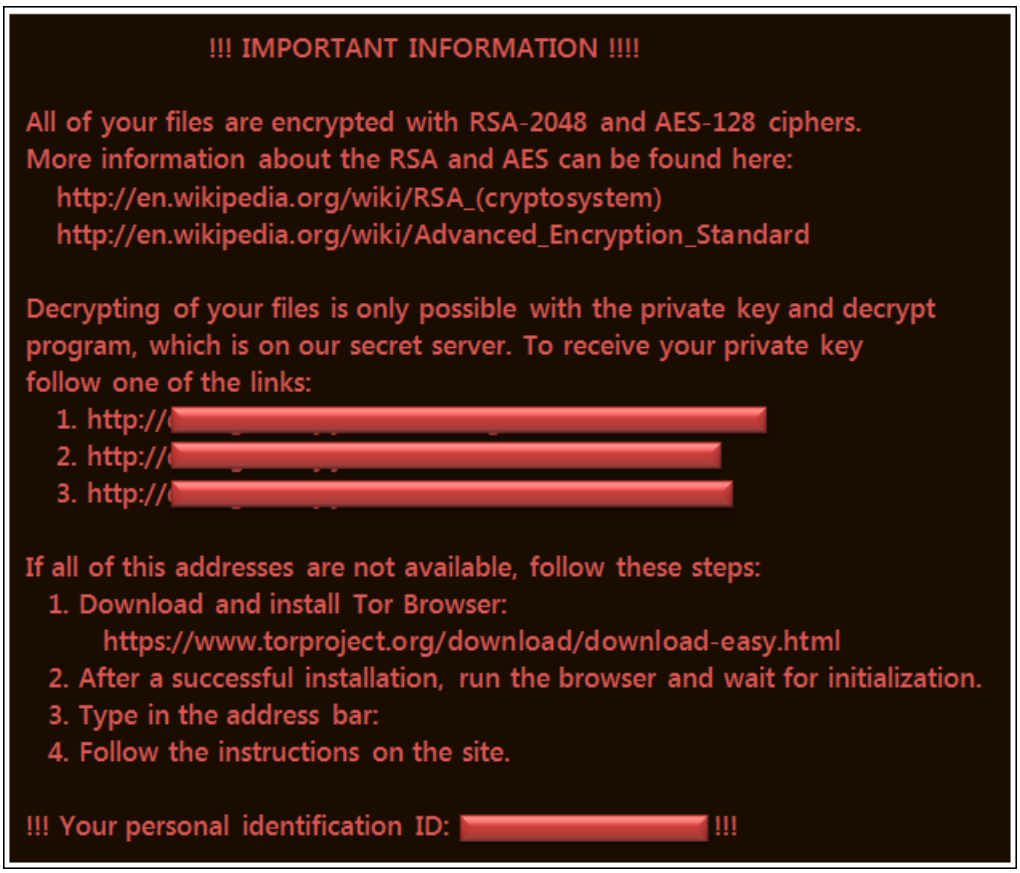
[5] Symantec, "2016 Internet Security Threat Report"

[6] Webroot, "Locky Ransomware"

Locky begins by creating a unique 16-character hexadecimal name for the victim, which it sends to the cybercriminals' remote server for identification and tracking purposes. Next, it scans the local drives and network shares (both mapped and unmapped) on the victim's computer, looking for files to encrypt. Locky encrypts more than 130 types of files, including image files (e.g., JPG, PNG), Microsoft Office files (e.g., DOCX, XLSX), and PDF files.

After it encrypts each file, it changes the filename, including the extension. The new extension is ".locky". The ransomware also deletes any shadow copies made by Windows' Volume Shadow Copy Service to make sure the victims cannot recover their files from these local copies.

Locky then creates a ransom note on the Windows desktop and in each folder where a file was encrypted. The desktop ransom note looks like this:



As you can see, a victim needs to click one of the links provided to get the private key that will decrypt the files. The links lead to the Locky Decrypter Page, which specifies the ransom and where to send it. The ransom is typically 0.5 or 1 bitcoin. (The bitcoin exchange rate varies. In mid-2016, a bitcoin was worth more than $550 USD.)

After the victim sends the ransom, the Locky Decrypter Page provides the private key. The victim can then use it to decrypt his or her files. The victim will also need to remove the ransomware from the computer.

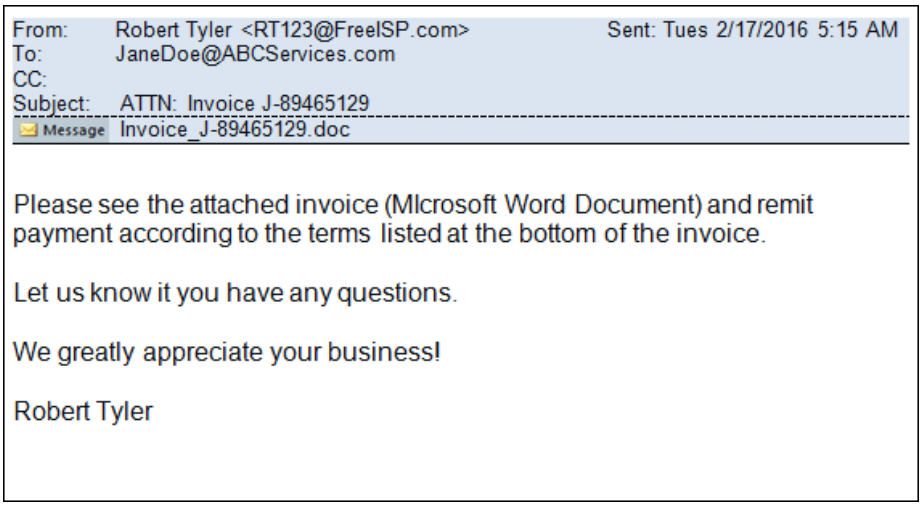
How Ransomware Is Spread

Cybercriminals use a variety of techniques to get ransomware on computing devices. Common ways include phishing and spear phishing emails as well as drive-by downloading. Another method that is not as common but just as effective is exploiting known vulnerabilities in servers.

Phishing and Spear Phishing Emails

To spread ransomware, cybercriminals often send out phishing and spear phishing emails. These emails use a convincing pretense to lure recipients into performing an action, such as clicking a link or opening an attachment. If the recipients fall for the ruse, their computers will likely become infected with ransomware.

Cybercriminals used this technique to distribute the Locky ransomware in February 2016. They crafted an email that told the recipients to see an attached invoice and remit payment according to the terms listed in the invoice. The attachment was a Microsoft Word document. Both the subject line and attachment's filename had the same invoice number, as the following shows:



Opening the email itself caused no harm. However, the same cannot be said about opening the attached Word file. It contained a macro.

A macro is a series of commands grouped together. Macros are not inherently bad. People use them to automate routine tasks, such as applying formatting. However, the macro in the file attached to the phishing email included commands that instructed computers to download the Locky ransomware from a remote server and install it.

If the phishing email recipients opened the attached file and Word was configured to automatically enable macros, their computers were infected with the Locky ransomware. An infection also occurred if the recipients manually enabled the macro.

In the Locky phishing emails, the attachment was a Word document, but other types of documents can be used in ransomware attacks. For instance, in January 2016, cybercriminals attached a ransomware installer disguised as a PDF file to a phishing email.[7] Simply opening that file unleashed the CryptoJoker ransomware on the victims' computers.

Drive-By Downloading

Another common way that cybercriminals spread ransomware is through drive-by downloading. Cybercriminals either build a malicious website or post malicious advertising (aka malvertising) on a legitimate one. Surprisingly, it is not social media or shopping websites that are most likely to have malvertising. The three most frequently exploited types of websites in 2015 were technology, business, and search websites.[8]

When users visit a malicious website or a legitimate website with malvertising, code is installed on their computers, without their knowledge. The code usually redirects the users' browsers to a server, where an exploit kit tries to find a known vulnerability. If one is found, it is used to install malware. In April 2016, cybercriminals delivered the Locky ransomware this way.[9] They took advantage of a vulnerability in Adobe Flash Player to install Locky on users' computers.

Exploiting Known Vulnerabilities in Servers

Cybercriminals do not just stick with their old tricks for delivering ransomware. They also come up with new ones. For example, in a series of attacks during March and April 2016, hackers exploited a known vulnerability in servers running Red Hat's JBoss software to install backdoors, which they then used to deliver ransomware.

Although this approach to spreading ransomware is new, the vulnerability exploited in the attack is not. Red Hat released an update that fixes it, but around 3.2 million servers have not been patched.[10]

Cybercriminals scan servers connected to the Internet, looking for these unpatched JBoss servers. When they find one, they exploit the vulnerability to access the machine. The cybercriminals then use a tool called JexBoss to install web shells (i.e., small scripts) that let them remotely control the server. They also use JexBoss to open a backdoor through which they install the Samsam ransomware.

To make matters worse, Samsam is self-spreading ransomware. An infected server will try to infect any Windows computers connected to it — those computers do not have to be running JBoss.

---

[7] Bleeping Computer, "The CryptoJoker Ransomware is nothing to Laugh About"

[8] Symantec, "2016 Internet Security Threat Report"

[9] Trend Micro, "Locky Ransomware Spreads via Flash and Windows Kernel Exploits"

[10] Talos, "Widespread JBoss Backdoors a Major Threat"

How to Protect Your Business from Ransomware Attacks

To help your company defend against ransomware attacks, you need to be proactive. You need to take measures that will help prevent an attack. You also need to take measures in case a ransomware infection occurs, despite your best efforts to prevent it.

Measures to Help Prevent an Attack

When it comes to ransomware, you want to prevent the infection from ever starting because, once it starts, there is little you can do to stop it. Toward that end, you should consider taking the following actions:

Use anti-malware software. It helps detect and block known ransomware and other kinds of malware.

Update operating system software and applications regularly. Cybercriminals like to target programs with known vulnerabilities. A perfect example is how cybercriminals are exploiting the vulnerability in the JBoss software. Patching these vulnerabilities reduces the number of exploitable entry points.

Keep email filtering tools up-to-date. These tools use various filters to help weed out phishing emails and spam. Most email programs include filtering tools, but you can also purchase advanced filtering solutions.

Teach employees about phishing and spear phishing emails. Show employees how to spot phishing and spear phishing emails. Also discuss the dangers of clicking links and opening attachments in emails, especially if the emails are from unknown senders. The Presstacular white paper "How to Spot Phishing Attacks and Defend Your Business against Them" covers these topics in detail.

Educate employees about drive-by downloading. Let employees know how drive-by downloading works. Stress the importance of avoiding any web content flagged as a potential security threat by their web browsers or anti-malware software, as it might contain malvertising or other malicious code.

Make sure that Word macros are disabled. A ransomware attack can be initiated by malicious commands hidden inside a Word macro, as was done in the February 2016 Locky attack. Unless macros are regularly used in work files, receiving a legitimate file that contains a macro is rare, according to security experts.[11] For this reason, it is a good idea to make sure that macros are not allowed to automatically run. If you are not sure how to do this, see the "How to Make Sure Macros Are Disabled on Your Computers" drilldown discussion on page 8.

[11] Webroot, "A look at a typical macro infection"

Drilldown Discussion:
How to Make Sure Macros Are Disabled on Your Computers

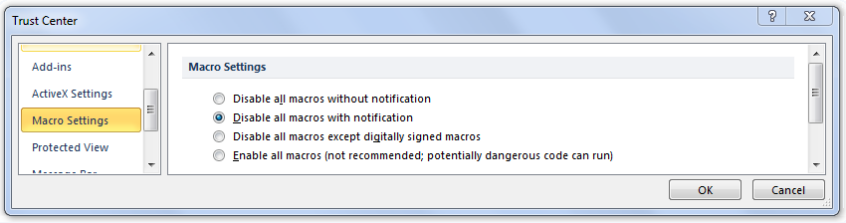
Ninety-eight percent of Microsoft Office-targeted threats use macros as the attack vector.[1] Thus, you should make sure that macros are not allowed to automatically run in Office applications (e.g., Word, Excel, PowerPoint). The only exception is if your organization regularly uses macros in files, in which case you might consider using digitally signed macros.

In Office applications, you have four macro settings from which to choose:

- **"Enable all macros".** When this setting is selected, all macros automatically run, without any notification. Both Microsoft and security experts recommend not using this setting.
- **"Disable all macros with notification".** This is the default setting. Macros are automatically disabled if they are present, but users get a security notification that reads "Macros have been disabled" accompanied by an "Enable Content" option. If users click that option, the macros run.
- **"Disable all macros without notification".** When this setting is chosen, macros are automatically disabled. Users do not get the security notification or the option to enable them.
- **"Disable all macros except digitally signed macros".** This setting is designed for organizations that use trusted publishers. If a file contains a macro that is digitally signed by a trusted publisher and the publisher has been added to the Trusted Publishers list on users' computers, the macro automatically runs. If the publisher is not in the Trusted Publishers list, the macro is disabled and users receive a security notification and the "Enable Content" option. Unsigned macros are disabled without any notification or option.

Each Office application has its own macro setting, so you need to check each one. Here is how to check the macro setting in Office 2010 and later applications:

1. Open any file in the application (e.g., open a DOCX file in Word or an XLSX file in Excel).
2. Select "Options" on the File menu.
3. Choose "Trust Center" in the left pane of the Options window.
4. Click the "Trust Center Settings" button in the right pane.
5. Select "Macro Settings" in the left pane of the Trust Center window.
6. Check to see which macro setting is selected in the right pane. If the "Enable all macros" setting is selected, change it to a more secure setting.



7. Click "OK" in the Trust Center window once the desired setting is selected.
8. Click "OK" in the Options window.

If your computers are running Office 2016 and your organization uses Group Policy, you have an additional way to block macros. You can take advantage of a macro blocking feature that Microsoft introduced in March 2016.[2]

---

[1] Microsoft, "New feature in Office 2016 can block macros and help prevent infection"

[2] Ibid.

Measures to Take in Case a Ransomware Infection Occurs

Cybercriminals are constantly devising new forms of ransomware and new ways to spread it. As a result, you need to take some measures in case a ransomware infection occurs. Specifically, you need to regularly back up your files and systems. You also need to test those backups.

Having restorable backups is important for another reason: Paying the ransom does not guarantee you will get your files back. The Kansas Heart Hospital in Wichita learned this the hard way.[12] After hospital officials paid the ransom, the cybercriminals gave them only partial access to their files and then asked for a second, larger ransom.

Plus, some amateur cybercriminals are trying to capitalize on the wave of ransomware attacks by sending out pseudo-ransomware. Dubbed Ranscam, this malware pretends to be ransomware. It displays a message that tells victims their files have been encrypted and they have to pay a ransom to get them back.[13] However, Ranscam deletes all their files, even if they have paid the ransom.

Waiting to Act Could Be a Costly Mistake

Now is the time to take action to prevent ransomware infections if you have not yet started. Waiting could be a costly mistake. Besides the expenses incurred from having to restore your systems and files, there will be lost income due to the disruption of your business operations.

We can help you take the necessary measures to protect your business from ransomware attacks. We can also help you set up effective backup and restore operations.

---

[12] Network World, "Kansas Heart Hospital hit with ransomware; attackers demand two ransoms"

[13] Talos, "When Paying Out Doesn't Pay Off"