WHAT IS RANSOMWARE?

Ransomware is a form of malware, or malicious software, used to encrypt sensitive files held in business and personal devices, essentially locking users out of their own data or networks. Once deployed, the ransomware encryption restricts access to files and the victim receives a notice that a “ransom” must be paid to unlock the data or device. The ransom request often requires payment by Bitcoin or other types of anonymous cryptocurrency. Access to data is supposed to be restored once the ransom is paid and the attackers provide a decryption key.

In a trend increasing in frequency, that data is often also stolen — either to demand additional payments from the victim or to sell it on the dark web.

Recently, there has been an escalation of ransomware incidents making headlines, including high-profile attacks on energy, financial services, healthcare and even cybersecurity industries. The FBI and Cybersecurity and Infrastructure Security Agency (CISA) reported a 62% increase in ransomware activity during the first half of 2021 over the same period the previous year.

With the rapid shift to remote work by millions of Americans and the threat of phishing, consumers and business are all at increased risk of ransomware attacks.

WHY IS RANSOMWARE INCREASING?

Ransomware is increasing in use because it works. One mistake by a single user has the potential to expose an organization’s entire network. Many people and organizations — up to 83% — admit to paying the ransom, giving criminals an easy way to make money without the hassle of breaking into bank accounts. (They may do that too, though, if they can access financial or personal information during a ransomware attack.)

Ransomware can be another way for cyberthieves to get their hands on your personally identifiable information (PII) while also profiting from the organizations and individuals urgently trying to regain access to their data.

While not every ransomware attack is labeled a data breach, they increasingly result in exposed data on the dark web. Likewise, not every data security incident is a reason to panic. Breaches come in a variety of sizes and personal data breach risk levels. The combined total of this activity over time paints the picture of the risks you might face — because once your PII is in the hands of an identity thief, you could be susceptible to more than a dozen types of identity theft and fraud.

HOW DOES A RANSOMWARE ATTACK WORK?

1. **Infiltration.** Ransomware often begins with phishing emails — a type of social-engineering attack that tries to fool the target into thinking the email is from a trusted sender, convincing them to open an infected attachment or click a link that downloads the malware. These attacks can be disguised as a fake invoice, holiday discount, updates from a trusted company or information on current events that makes the recipient more likely to click. Ransomware can be spread through other social engineering attacks (such as baiting or scareware), downloads from fake websites or clicking on malvertising: a fake ad that contains the ransomware.
2. **Encryption.** Once downloaded, the attack can either start encrypting files or give the criminal access so they can search for valuable business and personal files before encrypting them. In either case, the victim is left without access to the encrypted files.
3. **Extortion.** The files cannot be recovered without a decryption key known only by the attacker. When attempting to gain access, the victim will then find a message warning of the ransomware attack with instructions on how to complete the ransom payment, typically with a countdown of only a few days to heighten urgency and prompt victims to pay quickly.
4. **Exfiltration.** Ransomware gangs may also try to maximize their profits by not only blocking user access to sensitive, proprietary, business-critical data, but by stealing those files before encrypting them. The criminals can then blackmail the user for an additional payment to stop them from making the data public. They might also sell the stolen data to the highest bidder on the dark web.
5. **Removal (Maybe.)** Even paying the ransom doesn't completely stop ransomware because the malware remains on your device or computer until it is manually removed.

WHO DO ATTACKERS TARGET WITH RANSOMWARE?

Currently, attackers often focus their attention on larger organizations with large amounts of data and that always need access to their files. Not only do these companies typically have the resources to pay a ransom, but they also have added incentives to pay quickly. Unscheduled downtime can be expensive — up to $300,000 per hour or more, depending on the size of the organization. They also want to avoid reputational damage to their business.

In addition to businesses, local government agencies, schools and universities and healthcare organizations have become favorite targets of ransomware gangs.

While the ransomware gangs have focused primarily on large businesses, that does not mean individuals and small businesses are not at risk. On the contrary, three trends suggest they may see greater risk:

1. **Working from home.** While there are many benefits to both the employee and the employer, home networks and devices are typically not as secure as those inside the corporate network's protection. That makes remote workers an attractive target for cybercriminals looking for an easy entry point to access company data.
2. **Use of automation by cybercriminals.** Automation makes targeting small businesses and individuals as easy as targeting large companies.
3. **Ransomware as a service.** Ransomware gangs have adopted the "as a service" business model so anyone looking to make a quick buck can distribute ransomware. Distributors don't need any technical skills; they just spread the malware and share the profits with the ransomware gang. As these low-level cyberthieves look for targets, SMBs and individuals may find themselves in the crosshairs more frequently.

5 WAYS TO PROTECT AGAINST RANSOMWARE ATTACKS

1. **Validate a link before clicking on it.** Even though online surfing can take you from news stories to kitten videos in mere seconds, slow down. Attackers rely on users who will click on links in emails or fraudulent links on websites. Stop ransomware by making sure those links are legitimate before you surf.

2. **Back up your data regularly.** Creating a full backup of your computer (including files, applications, operating system, preferences etc.) ensures you always have a clean copy of your data that you can restore from in the event of a ransomware attack (or any other disaster). Regularly updating the backup and disconnecting the storage device from the computer once created (so it cannot be infected) makes restoring your system easier if you have to wipe your hard drive.
3. **Finetune your email spam filters.** Common ransomware arrives in emails with attachments that have ".EXE" or "PDF.EXE" as a file extension. If you can filter these files by extension, you can flag or block emails that include that designation. If you use these types of executable files in your business, arrange for clients and colleagues to use password-protected ZIP files instead.
4. **Update your software.** Install software updates and patches when they're available as they can close newfound software vulnerabilities exploited by cybercriminals.
5. **Use security tools.** Computer protection comes in many forms, from anti-virus to anti-phishing and anti-keylogging. Worried about mobile security? Look for tools such as Mobile Attack Control that can warn you of rogue apps, spyware, fake networks and other mobile risks. Consider a virtual private network (VPN) for your mobile device to further enhance personal and financial safety online.

PROTECT YOUR ORGANIZATION AGAINST RANSOMWARE ATTACKS

In addition to the personal protection guidelines described above, the following tips can help reduce the risk of an employee exposing your business to a ransomware attack.

1. **Train employees to distinguish malicious emails.** Employees can be the first line of defense or weakest link in your company's cybersecurity. Continuous educational and engaging training can help them spot potentially malicious links, attachments and websites, and understand how to report issues to your IT department or InfoSec team.
2. **Keep software updated.** Check for updates regularly on all your connected devices and send reminders to remote employees, as software security patches are released often. These updates help performance and close known security gaps to reduce the possible ways criminals can attack your systems. All it takes is one unpatched vulnerability to give a cybercriminal access.

3. **Isolate infected devices immediately.** Don't give malicious code the opportunity to spread across your network. Once a device has been identified as infected, disconnect it from the network immediately.
4. **Create a continuity plan.** Have a disaster recovery plan in place along with a solution for backing up all business data on all systems and devices. Determine the data and systems that are vital to your business operations and prioritize a backup and recovery plan. When you understand how a ransomware attack could affect your business and plan for contingencies, you can reduce the severity of an attack and recover that much quicker when it happens.
5. **Report the incident.** If you are targeted by ransomware, be sure to report the incident to authorities, regardless of the outcome, such as the FBI's Internet Crime and Complaint Center IC3 or the United States Computer Emergency Readiness Team (US-CERT). Also, note that the FBI does not advise any person or business to pay a ransom in response to a ransomware attack, as there is no guarantee that you will get any data back from the cyberthieves.