PUBLICATION

Key Takeaways from Recent Cyberattack Resulting in Demise of Hedge Fund

Authors: Matthew George White
February 24, 2021

We've all heard a lot about cybersecurity risks and how cyberattacks have dramatically increased since COVID-19 changed our daily work environments. A recent attack has resulted in the demise of a hedge fund and illustrates important steps for all organizations to consider. We will analyze and discuss key takeaways all organizations, and especially financial institutions, should consider in order to prevent such attacks.

In this recent cybersecurity attack, a fake Zoom invite kicked off a chain of events that ultimately forced a Sydney, Australian hedge fund to close shop after cybercriminals used the scheme to find a way into the fund's emails. The fraudulent Zoom invite, once clicked, planted malware on the hedge fund's network that permitted the cybercriminals to take control of the fund's email servers. Using this access, the cybercriminals issued $8.7 million in fraudulent wire transfer invoices, which were mistakenly approved by the fund. In so doing, the fund failed to heed multiple red flags, including wires to an unusual firm, the use of previously unused accounts, invoices addressed to incorrect recipients, and unusual categorizations of the transfers. Ultimately, this fraudulent scheme did enough damage to force the hedge fund to shut its doors.

This incident leaves us all asking: how could this happen given the numerous red flags that the hedge fund encountered? This incident reflects the failure of necessary internal checks and balances as well as appropriate policies and procedures for wire transfers and ensuring those procedures are followed in each and every instance. Additionally, this incident demonstrates that cybercriminals continue to develop innovative ways to target financial institutions. COVID-19 has created numerous new attack methods, including those related to the dramatic rise in the use of videoconferencing applications (like Zoom, Microsoft Teams, Webex, etc.) in work-from-home environments. Financial institutions, and all other businesses, need to continue to monitor and address these new threats with additional infrastructure and, importantly, with additional employee training. Potential training topics should include best practices for videoconferencing, how to avoid sharing credentials, and how wires should be approved and processed.

In sum, this incident demonstrates that financial institutions and businesses continue to be a prime target for cyberattacks. Be prepared and don't ignore red flags.

Key Takeaways:

- Update vigilance and training regarding the use of videoconferencing software tools, especially accepting invitations from unknown sources.
- Escalate security protocols to protect companies who are more vulnerable during the move to work-from-home due to COVID-19.
- Ensure proper use of checks and balances between all parties prior to the issuing of funds. For example, require voice verification as opposed to email.
- Educate and be aware of wire fraud techniques used by cybercriminals.

If you have any questions regarding the your cybersecurity practices, including developing and testing your policies and procedures for identifying and responding to red flags, training your employees, or any other aspect of your cybersecurity and data protection program, please contact Matt White, CIPP/US, CIPP/E, CIPM or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.