Jamison Stalter

A study of Cyberattacks

In the early summer of 2017 Equifax was subject to a series of cyber attacks from May to July. Compromising the personal information of over 147 million Americans, including names, Social Security numbers, birth dates, addresses, and, in some cases, driver's license numbers.

The nature of the attack was the exploitation of the Apache Struts vulnerability. Apache Struts is an open-source framework for creating Java-based corporate web applications. It offers a set of tools and practices to help simplify the development process and promotes the adoption of design patterns like the Model-View-Controller (MVC) pattern.

One prominent feature of Apache Struts, as highlighted in the context of the Equifax breach, is its susceptibility to security vulnerabilities. In the Equifax incident, attackers used a known vulnerability in the Apache Struts to gain unauthorized access to the company's systems. This cyber attack emphasizes the significance of updating frameworks and libraries and installing security fixes as soon as possible to reduce potential dangers. Equifax itself was not aware of the cyber attack until late July 2017 and publicly disclosed its cyber attack in September that year.

To prevent such exploitations it is important to implement prevention strategies. Investing in advanced monitoring systems to detect unusual or suspicious activities within the network and respond promptly to potential security incidents, and implementing a proactive approach to regularly update and patch software to address known vulnerabilities promptly could have mitigated this attack. It is also wise to develop effective communication strategies to promptly inform affected parties and the public about security breaches, fostering trust and transparency.

This attack could have been easily prevented, but due to poor negligence and improper monitoring, hundreds of millions of individuals were affected due to a known vulnerability.

Between April and September 2014, Home Depot was being invaded by one of the largest data breaches in retail history. Home Depot was not aware of the attack until September, 6 months after they had been infiltrated

The attackers gained unauthorized access to Home Depot's computer network. The hacker group then deployed malware on the company’s registers at the point of sale. Malware, short for malicious software, is designed to harm or exploit computer systems, networks, or users. Malware can be distributed through various means, including compromised software. The attackers reportedly used custom-built malware, which was designed to evade detection by antivirus software and was delivered through a third-party vendor's credentials, highlighting the risks associated with supply chain security.

The malware used in the Home Depot data breach of 2014 was a variation of the "Backoff" ransomware. Backoff is a form of point-of-sale (POS) malware that targets credit card data

handled by POS systems, primarily in retail settings. Backoff malware is notorious for its ability to scrape and capture data from payment card magnetic stripes when swiped through hacked POS terminals. The breach exposed sensitive information, including credit and debit card details, for approximately 56 million Home Depot customers. The attackers also gained access to email addresses of an additional 53 million customers.

The Home Depot Breach highlights the importance of securing and monitoring the use of third party software and its network activities. Especially within its cybersecurity departments. But the attack could have been prevented if proper monitoring of the company's network was enforced and a risk assessment of the third party software was evaluated properly.

Understanding cybersecurity is an everyday challenge and is the first step toward protecting your information. Your company, its clients, and even your own personal information at home are all at risk when it comes to a cyber attack. Many attacks can be prevented or mitigated as much as possible if the proper steps and procedures are enforced and funded. Overall, cybersecurity is a shared responsibility that must be taken seriously.