RANSOMWARE:
a survival guide

ALTARO

CONTENTS

EXECUTIVE SUMMARY

One of the most devastating and prevalent forms of malware threatening consumers and enterprises today is ransomware. The pervasive and damaging type of malware encrypts data and holds it for ransom, extorting victims to pay up or lose out. In this e-book, you will learn about ransomware, how to defend yourself and your users against it, and how to respond should you fall victim to it. At the end of this guide you will also find additional resources and material to learn more.

INTRODUCTION

Ransomware – it's a name that conveys a lot about what can potentially be the most devastating form of malware you might ever encounter. Ransomware is malicious software that parses your local hard drive, any attached removable storage, and even mapped network drives for your data. When it finds data files, like images and media and documents and databases and presentations and more, it encrypts them so that you cannot access them. It then provides you with an ultimatum-pay up, or kiss your data goodbye. While it may be a pain to have to format your computer and reinstall your operating system and all your apps when normal malware hits, that effort is at least manageable. But when irreplaceable photos and videos, or documents you've spent days to weeks creating, or databases containing information you cannot possibly recreate are gone, what can you do? Ultimately, you can either choose to lose that data, or pay off the attackers' ransom demands.

The problem is particularly challenging to deal with when the malware used to distribute the ransomware is so new that it constitutes a "zero-day attack." Zero-day malware is so new that traditional antivirus software, which use signature files to identify known malware, do not detect it.

When attackers combine this zero-day malware with targeted attacks on your business, known as spear phishing attacks, you can quickly find yourself in a very bad situation. But take heart, as this is not a lost cause nor reason to cancel your Internet circuit and go back to paper and pen. There are several things end users and businesses can do to help avoid becoming a victim, as well as strategies you can employ to recover without having to pay up. Keep reading to learn more!

RANSOMWARE EXPLAINED

Ransomware is a type of malware that is becoming more and more common lately. Wikipedia's page on ransomware defines it as "a Cryptovirology attack carried out using covertly installed malware that encrypts the victim's files and then requests a ransom payment in return for the decryption key that is needed to recover the encrypted files." Microsoft's blog post on ransomware defines it as "Ransomware is a type of malware that holds computers or files for ransom by encrypting files or locking the desktop or browser on systems that are infected with it, then demanding a ransom in order to regain access." Both are accurate, but really don't convey the nastiness that is ransomware. Consider all the data on your computer, or that you have Change access to on the network. That could be your kid's first birthday party or their high-school graduation, or the video of your wedding, or your tax returns for the past five years, or the only surviving copy of your grandmother's best recipes. Or, it could be the RFP from your largest customer, or the secret formula for your company's best product, or that workbook you base your business predictions on that has evolved over the past five years and which you cannot function effectively without.

Whatever that data is…imagine that I took it from you. I dangle it in front of you, and demand that you give me your lunch money or I will drop it into the toilet and flush it away forever. It's right there. You can see it. But you cannot do anything about it except pay up. That's what ransomware is. It's an Internet bully blackmailing you for your lunch money, but on a cyber scale.

Ransomware encrypts your data using algorithms that cannot be cracked or reversed in practical terms. We're not talking about password protecting a Word document. We're talking about applying things like AES 256 or other strong encryption to all of your critical data, using a key that is unique to you. Either you pay up, or you lose the data. No one is going to brute force the password, or figure out a way to reverse it for you. You can't go online to find someone else who fell victim, paid up, then posted the passphrase online so you wouldn't have to do the same thing. You can either pay up, or consider all of the encrypted data to be gone baby gone and lost forever.

Some ransomware just renders your files inaccessible, with a text file left in the directory for you to find in order to read the ransom note. Others can open a web browser and open the ransom note from a web server, or pop up a dialog box. The most recent, Cerber, went so far as to include an audio ransom note. However, a victim becomes aware of the fact that they are now in a bad way, the ransom demands have some things in common. Tim Rains of Microsoft recent published a blog post entitled "Ransomware: Understanding the Risk" which summarizes the common elements of ransomware very well. Common elements in ransom notes include:

- making encrypted data unrecoverable after a certain period of time
- threatens to post captured data publicly
- claims to be law enforcement and threaten prosecution
- an increasing cost for the ransom the longer the user waits to pay up
- threats to render the machine unbootable
- threats to erase all data and render all enterprise computers inoperable
- demands payment through various difficult or impossible to trace methods, with Bitcoin being the most common today.

Users can pay up in the hope that they get the decryption key, or they can flatten their systems and start over again, hopefully restoring their data from backup. If they choose to pay, they may have to visit a website linked in the ransom note in order to process the payment. They may or may not receive the decryption key as soon as they enter payment…that's of course another risk. You pay up, and are still out your data.

Let's look more closely at some of the major ransomware variants that are in the wild.

HISTORY AND MAJOR VERSIONS

Ransomware is not exactly new, but it's definitely experiencing a surge in commonality. The first known and documented ransomware was all the way back in 1989, with a piece of malware known as both AIDS and PC Cyborg. 2005 saw more ransomware with several different types in the wild that were both more widespread and sophisticated. Ransomware "hit the big time" in 2013 with Cryptolocker, a type of malware that made widespread news and is estimated to have netted attackers millions of dollars. Let's take a closer look at some of the most significant versions of ransomware since 2005.

AIDS/PC CYBORG

Known by both names, this ransomware was allegedly written and used by a single individual, Joseph Popp, in 2005. AIDS would both encrypt and hide files and demand a US $189 ransom to regain access to the data. Popp was arrested but found unfit to stand trial. Interestingly, AIDS used symmetric key encryption, and the key was stored in the code of the malware. Of course, for most of his victims, this made no difference.

GPCODE

First appearing around 2005, there have been numerous variants of Gpcode. Early versions used symmetric key encryption and/or deleted the unencrypted versions of files, making it fairly easy for some users to recover their data without paying the $100 to $200 ransom demand left in TXT files in each directory. Others used a proprietary algorithm which was flawed and quickly broken by researchers. As Gpcode evolved, it started to use asymmetric encryption and proper encryption algorithms such as RSA and/or AES, and overwriting the unencrypted files to prevent recovery without payment.

REVETON

In 2012, the ZeuS botnet gave rise to the Citadel Trojan which was used to spread Reveton, a piece of ransomware with a new twist started to hit mostly European victims. Purporting to be from a law enforcement agency, and frequently branded or customized to the region the victim was in, this ransomware claimed that illegal content had been found or illegal activity detected, and fines had to be paid to the particular law enforcement agency to unlock the computer. Of course, these "fines" had to be paid through various online and anonymous means. The warnings frequently included the victim's IP address to convey legitimacy, and some even took images from the victims' webcam to appear as if the user was under surveillance. In a twist of fate that shows even some of the darkest clouds have silver linings, one victim was actually guilty of child pornography and turned himself in to his local law enforcement. Several arrests have been made in connection to Reveton but it is still in the wild with new variants cropping up.

CRYPTOLOCKER

Ransomware became a part of practically every computer users' vocabulary with the appearance of CryptoLocker in 2013. Using asymmetric encryption, overwriting the unencrypted files, demanding ransom payable in the untraceable crypto-currency Bitcoin, and spawning multiple variants including some ransomware as a service, it's estimated that victims have paid US $27 million in ransom since CryptoLocker first struck. The original CryptoLocker was eventually shut down when a cooperative operation between several law enforcement and industry players took down the ZeuS botnet, but new variants continue to crop up.

CRYPTOWALL

Becoming prominent in 2014, one of CryptoWall's most common distribution methods was through malvertising on the Zedo ad network. Countless sites were unwittingly contributing to the spread by hosting ads they didn't even realize were bad. CryptoWall has evolved a few times, and includes spreading through Javascript in email attachments, and the ability to encrypt not only files but also the shadow copies created by the Windows Volume Shadow copies, as well as installing malware to steal passwords and Bitcoin wallets.

CERBER

The most recent ransomware is known by several names, including Cerber. This malware typically spreads through email, and after encrypting your files, plays an audio file as well as displaying its ransom demands on screen. It provides very detailed instructions on how to obtain a Bitcoin wallet, purchase Bitcoins, and pay up to get your decryption keys. All in all, it's very thorough. It has also been observed to connect to remote systems through the Tor network, but whether that is for registering another victim or loading other malware has not been confirmed.

WHY ANTIVIRUS SOFTWARE ALONE IS NOT SUFFICIENT

Many users may think that as long as they have antivirus software, they should be protected. If only it were that easy. There are two main problems with antivirus software. One is straightforward to address, though not that easy. Older ransomware can be caught by your antivirus software, but that usually depends upon signature files to catch malicious code before you run it. The first problem posed by that is depending upon users, especially end users at home, to run antivirus software, keep it current, and set it to scan all files on access. Getting users to buy antivirus software after the free trial is up is hard enough, but if they think antivirus software slows their system down, they are just as likely to disable or uninstall it, rendering it worse than worthless since most users will act as if they have antivirus software and take unnecessary risks.

The second problem with antivirus software is that if it depends upon signatures to detect malware, then it must have an up to date signature file. That means that the malware has to have been around long enough to be detected, and added to the signature file. Often, ransomware and zero-day attacks go in the same breath, meaning that the particular ransomware is so new that there is no signature file for it. When you download an infected file or receive an infected attachment for which there is no signature, your files are encrypted before you know what has happened.

Admins may think that antivirus software on their servers will protect them from ransomware if it gets into their environment through a user's system. If only it were so. Ransomware running on a client PC that is accessing data on file shares to encrypt it looks, to antivirus software running on the server, no different from legitimate access by users to that data. If the user has Change permissions to the data, then the malware will be able to encrypt the data stored on the servers, without triggering any response from antimalware software running in the server. Your sysadmins think they are protected…but they aren't.

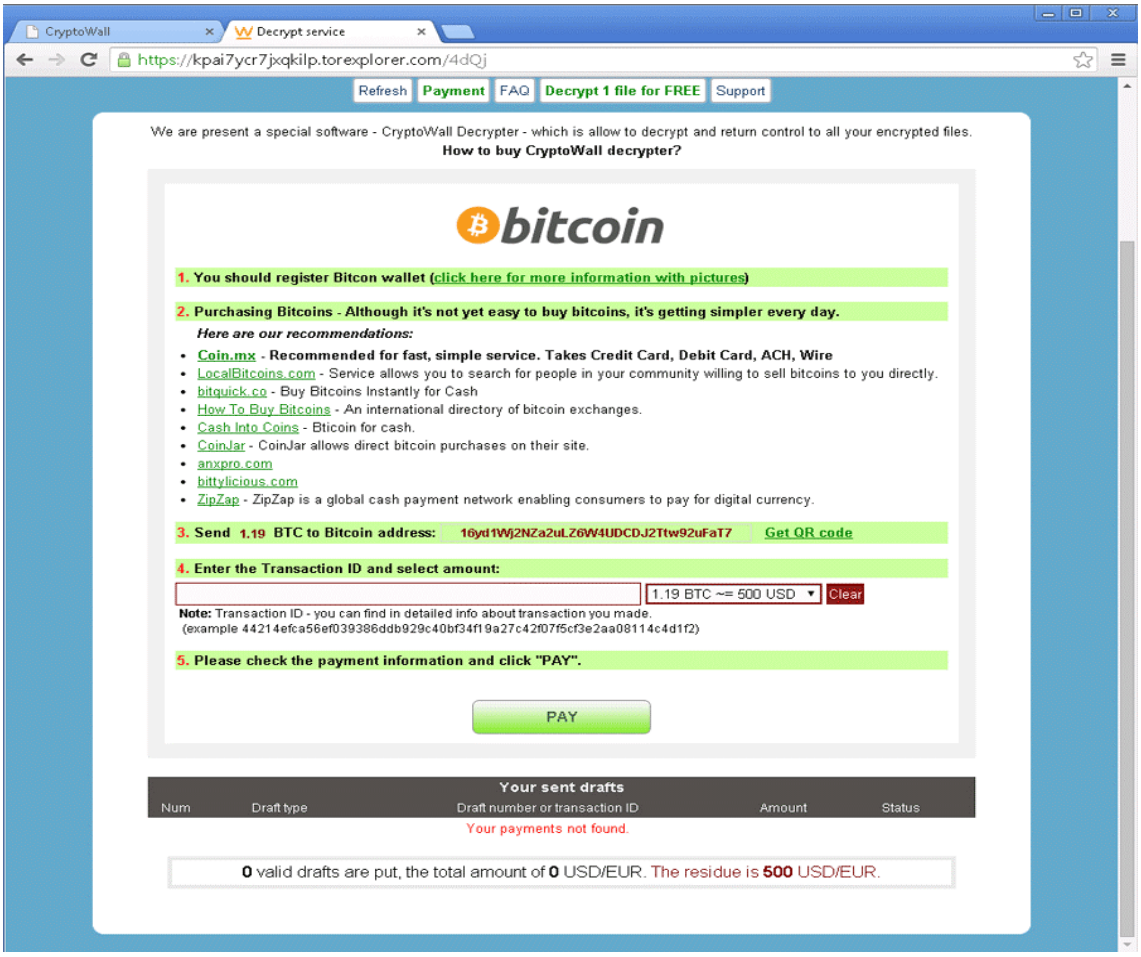
WHAT TO LOOK FOR

The biggest problem with looking for signs that ransomware is running rampant somewhere in your environment is that the symptoms are all there after the damage is done. Anything you could look for to determine if ransomware is present will only be there as a result of the malware having already encrypted your files. However, the quicker you can identify it's somewhere on your network, the sooner you can start to respond, so here are some things to look for.

RANSOM DEMANDS

The most obvious sign you've been hit by ransomware is the actual ransom demand that pops up on screen. These are not subtle. They aren't cut out from newspaper clippings, but they are just as intimidating. Here are some examples.

CryptoWall presents a straightforward sales pitch to buy CryptoWall decrypter. Grammar is not their strong suit, but the colours are rather soothing, as if to imply it's going to be okay.



We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- **Coin.mx - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bticoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.19 BTC to Bitcoin address: 16yd1Wj2NZa2uLZ6W4UDCDJ2Ttw92uFaT7

4. Enter the Transaction ID and select amount:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

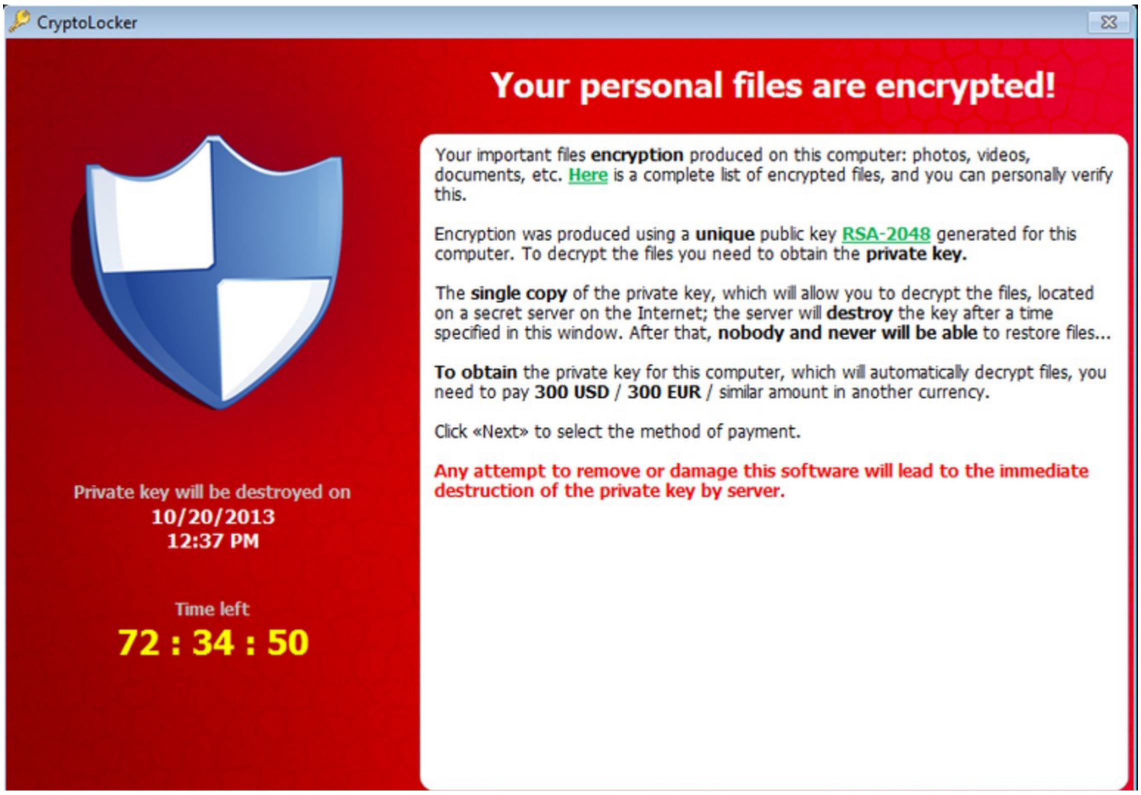
5. Please check the payment information and click "PAY".

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status
		Your payments not found.		

0 valid drafts are put, the total amount of **0** USD/EUR. The residue is **500** USD/EUR.

CryptoLocker, on the otherhand, presents an in-your-face do this or else notification, with red, the colour of danger.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

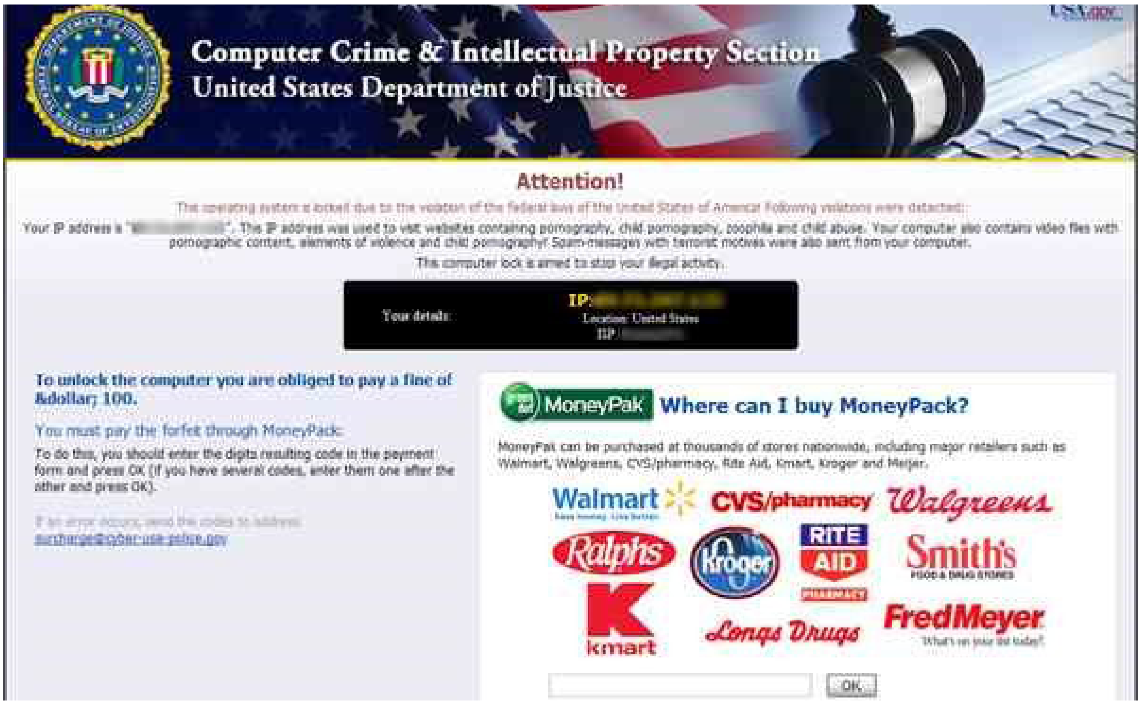
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50

THREATS FROM "LEGAL AUTHORITIES"

As detailed above, Reveton purports to be from a legal authority and the ransom is disguised as a "fine."



Computer Crime & Intellectual Property Section
United States Department of Justice

Attention!

The operating system is locked due to the violation of the federal laws of the United States of America! Following violations were detected:

Your IP address is "[redacted]". This IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

Your details: IP:[redacted]
Location: United States
ISP: [redacted]

To unlock the computer you are obliged to pay a fine of &dollar; 100.

You must pay the forfeit through MoneyPack:

To do this, you should enter the digits resulting code in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address: surcharge@cyber-usa-police.gov

MoneyPak **Where can I buy MoneyPack?**

MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Walmart, Walgreens, CVS/pharmacy, Rite Aid, Kmart, Kroger and Meijer.

OK

INACCESSIBLE FILES

Data on network shares that cannot be opened is one sure sign. Some ransomware renames files as well as encrypting them, so strange names on files is another sign.

USER REPORTS

Users need to understand how important it is to immediately contact the help desk if a ransom demand pops up on their screen, and the help desk needs to know that they need have the user immediately disconnect their system from the network, and then to notify information security upon receiving a user report.

LOG FILES

If you are monitoring your logs and auditing file system access, sudden spikes in file system access, especially with renames, is a pretty good warning. The same could hold true for audit failures if a system/user attempts to modify all files in a directory and fails. The ransomware is going to try to modify any data it can access. It won’t first peek to see if it has change or only read permissions.

PROTECTION STRATEGIES, OR THE BEST DEFENSE IS A LAYERED DEFENSE

There are several things you can do to help protect yourself from ransomware. Protection strategies are intended to provide protections against an attack getting in, or succeeding, in the first place. These can include several things which you may already be doing.

LIMITING USER RIGHTS

Least privilege is a key component of protecting against any malware, including ransomware. If users don't need admin rights to their systems, don't give it to them. That way, malware may not even be able to run on their system since most types must be executed. Limiting file system access on network shares to Read for data that users don't need to make changes to will prevent ransomware from encrypting those files. Eliminating shares that are open to all, or worse, allow anonymous access, is always recommended, but can reduce the scope of damage ransomware could cause.

ANTIMALWARE SOFTWARE

Even with the threat from zero day attacks, antimalware software is critical and should be running on ALL systems that have a network card. Workstations and servers alike should always run antimalware software that reports back to a central console, scans on all real time access, and checks for updates several times a day. The best antimalware software supports push updates, and can be locked so that even system admins cannot disable it. Because if they can, you know that they will. It only takes on system, run by a user with admin rights, to become infected with ransomware to cause you mass damage.

BLOCKING ATTACHMENTS

Many types of malware propagate through email, either as attachments or embedded as Javascript. While there are some definite impacts to business functionality with these suggestions, you might consider blocking all attachments at the email gateway, and rendering all emails as plaintext only, to eliminate these vectors. Again, your business may rely upon attachments, and your users may demand RTF or HTML email, so make sure your email gateway also scans for malware to help reduce the risks. Zero-days are still a threat, but every little bit helps.

EXECUTION CONTROL

Some companies with well-defined workstation images, standard deployments of software, and the ability to push any/all apps users require, may be able to implement an execution control policy so that unapproved/unrecognized applications cannot run on workstations. Windows 7 and later can use AppLocker to manage software running on workstations. Applocker can

Help prevent malicious software (malware) and unsupported applications from affecting computers in your environment.

- Prevent users from installing and using unauthorized applications.
- Implement application control policy to satisfy portions of your security policy or compliance requirements in your organization.
- You can read more about AppLocker at https://technet.microsoft.com/en-us/library/hh831440(v=ws.11).aspx

New improvements in Microsoft's Edge and Internet Explorer web browsers enable them to run in a sandbox, so even if malware is downloaded, it cannot break out. Other browsers have similar technologies in various stages of implementation that will also help with this, when the malware is loaded by the browser rather than downloaded and then run.

SCANNING DOWNLOADS

Ensuring that your users' Internet access goes through a web content filter before it gets to them is a very effective way to block malware through compromised websites, infected downloads, malvertising, etc. You don't have to play Internet cop and dictate where they can and cannot go on the Internet if you don't want to, just use the content filters to protect against malware. Malware can be contained in downloads or code embedded in websites, but some attackers are taking advantage of advertising networks to deliver their malware. Known as malvertising, attackers post malicious content to ad networks hosted on legitimate websites. Blogs, SMB websites, and social networks frequently use advertising networks to generate revenue, but have little to any visibility or control over what ads are served, since they are not hosting the actual advertisements. When an attacker can inject malware into an ad, they can deploy it through dozens to hundreds of websites.

IMPLEMENT, AND USE, PAWS

Use restricted access workstations for running backup and restore jobs, and ensure that admins only use these for administrative tasks and not surfing the Internet, downloading or installing other software, etc. Microsoft advocates the concept of the Privileged Access Workstation https://technet.microsoft.com/windows-server-docs/security/securing-privileged-access/privileged-access-workstations as an approach to mitigate risk, and it's a great one to consider. Sure, it will cost you more for hardware and operating system, and admin tasks will take longer to perform, but all of those together are a bargain compared to the costs of a single ransomware event.

USE EXCHANGE ONLINE PROTECTION WITH ADVANCED THREAT PROTECTION

One of the biggest challenges with ransomware is that it is so often zero-day malware. Signatures don't exist yet, so signature based antimalware cannot protect users. With email being a very popular distribution method for ransomware, message hygiene solutions that do more than just signature based scans are going to become more and more important to protect users. Microsoft offers Exchange Online Protection for both Office 365 and on-prem systems to perform your traditional message hygiene, but also offers Advanced Threat Protection to help against zero-days. Like a TSA agent blowing up a suitcase, ATP actually opens and executes all attachments in sandboxed virtual machines. If a piece of malware is embedded, it will catch the behaviours like writing to files, reading from memory, adding registry keys, etc. before the attachment gets to the recipient. While nothing is 100% foolproof, it's pretty effective.

PLAN FOR THE FUTURE

Today, ransomware goes after files that end users create/modify/depend upon, either for their professional or personal lives. Exchange databases, SQL databases, Active Directory DITs, etc. have not been seen to be targets…but that could all change in the future, especially given the extremely high value of such targets. Make sure that the service accounts under which your core applications run are not the same accounts users (even admins) use to do anything else, and be very careful to limit what admins do while logged on as admins.

USER TRAINING

Yes, yes, I know. The last thing you want to do is get into end user training, but they are not only the reason you have a job, they are also your last line of defense! No matter what you do, something, sometime, is likely to get through. Training your users to be suspicious of any attachments in email, and to only download software from known good websites will go a long way to reducing the chances of infection. Ensuring they know they can report any oopses without fear of getting in trouble will help minimize the damages from someone making a mistake. And for Pete's* sake, please make sure users know it's not only okay, but actually encouraged, that they report it if something goes wrong. Don't yell at them for clicking something they shouldn't have, or the next user won't say a word, choosing instead to slowing walk the other way while a machine gets pawned.

** Pete is the desktop admin we have locked in the basement working on end-user training. We'll let him out as soon as he agrees to actually deliver the training too!*

MITIGATION STRATEGIES, OR HOW DO I LIMIT THE DAMAGE?

An ounce of prevention is worth a pound of cure, but no matter how hard you try, the odds are stacked against you. At some point, you are going to need that cure and this is where being proactive is so critical. Taking some extra effort now can make the eventual ransomware attack a relative non-issue. Sure, you will need to reimage the machine, but at least you won't be paying up or losing data!

LEAST PRIVILEGE

If your users don't have admin rights to their machines, the odds of them downloading and running malware is pretty slim. But if they do, and let's face it, they probably do, least privilege in the file system can still minimize the damage that malware can do. If users don't need CHANGE access to data, don't give it to them. READ is often good enough, and with only READ, any malware running in their security context will be unable to encrypt those files.

BACKUPS, BACKUPS, BACKUPS

As with any other possible data loss, having backups makes it straightforward to recover. When your backup your data, you have a way to recover. But there are lots of strategies for backup, and lots of ways to do backups, both right and wrong. Ensuring you have the right approach is critical to ensuring your mitigations will be successful.

If you read closely the examples of ransomware above, you saw CryptoWall not only will encrypt your files, but can also encrypt the VSS copies of data you may be storing online to protect against data loss. Files stored using local copies synched to the cloud can help with this if versioning is enabled. Once you have a clean machine, you can log onto the web portal and delete the encrypted versions and recover the unencrypted version. That's a great approach for personal files, but not for enterprise data. For that, you must have backups. Ensure these backups are stored offline and inaccessible from users, so that if a piece of ransomware does get into your environment and starts wreaking havoc, it cannot access these backups. Disk to disk backups can be a workable strategy, as long as the backup copy is not accessible, but when it comes to ransomware, offline backups are a definite step up.

Of course, what do you back up and how often do you do it? Backups can be costly from many perspectives, including administrative overhead, costs of tapes and storage, offsite storage, and coordinating backup windows. Here are some strategies to provide the most mitigation against malware. Here is an approach sysadmins can take to help protect their data.

1. Take the time to identify and categorize all data on the network. While it might be great to clean up, reorganize, and consolidate, resist the urge to do that right now. You want to get your backup strategy down first. Then you can worry about Spring Cleaning.

2. Perform full backups daily for end user data, as this is the data most likely to be encrypted by ransomware. You may not need to store these backups offsite, or at least not each day's worth, but you do want to make sure you have a backup of everything that could easily fall victim to ransomware.

3. Perform full backups daily for enterprise data which end users have direct CHANGE access to. Not only is this data likely to be encrypted by ransomware, it will be the costliest to lose when that happens. Since this data is so critical, it makes sense to store it offsite every day to mitigate risks from site disasters. Offline replication to a secondary site may be an option here.

4. Use a combination of incremental and full backups for data that is not directly accessible to end users but is important to protect.

5. Whether using tape or disk, ensure that you store all backups offline to ensure that they cannot be accessed by users, including administrative users, who might fall victim to ransomware. This can be referred to as a "two-step" backup plan, and ensures that your data is protected even if a "wildfire" event occurs because an admin launches ransomware. Tapes are not something an admin could mount like a filesystem, but disk to disk based storage is easily accessible to admins, and we all make mistakes too. Keeping a second, offline backup ensures you have something to fall back to.

6. Don't forget local data! No matter how many times you tell users not to, they are always going to store some data on their local machine. Implement a backup solution that works with your workstations as well as your servers, so that nothing gets missed. Again, the costs for that are negligible compared to what paying a single ransom demand would cost.

When choosing a backup solution, here are some things you should look for:

1. Full support for all operating system versions on your network. Remember, don't overlook your workstations when evaluating this.

2. The ability to backup deltas only, both to save time and bandwidth.

3. For your workstations, automatically initiated backup operations when network connectivity is established, so that you don't have to rely on end user action and you protect all those travelling users too.

4. Consider versioning, especially to protect against ransomware that gets into your environment and runs for a period of time before it is detected.

5. Ensure your backups are inaccessible to users who might inadvertently execute malware. Those backups are no good to you if they too are encrypted. Don't look at files replicated to another location as safe unless users have no rights and access to them.

6. Time, time, time-it's all about the time. A Full Backup every single night could take a lot of time every single night, but the restores will be the fastest possible. Using incremental or differential will make restore times take longer. How frequently you back up determines how much data you could still lose. Your Recovery Time Objective (RTO) is how long you want it to take to get back up and running. Your Recovery Point Objective (RPO) measures how much data could be lost if you must resort to a restore. Companies that must run 24x7 don't have backup windows, and might short themselves in the interest of keeping production going. That may seem smart in the short term, but consider the larger ramifications. If you are losing $10K an hour waiting for a restore, paying a $5K ransom to decrypt your files is a bargain. If your daily backup misses data created today with a value in excess of the ransom, then again the financial decision may be to pay up. Make sure your backup/restore solution has both the RTO and the RPO to support the business need. And if your current solution doesn't, you really want to look at its replacement. You don't want to create a situation where paying the bad guys off is a good business decision. That's a little too much like the digital equivalent of paying the mob for protection!

7. Consider Altaro's flagship product, Altaro VM Backup. While data located on a user's workstation is certainly valuable, any core piece of company data should reside on a server somewhere in the environment. Add on top of that, that the vast majority of business computing workloads are now hosted on top of some virtualization technology such as Hyper-V or VMware, you need a backup solution that can address the main data protection concerns of backup today. Altaro VM Backup can backup and protect entire virtualized workloads, and in the event of a ransomware event, can recovery just the affected files or the entire workload if needed.

INSURANCE

Talk to your insurance provider. An increasing number of agencies are starting to offer policies to protect against financial loss from hacking, malware, et al and ransomware may fall into scope for this. It won't do anything to prevent your users from opening a piece of ransomware, but it will help offset the financial costs of any response or ransom paid, or offset the loss from unrecoverable data.

REACTION STRATEGIES, OR WHAT DO I DO NOW?

Suppose the worst occurs, and ransomware strikes. How you react may depend on how thorough and successful your mitigation strategies are at minimizing the damage.

SINGLE WORKSTATION FALLS VICTIM, LOCAL DATA ONLY WITH BACKUPS

If a single workstation falls victim to ransomware, and you have a backup of all critical data, there's no way you should consider paying the ransom demand. You should work through your normal InfoSec response plan, if you have one. But if not, here's some steps you could take.

1. Isolate the machine. Disconnect it from the network, and ensure no user accesses it. Create a forensic image of the machine to support any investigation. You may instead simply pull the hard drive and swap in a new one so you can get the machine reimaged so the user can go back to being productive. Just be sure that you maintain chain of custody on the drive or image, and secure it for investigation later. Seal it in a tamper evident bag, record who did what to get it to that point, and then lock it away.

2. Notify law enforcement of the incident and the demand for payment. In the US, you can report this to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/default.aspx. Check with your local law enforcement agency if outside of the United States.

3. Make sure though that you identify how the ransomware got into the system, and take the opportunity to ensure everyone learns from the mistake to help prevent it from happening again. That means interviewing the user, reviewing logs on your messaging hygiene system, and going through proxy logs. It's important to identify the source to ensure no one else falls victim to the same thing.

SINGLE WORKSTATION FALLS VICTIM, LOCAL AND NETWORK DATA WITH BACKUPS

Again, proper backups may make this a relative non-event, but that the user had CHANGE access to network data means your restore operations will take longer, more users were likely impacted, and it is more important that you both identify how the ransomware got in, and reevaluate user permissions to see if they are too broad. Working with InfoSec and notifying law enforcement are still key and may help to bring the attackers to justice and prevent this from happening to others.

1. Isolate the machine. Disconnect it from the network, and ensure no user accesses it. Create a forensic image of the machine to support any investigation. You may instead simply pull the hard drive and swap in a new one so you can get the machine reimaged so the user can go back to being productive. Just be sure that you maintain chain of custody on the drive or image, and secure it for investigation later. Seal it in a tamper evident bag, record who did what to get it to that point, and then lock it away.

2. Notify law enforcement of the incident and the demand for payment.

3. Make sure though that you identify how the ransomware got into the system, and take the opportunity to ensure everyone learns from the mistake to help prevent it from happening again. That means interviewing the user, reviewing logs on your messaging hygiene system, and going through proxy logs. It's important to identify the source to ensure no one else falls victim to the same thing.

4. Check the audit logs for all data to which the user has access. Evaluate any file that has been changed to confirm it is still a good copy.

5. Ensure that any other systems which accessed the same data as the infected system are double-checked to confirm the malware has not spread.

6. Make sure though that you identify how the ransomware got into the system, and take the opportunity to ensure everyone learns from the mistake to help prevent it from happening again.

MULTIPLE WORKSTATIONS FALL VICTIM, DATA HAS BACKUPS

Of course you have to ensure the ransomware is gone by burning all the machines with fire… I mean, reimaging them all, but if multiple machines have ransomware, you have a much bigger problem on your hands. You must identify how that malware spread. It may be that everyone downloaded the same file, which means your web filtering solution isn't. Or perhaps it came in through an email and hit a distribution list, which means you need to look at tightening up your email hygiene solution and restricting access to distribution lists from outside senders. But it could also mean that an attacker has gained a foothold on your network, has remote access, and is propagating the ransomware across your network. If that has happened, everything is at risk. The common wisdom amongst information security professionals today is to presume breach, and it's been a core principle that you cannot prove a negative, which means every network everywhere is probably pwned and we're all doomed! But seriously, if you cannot find a common cause for multiple machines becoming infected with ransomware, you have to assume you're pwned. Burning it all down and starting over may be the only way to ensure your system is clean. If you don't have an information security team, seek professional services immediately to help assess that need, and if it is necessary, to complete the work. Beyond that, the guidance is the same as above.

ANYTHING FALLS VICTIM AND YOU DON'T HAVE A BACKUP

In the worst case scenario, you may have no other choice but to pay up. Consider the ransom demand, and measure that against the cost to replace or recreate the encrypted data. If the data, or the cost to replace it, outweighs the ransom demand, you may have to pony up the cash. But consider the demand and how likely it is that, after you have paid, you will actually get your data back. The more "professional" attackers will have better grammar, will require payment through Bitcoin, and you may be able to find out more online from others who have been victimized to confirm whether they received the decryption keys after paying up, or not. With many ransomware attacks, time is of the essence, since the offer may expire or the ransom go up, so move smartly. And no matter what, ensure you contact local law enforcement for guidance. Ransomware is a serious problem online, with elements of extortion, racketeering, and conspiracy, and by contacting law enforcement, you may be able to recover some of your losses or at least contribute to the apprehension and prosecution of the attacker(s.)

1. Check online to see if anyone else has reported being hit, and more importantly, actually being able to recover their data after paying the ransom.

2. Evaluate whether it is more cost effective to pay the ransom, or lose the data. Depending upon what it is, you may be able to live without it, or recreate it. Even if it's more expensive to do this, it may be the more reliable approach than paying a ransom to some random bad guy.

3. Move quickly. Often, ransoms will either increase over time, or the option to pay the ransom will expire, or the culprit will disappear, and then you have one less choice.

In any situation where you fall victim to malware, you should also submit a sample of the ransomware to your antimalware vendor, messaging hygiene vendor, web content filtering vendor, etc. If it's a zero-day, and you caught it first, you can at least help others by providing a sample to those vendors so they can update their signatures.
It's of little solace to you, but it's the right thing to do once you have contained the threat.

CLOSING REMARKS

Ransomware can be devastating to any business that is unprepared, or just another technological nuisance for those that are. While there are many strategies a company can take to protect themselves, ultimately it is the tried and true technology of backups that can spell the difference between bother and disaster. Ensuring you have a layered set of protections and a backup strategy without gaps will make sure that when ransomware gets in, and odds are it will, you will be ready to recover quickly and completely, and get your users back up and running in short order.

ADDITIONAL RESOURCES

Would you like to know more? Check out these online resources:

- Ransomware on Wikipedia: https://en.wikipedia.org/wiki/Ransomware
- Privileged Access Workstations: https://technet.microsoft.com/windows-server-docs/security/securing-privileged-access/privileged-access-workstations
- Applocker: https://technet.microsoft.com/en-us/library/hh831440(v=ws.11).aspx
- Advanced Threat Protection: https://blogs.office.com/2015/04/08/introducing-exchange-online-advanced-threat-protection/
- Altaro VM Backup: http://www.altaro.com/vm-backup/
- The FBI's Internet Crime Complaint Center: https://www.ic3.gov/default.aspx

ABOUT ALTARO

Altaro Software (www.altaro.com) is a fast growing developer of easy to use backup solutions used by over 30,000 customers to back up and restore both Hyper-V and VMware-based virtual machines, built specifically for SMBs with up to 50 host servers. Altaro take pride in their software and their high level of personal customer service and support, and it shows; Founded in 2009, Altaro already service over 30,000 satisfied customers worldwide and are a Gold Microsoft Partner for Application Development and Technology Alliance VMware Partner.

ABOUT ALTARO VM BACKUP

Altaro VM Backup (formerly known as Altaro Hyper-V Backup) is an easy to use backup software solution used by over 30,000 SMB customers to back up and restore both Hyper-V and VMware-based virtual machines. Eliminate hassle and headaches with an easy-to-use interface, straightforward setup and a backup solution that gets the job done every time.

Altaro VM Backup is intuitive, feature-rich and you get outstanding support as part of the package. Demonstrating Altaro's dedication to Hyper-V, they were the first backup provider for Hyper-V to support Windows Server 2012 and 2012 R2 and also continues support Windows Server 2008 R2.

For more information on features and pricing, please visit:

http://www.altaro.com/vm-backup/

Don't take our word for it – Take it for a spin!

DOWNLOAD YOUR FREE COPY OF ALTARO VM BACKUP
and enjoy unlimited functionality for 30 days. After your 30-day trial expires you can continue using the product for up to 2 VMs for free, forever. No catch!

ALTARO VM BACKUP

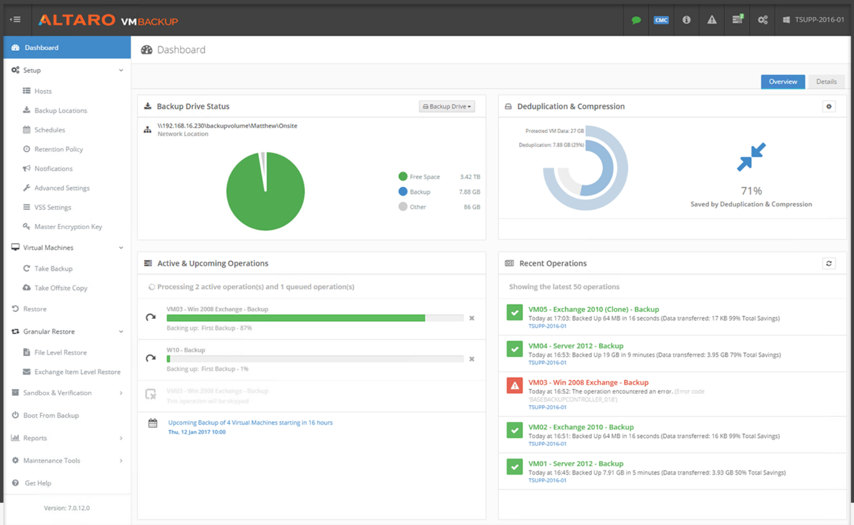
Altaro VM Backup - Trusted by over 30,000 SMBs

New v7! Altaro VM Backup for Hyper-V & VMware. Hassle-free and affordable VM backup software.
Grab your free copy for 2 VMs now!

- ✓ Hassle-free and effective
- ✓ Unbeatable Value
- ✓ Outstanding Support

Free for 2 VMs, forever.

Back up unlimited VMs for 30 -days. After 30-days you get 2 VMs for free, forever. Download now!



\\192.168.16.230\backupvolume\Matthew\Onsite
Network Location

Free Space	3.42 TB
Backup	7.88 GB
Other	86 GB

Protected VM Data: 27 GB
Deduplication: 7.88 GB (29%)
71%
Saved by Deduplication & Compression

Processing 2 active operation(s) and 1 queued operation(s)

VM03 - Win 2008 Exchange - Backup
Backing up: First Backup - 87%

W10 - Backup
Backing up: First Backup - 1%

VM03 - Win 2008 Exchange - Backup
This operation will be skipped

Upcoming Backup of 4 Virtual Machines starting in 16 hours
Thu, 12 Jan 2017 10:00

Showing the latest 50 operations

VM05 - Exchange 2010 (Clone) - Backup
Today at 17:03: Backed Up 64 MB in 16 seconds (Data transferred: 17 KB 99% Total Savings)
TSUPP-2016-01

VM04 - Server 2012 - Backup
Today at 16:53: Backed Up 19 GB in 9 minutes (Data transferred: 3.95 GB 79% Total Savings)
TSUPP-2016-01

VM03 - Win 2008 Exchange - Backup
Today at 16:52: The operation encountered an error. (Error code 'BASEBACKUPCONTROLLER_018')
TSUPP-2016-01

VM02 - Exchange 2010 - Backup
Today at 16:51: Backed Up 64 MB in 16 seconds (Data transferred: 16 KB 99% Total Savings)
TSUPP-2016-01

VM01 - Server 2012 - Backup
Today at 16:45: Backed Up 7.91 GB in 5 minutes (Data transferred: 3.93 GB 50% Total Savings)
TSUPP-2016-01

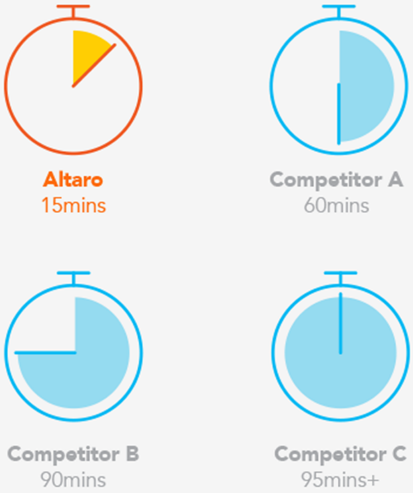
Backup Now!

Up and running quickly, without the need for complex configurations!

With Altaro VM Backup, you can install and run your first virtual machine (VM) backup in less than 15 minutes. Get up and running quickly, without the need for complex configurations or software dependencies.

Altaro VM Backup is designed to give you the power you need, without the hassle and steep learning curve.

- **Easy to use, intuitive UI** - making it easy to implement a rock solid backup strategy
- **Managing and configuring backup/restore jobs across multiple hosts has never been simpler**
- **Full control & scalability** - Monitor and manage all your Hyper-V and VMware hosts from a single console



Virtual machine backup software packed with powerful features for Hyper-V and VMware.

View Features

FOLLOW ALTARO

Like our eBook? **There's more!**

Subscribe to our Hyper-V blog http://www.altaro.com/hyper-v/ and receive best practices, tips, free Hyper-V PowerShell scripts and more here: http://www.altaro.com/hyper-v/sign-up/

Follow Altaro at:

SHARE THIS RESOURSE!

Liked the eBook? Share it now on: