Top 5 Cybersecurity Threats Facing Title Industry in 2018 – Part 2

Overview

In part 1 of this 5-part series, we examined business email compromise, which occurs when a hacker gains access to a corporate email account and assumes the identity of the corporate user in order to defraud the company, employees, customers, or partners.

According to the FBI, participants involved in real estate transactions are particularly targeted in such attacks. The average successful wire fraud amounts to $140,000 compared to the average successful bank robbery of $6,500. The real estate sector alone had more than 9,600 victims and lost over $56 million in 2017, according to the FBI.

Unfortunately, business email compromise is on the rise, and from personal experience I can tell you that it is all too common in the title industry. Today we will examine ways in which malicious actors are able to take over accounts to accomplish their goals.

Threat #2 – Phishing / Account Takeover

The Problem

User credentials are the holy grail of hacking, and the means by which hackers accomplish their ends. Just think about it from a hacker's perspective – would you rather try to break in the well-fortified front door of a corporate network (the firewall) or simply steal someone else's key? It is much easier to obtain corporate credentials and walk right into a network than it is to try and defeat the network's defenses.

Hackers are looking for the easiest way into your network: your employees. The techniques used are simple, repeatable, automatable, and effective. They prey on human nature – your inability to remember multiple complex passwords, your desire to please your boss, your distraction-filled workday, etc.

Widespread password reuse and regular third-party breaches make all companies vulnerable to account takeover attacks. In fact, 81% of hacking-related breaches used stolen or weak passwords and over 80% of users have reused their password across two or more websites.

Phishing attacks are on the rise, with over 76% of businesses reporting being victims of phishing attacks in the past year. According to a Verizon Data Breach report, 30% of phishing messages are opened by the target users and 12% of those users open the attachment or click on the included link.

How It Works

The simplest way to obtain corporate credentials is to simply download or purchase a list of already-stolen credentials. When a hacker breaches a network, they often put the stolen credentials up for sale, or even for free, on the dark web. There are literally billions of stolen credentials on the dark web, with millions more being added each week. For anyone with moderate computer savviness, it is trivial to load these lists into hacking tools which automate the process of testing thousands of credentials. This is called “credential stuffing.” If the malicious actor doesn’t have a list of stolen passwords, they can still use the credential stuffing software to attempt the most common passwords – i.e. “password”, “Password1”, “123456”, etc.

Another method used to steal corporate credentials is phishing. Phishing is simply an attempt to obtain sensitive information by fooling a user. Generally, this takes the form of an email disguised to look like your boss, coworker, friend, vendor, or someone that you trust. The email will often ask you to open a document or click a link. The documents usually contain malware and the links usually take you to a website designed to steal your credentials or infect you with malware.

How to Protect Your Organization

1. Use effective email security

First, you should put systems in place to detect and prevent phishing emails from ever reaching your employees. A secure email gateway with effective spam/phishing detection should be implemented. Many title companies rely on the built-in security from their email vendor, and in my experience, it simply is not effective enough.

Third party vendors that specialize in email security often have more effective algorithms and will block more phishing emails. Take a look at Gartner’s magic quadrant for secure internet gateway to get an idea of the best vendors.

2. Train your employees

Recognizing that no email security product is perfect, phishing emails are going to make it to your employees’ inbox. At that point, it is up to your employees to detect and delete the malicious email.

Arm your employees with the ability to prevent breaches by educating them about their role in protecting the organization and enabling them to detect phishing emails. Run regular phishing simulations to test your users and offer additional training when needed. A study done by

KnowB4 showed that training combined with phishing simulations decreased careless email clicking to 13% after 90 days and to 2% after 12 months.

3. Prevent access to malicious phishing websites

While training and testing can go a long way to reducing the efficacy of phishing attacks, it only takes one wrong click to cause enormous damage to your business. Having systems in place to prevent access to malicious websites can protect your organization when email filtering and user training have both failed.

Run all internet traffic through a secure internet gateway, which will block phishing websites, malware downloads, command and control communication, and other malicious internet traffic. These systems are very effective and are probably the easiest security layer to implement.

4. Prevent malware (and non-malware)

Malware can sit on your employee devices and collect everything that your employees do or input, including credentials. Traditional antivirus is no longer effective, as it relies on signature-based detection, meaning it only detects what it knows. That leaves your company vulnerable to fileless malware, zero-day attacks, and non-malware attacks. Non-malware attacks use legitimate software, such as PDF's, Word documents, macros, and PowerShell to infect a computer without alerting antivirus solutions.

With over 53% of breaches utilizing non-malware, it is clear that a new approach is needed. Next-generation antivirus solutions are able to use behavior analysis and machine learning to analyze the behavior of the software running on your computer and are able to detect malicious processes without the need for signatures. This means they can detect malware, non-malware, zero-day, and fileless malware where traditional antivirus can't.

5. Enable multi-factor authentication

Multi-factor authentication is a way to confirm a user's identity by utilizing two or more pieces of evidence from two or more different sources: something you know, something you have, or something you are. The most common example of this is entering your username and password (something you know), then entering a second unique code that is sent to your cell phone (something you have). The idea is that even if hackers obtain one of these authentication mechanisms, they will likely not be able to obtain the second required mechanism, rendering the stolen credentials useless.

6. Monitor the dark web

It requires a higher level of sophistication from the hacker, but even multi-factor authentication can be circumvented. With billions of stolen credentials available on the dark web and millions added each week, wouldn’t you like to know when your employee credentials show up for sale? Monitoring the dark web can alert you to just that and allow you to change the affected password before attackers are able to use it against your systems.

Next Time…

In the next post, we’ll talk about ways that systems get hacked and how data gets exfiltrated.

Drew Bradford is a TLTA member and President of Sigma InfoSec, a company that provides enterprise-class cybersecurity solutions to the title industry.