Integris.

Just the Facts:

Your Guide to Malware Basics

Integris.

CONTENTS

03 DEEPER THAN VIRUSES?

04 MALWARE ISN'T THAT BIG OF A THREAT... IS IT?

05 THE MOST COMMON MALWARE ATTACKS

- 05 Viruses
- 05 Ransomware
- 05 Trojans
- 05 Grayware
- 05 Worms

06 FIVE SIGNS THAT YOUR NETWORK OR HARDWARE IS INFECTED

07 CAN YOU AFFORD NOT TO HAVE IT SECURITY SERVICES?

INTRODUCTION: DEEPER THAN VIRUSES?

In today's world, hackers and cybercriminals are getting more sophisticated. Viruses are just the beginning.

Years ago, anti-virus software was all you needed to stay protected in the face of cybercrime. We all knew the drill: recognize and delete suspicious emails, stay away from open Wi-Fi networks, and install an anti-virus software to keep your data safe.

These steps, while important, aren't enough anymore. Cybercriminals have risen to the challenge and are routinely introducing new, devastating attacks including grayware and ransomware. Each attack they invent requires a new response. The days of a "one size fits all" security strategy are gone.

You may think you are safe because your business is a small to medium sized enterprise. Hackers aren't interested in your company, right?

In 2018, Verizon released its Data Breach Investigations Report that shows this is a dangerous way to think: according to the study, small to medium sized businesses make up an astonishing 58% of cyberattack targets.

This eBook is your essential guide to understanding the mind of a cybercriminal. You will not only learn how and why hackers target businesses; you will also learn how to stop them.

Integris believes that small and medium-sized businesses are just as important as large enterprises. We devote the same effort to protect all our clients, regardless of the size of their company.

MALWARE
MALWARE ISN'T THAT BIG OF A THREAT... IS IT?

Believing your small to medium sized business is safe from cyber threats is a mistake that could cost you. The following examples of successful cyberattacks cost over $2.3 million for businesses, just like yours.

Maine: Welfare Office

Human error accounted for nearly $798K for the state of Maine's Health and Welfare Offices in 2017 when an outsourced IT provider released 2000 records containing sensitive data to a free, grayware infested website. This was a bad move on several levels, from lawsuits to HIPAA violations.

LESSON LEARNED: free apps are never a good choice when dealing with highly sensitive data such as social security numbers and dates of birth.

Communications and Safety Services Provider

An employee error in Missouri resulted in $180k of damages in 2012. The employee unknowingly opened an infected email attachment. Once the virus was installed, hackers added additional employees to the company's payroll and wired between $5,000 and $9,000 to multiple people in Ukraine.

LESSON LEARNED: Use an effective spam filter.

Law Firm

Small businesses make important, irresistible targets, too, as witnessed by a 2017 attack on a law firm that cost the ten employees $743k. The mode of attack was ransomware. The hackers initially requested $25,000 to release the encryption key, but after the law firm paid the ransom, the key didn't work. The hackers then demanded an additional $18,000 before releasing a key that allowed the firm to access its files once again. By the time the dust settled, the small law firm had lost an estimated $700k in business and three months of productivity.
LESSON LEARNED: Keeping backup files is essential to speedy restoration in the face of a ransomware attack.

Construction Company

In 2009, a Maine construction company with less than 50 employees on its payroll fell victim to a Trojan that cost the contractor over a half-million dollars in the span of one week. The Trojan had been unintentionally installed on a company computer and gained access to the company's financial information, including the bank account login information.

LESSON LEARNED: A simple employee education program along with a "zero unapproved software installation policy" could have prevented this attack.

City Municipal Court

The Conflicker worm has caused $9 billion in damages, infected over 15 million computers, and is still ongoing. Experts in cyber security research have yet to stop this malware, which cost one city $25k in emergency IT consulting fees. In addition, the hours of lost productivity due to network bogging with Conflicker has yet to be added into the total losses associated with the worm's impact on the city.

LESSON LEARNED: The Conflicker worm could have been stopped with a simple security patch update.

The take-away from each of these examples is that, with proper action, every one of the attacks could have been prevented.

MALWARE
THE MOST COMMON MALWARE ATTACKS

Integris Techs spend a lot of time in the field. They have gathered the most common malware attacks they deal with daily, along with a few tips for avoiding them. Here are a few frequently seen players in the malware game.

Viruses

Viruses are the "old-timers" of the malware world. Although they can be found globally, they tend to be focused on individuals and companies within the United States. They are primarily spread through attachments and files. Once opened, the files rapidly spread the malware through the computer itself and to other computers within your network. Along its way, a virus will destroy and alter any application or document it reaches. Some viruses are designed to steal information from your network.

Employee education is an important step in battling viruses, but you need email-based antimalware software and a high-end spam filter along with routine IT audits to complete your anti-virus strategy.

Ransomware

Ransomware uses extortion and encryption to "kidnap" your data. Hackers then leave a "ransom note" with a promise to supply a "key" to unencrypt your data for money, usually digital currency. Many ransomware attacks do not follow through on restoring your data despite receiving payment. It's estimated that 22% of businesses infected with ransomware will ultimately end up shutting their doors forever following the attack.

There is usually no way to successfully recover data lost during a ransomware attack unless you have a secure backup and defense strategy. "Boxed" antimalware programs are seldom able to keep up with the ever-changing dynamics of ransomware attacks. A cloud-based backup service is an affordable option to keep your data accessible in the face of evolving ransomware threats.

Trojans

Just like the mythical Trojan horse, Trojan programs seem harmless but, when opened, unleash havoc on your network. In 2017, Trojans accounted for 41% of computer infections per Comodo's Global Malware Report. Google Play Store was an unsuspecting source of a Trojan that was forwarding text messages without permission by using a barcode scanning app.

Trojans are typically enabled by users who bypass a network's security software. Social Engineering, commonly known as phishing, is a cyber attack that seems to come from a trusted source. Once the hacker has gained the trust of your employees, sensitive information is shared via email responses.

Because Trojans appear to be harmless apps, your best defense is employee education. Buyer beware: use extreme caution when installing free software or apps, even from a trusted source like Google. A strict implementation of a "do not install unapproved software" policy is a great starting point to protect your network.

Grayware

Grayware is more of a nuisance than an outright cyber threat. It often comes along with free software or installed on new hardware. In 2017, grayware was found pre-installed on nearly 250 million computers. These computers had grayware that automatically changed default browsers, which could have granted remote access of the affected computers. While it doesn't destroy information or alter and steal data, it slows the functionality of your network. Grayware can reveal private information and bog down your hardware with ads and other unwanted distractions.

Windows 10 has a "Refresh" feature that will take the computer back to its original settings while maintaining all critical applications and documents. To remove grayware, all hardware should be wiped periodically. IT providers can do this function in a fraction of a time while ensuring all your critical settings remain intact.

MALWARE
FIVE SIGNS THAT YOUR NETWORK OR HARDWARE IS INFECTED

It used to be easy to detect malware. If your computer was running slower than normal or otherwise performing poorly, you figured that you had been infected. Those days are long gone. Today's hackers keep improving their attacks, making malware increasingly harder to detect.

1. You are receiving strange emails from your contacts, or they report receiving strange emails from you
2. Strange web pages open in a new browser window
3. Unknown browser toolbars and apps appear on your computer without being actively installed by you
4. The file and folder names in your storage have been changed without your knowledge

These are telltale signs that you have an active malware incident on your network. To stop the malware from spreading, isolate the infected computers immediately and shut them down. An IT specialist must be called in to stop the destruction; if you have a subscription to managed IT services, this should be a covered feature of your package. If you rely on "fix it after it breaks," you must contact an IT professional immediately.

Never try to address a malware incident alone.

IT SECURITY SERVICES
CAN YOU AFFORD NOT TO HAVE IT SECURITY SERVICES?

Today's hackers are merciless. They will infect your network, drain your resources, steal sensitive data, then move on to the next victim without a second thought for the destruction they leave behind.

Cybersecurity is, without a doubt, one of the most important IT investments you can make. Budgeting for this service is, however, confusing. How much security do you need? Too little, and you are at risk. Too much, and your IT provider is taking advantage of you and costing you money you don't really need to spend.

Try this simple formula to see your cost of a breach vs your cyber security budget:

# of Incidents Per Year + **Potential Loss Per Incident ($)**

= **Annual Breach Costs**

Sticking to this formula means that your planned security budget doesn't exceed the cost of a breach. The costs of a breach will vary according to your business's industry and location. Kaspersky Lab explains that while the average breach for a small business may cost around $117,000 the number will increase nearly ten times that amount if your industry is healthcare. Depending on your industry and the number of cyberattack incidents on your network per year, your security budget could be nearly $700,000 with most providers.

Integris takes the guesswork out of your cyber security budget. We charge a flat monthly fee that covers you. As in, really covers you.

- ✓ Malware free inboxes? Covered.
- ✓ Software vulnerability patching? Covered.
- ✓ Top of the line firewall protection? Covered.
- ✓ Data backup and recovery plans? Covered.
- ✓ Employee education programs? Covered.

Integris promises many other services as well, and all at a fixed price well below the cost of a single data breach.

This eBook has taught you the basics of malware, from spotting the most common attacks to preventing them altogether. By now you've probably already figured it out: without a 24/7 targeted security platform, you are at risk.

Integris offers cybersecurity solutions to provide continuous protection from all cyberthreat, old and new. We understand that each business' security needs are as unique as the business itself. That's why we provide your network cutting-edge security, including:

- Professionally configured antivirus software
- Advanced intrusion prevention systems
- Firewalls
- Data back-up and recovery solutions

All our security features are configured, installed, centrally managed, and monitored by a professional IT team for less than most Managed Services Providers charge for a single technician's services.

Contact Integris for a free, no-obligation consultation today and see how we can put your network's security fears to rest and let you get back to what you do best: growing your business.

CONTACT US FOR A FREE, NO-OBLIGATION CONSULTATION