CASE STUDY

Threat Actors Collect Fraudulent Tax Refunds After Theft From Accounting Firm

INDUSTRY
Professional Services

EVENT TYPE
Cyber Tax Fraud

REVENUE
$1-3M

EMPLOYEE COUNT
1-25

LOCATION
Pennsylvania

KEY COVERAGE
Breach Response

Businesses should exercise caution and scrutinize the security practices of their partners, particularly those that have access to data and other privileged information.

A small accounting firm discovered signs of a cyber event after the tax filings for nearly two dozen clients were flagged as fraudulent and blocked by the Internal Revenue Service. Months earlier, a threat actor had stolen and submitted the filings, rerouting the tax refunds to another account for financial gain. Unaware of any compromised accounts, the firm contacted Coalition to explore the matter.

After selecting to work with Coalition Incident Response[1] (CIR), the firm's tax filing software was investigated to determine if credentials had been compromised or if a threat actor had accessed the firm's actual network. CIR discovered that illegitimate user accounts had been created within the firm's software account and that an unauthorized computer was used to submit the fraudulent tax returns.

To avoid detection and bypass administrative permissions, the threat actor created a lookalike domain and email address to mimic the firm's. The firm claimed the software provider should've flagged these actions, while the software provider claimed it sent an email alert — but there was no trace of any such communication.

Ultimately, CIR found evidence of business email compromise but was unable to connect it to the tax fraud due to the amount of time that lapsed between the event and its discovery. The firm was dismayed that the threat actor was able to operate so freely within the software platform without being noticed, but, fortunately, one key coverage came into play: Breach Response[2] handled the cost of forensic investigation, as well as the notification costs and credit monitoring for clients whose data was compromised. After the accounting firm paid its $2,500 self-insured retention, its policy covered the remaining $31,000.

Lesson Learned: Exercise Security Diligence When Partnering with Third-Party Vendors

Businesses that are dependent upon third-party applications and software, especially those that are smaller or with fewer resources, often assume that strong security controls are built into the vendors' products and procedures. When engaging with new vendors, businesses should exercise caution and scrutinize the security practices of their partners, particularly those that have access to data and other privileged information.

Coalition brings together active monitoring, incident response, and comprehensive cyber insurance designed to help mitigate your organization's cyber risk. To learn more, visit coalitioninc.com.

[1] *Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.*

[2] *The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.*