THE BUSINESS GUIDE TO

How You Can Avoid Becoming a Victim

Revolution group

datto

Table of Contents

Revolution group

INTRODUCTION

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

Unless you've been living under a rock, you are probably well aware that ransomware is a hot topic in the news today. Organizations 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 eBook, you'll learn how 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.

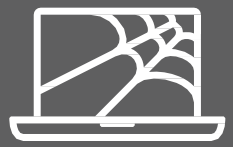
RANSOMWARE TODAY

With many types of ransomware in existence, the usual targets are Microsoft Office, Adobe PDF and image files. McAfee predicts that additional types of files will become targets as ransomware continues to evolve. It is important to learn how ransomware works and how to protect yourself from becoming a victim.

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 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.

*AES stands for Advanced Encryption Standard and is a specification for the encryption of electronic data establish by the National Institute of Standards and Technology in 2001.

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.



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 appear to come from a trusted institution (such as a bank) asking you to perform a routine task. Sometimes, ransomware uses scare tactics to coerce victims, such as claiming that the computer has been used for illegal activities. Once the user takes action, the malware installs itself on the system and begins encrypting files.

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 complicated 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.

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

Ransomware is constantly evolving and new variants are appearing all the time. 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.

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.

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 payment.

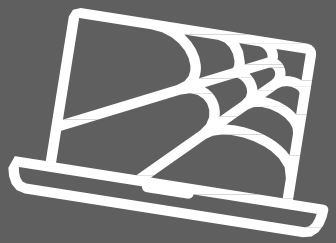
CryptoWall

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.

*RSA stands for Rivest, Shamir, and Adelman who are the inventors of the RSA technique.
*AES stands for Advanced Encryption Standard and is a specification for the encryption of electronic data establish by the National Institute of Standards and Technology in 2001.

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.



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 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.

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, TeslaCrypt gives a few choices for payment: Bitcoin, PaySafeCard and Ukash.

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 mistakenly referred to as CryptoLocker. Torrentlocker 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 comprised of education, security and backup.

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

Education

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 and 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.).

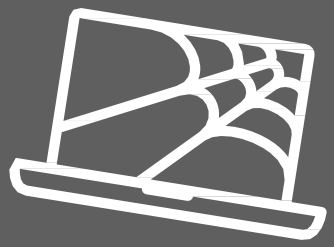
Conduct bi-annual formal training to educate staff about the risk of ransomware and other cyber threats. When new employees join the team, make sure you send them an email to bring them up to date on cyber best practices. It is important to ensure that the message is communicated clearly to everyone in the organization, not passed around via word of mouth. Lastly, keep staff updated as new ransomware enters the market or changes over time.

Security

Antivirus software is 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 minimize vulnerabilities.

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.

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

To create a series of recovery points, total data protection solutions take snap-shot based, incremental backups as frequently as every five minutes. 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 allows you to continue operations while your primary systems are being restored and with little to no downtime.

Revolution group

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 weapons. That's why you need top-notch security software and backup.

Spreading knowledge about 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.

About Revolution Group

Revolution Group is a top-rated, award-winning technology services provider in Central Ohio. Revolution Group can solve your business bottlenecks by gaining insight into your day-to-day business processes and providing your company with solutions that will streamline those processes. Revolution Group allows organizations to discover their full potential and then take the appropriate actions based on those discoveries. Not only does Revolution Group provide their customers with managed IT services, they also provide Salesforce consulting and implementation services, and ERP Manufacturing services.

For more information about Revolution Group, visit www.revolutiongroup.com, read our blog, or follow us on the social media sites below.

Call us today at (614) 212-1111