Ransomware Threats

Bank of America Merrill Lynch

Crimes involving ransom have existed since the beginning of time. Bad actors are always looking for ways to exploit businesses. Ransomware is quickly becoming a formidable force in the cyber threat landscape. Ransomware is growing due to easy access and anonymity of digital currency payment options and advancements in malware. Ransomware security attacks may compromise systems in a matter of minutes and businesses must have a strategy and plan to minimize business impact and data loss.

What is ransomware?

Ransomware is malware that can lock up any type of internet connected device, preventing access to stored information or functionality until a financial ransom is paid. Ransomware is one of the most destructive types of cybercrime, with many victims unable to recover lost information and assets encrypted by criminals.[1] Ransomware has grown rapidly in popularity among cybercriminals as they see these attacks monetized directly and easily. The preferred method of infection is through phishing email campaigns. These typically include a malware-laden attachment disguised as an invoice or receipt. Once the attachment is opened and the malware executes, file encryption commences.[2]

How does ransomware impact my business?

Financial impact. A key factor an organization must determine is whether or not to pay a ransom. While law enforcement and cybersecurity experts typically recommend against it, up to 64% of organizations have shown a willingness to pay demands.[3] While each organization that agrees to pay a ransom hopes to recover their information, many do not. Whether by design or accident, some ransomware attacks encrypt information without a path to recovery. This leads to greater financial impacts. Additionally, not sending the necessary decryption keys, bad actors then increase the ransom demands incrementally after each payment deadline is missed. Depending on the extent of the information and resources locked up by encryption, the recovery costs and associated business productivity downtime can be extreme.

Business disruption. Bad actors use ransomware attacks to encrypt information without a path to recovery. The purpose of these attacks is disrupting or destroying an organization, rather than make money for the cybercriminals. Only approximately 47% of victims who paid a ransom actually got their data back.[4] This type of non-monetary attack is typically deployed by Nation State threat actors and Hacktivist organizations whose primary goal is to cause embarrassment to the organization or business.

Ransomware decoys. A recent trend is ransomware used as a decoy, distracting attention from a primary cyberattack simultaneously conducted. The primary goal of the cyberattack is data theft, often stealing thousands of files from an organization. When thus objective is met, fraudsters cover their tracks by deploying fake ransomware that wipes the evidence of the earlier data theft.[5] Encrypting hard drives with ransomware malware makes forensics investigations virtually impossible, so unless investigators are paying attention, these attacks mimic ransomware, rather than potentially more damaging corporate espionage.

Evolving Strategies

Email phishing campaigns remain the favorite ransomware delivery mechanism due to ease of use.[6] Phishing campaigns use social engineering tricks to lure recipients into opening emails and attachments. Phishing exploits the victim's likelihood to trust, believing an email came from a legitimate source. Once trust is achieved, the fraudster baits them into activating the ransomware.

Ransomware as a service. Because ransomware is

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[2] https://www.symantec.com/security-center/threat-report
[3] https://www.symantec.com/security-center/threat-report
[4] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[5] https://www.symantec.com/security-center/threat-report
[6] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

successful, bad actors are providing ransomware infrastructure and experience for sale.[7] Sellers of prebuilt ransomware solicit the products for a certain percentage of the buyer's profit and the buyer is free to infect victim's devices. This is a mutual benefit, wherein the seller remains anonymous while gaining a percentage of the attack profit and the buyer can perform ransomware attacks without needing technical skills.

Network lingering. As organizations increase cybersecurity awareness, backing up sensitive data and storing it in remote locations, fraudsters take their time, lingering on networks and devices locating and encrypting the most sensitive and critical data, including critical backups with ransomware. This approach also allows cybercriminals time to create back doors in systems for remote access in the future.[8]

Best Practices

Education. Continuous security education and training programs are the most successful ways to thwart attacks. The goal of an effective education program is educating users about current schemes and how to use their devices more securely. Organizations should test their users continuously with hands-on exercises, such as fake phishing emails, to ensure that proper cyber hygiene is observed.

Creating backups is one of the most important steps an organization can take to secure its data. Restoring data from backups after a ransomware attack is preferred over paying ransom without a guarantee that the data will be recovered.[9] Based on the likelihood that cybercriminals may attempt to encrypt backups during an attack, disconnect backups physically and logically from source data.

Staying vigilant helps organizations protect critical data and assets. Develop a proactive strategy that addresses ransomware risks. Conduct tabletop exercises to determine the survivability of a ransomware attack.

Conclusion

Ransomware is one of the most critical online threats faced by organizations and consumers. Based on current trends, it appears that this will continue into the foreseeable future. Organizations and consumers need to remain vigilant to detect and defend against ransomware attacks. Patching systems, effective data backup strategies, and robust user awareness and training are the primary defenses that guard against ransomware attack impacts.

For more information

For more information about Risk assessments and Incident response plans, visit our Fraud Education site through CashPro Assistant at: https://cashproonline.bankofamerica.com/cpocms/sites/CashProUniversity/Landing/Fraud/page.htm

[7] https://www.securitymagazine.com/articles/88786-ransomware-as-a-service-hackers-big-business

[8] https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-Ransomware_POV_noCM_AODA.PDF

[9] https://krebsonsecurity.com/2016/01/ransomware-a-threat-to-cloud-services-too/