alarming new finding. Hackers are now specifically targeting your firm. With most firms using relatively similar software and service providers, a flaw found in one ...

Jun. 18, 2018

Much to the ire of businesses worldwide, hackers have ceaselessly attempted to penetrate their computer systems and abscond with valuable information. While seemingly no business sector is beyond the reach of opportunistic hackers, the financial services industry has been particularly sensitive to these intrusions due to the vast quantities of personal information stored therein. Yet, like all systems found in the business world, specialization of skills is a natural outgrowth.

Unfortunately for accounting firms nationwide, this specialization has resulted in an alarming new finding. Hackers are now specifically targeting your firm. With most firms using relatively similar software and service providers, a flaw found in one system can be easily replicated in countless others. The game of cybersecurity cat-and-mouse is quickly accelerating against your firm.

Authors: You're most famous in the cybersecurity world for discovering some of the most high-profile breaches in history such as those at JPMorgan, Adobe, and Lexis Nexis. How did you discover that there is a gang of cybercriminals focusing on CPA firms?

Alex Holden: We monitor a number of Dark Web forums and information exchanges. In this particular case, one of the lesser known forums was used for this type of data exchange. Fortunately for us, hackers disclosed more information than they wanted to, allowing this glimpse into their activities.

Do you have any indication where these criminals are located geographically?

Alex: We have no clear indication where they are from geographically. We can only

criminals prefer?

Alex: The CPA's computer had some kind of virus allowing data logging along with screenshots and keyboard inputs from the victim. This was non-disruptive, seamless, for the victim as likely the infection and operation of his computer.

Once the criminals have stolen data from these firms, how are they distributing the data?

Alex: The stolen data is not as useful as the hackers' ability to generate profits. This crime model deals more with tax refunds than any other abuse vector. It is unclear how if actual data was exfiltrated or was the victim's computer was used as a conduit to commit tax fraud.

In your experience, what size accounting firm are they targeting, and why?

Alex: Accounting firms are targeted not based on size but on an opportunity. While larger firms may have dedicated IT and data security staff, they are also a significantly attractive targets for potential profits. Yet smaller firms who operate on a one-on-one basis are easier targets because of lack of data security measures. At the end of the day, you are likely to do business with a smaller firm because of personal touch and trust, but this personal touch may come with an expensive price tag of missing a lot of critical data security safeguards.

For a small accounting firm, with a very limited cybersecurity budget – if any, what are some cost-effective ways that can lessen their odds of being compromised that are often overlooked?

Alex: Smaller firms invest in commercial-grade accounting software, yet the data security side is far below the commercial grade or may be missing. Basics: patch your system regularly, don't miss any updates; buy anti-virus and anti-malware software

and keep it up-to-date; do not use your work computer for any other purpose than

policies are definitely needed. But what is usually lacking is a deeper understanding of security threats and poor password policies. End-user education around data security must be a paramount concern for larger firms and re-using or assigning weaker passwords should not be tolerated.

What is deep web monitoring and why would an accounting firm need such a service? Could they include this service for their own clients?

Alex: This tax season we saw tax data of tens of thousands of victims traded on the Deep and Dark Web by hackers. At the same time, exploitation of accounting firms is visibly on the rise and this particular incident is not a unique occurrence. To see what hackers are targeting and if you are on a list of targets or victims is sometimes a quick check that may save you not only money, but reputational loss. And knowing if your clients have been already compromised, in many cases, may allow you to help them proactively as recovery from tax fraud is not an easy task at all.

Understanding that no computer system is ever 100% secure, how important is a breach response plan, and when should a company start seeking assistance in crafting and implementing such a plan?

Alex: Breach or Incident Response Planning is essential for a company of any size. Pretty much like dealing with any kind of incident (car accident, fire, etc.) it is much better to put some or a lot of thought into your response than trying to ad-lib during crisis. Your ability to find the right partners that will help you with the recovery process cannot be hindered by timing of a breach. Knowing who to call, what to do and how to respond is critical. In many cases, doing things the right way and quickly can minimize the impact of an incident.

Are there any new cybersecurity tools that you are particularly excited about that firms should be aware of?

Alex: I do not want to endorse any specific vendors but rather want to highlight

and more devastating as hackers are getting better at their evil tasks and not caring about the devastation they leave in their path.

When asked for comment concerning the above revelations, Anthony Valach, counsel at BakerHostetler cautioned accounting firms to consider the larger ramifications for their own clients. "It doesn't matter what time of year it is, it's always W-2 season. Remember, the main goal of these actors isn't to steal someone's identity, it's to monetize the information as quickly as possible. If they get W-2s, they will try to file fraudulent tax returns."

On a more optimistic note, he did add that many breaches he works on center around fundamental security measures that would have been easily rectified. "Yes, there government-backed actors looking to cause chaos, but the run of the mill hacker is trying to turn information into money as quickly as possible. If they can't do that easily, or at least have a reasonable chance at doing so, they will move on to the next one."

Garrett Wagner, CPA/CITP and founder of consulting firm C3 Evolution Group, emphasized the need to educate your staff. "Internally, they need to provide regular training and reminders to their staff about the various threats and email attacks currently being used." Furthermore, he noted the often-overlooked client vulnerability saying, "Externally, they need to remind their clients of the tools they have to send secure communications. Nothing is worse than having all the tools and resources to keep data secure than to have all your clients email un-encrypted emails into the firm on a regular basis."

No matter how secure you may think your computer systems may be, we are entering a new and dangerous phase for accounting firms worldwide. It is well worth the time and energy to commit to investigating new cybersecurity technologies and employee

training programs. As with all things in life, the longer you wait, the more painful

IP Cybersecurity Law.

Firm Management