RANSOMWARE ATTACKS ARE DATA BREACHES AND FINALLY STARTED TO BE REPORTED PROPERLY BY MAJOR COMPANIES

SERGIO GUIDA
Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: Cybersecurity - data breach - Ransomware attacks

Category: Legal Area

Several big corporate victims of ransomware attacks realized that those are data breaches and began to notify employees and clients about stolen data.

Usually, pirates steal unencrypted files before encrypting a breached network, then they use these stolen files as leverage by threatening, if a victim does not pay the ransom, to sell the data or leak, publicly posting them on 'data leak sites' created just to shame the victim.

As reported by Bleeping Computer (a resource site for answering computer, security, and technical questions. All services to the public are free and their analyses on newly detected ransomware families have been covered in major media ranging from NBC News to the BBC), "this tactic is being conducted by almost all ransomware operations".

The data stolen in these attacks can be damaging to a company as it commonly includes financials, trade secrets, unpublished reports, and emails. It's also a massive problem for employees whose social security numbers, passports, medical records, termination letters, bank accounts, salary information, and more are stolen in this attack: they are data breaches, indeed.

Unfortunately, "many companies choose to sweep ransomware attacks under the rug and do not adequately disclose that personal data was stolen, even to employees who were affected.

Numerous times in the past, employees of attacked firms have contacted Bleeping Computer to learn more about what was stolen in an attack because the company they work for was denying it" and not providing any information.

First of all, "the denial of stolen data is not fair to employees, as the attackers could use their stolen personal information for identity theft and fraud. If an employee does not know what happened, they have no way to protect themselves". But recently "corporate victims are finally starting to issue data breach notifications when affected by a ransomware attack" and "most of them offer free credit

monitoring and identity theft protection to affected employees and clients so that they can be alerted if their data is used publicly or for fraud".

Some of the major companies that Bleeping Computer has seen issuing data breach notifications include RailWorks (a US Railroad Contractor), ExecuPharm (a Global Functional Service Contract Research Organization, who provides clinical research support services for the pharmaceutical industry), Cognizant (one of the largest IT managed services company in the world); those companies "should be lauded for not only doing what they are supposed to under privacy laws but also doing the right thing by their employees".

Moreover, in some particular sectors, pirates' attacks have much heavier consequences especially for customers and final users.

One first example is the healthcare sector. The end of 2019 saw a host of ransomware attacks and vendor-related breaches that outpaced previous years: a whopping 41.4 million patient records breached in 2019, fueled by a 49 percent increase in hacking. And despite the COVID-19 crisis, the pace of healthcare data breaches in 2020 continues to highlight some of the sector's biggest vulnerabilities.

As seen with the biggest healthcare data breaches of the year, providers still have a great deal of work to do when it comes to securing remote connections, properly disposing documents, and educating users to prevent the frequency of successful phishing attacks – as well as delays in detection and breach notifications.

It will be enough to summarize some details of the 'Magellan Health Data Breach': the extent of the ransomware attack that hit Magellan Health (an American for-profit managed health care company, focused on behavioral healthcare, ranked 475 on the Fortune 500 in 2018) in April became clear in July, with eight Magellan Health affiliates and healthcare providers reporting breaches stemming from the incident. The company was the victim of a sophisticated cyberattack, in which hackers first exfiltrated data before deploying the ransomware payload. By leveraging a social engineering phishing scheme that impersonated a Magellan client, the attackers were able to gain access to the system five days before the ransomware attack.

The investigation determined hackers first installed malware able to steal employee credentials and passwords to gain access to the affected server; patient data was also compromised in the event, including health-related information such as health insurance account data and treatment information. With its tally of 365,000 breach victims, the Magellan incident is the third-largest reported healthcare data breach in 2020, so far. The second example is the semiconductors & related devices industry. System-On-Chip maker MaxLinear (a New York Stock Exchange-traded company and a provider of

RF, analogue, and mixed-signal integrated circuits for the connected home, industrial, and infrastructure applications) disclosed that some of its computing systems were encrypted by Ransomware operators, after an initial breach that took place in April.

In the data breach notification, MaxLinear states "we immediately took all systems offline, retained third-party cybersecurity experts to aid in our investigation, contacted law enforcement, and worked to safely restore systems in a manner that protected the security of information on our systems". The company says that this leaked information could include personally identifiable (PII) and financial information such as "name, personal and company email address and personal mailing address, employee ID number, driver's license number, financial account number, Social Security number, date of birth, work location, compensation and benefit information, dependent, and date of employment."

The company also states that the incident has led to an enterprise-wide password reset and that the breach was disclosed to the appropriate law enforcement authorities.

Source: bleepingcomputer.com/news/security.

Link: https://www.bleepingcomputer.com/news/security/companies-start-reporting-ransomware-attacks-as-data-breaches