Fueling the Fire: How Extortion Has Changed the Face of Data Breaches

02/17/2020

Ransomware attackers typically encrypt victims' data and demand ransom in exchange for the decryption keys. Ransomware is not a new cybercriminal activity. In fact, ransomware attacks are over 30 years old.[1] However, around the mid-2010's, ransomware attacks really took off, growing in prominence, volume and sophistication. Where once ransomware developers wrote their own code, modern attackers utilize more sophisticated 'off the shelf' options and ransomware-as-a-service, which made household names of CryptoLocker and Locky. Not stopping there, attackers upped their game in terms of methods of delivery and algorithms. As sophistication rose, so did ransom demands. CryptoLocker extorted $3 million for its creators by 2013 and its variant, CryptoWall, exceeded the $18 million mark by 2016.

Threats to leak stolen data online are also not new, but the actual publishing of data has been few and far between. This led to victims to believe that attackers could not access the data itself, so ransomware attacks have historically not been viewed as data breaches by its victims. However, this perception is quickly changing.

In 2019, we saw Maze ransomware and its variants, such as Sodinokibi and DoppelPaymer, raise the stakes again. These attackers are now maximizing the payout by not only deploying crypto-locking malware, but also stealing data prior to locking the system. Adding insult to injury, these attackers pressure their victims by threatening to or actually publishing stolen data when victims fail to meet ransom deadlines. Even worse, they have also placed stolen content for sale on the dark web.

Maze ransomware attackers began reeking havoc in the United States in November 2019 when it attacked Allied Universal, a California-based security company, demanding 300 bitcoins (approximately $2.3 million) to decrypt the network, and threatened if their ransom was not paid, Allied's files would be released. When Allied missed the ransom payment deadline, attackers published 700 MB of data and files. Some of this information included termination agreements, contracts, medical records, server directory listings, encryption certificates and exported user lists from active directory servers.

Ransomware operators got serious in December 2019, attacking the City of Pensacola, Florida and publishing stolen information when the City failed to pay the ransom. However, with its attack on Southwire, a Georgia wire and cabling company, attackers took its publication to a new level. The ransomware attackers demanded 850 bitcoin (nearly $6 million) in ransom. When the demand was not paid, attackers built a website using an Irish ISP to publish the stolen data. Some of the information typically disclosed by Maze includes the initial date of infection, several stolen Microsoft Office, text and PDF files, the total volume of files taken from victims, IP addresses and infected server machine names. Southwire ultimately obtained an injunction in Ireland to force shut down of the ISP and has filed suit against its "John Doe" attackers in federal court in Georgia for violation of the U.S. Computer Fraud and

Abuse Act. However, Maze attackers have registered two public sites hosted by two companies incorporated in China.

In January, Maze ransomware attacks have potentially impacted between 45 and 180 victims, prompting the FBI to issue a warning that these attacks have increased on the private sector. Its victims include businesses in the accounting, construction, medical and legal professions.

Maze has not been shy about monetizing its activities by requiring separate ransoms for decryption and for deletion of the stolen information. Once upon a time, victims may have been able to avoid reporting incidents if there was evidence confirming data was not accessed or used, but extortion complicates this matter. Now, ransomware attacks are data breaches and victims need to be concerned about recovering their files and how to address if their stolen unencrypted files were leaked to the public.

---

[1] The first known ransomware attack occurred in 1989 when Joseph Popp, PhD, an AIDS researcher, distributed 20,000 floppy disks to fellow AIDS researchers in 90 countries saying the disks contained a computer-based application that gauges a person's risk of contracting AIDS based on a questionnaire. However, Dr. Popp had infected the disks with malware with what became known as the digital version of the AIDS virus. https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html