Having trouble reading this email? View it in your browser.

March 2020

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Beazley Cites Ransomware as the Top Threat for Cyber-Attacks in 2020

By Ben Patton

Insurance provider Beazley has issued a report (free registration required) detailing the landscape of cyber-attacks over the past year. The report dives into the nature and causes of attacks reported to the insurer and offers practical advice on how companies can defend themselves from malicious actors.

What Do the Numbers Say?

Hacking (e.g., phishing, SQL injection, DDoS, etc.) and malware (e.g., ransomware, trojans, rootkits, etc.) were the top cause of loss in 2019 with accidental disclosure in a distant second. In 2019 alone, Beazley Breach Response (BBR) Services saw 775 ransomware attacks, an astounding 131% increase from 2018. Notably, business email compromises decreased in 2019, a trend that BBR Services contributes to a focus on ransomware given the high payouts. With the increase in ransomware incidents also came an increase in payment demands for each attack, reaching as high as eight figures for larger targets.

Who Was Affected the Most?

Healthcare entities and financial institutions were hit the hardest by data incidents in 2019, combining for over 50% of all targeted attacks. However, government, manufacturing and construction businesses formed the top three for reported ransomware incidents while healthcare and financial institutions were at the bottom of the list. Additionally, BBR Services reported an increase in reported attacks through companies' IT managed service providers (MSPs).

SUBSCRIBE

ARCHIVE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

What's Next?

With the evolution of ransomware, attackers are starting to employ more sophisticated techniques. For example, BBR Services reported a dramatic increase in ransomware variants such as Sodinokibi and Ryuk that deploy with trojans such as TrickBot and Emotet designed to harvest credential data. Traditionally, attackers deployed a ransomware's payload and exited the system. However, with the change in tactics and extortion demands, there is a heightened risk of access *and exfiltration* of data, which may result in additional legal notification obligations and business concerns.

Additionally, BBR Services expects an increase in attempts to compromise MSPs. When an MSP is hit with ransomware, all downstream operations for each customer are affected and recovering as quickly as possible is essential. As such, MSPs are extremely valuable targets for attackers.

How to Minimize These Risks

While attackers' methods continue to evolve, the most common forms of entrance into a company's network are through phishing emails or gaining unauthorized access via remote desktop protocol (RDP). BBR Services suggests locking down RDP, requiring multi-factor authentication wherever possible, disabling PowerShell and religiously patching systems. Ensuring that sensitive information is encrypted in transit and at rest is also an excellent way to minimize the risk of loss. Above all, maintaining multiple backup copies of data stored in secure locations and periodically testing these backups can be vital to restoring data in the event of a ransomware incident.

Ben Patton
Associate
206.344.7625
bpatton@shb.com

Colman McCarthy
Associate
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate
813.202.7151
kpaine@shb.com

Lischen Reeves
Associate
816.559.2056
lreeves@shb.com

The choice of a lawyer is an important decision and should not be based solely upon advertisements.

© Shook, Hardy & Bacon L.L.P. All rights reserved.

Unsubscribe | **Forward to a Colleague** | **Privacy Notice**