CYBERSECURITY

Grubman Shire Meiselas & Sacks Attack and the Evolution of Ransomware

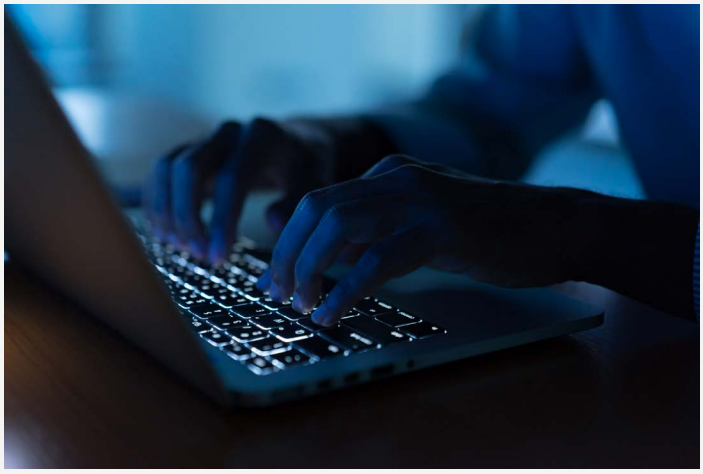
The ongoing COVID-19 pandemic and ensuing rapid transition to remote work has greatly increased companies' exposure to cyber security threats. In particular, the frequency and severity of ransomware attacks on businesses in all industries are on a sharp rise. The large amount of sensitive information collected, managed and stored by professional services firms makes them distinctly vulnerable. In May 2020, the prominent entertainment law firm, Grubman Shire Meiselas & Sacks (GSMS), fell victim to a vicious and widely publicized ransomware attack. The GSMS attack is a vivid reminder of how real the threat of ransomware is for professional services firms.

GSMS Attack

On May 8, 2020, it was reported that GSMS's computer system had been taken over by the REvil group, a cybercriminal gang. The REvil group initially set the ransom demand at $21 million but when the group discovered files related to Donald Trump the demand was increased to $42 million. The attack on GSMS resulted in loss of sensitive data belonging to the likes of Lady Gaga, Madonna, Bruce Springsteen and Elton John. GSMS has refused to pay the ransom to date, as recommended by the FBI. The firm has recovered some of the lost data through privately hired individuals; however, unfortunately, much of the stolen data is still at large and available for purchase online.

Ransomware 2.0

The first ransomware attacks were seen in the late 1980s. However, it wasn't until the mid-2000s that the attacks focused on encrypting files and demanding payment for release of the locked system. By the mid-2010s, ransomware was mainstream and, in 2016, Ransomware as a Service (RaaS) began being offered by deceitful vendors. The RaaS model provides a subscription service to anyone willing to pay a fee to use a ransomware tool for profit, no coding skills needed. Ransomware has rapidly evolved into a mature and profitable business. And, like any other business model that works, it continues to evolve in an effort to increase its profitability.



The latest iteration of ransomware – Ransomware 2.0 – involves a "one-two-punch" (1) cybercriminals lock your system; and (2) cybercriminals steal your most sensitive information. This was what we saw in the attack on GSMS. The REvil group demanded a ransom payment to release encrypted files as well as an additional payment to permanently remove stolen information from their own system. Increasingly, these sophisticated attackers release small pieces of stolen data to their website and make it available for purchase by the public to encourage payment.

Takeaways

The continuing evolution of ransomware and the attack suffered by GSMS highlights the importance of having strong network security and privacy controls in place to keep your business and sensitive information secure. Below are a few tips to assist you in mitigating a similar situation:

- **Employee Training:** While it may be impossible to eliminate exposure to human error, methods such as mandatory seminars, regular training, and phishing test emails are effective in mitigating the risk.
- **Incident Response Readiness:** Firms should create procedures to minimize business interruption and limit potential damages. In addition to ensuring you have a strong incident response plan, you should test the plan regularly, in the same way you conduct fire drills.
- **Review Your Cyber Insurance Policy with Your Broker:** Today, many traditional insurance products include some cyber coverage. However, in most instances, the coverage provided in those products is very narrow in scope. Stand-alone cyber insurance policies offer a broad range of first and third party coverages intended to protect an organization in the event of a ransomware attack. A comprehensive cyber insurance policy is a key element of any cyber risk management program.

Let's Talk

Find out how EPIC Insurance Brokers & Consultants can help your business.

Visit epicbrokers.com →