Out and about the industry.

Stalking Marketers on the Dark Web is Big Business. By Mark Radosevich 02/02/18

Over the past months, I've encountered various stories of ransomware attacks on marketer businesses throughout the country. New to the subject and the seemingly widespread randomness of the situation, prompted me to take a closer look at the problem. Up to now, I had a vague notion of malware and computer hacking but my investigation has revealed that the problem is much wider than expected and given the amount of customer data and cash that regularly passes through a petroleum wholesale business, unsuspecting oil marketers are increasingly being targeted, and many are quite vulnerable to attack. This is a growing problem, with analysts predicting that ransomware attacks may double by next year.

The president of a Tennessee-based fuel marketer related his account of trying to log onto the company's computer network on a recent Saturday morning and encountering a cryptic note with a skull and crossbones graphic notifying him his company the files had been encrypted, rendering them unobtainable unless a ransom of $50,000 *in Bitcoin* was paid. When he called the office, dispatch confirmed the lockdown was for real. At that point, he said that the feeling of helplessness and frustration in not being able to operate was almost overwhelming. To add insult to injury, he now had to figure out how to obtain Bitcoin. Not a small feat for the uninitiated on a Saturday. In the end, the Bitcoin was secured through various "Bitcoin Brokers," the ransom paid and the files recovered after several days of operating blind. This was followed by the firing of IT personnel and a comprehensive reassessment of internal controls and security processes.

Other marketers interviewed confirmed that that they had been hacked and either refused to pay the ransom, and subsequently reconstructed their data or they refused to pay and suffered little harm due to their security and data backup protocols. But there is little doubt that this problem exists in our industry and its prevalence is growing. Following are a few nuggets of information that I learned from my investigation and recommendations that marketers should take to heart.

Ransomware is malware working on the dark web that uses vulnerabilities in the central nerve of a computer, called the kernel, where antivirus programs have difficulty detecting. It infects network computers when someone opens an attachment or website link from a malicious email message. Attackers can also deliver ransomware directly to a network if it has already been infected with a backdoor through which they can enter. Ransomware is the tainted attachment in an email blast that knocks on thousands of doors. The bad guys have access to encrypt the data when someone answers the door and opens the attachment or visits tainted websites.

Several years ago a program called WannaCry held hundreds of thousands of computer data files hostage until a small $300- $500 ransom was paid. Another recent version, TorrentLocker, harvested email lists from victims' computers, and then spammed itself to other victims; amassing almost 3 million emails of unsuspecting ransomware candidates. The potential rewards are great if only a small fraction of the targeted computers become infected.

Ransomware attacks couldn't be nearly as successful if it wasn't for the existence of Bitcoin or other virtual currencies, which allow these transactions to be nearly anonymous, as traditional banking intermediaries are not involved. Payment is through a simple file transfer between two people or companies. Bitcoin transactions are documented on a virtual open ledger but names don't have to be

attached to the parties involved. Further complicating the mess, when one is pressed to pay a large ransom, is buying it on the open market where purchase amounts are limited. This requires the use of brokers and the vagaries of value for this virtual currency. I found it interesting to note that many large companies are stock piling bitcoin in the eventuality of a future attack. Even for the most technically sophisticated companies, it's not a matter of if; it's a matter of when a successful attack happens and having the ability to get back up and running fast.

Keys to fighting ransomware:

Some protection simple steps include restricting the ability of people to add programs to computers, using antivirus program subscription software and backing up files every day, with the central database stored on a devise that is isolated and not online. Prohibit employees from using company computers for personal things like, surfing the web, emails or opening emailed attachments. Next, dedicate the resources to hire top notch IT specialists and instruct them to constantly be up to date on information and procedures. Employ better employee security protocols using unique passphrases versus simple passwords, and be dedicated about making regular passphrase or password system changes. Stop allowing third party vendors to independently access company computers or systems for any reason. And remember the parting words of the Tennessee marketer I previously referenced, "when you think you've done enough, think again because you can never have enough protection."

Petroleum marketer associations can spearhead the fight

Historically, state petroleum marketer associations are tasked to address industry regulation and legislation to the benefit of our industry. Given the real and growing danger of the ransomware problem, I propose that "cybercrime prevention" be formally adopted as a third area of primary emphasis on the state level and nationally through the PMAA. This can include creating a stable of approved IT consultants to conduct training seminars and individual site assessments at association member businesses to highlight potential security weaknesses and insure that internal controls and procedures are of the highest standard. Rather than keeping incidences of hacking a dark and embarrassing secret, I propose bringing the problem into the light by the formation of a new association committee entitled "IT Security." This committee will be tasked with facilitating training, coordinating IT vendor participation and as an official platform to share successes and potential threats encountered by member companies. If promoted properly, this new committee should also provide state associations with a new and valuable benefit to motivate non-member companies to join and become involved.

Mark Radosevich is a strong industry advocate and seasoned petroleum veteran, serving both oil companies and marketers over his long career. He is president of PetroActive Real Estate Services, LLC, offering confidential mergers & acquisition consultation, representation and financing services exclusively to petroleum wholesalers. Mark can be reached by email at mark@petroactive.net and directly by phone at 423-442-1327, his full professional bio can be found at www.petroactive.net.