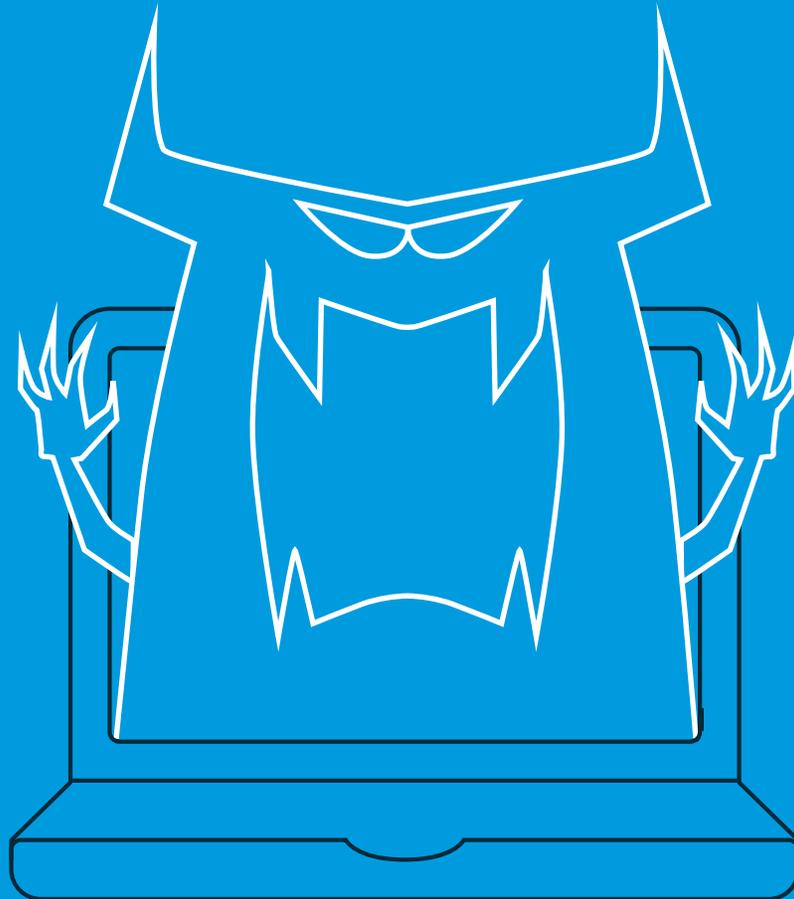MIRUS

THE BUSINESS GUIDE TO RANSOMWARE

Everything 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, a type of malware that encrypts data on infected systems, has become a lucrative option for cyber extortionists. When the malware is run, it locks victim's files and allows criminals to demand payment to release them.

Unless you've been living under a rock, you are probably well aware that ransomware is a hot topic in the news these days. Organisations of all types and sizes have been impacted, but small businesses can be particularly vulnerable to attacks. And ransomware is on the rise. In a recent study conducted by security software vendor McAfee Labs, researchers identified more than 4 million samples of ransomware in Q2 of 2015, including 1.2 million new samples. That compares with fewer than 1.5 million total samples in Q3 of 2013 (400,000 new). 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 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 organisation is prepared.

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 £350, though we've seen much higher. 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.

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 the 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 as well.

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.

Spam botnets and exploit kits are relatively easy to use, but require some level of technical proficiency. However, 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 attacks.

COMMON TYPES OF RANSOMWARE

As noted above, 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 over £2 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 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

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.

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.

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.
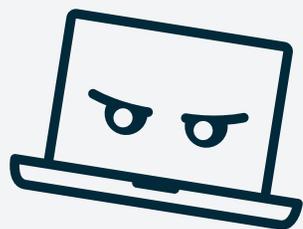
Locky
Locky is a relatively new type of ransomware, but its approach is familiar. The malware is spread using spam, typically in the form of an email message disguised as an invoice. When opened, the invoice is scrambled, and the victim is instructed to enable macros to read the document. When macros 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?

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.

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.

KeRanger

According to ArsTechnica, KeRanger ransomware was recently discovered on a popular BitTorrent client. KeRanger is not widely distributed at this point, but it is worth noting because it is known as the first fully functioning ransomware designed to lock Mac OS X applications.
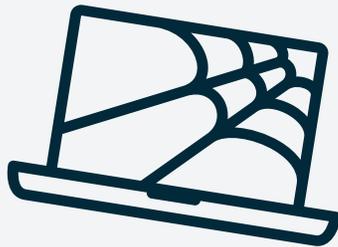
PROTECT AGAINST RANSOMWARE

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.).

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.

Conduct bi-annual formal 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 organisation, not passed around on a word of mouth basis. Lastly, keep staff updated as new ransomware enters the market or changes over time.
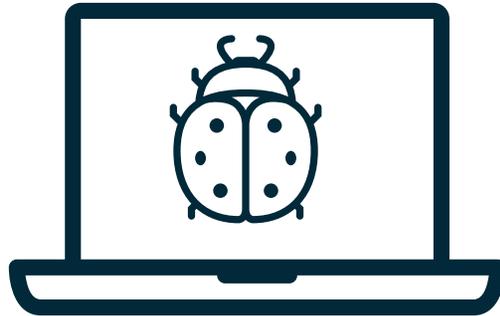
Security: Antivirus software should be considered essential for any business to protect against ransomware and other risks. Ensure your security software is up to date, as well, in order to protect against newly identified threats. Keep all business applications patched and updated in order to minimise vulnerabilities.

Some antivirus software products offer ransomware-specific functionality. Sophos, for example, offers technology that monitors systems to detect malicious activities such as file extension or registry changes. If ransomware is detected, the software has the ability to block it and alert users.

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

Backup: Modern total data protection solutions, like Datto, 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.

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. Datto's version of this business-saving technology is called Instant Virtualisation, which virtualises systems either locally or remotely in a secure cloud within seconds. This solution ensures businesses stay up-and-running when disaster strikes.

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

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 that will help you pick up the pieces when all else fails. Consider using a modern backup product that offers features that can permanently eliminate downtime.

You also might be interested in...

FREE EBOOK

A Simple Guide to Cyber Security

Prepare your business for everything!

DOWNLOAD NOW