THE RANSOMWARE THREAT TO COMPANIES

Just like computers, malware have evolved over the years. First, malware were just generic computer viruses, but categorizing and defining malware types soon became necessary to better understand and defend against malicious software. Computer users started hearing and learning terms such as worm, trojan, and rootkits. Each malware did something unique and posed a different threat to computers and companies. The companies defending against malware had to change their processes over time to address the ways the computers could be infected by the malware.

Computer security to protect against malware began with floppy disks being write-protected before being inserted into a computer. Floppy disks were then replaced with CD-ROMs and eventually thumb drives. With the growth of email, attachments were the easiest way for a computer to be infected. The internet then provided the ability for drive-by downloads and compromised websites. Users were told they could not trust any links in those emails. The list goes on and on.

The current scare word in malware is ransomware. When activated, ransomware encrypts the contents of a computer, and the user can only see a single screen explaining that their data are lost and they need to make a payment to return those data. The money is usually requested in Bitcoin to make the payment harder to trace. A deadline is sometimes given or a countdown clock appears to add to the urgency of the issue.

For a company, the danger is that one system is usually not the only part of the network that is infected. Often, one attack is just the first sign that the hackers are in the network and have been for some time. One system quickly becomes multiple systems, and the systems that are not infected by the ransomware are usually shut down or disconnected by the company to prevent further spread. Company data have often already been exfiltrated out of the network by this point, and the ransomware are just a way to cover the attacker's tracks in addition to getting paid.

Colonial Pipeline was the victim of a ransomware attack that made the news in May 2021. The pipeline, which carries approximately 45 percent of the U.S. East Coast fuel supply, had to be shut down after a ransomware attack. The shutdown caused fuel shortages and a rise in gas prices up the East Coast.

While the attack brought down a critical piece of energy infrastructure, debate has occurred regarding whether the shutdown was the goal or if the company was just a target of opportunity. The critical nature of the shutdown gave the company a higher incentive to pay for the decryption keys; however, such a highly visible attack brought the full weight of law enforcement organizations on the attackers.

In this case, the company paid $4.4 million in Bitcoin for the decryption keys, but the decryption keys were only the start of the remediation process. Data were already exfiltrated from the company, which needed to be addressed. For noncritical systems, replacing or restoring from backup files is often easier and quicker than decrypting. The systems with critical data that were decrypted might have other malware or software left behind by the hackers and need recreation from clean images. The full extent of the invasion is seldom completely defined, and the cleanup from the incident is likely to cost additional millions of dollars.

How does a company justify choosing to pay the ransom? In a quote from the company CEO, "It was the right thing to do for the country." But this decision is also controversial. According to the U.S. Department of the Treasury, paying ransomware could violate economic sanctions to a banned foreign entity or group, and the company could be held civilly liable for the action, which would turn the victim of the crime into a criminal.

Would you pay if ransomware took over your company? Would you call law enforcement and have the breach become public knowledge? These questions test the ethics, values, and moral code of impacted companies. In a better world, no one would pay the ransom, and the attacks would stop. Companies would be commended for fully disclosing events for the greater good rather than protecting their company image. As an industry, we are moving in the right direction with such publicized discussions.

Start planning now before your company finds itself in a crisis. Assess your current cybersecurity posture, build your security policies and procedures, and engage with an experienced and trusted cybersecurity partner for advice and direction.

For more information please contact Rick Bush, Cybersecurity Architect, RESPEC, rick.bush@respec.com.

RESPEC

Rick Bush

CISSP GCIH GPEN GCFE

CyberSecurity Architect

RESPEC