All about Ransomware:

Ever wondered what all the ransomware fuss is about? You've heard about it at the office or read about it in the news. Maybe you've got a pop-up on your computer screen right now warning of a ransomware infection. Well, if you’re curious to learn all there is to know about ransomware, you’ve come to the right place. We'll tell you about ransomware’s different forms, how you get it, where it came from, who it targets, and what to do to protect against it.

What is ransomware?
Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card.

How do you get ransomware?
There are several different ways that ransomware can infect your computer. One of the most common methods today is through malicious spam, or malspam, which is unsolicited email that is used to deliver malware. The email might include booby-trapped attachments, such as PDFs or Word documents. It might also contain links to malicious websites.

Malspam uses social engineering in order to trick people into opening attachments or clicking on links by appearing as legitimate—whether that’s by seeming to be from a trusted institution or a friend. Cybercriminals use social engineering in other types of ransomware attacks, such as posing as the FBI in order to scare users into paying them a sum of money to unlock their files.

Another popular infection method, which reached its peak in 2016, is malvertising. Malvertising, or malicious advertising, is the use of online advertising to distribute malware with little to no user interaction required. While browsing the web, even legitimate sites, users can be directed to criminal servers without ever clicking on an ad. These servers catalog details about victim computers and their locations, and then select the malware best suited to deliver. Often, that malware is ransomware.

Malvertising and ransomware infographic.
Malvertising often uses an infected iframe, or invisible webpage element, to do its work. The iframe redirects to an exploit landing page, and malicious code attacks the system from the landing page via exploit kit. All this happens without the user’s knowledge, which is why it’s often referred to as a drive-by-download.

Types of ransomwar

There are three main types of ransomware, ranging in severity from mildly off-putting to Cuban Missile Crisis dangerous. They are as follows:

Scareware

Scareware, as it turns out, is not that scary. It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe.

A legitimate cybersecurity software program would not solicit customers in this way. If you don't already have this company's software on your computer, then they would not be monitoring you for ransomware infection. If you do have security software, you wouldn't need to pay to have the infection removed—you've already paid for the software to do that very job.

Screen lockers

Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine. However, the FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

Encrypting ransomware:

This is the truly nasty stuff. These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you. Unless you pay the ransom—for the most part, they're gone. And even if you do pay up, there's no guarantee the cybercriminals will give you those files back.

History of ransomware:

The first ransomware, known as PC Cyborg or AIDS, was created in the late 1980s. PC Cyborg would encrypt all files in the C: directory after 90 reboots, and then demand the user renew their license by sending $189 by mail to PC Cyborg Corp. The encryption used was simple enough to reverse, so it posed little threat to those who were computer savvy.

With few variants popping up over the next 10 years, a true ransomware threat would not arrive on the scene until 2004, when GpCode used weak RSA encryption to hold personal files for ransom.

In 2007, WinLock heralded the rise of a new type of ransomware that, instead of encrypting files, locked people out of their desktops. WinLock took over the victim screen and displayed pornographic images. Then, it demanded payment via a paid SMS to remove them.

With the development of the ransom family Reveton in 2012 came a new form of ransomware: law enforcement ransomware. Victims would be locked out of their desktop and shown an official-looking page that included credentials for law enforcement agencies such as the FBI and Interpol. The ransomware would claim that the user had committed a crime, such as computer hacking, downloading illegal files, or even being involved with child pornography. Most of the law enforcement ransomware families required a fine be paid ranging from $100 to $3,000 with a pre-paid card such as UKash or PaySafeCard.

Average users did not know what to make of this and believed they were truly under investigation from law enforcement. This social engineering tactic, now referred to as implied guilt, makes the user question their own innocence and, rather than being called out on an activity they aren't proud of, pay the ransom to make it all go away.

Finally, in 2013 CryptoLocker re-introduced the world to encrypting ransomware—only this time it was far more dangerous. CryptoLocker used military grade encryption and stored the key required to unlock files on a remote server. This meant that it was virtually impossible for users to get their data back without paying the ransom. This type of encrypting ransomware is still in use today, as it's proven to be an incredibly effective tool for cybercriminals to make money. Large scale outbreaks of ransomware, such as WannaCry in May 2017 and Petya in June 2017, used encrypting ransomware to ensnare users and businesses across the globe.

Mac ransomware

Not ones to be left out of the ransomware game, Mac malware authors dropped the first ransomware for Mac OSes in 2016. Called KeRanger, the ransomware infected an app called Transmission that, when launched, copied malicious files that remained running quietly in the background for three days until they detonated and encrypted files. Thankfully, Apple's built-in anti-malware program XProtect released an update soon after the ransomware was discovered that would block it from infecting user systems. Nevertheless, Mac ransomware is no longer theoretical.

Mobile ransomware

It wasn't until the height of the infamous CryptoLocker and other similar families in 2014 that ransomware was seen on a large scale on mobile devices. Mobile ransomware typically displays a message that the device has been locked due to some type of illegal activity. The message states that the phone will be unlocked after a fee is paid. Mobile ransomware is often delivered via malicious apps, and requires that you boot the phone up in safe mode and delete the infected app in order to retrieve access to your mobile device.

Who do ransomware authors target?

When ransomware was introduced (and then re-introduced), its initial victims were individual systems (aka regular people). However, cybercriminals began to realize its full potential when they rolled out ransomware to businesses. Ransomware was so successful against businesses, halting productivity and resulting in lost data and revenue, that its authors turned most of their attacks toward them. By the end of 2016, 12.3 percent of global enterprise detections were ransomware, while only 1.8 percent of consumer detections were ransomware worldwide. And by 2017, 35 percent of small and medium-sized businesses had experienced a ransomware attack.

Geographically, ransomware attacks are still focused on western markets, with the UK, US, and Canada ranking as the top three countries targeted, respectively. As with other threat actors, ransomware authors will follow the money, so they look for areas that have both wide PC adoption and relative wealth. As emerging markets in Asia and South America ramp up on economic growth, expect to see an increase in ransomware (and other forms of malware) there as well.

What to do if you're infected

The number one rule if you find yourself infected with ransomware is to never pay the ransom. (This is now advice endorsed by the FBI.) All that does is encourage cybercriminals to launch additional attacks against either you or someone else. However, you may be able to retrieve some encrypted files by using free decryptors.

To be clear: Not all ransomware families have had decryptors created for them, in many cases because the ransomware is utilizing advanced and sophisticated encryption algorithms. And even if there is a decryptor, it's not always clear if it's for right version of the malware. You don't want to further encrypt your files by using the wrong decryption script. Therefore, you'll need to pay close attention to the ransom message itself, or perhaps ask the advice of a security/IT specialist before trying anything.

Other ways to deal with a ransomware infection include downloading a security product known for remediation and running a scan to remove the threat. You may not get your files back, but you can rest assured the infection will be cleaned up. For screenlocking ransomware, a full system restore might be in order. If that doesn't work, you can try running a scan from a bootable CD or USB drive.

If you want to try and thwart an encrypting ransomware infection in action, you'll need to stay particularly vigilant. If you notice your system slowing down for seemingly no reason, shut it down and disconnect it from the Internet. If, once you boot up again the malware is still active, it will not be able to send or receive instructions from the command and control server. That means without a key or way to extract payment, the malware may stay idle. At that point, download and install a security product and run a full scan.

How to protect yourself from ransomware:

Security experts agree that the best way to protect from ransomware is to prevent it from happening in the first place.

Read about the best ways to prevent a ransomware infection.
While there are methods to deal with a ransomware infection, they are imperfect solutions at best, and often require much more technical skill than the average computer user. So here's what we recommend people do in order to avoid fallout from ransomware attacks.

The first step in ransomware prevention is to invest in awesome cybersecurity—a program with real-time protection that's designed to thwart advanced malware attacks such as ransomware. You should also look out for features that will both shield vulnerable programs from threats (an anti-exploit technology) as well as block ransomware from holding files hostage (an anti-ransomware component). Customers who were using the premium version of Malwarebytes for Windows, for example, were protected from all of the major ransomware attacks of 2017.

Next, as much as it may pain you, you need to create secure backups of your data on a regular basis. Our recommendation is to use cloud storage that includes high-level encryption and multiple-factor authentication. However, you can purchase USBs or an external hard drive where you can save new or updated files—just be sure to physically disconnect the devices from your computer after backing up, otherwise they can become infected with ransomware, too.

Then, be sure your systems and software are updated. The WannaCry ransomware outbreak took advantage of a vulnerability in Microsoft software. While the company had released a patch for the security loophole back in March 2017, many folks didn't install the update—which left them open to attack. We get that it's hard to stay on top of an ever-growing list of updates from an ever-growing list of software and applications used in your daily life. That's why we recommend changing your settings to enable automatic updating.

Finally, stay informed. One of the most common ways that computers are infected with ransomware is through social engineering. Educate yourself (and your employees if you're a business owner) on how to detect malspam, suspicious websites, and other scams. And above all else, exercise common sense. If it seems suspect, it probably is.

Keep up to date on the latest ransomware news in Malwarebytes Labs.