QBR your data, our business

EBOOK

THE BUSINESS GUIDE TO RANSOMWARE

Everything you need to know to keep your company afloat

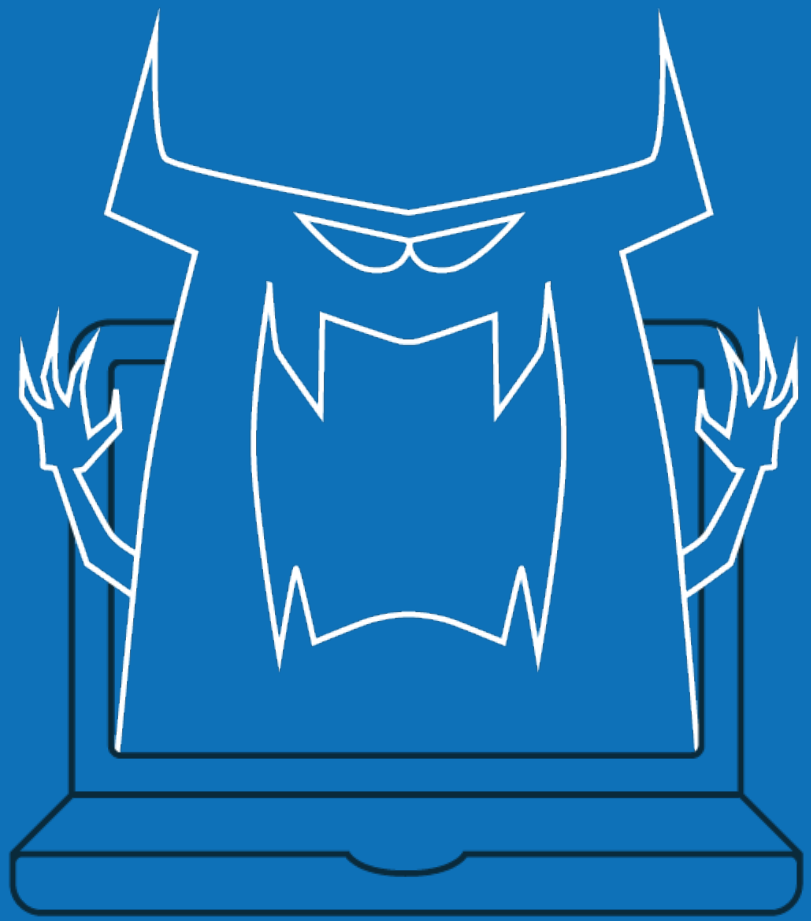


Table of Contents

INTRODUCTION

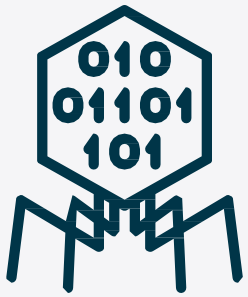
More and more, ransomware has emerged as a major threat to individuals and businesses alike. Ransomware is a type of malware that encrypts data on infected systems and has become a lucrative option for cyber extortionists. When the malware is run, it locks a victim's files and allows criminals to demand payment to release them.

You are probably well aware that ransomware is a hot topic in the news these days. Organizations of all types and sizes have been impacted, but small businesses can be particularly vulnerable to attacks. And ransomware is on the rise. Just to give you an idea of its magnitude, there were 56,000 ransomware infections in March of 2016 alone! $209 million was paid to these ransomware criminals in Q1 2016 (CNN tech, 2016)[1]. These numbers just keep on rising!

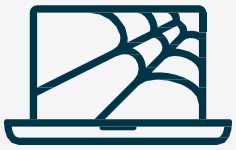
Ransomware is distributed in a variety of ways and is difficult to protect against because, just like the flu virus, it is constantly evolving.

There are however ways to protect your business against ransomware attacks. In this e-book, you'll learn how the malware is spread, the different types of ransomware proliferating today and what you can do to avoid or recover from an attack. Hiding your head in the sand won't work, because today's ransom seekers play dirty. Make sure your organization is prepared!

1. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/



The Angler exploit kit uses HTML and JavaScript to identify the victim's browser and installed plugins, which allows the hacker to select an attack that is the most likely to be successful. Using a variety of obfuscation techniques, Angler is constantly evolving to evade detection by security software products.



RANSOMWARE TODAY

There are a few dominant types, or families, of ransomware in existence. Each type has its own variants. It is expected that new families will continue to surface as time goes on. Historically, Microsoft Office, Adobe PDF and image files have been targeted, but McAfee predicts that additional types of files will become targets as ransomware continues to evolve.

Most ransomware uses the AES algorithm to encrypt files, though some use alternative algorithms. To decrypt files, cyber extortionists typically request payment in the form of Bitcoins or online payment voucher services, such as Ukash or Paysafecard. The standard rate is about $500, though there have been cases of a much higher fee (ranging between $20k - $40k). Cyber criminals behind ransomware campaigns typically focus their attacks in wealthy countries and cities where people and businesses can afford to pay the ransom. In recent months, we've seen repeated attacks on specific verticals, most notably healthcare and education.

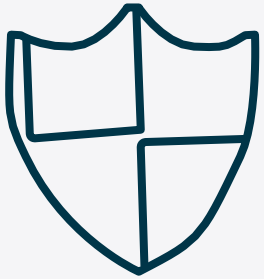
How ransomware is spread

Spam is the most common method for distributing ransomware. It is generally spread using some form of social engineering; victims are tricked into downloading an e-mail attachment or clicking a link. Fake email messages might appear to be a note from a friend or colleague asking a user to check out an attached file, for example. Or, email might come from a trusted institution (such as a bank) asking you to perform a routine task. Sometimes, ransomware uses scare tactics such as claiming that the computer has been used for illegal activities to coerce victims. Once the user takes action, the malware installs itself on the system and begins encrypting files. It can happen in the blink of an eye with a single click.

Another common method for spreading ransomware is a software package known as an exploit kit. These packages are designed to identify vulnerabilities and exploit them to install ransomware. In this type of attack, hackers install code on a legitimate website that redirects computer users to a malicious site. Unlike the spam method, sometimes this approach requires no additional actions from the victim. This is referred to as a "drive-by download" attack.

The most common exploit kit in use today is known as Angler. A May 2015 study, conducted by security software vendor Sophos, showed that thousands of new web pages running Angler are created every day. The Angler exploit kit uses HTML and JavaScript to identify the victim's browser and installed plugins, which allows the hacker to select an attack that is most likely to be successful. Using a variety of obfuscation techniques, Angler is constantly evolving to evade detection by security software products. Angler is just one exploit kit; there are a variety of others in use today.

Spam botnets and exploit kits are relatively easy to use, but require some level of technical proficiency. However, there are also options available for aspiring hackers with minimal computer skills. According to McAfee, there are ransomware-as-a-service offerings, hosted on the Tor network, allowing just about anyone to conduct these types of attacks. Scary!



There are also options available for the aspiring hackers with minimal computer skills. According to McAfee, there are ransomware-as-a-service offerings hosted on the Tor network, allowing just about anyone to conduct these types of malicious attacks.

COMMON TYPES OF RANSOMWARE

As previously noted, ransomware is constantly evolving and new variants are appearing all the time. So, it would be difficult, if not impossible, to compile a list of every type of ransomware proliferating today.
While the following is not a complete list of today's ransomware, it gives a sense of the major players and the variety in existence.

CryptoLocker

Ransomware has been around in some form or another for the past two decades, but it really came to prominence in 2013 with CryptoLocker. The original CryptoLocker botnet was shut down in May 2014, but not before the hackers behind it extorted nearly $3 million from victims. Since then, the CryptoLocker approach has been widely copied, although the variants in operation today are not directly linked to the original. The word CryptoLocker, much like Xerox and Kleenex in their respective worlds, has become almost synonymous with ransomware.

CryptoLocker is distributed via exploit kits and spam. When the malware is run, it installs itself in the Windows User Profiles folder and encrypts files across local hard drives and mapped network drives. It only encrypts files with specific extensions, including Microsoft Office, OpenDocument, images and AutoCAD files. Once the dirty work is done, a message informing the user that files have been encrypted is displayed on said user's screen demanding a Bitcoin's payment.

CryptoWall

CryptoWall gained notoriety after the downfall of the original CryptoLocker. It first appeared in early 2014, and variants have appeared with a variety of names, including: Cryptorbit, CryptoDefense, CryptoWall 2.0 and CryptoWall 3.0, among others. Like CryptoLocker, CryptoWall is distributed via spam or exploit kits.

The initial version of CryptoWall used an RSA public encryption key but later versions (including the latest CryptoWall 3.0) use a private AES key, which is further masked using a public AES key. When the malware attachment is opened, the CryptoWall binary copies itself into the Microsoft temp folder and begins to encode files. CryptoWall encrypts a wider variety of file types than CryptoLocker but, when encryption is complete, also displays a ransom message on a user's screen demanding payment.

CTB-Locker

The criminals behind CTB-Locker take a different approach to virus distribution. Taking a page from the playbooks of Girl Scout Cookies and Mary Kay Cosmetics, these hackers outsource the infection process to partners in exchange for a cut of the profits. This is a proven strategy for achieving large volumes of malware infections at a faster rate.

The spam campaigns spreading Locky are operating on a massive scale. The malware is spread using spam, typically in the form of an email message disguised as an invoice. When opened, the invoice is scrambled and the victim is instructed to enable macros to read the document.

When CTB-Locker runs, it copies itself to the Microsoft temp directory. Unlike most forms of ransomware today, CTB-Locker uses Elliptic Curve Cryptography (ECC) to encrypt files. CTB-Locker impacts more file types than CryptoLocker. Once files are encrypted, CTB-Locker displays a ransom message demanding payment in, you guessed it, Bitcoins.

Locky

Locky is a relatively new type of ransomware, but its approach is familiar. The malware is spread using spam, typically in the form of an email message disguised as an invoice. When opened, the invoice is scrambled, and the victim is instructed to enable macros to read the document. When macros are enabled, Locky begins encrypting a large array of file types using AES encryption. Bitcoin ransom is demanded when encryption is complete. Are you sensing a pattern here?

The spam campaigns spreading Locky are operating on a massive scale. One company reported blocking five million emails associated with Locky campaigns over the course of two days.

TeslaCrypt

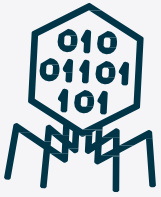
TeslaCrypt is another new type of ransomware on the scene. Like most of the other examples here, it uses an AES algorithm to encrypt files. It is typically distributed via the Angler exploit kit specifically attacking Adobe vulnerabilities. Once a vulnerability is exploited, TeslaCrypt installs itself in the Microsoft temp folder. When the time comes for victims to pay up, TeslaCrypt gives a few choices for payment: Bitcoin, PaySafeCard and Ukash are accepted here. And who doesn't love options?

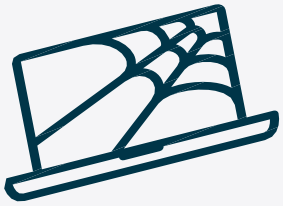
TorrentLocker

TorrentLocker is typically distributed through spam email campaigns and is geographically targeted, with email messages delivered to specific regions. TorrentLocker is often referred to as CryptoLocker, and it uses an AES algorithm to encrypt file types. In addition to encoding files, it also collects email addresses from the victim's address book to spread malware beyond the initially infected computer/network— this is unique to TorrentLocker.

TorrentLocker uses a technique called process hollowing, in which a Windows system process is launched in a suspended state, malicious code is installed, and the process is resumed. It uses explorer .exe for process hollowing. This malware also deletes Microsoft Volume Shadow Copies to prevent restores using Windows file recovery tools. Like the others outlined above, Bitcoin is the preferred currency for ransom payment.

Let's help employees help themselves by learning the different types of scams used by hackers.





CYBER SCAMS 101

At the root of the majority of ransomware attacks is the tactic of social engineering, leveraged by hackers, which involves manipulating a person in order to access corporate systems and private information. Social engineering plays into human nature's inclination to trust. For cyber criminals, it is the easiest method for obtaining access to a private corporate system.

Here are the most common and effective social engineering scams;

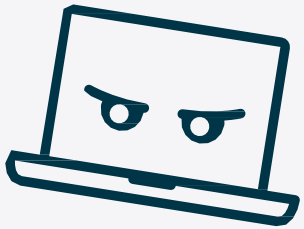
Phishing: the leading tactic leveraged by today's ransomware hackers, typically delivered in the form of an email, chat, web ad or website designed to impersonate a real system and organization. Often crafted to deliver a sense of urgency and importance, the message within these emails often appears to be from the government or a major corporation and can include logos and branding.

Baiting: involves offering something enticing to an end user in exchange for private data. The "bait" comes in many forms, both digital, such as a music or movie download, and physical, such as a branded flash drive left out on a desk for an end user to find. Once the bait is taken, malicious software is delivered directly into the victim's computer.

Quid Pro Quo: involves a request for the exchange of private data but for a service. For example, an employee might receive a phone call from the hacker posed as a technology expert offering free IT assistance in exchange for login credentials.

Pretexting: when a hacker creates a false sense of trust between themselves and the end user by impersonating a co-worker or a figure of authority within the company in order to gain access to private data. For example, a hacker may send an email or a chat message posing as the head of IT Support who needs private data in order to comply with a corporate audit (that isn't real).

Tailgating: when an unauthorized person physically follows an employee into a restricted corporate area or system. The most common example of this is when a hacker calls out to an employee to hold a door open for them as they've forgotten their RFID card. Another example of tailgating is when a hacker asks an employee to "borrow" a private laptop for a few minutes, during which the criminal is able to quickly steal data or install malicious software.



Security software is essential, however, you can't rely on it alone. A proper ransomware protection strategy requires a three-pronged approach, comprising of education, security, and backup.

PROTECT AGAINST RANSOMWARE

Cyber criminals armed with ransomware are a formidable adversary. While small-to-mid-sized businesses aren't specifically targeted in ransomware campaigns, they may be more likely to suffer an attack.

Frequently, small business IT teams are stretched thin and, in some cases, rely on outdated technology due to budgetary constraints. This is the perfect storm for ransomware vulnerability. Thankfully, there are tried and true ways to protect your business against ransomware attacks. Security software is essential, however, you can't rely on it alone. A proper ransomware protection strategy requires a three-pronged approach, comprising of education, security and backup.

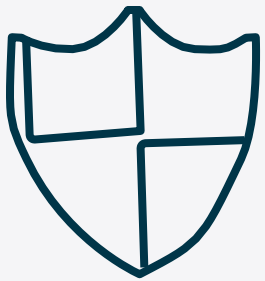
Education

First and foremost, **education** is essential to protect your business against ransomware. It is critical that your staff understands what ransomware is and the threats that it poses. Provide your team with specific examples of suspicious emails with clear instructions on what to do if they encounter a potential ransomware lure (i.e. don't open attachments, if you see something, say something, etc.). By educating them on the types of social engineering tactics, as listed on page 6, and showing them examples of such scams would be a great idea and would definitely help in reducing the likelihood of becoming a ransomware victim.

Conduct bi-annual training to inform staff about the risk of ransomware and other cyber threats. When new employees join the team, make sure you send them an email to bring them up to date about cyber best practices. It is important to ensure that the message is communicated clearly to everyone in the organization. Lastly, keep staff updated as new ransomware enters the market or changes over time.

Security

Cybersecurity technology starts with **antivirus software**. Antivirus, as its name implies, is designed to detect, block and remove viruses and malware. Modern antivirus software can protect against ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, adware and spyware. Some products are designed to detect other threats, such as malicious URLs, phishing attacks, social engineering techniques, identity theft and distributed denial-of-service (DDoS) attacks.



A Business Continuity solution is the #1 solution for cybersecurity protection

A **network firewall** is also essential. Firewalls are designed to monitor incoming and outgoing network traffic based on a set of configurable rules – separating your secure internal network from the Internet, which is not considered secure. Firewalls are typically deployed as an appliance on your network and in many cases offer additional functionality, such as virtual private network (VPN) for remote workers.

Patch management is an important consideration as well. Cyber criminals design their attacks around vulnerabilities in popular software products such as Microsoft Office or Adobe Flash Player. As vulnerabilities are exploited, software vendors issue updates to address them. As such, using out-dated versions of software products can expose your business to security risks. There are a variety of solutions available that can automate patch management.

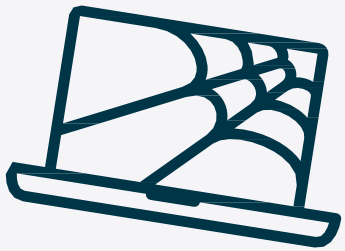
Recent studies have reported that weak passwords are at the heard of the rise in cyber theft, causing 76% of data breaches. To mitigate this risk, businesses should adopt **password management** solutions for all employees. Many people have a document that contains all of their password information in one easily accessible file – this is unsafe and unnecessary. There are many password management apps available today, allowing users to keep track of all of their passwords. If any accounts are compromised, they can change their passwords quickly. Encryption is also an important consideration. Encrypting hard drives ensures that data will be completely inaccessible.

However, because ransomware is constantly evolving, even the best security software solutions can be breached. This is why a secondary layer of defense is critical for businesses to ensure recovery in case malware strikes: backup.

Backup – *The #1 Solution for Cybersecurity Protection*

Modern total data protection solutions, or **Business Continuity** solutions, like QBR, take snapshot-based, incremental backups as frequently as every five minutes to create a series of recovery points. If your business suffers a ransomware attack, this technology allows you to roll-back your data to a point-in-time before the corruption occurred. When it comes to ransomware, the benefit of this is two-fold. First, you don't need to pay the ransom to get your data back. Second, since you are restoring to a point-in-time before the ransomware infected your systems, you can be certain everything is clean and the malware can not be triggered again.

Business Continuity ensures businesses stay up-and-running when disaster strikes.



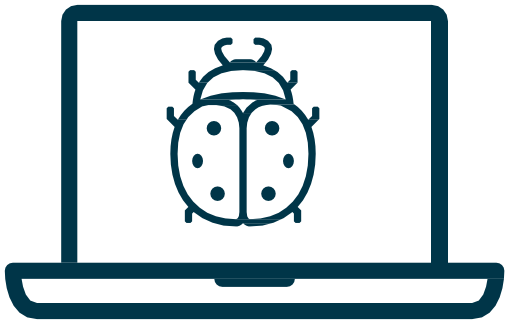
Additionally, some data protection products today allow users to run applications from image-based backups of virtual machines. This capability is commonly referred to as “recovery-in-place” or “instant recovery.” This technology can be useful for recovering from a ransomware attack as well, because it allows you to continue operations while your primary systems are being restored and with little to no downtime. QBR’s version of this business-saving technology is called Instant Virtualization, which virtualizes systems either locally or remotely in a secure cloud within seconds. This solution ensures businesses stay up-and-running when disaster strikes.

ABOUT QBR

QBR (Quick Backup Recovery) is a Business Continuity solution and service, provided by Namtek Consulting Services. It enables users to deliver Recovery Time Objectives (RTO) that meet or exceed the expectations of any Business Continuity plan. QBR has both on-site and off-site capabilities; it performs ‘real-time’ data and full machine backups through virtualization on the QBR device itself and pushes these backups to the Cloud, for optimal data security.

During a crisis, to recover an entire server or simply to fetch a file on one desktop computer, QBR allows for instant data recovery either from the QBR device or from the Cloud. All of this can be done from within a simple management interface, with the help of Namtek Consulting Services’ Disaster Recovery experts. The Business Continuity service solves the worries of business owners and ensures minimal downtime and no data loss. It’s a much-needed insurance policy for a company’s data.

Visit www.quick-backup-recovery.com to learn more or contact us at sales@namtek.ca.



CONCLUSION

Cyber extortionists using ransomware are a definite threat to today's businesses from the local pizza shop to the Fortune 500. However, a little bit of education and the right solutions go a long way. Make sure your employees understand what to watch out for and you can avoid a lot of headaches. Never underestimate the dedication or expertise of today's hackers. They are constantly adapting and improving their weapon of choice. That's why you need top-notch security software and backup. Keep your business safe and give your nerves a break.

To sum it all up, knowledge spreading and security software can help you avoid cyber attacks. Patch management is essential. Be certain that your software is up-to-date and secure. In the end, it is backup, or more precisely Business Continuity, that will help you pick up the pieces when all else fails. Consider using a modern Business Continuity solution, like QBR, that offers features that can permanently eliminate downtime.

CONTACT US

Namtek Consulting Services
400 Blvd Curé-Labelle, Suite 304
Laval, QC H7V 2S7 Canada
Email: sales@namtek.ca
Tel: 450-681-3009
www.namtek.ca