How malware poses risk to your business:

Malware comes in many shapes and sizes but one of the most notable types is ransomware. According to ibm.com “Ransomware is a type of malware that holds a victim’s data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker.” Ransomware can cause financial damage to business assets as well as cause substantial amounts of downtime to business-critical services such as web applications. The most notable ransomware variant is WannaCry ransomware, which has done considerable damage to businesses across the world. According to Cisa.gov WannaCry ransomware tries to exploit windows machines running the smbv1 service, which it uses to push itself through a network like a worm. It is also said that if you do happen to be infected it is best to isolate all devices from the network and restore from clean backups. You should never try to pay a ransom on any infected device instead of restoring devices from a backup.

The next thing to consider is why threat actors create and spread ransomware. Threat actors are motivated by many reasons but when it comes to ransomware it is usually for financial reasons. The whole premise of this type of malware is that it infects your filesystem by encrypting it then you are promised a decryption key in exchange usually for bitcoin or some other form of cryptocurrency. Ransomware a lot of the time is made by hacker groups. According to checkpoint.com WannaCry was allegedly developed by a group called “Lazarus” A group that originated in North Korea. The Lazarus group is now seen as an Advanced persistent threat. Malware and viruses have been a problem for more than 40 years, but the more advanced computers get so do viruses/malware. Ransomware is not only a type of malware, but it is business oriented for groups. Hacker groups need funds to continue running so making ransomware can provide a ROI which makes sense from the perspective of a threat actor. However, it is not ethical to launch ransomware attacks on businesses.

The next type of malware that can cause damage to your business is a rootkit. Rootkits are malicious software programs usually designed to run undetected. A rootkit is usually used to plant backdoors in systems and watch targets for extended periods undetected. Smart attackers can use rootkits to exfiltrate information out of your business. Rootkits can be used to gather and sell confidential information about your business and to launch attacks within your business. Rootkits can be installed in many ways such as plugging a malicious thumb drive into your computer, or through the click of a suspicious link. Rootkits often stay undetected in PCs for an exceedingly long time. Another thing that is not great about rootkits is that they can be stored into your bootloader or firmware making it difficult to remove it from your computer. Rootkits can even be kernel level which is deep level access that the attacker would have against your machine. Overall rootkits are dangerous to your business since they can have full control over your system and monitor your activity and further plant malware into your system or even network. To remove rootkits the best thing you can do is restore them from a clean backup. The best thing to do to avoid rootkits is to make sure that your hardware, software, and operating system are all up to date and to avoid using legacy operating systems, and or hardware as these are vulnerable to being taken advantage of by rootkits.

The next type of malware that can inflict damage to your business is spyware. One of the most well-known types of spyware is a keylogger which is designed to log your keystrokes and then usually send the results to either a c2 server or email. Keyloggers are dangerous to your business if undetected because they can grab your credentials of personal or business-related accounts. Keyloggers are usually used to gather passwords or banking information. Keyloggers can be used to gather information to spy on people too such as search history. Regardless keyloggers are usually used for nefarious purposes Keyloggers come in two forms, one being in a software format that needs to be installed, the other being hardware based which usually plugs into a USB port into a computer. You can mitigate these threats by blocking or disabling USB ports in windows settings.

Another attack method your company should be aware of is called "phishing." According to omegasystemscorps.com "PHISHING – a form of cyberattack that tricks people into sharing sensitive information or taking destructive actions through seemingly harmless emails and messages." To give an example of this definition a threat actor could target the email address of a CEO and pretend to be an IT (Information Technology) helpdesk worker claiming the CEO needs to reset their password and to click a link where they can reset their password that redirects them to a malicious website where the CEO could accidentally enter their credentials into this malicious website. The scary thing about phishing is that it is usually calculated and targeted against businesses trying to gather money or network access. One big example of a phishing attack that had devastating consequences against a business according to bluevoyant.com is "Between 2013 and 2015, a phishing campaign caused Facebook and Google losses of $100 million. The attackers took advantage of the fact that both companies had a Taiwanese supplier called Quanta. The attackers sent a series of fake invoices, pretending to be from Quanta, and the invoices were paid by Facebook and Google. Eventually, the fraud was discovered, and Facebook and Google took legal action." This is just one example of a phishing attack that caused 100 million dollars of damage to two of the biggest technology companies in the world.

Something to be aware of with malware and social engineering attacks is that they can cause severe damage to your business. The damage that these attacks can cause to your business is financial, reputational, and trust of your company in general. A big example of an attack that took place in 2020 was the SolarWinds attack. According to Cisecurity.org (Center for internet security) the SolarWinds attack happened through a supply chain exploit that allowed threat actors to place a backdoor into the software of the SolarWinds platform causing direct harm to hundreds of businesses. Through planting a backdoor in one software program alone many different businesses were compromised due to the back door in the software. Something scary about supply chain issues is that they usually will not just compromise one business but compromise many businesses. Diving deeper into the malware/backdoor that was implanted into SolarWinds products it was found through crowdstrike.com more information about the backdoor. According to crowdstrike.com sunspot malware implanted the sunburst backdoor into the SolarWinds product. In the technical analysis section, it was said that the malware was most likely created on 2-20-2020. The hash of the malware is

“c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168” which when pasting this hash into virustotal.com there are 56/73 security vendors that flagged this hash as malicious and three sandboxes that flagged the hash as malicious. According to techtarget.com this piece of malware infected Microsoft systems and affected its customers in a negative fashion. This piece of malware not only infected many businesses, it infected one of the biggest technology companies in the world. This shows how much impact and financial damage even one piece of malware can cause to your business or other businesses in this example. This also shows why cybersecurity and monitoring the supply chain of your business is an important aspect of keeping your business as risk free as possible. As criminals become increasingly advanced malware has become more of a business model for criminals to gain profit compared to relatively harmless “malware” viruses of the 80’s to early 2000’s. Advanced persistent threats are a threat to your company and its information, and this is why your company needs to be prepared for cyber risks and threats that could harm your organization. As network security advances so do threat actors and the malware they create that can pose threats to your organization. Threat actors a lot of the time will try to gather ransoms or exfiltrate confidential information from your organization as these both can help them gather profits.

Another example of malware that had a significant impact on businesses is the Mydoom virus. According to allaboutcookies.org the Mydoom virus caused businesses 38 billion dollars (about $120 per person in the US) worth of damage in 2004. This virus spreads through infected machines that will send emails to other computers. 38 billion dollars through a single malicious program is hard to wrap your head around. This again goes to show how much financial risk malware can pose to your business.

The first step to mitigating risk is to have the knowledge that the risk is possible in the first place. There are many ways to mitigate malware from your systems. First, to prevent phishing emails your organization should be implementing a phishing training program. The next thing your organization should do is implement EDR’s (Endpoint Detection and response) into all endpoints within your organization if your budget allows you to do so. If your company has the budget to do so they should consider hiring network security professionals to help prevent breaches and in the case of a breach to prevent the malware from wreaking havoc within your organization. Malware poses a major risk to your business but at the same time there are many things you can do to mitigate malware and other cyber-attacks within your business. It is important to keep up to date on cyber breaches and cyber-attacks as well as new malware that can pose threats to your organization. As cybercrimes increase the likelihood of your business being affected by cybercrime and malware increases. Another thing you can do for your business is hire a Penetration tester (In layman's terms ethical hacker) that performs tests against specified targets such as a web application server that helps gauge your company’s current network security position. To summarize, you can mitigate risks by performing phishing training against end users, hire network security professionals, buy and implement EDR software on endpoints, and hiring a pentester to test your organizations network security and how it handles attacks from an outside or insider threat actor.

Sources cited:

"What Is Ransomware?" *IBM.com*, IBM, www.ibm.com/topics/ransomware. Accessed 3 Apr. 2024.

"What Is WANNACRY/WANACRYPT0R?" *Cisa.Gov*, National Cybersecurity and Communications Integration Center, www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf. Accessed 3 Apr. 2024.

Burdova, Carly. "What Is a Rootkit and How to Remove It? ." *Avast.Com*, Avast-Academy, 22 July 2021, www.avast.com/c-rootkit.

Gillis, Alexander S. "Keylogger (Keystroke Logger or System Monitor)." *Techtarget.Com*, Tech Target, www.techtarget.com/searchsecurity/definition/keylogger. Accessed 3 Apr. 2024.

"How Phishing Can Impact Your Business." *Omegasystemcorp.Com*, omegasystemcorp, https://omegasystemscorp.com/insights/blog/how-phishing-can-impact-your-business/. Accessed 3 Apr. 2024.

"8 Devastating Phishing Attack Examples (and Prevention Tips)." *Bluevoyant.Com*, Blue Voyant, www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips. Accessed 3 Apr. 2024.

CrowdStrike intelligence team. "SUNSPOT: An Implant in the Build Process." *CrowdStrike. Com*, CrowdStrike, 11 Jan. 2021, www.crowdstrike.com/blog/sunspot-malware-technical-analysis/.

"The SolarWinds Cyber-Attack: What You Need to Know." *Cisecurity.Org*, Center for Internet Security, 15 Mar. 2021, www.cisecurity.org/solarwinds#Resources.

Croft, Patti. “11 of the Most Dangerous Computer Viruses and How to Avoid Them.” Edited by Catherine McNally, *Allaboutcookies.org*, All About Cookies, 28 Feb. 2024, allaboutcookies.org/most-dangerous-computer-viruses.

Oladimeji, Saheed, and Sean Michael Kerner. “SolarWinds Hack Explained: Everything You Need to Know.” *Techtarget.Com*, Tech Target, 3 Nov. 2023, www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.