LAYERED PROTECTION

ControlNow™ Whitepaper

Thirteen Days of Cybercrime.

CONTROLnow™

Table of contents

Introduction

Thirteen days. A mere heartbeat in the pulse of a lifetime and yet hundreds of thousands, if not millions, of dollars were lost to cybercrime in that short timeframe. All these incidents (and many more that have gone unreported) took place from 25 September 2014 to 8 October 2014. This is the scary reality of having your business on the Internet today.

Some examples of security breaches this paper looks at:

- Active exploit of Bash Shellshock Flaw, 500 million Unix and Linux machines affected
- Japan Airlines confirms compromise of 750 thousand customers
- Trip Advisor's website Viator confirms 1.4 million payment card holder breach
- JP Morgan Chase security breach affects 76 million households and 7 million businesses
- Australian Broadcasting Corporation hit with Ransomware disrupts 24-hour news program

Business on the Internet – a Scary Reality

Let's examine the Shellshock flaw for a moment and analyze the recent events from an SMB perspective.

Maybe you're a small business with a couple of servers, a dozen or so workstations and a few other devices – maybe your business has a Postage Meter, Voice over IP phone, Web Camera, Firewall, Backup Appliance, and Wireless Access Point. How could this possibly affect your "all Windows" network?

Although businesses everywhere are under the mistaken impression they only run Windows, the modern network has many machines connected to it that use a flavor of Unix as an embedded system–like your firewall. These highly reliable and almost forgettable machines, run on your network. They usually have a webserver embedded for configuration, and this feature runs on Unix. This makes your small business as vulnerable as any other company with a big Unix server farm. Even if you don't host your own website (having outsourced that to a hosting provider) the server it runs on may also be vulnerable.

Can you imagine a virus that targets your entire embedded infrastructure? Well, the cybercriminals can.

Let's look at some of the recent, major security breaches. Japan Airlines had all its customers' personal information stolen. Twenty-three computers were infected by malware that was believed to have arrived as a phishing email. Experts say that the infection lasted more than a month.

The compromise of Trip Advisor's Viator website was even more devastating. They didn't even know they were breached until they were notified by law enforcement! Investigators were looking into fraudulent payment card transactions that had one source in common – the Viator website. According to the Verizon Data Breach Investigation Report[1], 66% of breaches took months or even years to discover. And a recent Ponemon Institute[2] report, sponsored by Solera Networks (a Blue Coat company) found that, on average, it is taking companies three months to discover a malicious breach and then more than four months to resolve it. In other words, the cybercriminals are able to find a home and stay as unwelcome guests for a very long time.

[1] http://www.verizonenterprise.com/DBIR/2014/
[2] http://www.ponemon.org/local/upload/file/Post%20Breach%20Boom%20V7.pdf

Don't Collect Credit Card Information? Doesn't Matter

The damper for small business owners is that many believe they are immune from this sort of attack because they don't have a website that collects credit card or personal information. Maybe, but the chances are, they use websites as a small business and maybe they have their own cloud-based solutions for Customer Resource Management (CRM), Enterprise Resource Management (ERP), or even just Hosted Payroll or Accounting Software.

One of the most important aspects of business is the ability to take money for your goods or services. It seems simple enough, but in this day and age, between credit and debit transactions online and off, we turn to payment processors like JP Morgan Chase[3].

Although JP Morgan Chase indicates that, in the recent breach, financial information was not compromised; personal information was. Personal information cannot be easily changed and can be used for social engineering attacks on the wealthy or vulnerable aging adults. Your date of birth alone is frequently used as identifying information, and the cybercriminals can use it as targeting information.

And yet another victim of Ransomware (like so many other companies) was the Australian Broadcasting Corporation. The malware arrived as a link on an email claiming to have come from the Australian Post, the subject and contents appeared to be about a package that could not be delivered.

[3]http://www.marketwatch.com/story/did-the-jp-morgan-chase-cyber-attack-affect-you-good-luck-finding-out-2014-10-07

Businesses Need to Protect Themselves from all Angles

These examples illustrate how the business network of today is unable to fend off adversaries without some help.

The biggest threats out there arrive in one of two mechanisms and infect in up to three different manners:

1. As email with a dangerous attachment
2. By a visit to a dangerous website
3. By an email with a compelling story and a link to a dangerous website

The vast majority of malware infections are because a user was either tricked or was being careless.

The most dangerous malware comes in the form of "crimeware". This sophisticated software automates the retrieval of credentials related to banking and online shopping. Cybercriminals have added a host of features to try and remain undetected and grab as much information as possible on infected systems.

They have built modules designed for specific functions; a global network of Command and Control servers can activate all of these features once the malware has infected a target. These toolkits have capabilities such as port scanning, password stealing, system information gathering, digital certificate theft, remote desktop connectivity and even hard disk wiping and destroying. More advanced features are specifically designed to infiltrate and steal information in Automated Teller Machines or Point of Sale Terminals.

A recent version of the "Black Energy" family of crimeware has been reported to infect systems using ARM and MIPS processors - this malware can compromise networking devices manufactured by Cisco Systems; making a Black Energy infection very hard to remove.

When a computer is infected with malware it usually becomes a part of what is known as a "botnet". The malware then begins to look for a Command and Control server to check-in with – in fact it checks in regularly, transferring stolen information and awaiting instruction on what to do next. The majority of this Command and Control communication is done using the common web protocols of http or https. Obviously, if web traffic is detected when no one is in the office, you can be pretty sure something is trying to communicate out to the Internet.

Once the check-in has been completed it may receive instructions to send spam, host a malicious website, attack other hosts on the Internet as in a denial of service attack, and provide domain name service (DNS) for the Command and Control infrastructure. With ransomware the Command and Control server tells the malware to "Encrypt all the data it can find". On a network system this could encrypt and hold ransom a great deal of data.

Businesses Need to Protect Themselves from all Angles

Ransomware infections are usually only successful if the encryption key can be sent to the Command and Control server. If the Ransomware fails to find the Command and Control server it may not complete its encryption task.

It is the network communication activity that usually betrays the presence of a criminal malware infection. If suddenly your network becomes very slow and you have the presence of mind to call your ISP and ask about your traffic, you may hear the words "It seems like a lot of data is leaving your network".

Cybercrime as a Service

Fast flux DNS hosting is a foundational part of "Cybercrime as a Service" and an advanced method for a malware infection to try and locate its Command and Control server. Malware is set to use a Domain name Generation Algorithm or (DGA) and synchronizes with other DGA's to turn a ridiculous looking URL like http://ahjdshjksdhj.ru into an IP address of a Command and Control Server. The malware constantly generates new domains to ensure a connection is maintained to infected servers and other infected machines using the same DGA.

Not only does Fast Flux DNS attempt to obscure malware communication, but it also uses rapid updates of DNS information to disguise the location of websites and other Internet services that host illegal activities. Fortunately DGA's, which became predictable after a few thousand samples, are fairly easily detected by web content filters and the more scrupulous DNS providers themselves.

Besides the extremely rare and occasional "over–the–wire hacking" where hackers probe your firewall for weaknesses or vulnerabilities, it's mostly website visits that are the ultimate source of malware infections.

Most small and medium businesses maintain a website of some sort. Perhaps a very simple one, using a common Content Management System (CMS) like Drupal or WordPress. Although the organization may even be diligent in patching and updating workstations and servers, the hosting server and its applications may go neglected as it is frequently hosted offsite by a third-party hosting service.

This is exactly the scenario that recently exploited many websites running Drupal 7, a popular CMS. Vulnerability in this CMS allows an attacker to send specially crafted requests resulting in arbitrary SQL execution, leading to compromise of the hosted site.

Criminals quickly developed multiple exploits and many websites fell victim, and were forced to work as part of a bot army. These malicious websites infected any machine visiting the website with scripts that attempted to find a system with a vulnerability that could be exploited, with the ultimate aim of infecting more and more machines.

How your SMB can Avoid Being Compromised

So with all these "big name" organizations falling like dominoes, how is the SMB going to avoid being compromised? What steps are needed and, most importantly, what products and services are going to help fend off the enemy at the gates?

There are a number of solutions required to keep your network from being compromised, along with potentially all the accounts for your cloud-based services.

Patch Management
Patches correct security and functionality problems in software. From a security perspective, patches address vulnerabilities, that are exploited by malware. Applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Having all the necessary patches in place will prevent any malware that your antivirus may not have a definition for.

A patched and up-to-date operating system and third-party applications, make a workstation or server a hard target to hack.

Antivirus
The importance of antivirus software cannot be underestimated. It protects the workstation or server from being compromised. New viruses are coming out all the time and it's the job of the antivirus software to keep up with the latest threats. This is achieved by daily updates of the antivirus database definitions, which counteract the latest threats to provide constant protection. Cybercriminals often use older software with known signatures to compromise your system; they hope it's not up-to-date with the latest definitions. If you use USB sticks between home and business; or your customers arrive with USB sticks; antivirus will prevent catastrophe.

Having servers and workstations protected with up-to-date antivirus, makes your business a hard target to hack.

Web Protection
There is nothing more effective than using a web filter to prevent a network being compromised by an accidental website visit. Most ransomware and modern criminal malware use web-based http or https to contact Command and Control servers located in many countries all over the world. Many of the "drive-by download" infections and links in spear phishing attacks use compromised web servers to infect visitors.

Web Protection constantly updates an ever–changing list of dangerously infected or known Command and Control websites. This prevents malware from having a chance to infect a workstation, by preventing access to a suspicious website. As an added bonus, if something has slipped by your defenses, having a web protection solution in place may prevent the cybercriminals from gaining access to your business network.

In the case of the Australian Broadcasting Corporation's ransomware infection, it's quite likely that a web protection solution could have prevented the infection by either blocking the visit in the first place, or preventing the transmission of the ransomware back to a known Command and Control server.

Web Protection works as a first and last line of defense and surrounds your business with an extra layer of cyber protection.

These three security solutions form a robust defense, crucial in preventing your business from being a part of the next case study or story on cybercrime.

Summary

The awareness of the cyber security problem and how it impacts our daily lives can hardly escape our attentions. In this paper we cited several examples of how cybercriminals are successfully attacking and inflicting loss on organizations. It is time to shore up the defenses; all indications suggest that the situation in cyber space will not improve until organizations, large and small, take tangible and reasonable steps to safeguard their network infrastructure.

A safer Internet is in everybody's best interest.

USA, Canada, Central and South America
4309 Emperor Blvd, Suite 400, Durham, NC 27703. USA

Europe and United Kingdom
Vision Building, Greenmarket, Dundee, DD1 4QB, UK

Australia and New Zealand
2/148 Greenhill Road, Parkside, SA 5063

www.controlnow.com/contact

CONTROLnow™