Top 5 Cybersecurity Threats Facing Title Industry in 2018 – Part 4

Overview

In part 1, 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. In part 2, we looked at some of the ways that hackers obtain and use stolen credentials in order to take over an account. In part 3, we explored the motives and methods of hackers.

In this post, we'll go deeper into today's malware and ways to prevent and detect infections.

Threat #4 – Malware

The Problem

Malware is rapidly evolving, both in the techniques used to exploit systems and the way in which it is delivered. New exploits and infection techniques are appearing with regularity, creating a cat and mouse game that antivirus vendors can never win. It is clear that traditional antivirus cannot keep up with the ever-changing threat landscape, as its reliance on identifying existing malware by definition means that it cannot prevent new or unseen attacks.

Highly sophisticated malware techniques are moving downstream as new tools and frameworks are made available making it easier for criminals to use these techniques with little technical expertise required.

It only takes one employee clicking on the wrong link or opening the wrong attachment to shut down an entire organization. With heavy reliance on IT systems and time-sensitive transaction requirements, title companies cannot afford to have their systems down due to malware or ransomware. According to a recent study by Sophos, the average cost of ransomware attack in 2017 was $133,000.

Today's Malware Trends

According to a recent report by The Center for Internet Security, unsolicited email, or "malspam", is by far the #1 initial infection vector. Malspam is simply an email that contains malware in the form of an attachment or a link to a malicious website. These emails are regularly bypassing filters and users are opening the attachments or clicking the links about 12% of the time, according to Verizon Data Breach findings.

Perhaps the biggest trend of the year is the use of fileless malware, which is malware that completely avoids antivirus detection by utilizing exploits, scripts, or legitimate system tools instead of malware executables. These attacks are often embedded inside of Word or PDF documents and are carried out silently by launching PowerShell or other scripting languages. The common pattern that we are seeing is a user receives an email with a Word document attached, the user opens the Word document, the document then silently launches PowerShell which downloads and launches malware from one or more websites. According to Ponemon, 77% of all successful malware attacks used fileless techniques in 2017.

Microsoft's Remote Desktop Protocol (RDP) is a tool used to remotely access your PC, but it is now increasingly being used by attackers as a way into your computer. Attackers scan every device on the internet looking for RDP, and when they find it they get in by performing brute force login attempts. Once inside, they are free to spread malware or ransomware to the entire network. According to Webroot, 66% of all ransomware infections in 2017 were delivered via RDP brute force.

As victims pay fewer ransoms, ransomware infections are on a steep decline. Attackers are increasingly using crypto-mining malware instead of ransomware to earn money. Crypto-mining malware sits silently on your computer, using your CPU to mine for cryptocurrency that goes straight to the attacker's untraceable digital wallets. This is a much stealthier alternative to ransomware and provides an immediate and direct source of revenue for the attackers. According to Checkpoint, crypto-miners have impacted 55% of all organizations globally.

How to Protect Your Organization

1. Prevent malware delivery vehicles

Understanding the most common malware delivery mechanisms is key to building up an effective defense. The vast majority of malware is delivered first by email. Invest in an effective email filtering service. If you are in Office 365, consider enabling Advanced Threat Protection for a few dollars more per month. Take a look at Gartner's magic quadrant for Secure Email Gateway to see other vendors.

Block malicious websites. With 12% of users clicking on malicious links in email, you need to implement a secure internet gateway that will prevent access to malicious websites. These gateways are constantly being updated with the latest threat intelligence to block the latest threats.

Patch your software regularly. Malware often exploits vulnerabilities in the software that you have installed. You need to patch the software regularly to help reduce your attack surface.

Disable admin tools that are utilized in fileless attacks such as PowerShell and Office macros. While these scripting languages are often use legitimately by your IT department, they may not be required on all of your desktops. Talk with your IT department and weight the pros and cons of these scripting languages.

Disable RDP or ensure it is only allowed securely over VPN. Never have RDP open to the internet. Computers with RDP open are regularly scanned and targeted in automated brute force attacks.

2. Implement next-gen antivirus

Unlike traditional antivirus, next-gen antivirus does not rely on virus signatures alone. In addition to signatures, next-gen antivirus uses machine learning to identify suspicious and malicious files that have not yet been catalogued in antivirus signatures. With the rapidly evolving malware landscape, next-gen antivirus is absolutely required these days.

3. Implement endpoint detection & response

Even next-gen antivirus cannot detect fileless malware. Only behavior-based detection systems, known as endpoint detection & response (EDR), can identify this type of malicious activity. EDR analyzes the behavior of everything running on your computer and can identify when an application is attempting to do something it should not, such as a Word document launching PowerShell and downloading files from the internet.

EDR systems watch and analyze every activity happening on every computer on your network. As a result, they can be very noisy and may involve full time security analysis in order to weed out the false positives and identify the true threats.

Next Time…

In the next post, we'll talk about having a plan in place for when people, technology, and processes fail.

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