Conversational
Ransomware Defense and Survival

A ConversationalGeek® Book

Sponsored by VEEAM

Learn about:

- What makes Ransomware so difficult to stop
- How to defend against, endure, and recover from a Ransomware attack
- The role of recovery in Ransomware survival

By Orlando Scott-Cowley (Cybersecurity Consultant. CISSP, CCSP, CCSK)

Sponsored by Veeam

Veeam® recognizes the new challenges companies across the globe face in enabling the Always-On Enterprise™, a business that must operate 24.7.365. Veeam has pioneered a new market of Availability for the Always-On Enterprise™ by helping organizations meet recovery time and point objectives (RTPO™) of less than 15 minutes for all applications and data, through a new solution that delivers high-speed recovery, data loss avoidance, verified recoverability, leveraged data and complete visibility. Veeam Availability Suite™, which includes Veeam Backup & Replication™, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs, while always supporting the current and future business goals of Veeam customers.

Founded in 2006, Veeam currently has 45,000 ProPartners and more than 230,000 customers worldwide. Veeam's global headquarters are located in Baar, Switzerland, and the company has offices throughout the world.

To learn more, visit
www.veeam.com .

Conversational Ransomware Defense and Survival

By Orlando Scott-Cowley

ConversationalGeek®

Conversational Ransomware Defense and Survival

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Orlando Scott-Cowley
Project Editor:	J. Peter Bruzzese
Copy Editor:	John Rugh
Content Reviewer:	Karla Reina

Note from the Author

Ransomware has become the threat-du-jour for most enterprise organizations, as they struggle to keep up with the rapidly changing threat landscape and barrage of attacks from money-hungry cybercriminals and hackers. IT teams, cyber and info-sec departments, CISOs and CIOs are left feeling like they're stuck in a giant revolving door that rotates between states of secure and insecure in their environments. Ransomware is the latest in a line of threats to come rolling down their Internet connection causing that door to spin so fast everything becomes a sickening blur.

It's hardly surprising ransomware has become so ubiquitous and successful because of its frankly impressive ability to evolve. It sneaks past existing defenses like secure email gateways and desktop anti-virus with ease, then tricks users into running its viral payload themselves for that added killer punch. All of this, on top of our end-users facing other threats such as phishing, vishing, whaling (or business email compromise), plain old spam, malware and Internet villainy. Just when we thought we'd escaped the latest in that long list of threats, along comes ransomware to test out defenses and preparedness to the max.

If this sounds like you or your organization, then you're not alone. There are lots of euphemisms the security industry uses to describe this process. The most common is "arms race", but you'll also hear "red queen effect", "hamster wheel" or just a lot of muttering, swearing and cursing. The frustration of those affected by these problems is palpable, and most are now looking at a broader cross section of technologies to protect themselves and importantly to recover post-attack, rather than rely on pure-play security solutions alone.

I've been helping organizations protect themselves from a variety of security threats for many years now, and have seen these tactical pivots by hackers and cybercriminals over and over again. Sadly, all we can do is learn to adapt our protections, stay agile and make sure we don't sit back and hope for the best.

This book gives you a little insight into the ransomware threat, without being too complicated and technical, it'll help you understand ransomware and what to do to protect yourself and your organization.

Stay safe out there.

Orlando Scott-Cowley
CISSP, CCSP, CCSK.

The "Conversational" Method

We have two objectives when we create a "Conversational" book: First, to make sure it's written in a conversational tone so it's fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

"Geek in the Mirror" Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it's the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these "geek in the mirror" boxes are not to be skipped.

Within these boxes I can share just about anything on the subject at hand. Read 'em!

Ransomware: The Rise of Malware for Extortion.

Like a pre-owned car, ransomware isn't new, but it may be new to you. Unluckily, you may be learning all about ransomware the hard way. If you are, you have my condolences and I hope your backup regime was thorough enough that you're able to recover from the attack.

For those who have yet to be affected by ransomware but are keen to learn more about the threat, and importantly, how to protect yourself from it or recover once attacked, this book is for you.

Ransomware, or crypto-malware as it's sometimes known, was said to be 'invented' by the mysterious-sounding Dr. J L Popp back in

1989. Dr. Popp was in fact an evolutionary biologist who thought he would increase his notoriety at the World Health Organization AIDS conference in that year, by distributing malware infected diskettes to delegates in the hope they'd stump up $189 to have their computer repaired.

Since those unlikely beginnings, ransomware has come a long way. It's now a fully grown, mature threat to businesses and end-users alike. It's become so successful that ransomware is currently the number one threat to organizations, as well as the tool of choice for cybercriminals looking to earn money from a cybercrime spree.

You may have heard ransomware described in different ways too. Locker or crypto-malware are also common names for the same threat.

Ransomware is a type of malware, or computer virus, and is designed to extort money from its victims by either locking their computer to make it inaccessible, or more commonly encrypting some or all of the files. The cybercriminals and hackers who send and then control the ransomware are hoping victims will pay the 'ransom' in order to get their data back. More on that later.

Today, ransomware is mostly driven through ransomware-as-a-service platforms run by organized crime gangs. They have become so skilled at extorting money from victims, they even set up legitimate sounding 'customer service centers' to make it easier for you to pay the ransom. The average ransomware attack campaign can net the criminals millions of dollars in return for very little risk, expenditure or chance of being caught.

There are several ways you're likely to be infected by ransomware, but by far the most common is through a malicious email attachment pretending to be something it's not. A fake invoice is a great example. Other common infection mechanisms include

shortened links, malvertising, social media, SMS and even traditional old school spam emails. Ransomware even spreads throughout corporate networks, via the inbuilt SMB share system native to Microsoft Windows PCs on the network. I'll explain more about each of these a little later in the book.

Ransomware is a clever little beastie. How does it work?

Ransomware has become the poster child for successful malware everywhere, not only because it's so effective at what it does, but also because it's the model of agile, rapid development on the part of the cybercriminals who write it.

To give you an example, a popular piece of ransomware from 2015 called CryptoWall 2.0 was redeveloped from a completely new code base to CryptoWall 3.0 in as little as 48 hours after the former was effectively hobbled by the security community. The same malware was said to have earned its owners around $350 million.[1] Ask yourself how many enterprise organizations you know with that sort of budget and R&D capability, and you'll quickly see how significant this threat is to the majority of us.

Outgunned is only the starting cliché here, when it comes to ransomware.

So how does ransomware actually work, and what do you need to know about its capabilities to help you protect yourself and/or recover from an attack? Like any software, ransomware benefits

[1] http://www.darkreading.com/endpoint/with-$325-million-in-extorted-payments-cryptowall-3-highlights-ransomware-threat/d/d-id/1322899

from enhancements, bug fixes and improvements; here are a few important milestones to help you understand how 'far' ransomware has come:

Ransomware has always been about extortion; even the earliest versions were designed to trick you into paying money for some sort of fix to your computer. You'll remember the popularity of "fake-antivirus" programs a decade or so ago—although not specifically ransomware, they were designed to extort money from victims, and really set the scene for the cybercriminals as a gateway drug to the much harder class A malware they're addicted to today.

Early ransomware used a 'locker' technology to simply deny you access to your computer, often pretending to be delivered from a law enforcement agency such as the FBI. Again payment was demanded to allow the victim access to their computer. At this stage ransomware didn't encrypt files like is does today.

Very early on, cybercriminals learned the benefit of enterprise technologies such as encryption and email. The infamous Archievus Trojan was the first piece of malware to use asymmetric RSA encryption as a way of denying access to users' files, way back in 2006. Given the ubiquity and inherent trust of enterprise email systems, 2006 also saw email become the chosen distribution mechanism for ransomware too. Malicious email attachments, such as fake resumes, invoices and complaint letters were an easy dropper for malware.

Today's ransomware is much more complex, and is capable of encrypting the entire hard drive, as well as the majority of your files. These tactics have taken over from the basic early 'locker' versions, so it's worth spending a little time looking at how the encryption used in ransomware has developed too, so you understand that the only real defense against the threat is to be fully prepared in advance.

Early versions of file encrypting ransomware used relatively simple encryption compared to today's standards. Sometimes the private

keys for decryption were easily discovered, or weaker symmetric encryption was used, making reverse engineering easier.

CryptoTorLocker (2015), for example, was a variant that hid its decryption key in the malware executable. In other cases, the security community has managed to develop decryption tools, due to poor implementations of file encryption. But, these can't always be relied upon. By 2013, encryption standards had moved on from the early, primitive use of 256 or 666-bit RSA, to the much meatier defense and enterprise grade 256 bit AES with 2048 bit RSA keys. In a move to kick you while you're down, the malware writers also started deleting original files after they'd created an encrypted version, to further limit your ability to recover on your own successfully.

Ransomware is also learning to infect more and more types of devices. Early versions had a hard time of encrypting only a few files types on Windows PCs, but today's Windows malware will take the whole file system and in some cases encrypt your entire hard drive too. And Windows users aren't the only ones affected. The "we don't get viruses" Mac brigade are also starting to be impacted and are looking a little less smug. 2016 saw the arrival of KeRanger, the first legitimate OSX-based ransomware, delivered by BitTorrent client. Rather annoyingly, it's not just PCs and Macs at risk; other devices like Android OS-based smartphones are also targets now too from variants such as Lockerpin[2]. Even Smart TVs are at risk from Flocker[3].

The key to the success of ransomware is its reliance on the human element of computing, by which I mean the fallibility of the person between the chair and the keyboard, PEBKAC if you will. Take, for example, many of the ransomware attacks delivered by email; these

---

[2] http://www.welivesecurity.com/2015/09/10/aggressive-android-ransomware-spreading-in-the-usa/

[3] https://www.neowin.net/news/and-well-be-right-back-after-these-messages-and-ransomware

usually take the form of a very well worded email with an attachment. The email will detail the background to the attachment, encouraging the reader to open the file. Usually as soon as it happens, the ransomware is working away in the background quietly encrypting all the data in the victim's computer. Alarmingly, this often happens once the email has been 'cleared' by the usual gateway and desktop anti-virus applications. How does this happen, I hear you ask? Well, the avoidance of classic anti-virus technology is such an important note that I've dedicated a whole section to it later on.

Once the malware has been activated, it's often too late.

Victims will only realize they've been infected when the warning pops up on their screen. These warnings vary depending on the ransomware used, but will generally tell you all your files have been encrypted and you have to pay to get them back. Often there's a decreasing time-limit to 'encourage' payment before files are deleted—further adding to the tension of the moment.

Ransomware doesn't just spread by email though. There are a number of mechanisms that help it propagate. Look carefully and you'll see ransomware attacks delivered through SMS messages in a bid to entrap certain types of smartphone users. Social media is also an important hunting ground for the threat too; the private or direct messaging systems are abused by attackers who will rely on link shortening services to hide their malware-laden website from unsuspecting victims. Malvertising has also been used to deliver ransomware attacks. Attackers will compromise a legitimate online ad network, and use it to trick browsers into downloading their malicious payload—usually an exploit kit, like Angler or Neutrino—which then deploys ransomware to the victim.

These are commonly known as drive-by and watering hole attacks. In an enterprise networked environment ransomware can be even more insidious, as it will use the Windows networking SMB shares to propagate around the network, infecting other computers as it goes. This is why we see entire networks taken offline during ransomware attacks, as the threat loves the inherent trust built into our LAN infrastructure.

Some variants will even encrypt mapped and unmapped network drives as well as connected cloud services like Dropbox, OneDrive and Box.

Some ransomware superstars of recent times

When it comes to ransomware, these guys were top of their class. You should note the variance in tactics used by each as an indication of the capability of the malware writer, and consider how best you can protect yourself against this technology.

Before you read the following allow me to suggest now that recovery is the best protection from attacks of this sort.

CryptoLocker

The 2013 super-ransomware, that indicated a step change in the way cybercriminals were thinking about ransomware. CryptoLocker spread by malicious downloads from websites and infected email attachments, the content of which was always socially engineered to encourage action on the victim's part. CryptoLocker was the first ransomware to utilize ecurrency as a method of payment too, as Bitcoin was demanded for data decryption.

CryptoWall

Inspired by CryptoLocker, the CryptoWall ransomware was successful throughout 2014 and 2015, and takes the crown for being the most successful ransomware yet, earning its owners millions of dollars. CryptoWall also represents the introduction of ransomware-as-a-service platforms which allow anyone to graduate from traditional crime, i.e. burglary, car-crime, etc., to fully fledged cyber-criminal with little or no technical expertise. CryptoWall went through various versions, from 2.0, 3.0 to 4.0, notably being able to turn around a brand new version over a weekend.

Locky

Locky arrived on the scene for most of 2016, before eventually being retired. Locky is notable because of its reliance on malicious Microsoft Word and Excel macros spread by phishing attacks in email. Locky was delivered in bulk too, by the ominously capable Dridex cybercrime botnet.

PowerWare

Notable because of its reliance on Microsoft Word and the PowerShell scripting interface. As if that wasn't scary enough, PowerWare would infect users through Word files, by downloading a malicious script rather than a signature-able file, making detection even harder than usual.

Petya

Until Petya we'd gotten used to ransomware being a nuisance by encrypting files. Petya wasn't happy with this status quo, and decided to see that tactic and raise it the MBR (master boot record). Effectively, this disabled the entire PC, causing a BSOD (blue screen of death) crash, and adding a skull and crossbones warning when the user rebooted their PC.

Ransom32 & RAA

This ransomware makes the list because it didn't rely on classic mechanisms at all, and was built entirely from JavaScript. Easily defeated by email gateways by locking out .js file extensions, but not

so easy when dropped from malicious, drive-by or watering hole attacks from compromised websites. To add insult to injury, RAA would even drop a password stealer onto the victim's computer to hunt for login details.

Ransomware hits where it hurts. The pocket.

Ransomware can affect you in many ways, but all are likely to cost you money unless your protection preparedness are top notch.

The first you're likely to know about it is when the 'splash' screen or warning pops up to tell you "your files are encrypted".

It's likely the attackers will want to be paid in an ecurrency format like BitCoin, usually between $300-$800. But more recently, the amount has been as high as a few thousand dollars. Typically, 1 to 3 BTC is demanded, which at todays' exchange rate works out at between $1100 and $3400 respectively.

Note the attackers aren't greedy here, they're reliant on the volume of successful ransomware attacks to generate an income, rather than individual attacks. Their price point reflects a price that people will be prepared to pay, even stretch to, in order to get their data back. And, pay they will; about 20% of enterprises do, sadly[4]. Make the ransom too expensive and people will simply find a cheaper way of recovering data. The emergence of anonymous ecurrency like BitCoin has been credited with the success of ransomware, as they allow the effective gathering of money with no paper-trail. Receiving

[4] http://www.zdnet.com/article/two-thirds-of-companies-pay-ransomware-demands-but-not-everyone-gets-their-data-back/

payment by check or PayPal credit isn't something cybercriminals are too keen on, for obvious reasons.

I mentioned before how cybercrime gangs have become business savvy with regard to ransomware too. They quickly realized that making it easy, smooth and pain-free to pay your 'ransom' meant that more people were likely to pay. Call centers[5] and 'customer services centers' have sprung up[6], often staffed by convincing and well spoken people, who will kindly relieve you of your money in order to get your data back.

Should you pay? No. And you'll learn why throughout the rest of this guide.

It's also not just the cost of recovering from the individual ransomware infections you need to consider. If there's a wider network outage because of an outbreak, your business could be losing revenue due to lost productivity. There could also be a cost associated with damaged reputation after the attack and loss of customer confidence. Equally, the cost of just the clean up is often significant too.

Your inbox and the enemy within

Infected email attachments are probably the easiest and most popular way of delivering ransomware attacks, especially in an enterprise environment. The inherent trust that most end-users put in the contents of their 'work' inbox means it's simple for cyber-criminals and hackers to persuade the average business user to click on a link or run at attachment, which in turn infects their computer with ransomware. I'm often told by IT teams, CIOs and CISOs that

---

[5] https://www.engadget.com/2016/09/09/customer-service-matters-when-it-comes-to-ransomware/

[6] http://uk.reuters.com/article/us-usa-cyber-ransomware-idUKKCN0X917X

they've "just upgraded their email security gateway" and therefore must be safe.

The truth is the cyber-criminals are relying on this level of apathy to ensure they can sneak their malicious payload past your quickly out of date gateway or desktop security systems.

The Locky[7] ransomware is a good example of a variant that relied on email to propagate. Locky delivered infected .doc files which on first look didn't seem to contain anything malicious at all—or so your anti-virus software told you. However, Locky was the breed of malware that used malicious VBA macros within the word document to deploy the actual ransomware to the victim's computer.

To trick users into opening file attachments, attackers use all sorts of tactics. You'll see emails containing notices of court appearances, courier delivery notes, booking requests, speeding tickets, complaint letters, sales notices, invoices and travel itineraries to name but a few of the fake files they'll use. Social engineering plays a heavy part in persuading end-users to open the email, but also to trick them into running any code inside the file too. This code, of course, is the dreaded macro.

Macros: the gift that keeps on giving

Yes, the dreaded macro. Aside from the finance team and perhaps State Excel Champions, there are very few people who would, in normal daily life, use an Office document macro. So why is it that our users are tricked into running malicious macros all the time? Cybercriminals have become adept at using booby-trapped Word, Excel and even PowerPoint documents as a dropper for their

[7] https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/

malware; and our end users are falling for their tricks again and again.

If macros are a new concept to you, then the easy way to describe them is as a way to script or automate certain or repetitive processes in Microsoft Office documents. They're hugely popular with people who use Excel to do large calculations or maintain significant numerical data. Later, i.e. post Office 2010, versions of Microsoft Office have macros disabled by default, unless of course your IT team have re-enabled them for the sake of productivity. But that doesn't stop attackers trying to persuade end-users into clicking the "enable macro" button that appears at the top of the document. Often they'll claim the content of the file is obscured or even encrypted and that you'll need to "enable content" in order to read the message.

This is of course nonsense, but it's still an effective trick.

The trick here, as demonstrated well by Locky, is to send a 'clean' file to a victim. By clean I mean there is no signature-able content in the file, so therefore it won't get picked up by classic anti-virus tools. The majority of botnet and malware code generators are able to create polymorphic malware code, so every single piece of malware they send, i.e. per email address, is unique. This is done in an attempt to avoid signature and content scanning engines too. Once the 'clean-looking' yet malicious file is delivered to the victim, they will be tricked into opening said file and either auto-executing the macro, or manually enabling it themselves. Quietly in the background Microsoft Office is running the macro code, which in this case is downloading the actual malware from a remote site.

Once installed, the malware can even stay resident after Office is closed or the PC rebooted. Macros also allow processes to be forked and services to be created too; why is a secret only known to residents of Redmond, WA.? But once resident, the ransomware can go to work behind the scenes, encrypting all your file data as described above.

We're ok, we're a small business. Right?

Wrong. Ransomware attacks can strike any type of business, in fact smaller organizations are usually less well protected or have fewer IT resources than their larger counterparts. The impact is often greater in smaller businesses too, as the IT infrastructure plays a vital role in the day-to-day running of the operation.

There is often a reluctance to appreciate the risk presented to smaller businesses too. Many times I've heard business owners tell me, "we're safe, why would anyone want to hack us".

This always fills me with fear as it indicates an underlying level of general security apathy.

What we all need to realize is that there are cyber-criminals out there who will target every type of business, large or small. In fact sometimes, the smaller the better. Of course there's the usual fire-and-forget or scatter-gun tactic, where hackers will send millions of emails to prospective victims in the hope that some of it is successful. I call this general malicious Internet noise. But, there's also the type of hacker who will research a particular vertical or type of business, and tailor their attack specifically to that market. Hospitals, dental surgeons, acupuncturists, accountants, even pre-owned plant equipment sales offices have all been targeted with malicious content cleverly crafted to 'appeal' to them and their business.

So please don't think it won't happen to you, as it could and you don't want to be finding out the hard way that you're not prepared for the aftermath of the attack.

Paying the ransom. Yes or NO!

Do not pay the ransom. No, don't, just don't. There are several reasons why. The most commonly stated is that you're perpetuating the problem and negotiating with terrorists. Which of course you are; you need to realize that even the small amounts of money paid go towards the nastiest, darkest parts of humanity such as the

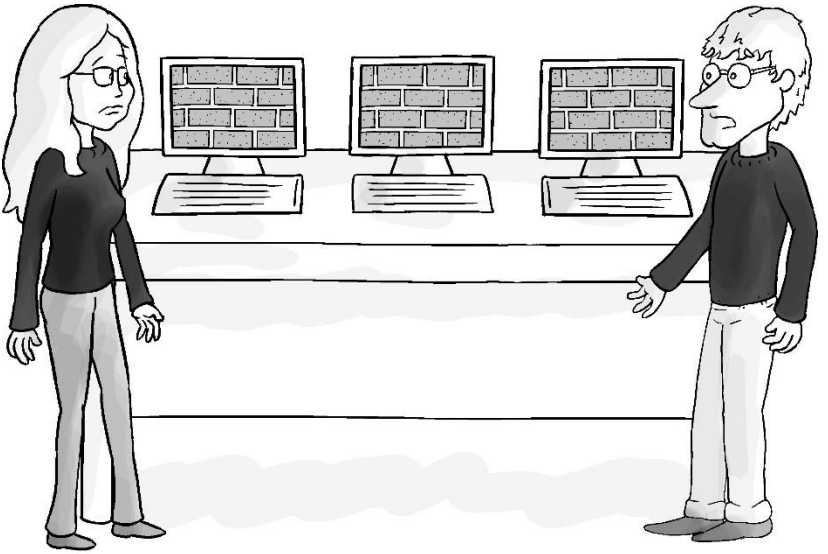
people-smuggling, sex-trafficking, drug-dealing, gun-running, organized criminal underworld. But perhaps more directly, there is no guarantee your files will be returned to their normal state, nor that you won't be reinfected at a later date.

So do not pay the ransom.

Of course, I do appreciate there will be times when you have absolutely no choice to pay, but these ought to only be related to personal computing losses, rather than enterprise IT. Not having a backup of family photos' is the scenario I see mentioned most often; but you should only really pay if you can come to terms with funding the list of activities I mentioned above. In an enterprise IT environment, restoring from a good and recent backup should be the only answer to your ransomware problem.

While the typical advice is NEVER to pay the ransom, that just isn't reasonable or responsible. Imagine a hospital where you might have systems that require immediate access to patient information that have been hit by a ransomware attack. Unless you can recover that data faster than a paid-for key from the bad guys, you may just HAVE to pay that ransom.

Ransomware Defense



"We paid the ransom but the computers are bricked."

We know now that ransomware is clever, it adapts and overcomes, and it specializes in sneaking past traditional security solutions like secure email gateways (SEG) and desktop anti-virus (AV). So when it comes to solving a problem like ransomware where do you start?

By the way, I'm not suggesting you're wasting money on your SEG or desktop AV, just make sure they're modern. For example use a SEG vendor who can apply additional checks to inbound attachments, like sandboxing, and make sure your desktop AV solution has similar and specific anti-ransomware protections; some will even prevent the spontaneous encryption of data and allow you to roll back if the worst happens.

But in my view, those are just the basics; get those right and you're half way to being protected. There are many other types of protection you should deploy.

The importance of patching everything, and patching often

There really isn't any excuse for not making sure your IT infrastructure is patched these days.

Ok, so I do come across some people who have some bespoke and highly tailored applications that only run on Windows XP or NT4 (yes, NT4), but the less we say about them the better. Patching everything, patching it often and making sure you stick to this regime is an important first line of defense against ransomware, in fact against most endpoint attacks that could target your users.

Looking back over the majority of the exploits from the last few years, you'll see they all rely on a vulnerability in an operating system, application, browser or plugin. These vulnerabilities are a fact of life when it comes to writing code, hence why vendors and software makers push patches and fixes out to their user base all the time. Most exploits are successful because they rely on the end-users computer being unpatched and therefore still vulnerable, so patching is a vital step you must take to help reduce the size of your threat landscape.

Don't just focus on operating system patches though, you have many 3rd party applications that also need patching, as well as browsers and their plugins too. Remember also to remove old versions of applications that are no longer supported, as these can present a foothold to attackers looking to compromise your computer too.

But we have desktop anti-virus!

This is a lament I hear all the time. "We have desktop anti-virus, we'll be ok, right?" It's a lament and a question all in one, like people are looking for reassurance. Sorry folks, but just relying on desktop anti-virus (AV) isn't going to protect you.

And, for the Mac users out there, the old "we uses Macs, we don't get viruses" line won't cut it either.

Of course there are many desktop or endpoint protection solutions that can offer some degree of protection, but those should really only be your last line of defense. If the attack gets as far as the OS on the desktop, then it's right inside your environment and has circumvented all of your other layers of security. Remember, we talk about defense in depth when it comes to cyber security.

CryptoWall 3.0 is a great example of what we're up against here. This ransomware variant is said to have made its owners in the region of $350 million, and turn around time from version 3.0 to 4.0 was a mere 48 hours. Imagine the resources the cybercriminals must have to be able to develop code that quickly, and with that size budget. I'd argue this is not the agility that most AV vendors can work with, sadly.

Modern AV systems rely on signatures and fingerprints to identify code or behaviors in malware. Cybercriminals and malware writers know this, and they write code to try and avoid detection. Polymorphism in malware is a great example of this cat and mouse game. Cybercriminals know that they need to stay ahead in the race against AV vendors, but they also rely on the 'lag' that exists between the vendor releasing a new signature and the time it takes to get that rolled out to all your desktops or endpoints. By the time the roll out is complete, the malware writers are releasing new code, and the whole process starts again.

This is why ransomware can sneak past desktop and endpoint protection systems with ease.

Some AV vendors will use a technique called sandboxing, which executes the file in a safe virtual environment as a way of checking the behavior of the file when run. For example the macro threat I mentioned earlier is detectable through sandboxing. However, no sooner have vendors rolled out a sandbox technology, than the malware writers are learning to evade detection, and the arms race continues. If your vendor uses a sandbox, make sure you've questioned them on the protections they build into it to avoid evasion by malware.

Better safe than sorry – the importance of backups

By now you may be thinking that all is potentially lost when it comes to ransomware. But that doesn't need to be the case; with proper preparation the impact of a ransomware attack can be mitigated easily. Backing up data and key infrastructure is the first step to ensuring you can continue operating and recover from a ransomware attack, and this has been proven by several high profile victims already. But, there's a catch here too. I'm not just talking about taking a shadow copy of your files and storing them on the network somewhere. As you know there are some ransomware variants that will actively hunt down and encrypt mapped and unmapped network drives, as well as cloud storage. We've seen already a few instances of backups being encrypted by ransomware too.

Why are backups so important? Consider the impact of a ransomware attack; you're basically going to suffer an outage of your IT infrastructure as everything is taken offline by the malware. Remember ransomware can spread throughout a corporate network once a single computer is infected, so you'll have to act fast to prevent this from happening, or rely on your backup regime to recover.

The following tips should help you keep your backups out of reach of the malware.

Applying the 3-2-1 rule to ransomware protection

There's a handy and timeless rule you can use to think about best-practice backups, the 3-2-1 rule Sadly, it's not something I invented, and the credit must go to the photographer Peter Krogh[8]. The rule will mean you always have an available and useable backup of your

[8] http://www.dpbestflow.org/backup/backup-overview

data and systems, and in a world where ransomware can instantly take you offline, that's a vital precaution.

So how does the 3-2-1 rule work? It's likely you're already following a similar process if you're serious about backups.

For many users, a straight copy of the data to another drive is about as complex as their backup gets.

Three. Ensure you have at least three copies of your data. Or to put it another way, 1 primary and two backups. Why? The probability of losing data is lower. Even in the worse case scenario, where both the production data and primary backup (typically located in the same environment) are lost, you still have the secondary backup. Several copies will protect you against those mundane problems like drive failures or data loss.

Two. Use at least two different media types to store the backups. Why? Media degrades, all media degrades, from tapes, to DVDs, to flash media, and it's all vulnerable to environmental factors as well as technical obsolescence. Currently the only single media type that is likely to outlast you, me and the universe is a glass nanostructure[9] that can store 360TB for around 13.8 billion years—but I'd argue that's a bit over the top for your backup routine. Two different types of regular media are enough for now.

One. Keep at least one copy of your backup offsite and offline. Why? To protect your backups from environmental issues like fire, flood, theft and electromagnetic problems. This is likely to be the best practice you follow today, but make sure offsite is actually "offsite in a secure location". In the back of your car, or at home in a cupboard isn't classified as a secure environment for offsite data. The cloud can be used for offsite backups, but at least make sure these are

[9] http://www.theverge.com/2016/2/16/11018018/5d-data-storage-glass

offline until you need them—remember how some ransomware will encrypt mapped network drives too.

Best practice backup advice for the age of ransomware

The 3-2-1 rule isn't the only backup protection you ought to take. There are several other useful and incredibly simple considerations for backups that could help when it comes to ransomware.

It's important here not to fall for the convenience bias, i.e. making your life easier in exchange for weaker security.

Think about the accounts that control and store your backups. Don't back up data with a network administrator account, use a dedicated service account that is only there for running backup processes and doesn't have wider network access. Also disable or remove local administrator rights from normal end users. You'll protect them from 90% of the threats that face the end point just by doing this alone. Without admin rights, malware and ransomware has a much harder time infecting a computer.

Keep your backups 'air-gapped' as much as possible; by this I mean offsite and offline, but also disconnected when not in use. Backing up to an attached storage device, such as a removable hard drive is a sensible idea, but once the job is complete, remove the device so it can't be overwritten by any malware that might affect that computer. If possible, it's always a sensible idea to auto-eject any removable backup media and tapes once a backup is completed. I've yet to meet a ransomware that is able to physically pop the media back in again.

Using the cloud as a storage location for backups, or even using a dedicated cloud backup agent is a sensible idea too, especially for consumer or individual computers that are valuable or that can't

store their file data centrally in an enterprise environment. However, always make sure you can set the backup to offline somehow, as offsite and offline is an essential protection here.

Similarly easy, re-imaging of devices and computers is a must if you're not able to fully restore bare-metal backups to end user computers. Bare-metal recovery is largely reserved for production servers, whereas end user computers are generally only backed up to a file level. So being able to restore a 'vanilla' OS to end user devices is as vital as restoring the file data. Imaging platforms allow devices to be recovered to their 'as new' state in the event of an attack, and also serve a useful purpose as a deployment tool for everyday infrastructure management. However, do ensure you keep your images up to date—image OS, apps and patch level should be reviewed on a regular basis.

User awareness understanding

Human nature has become the weakest link in most enterprise cyber-security strategies. Social engineering is an easy way for any attacker to trick an employee into carrying out a number of tasks for them; it doesn't require any particular expertise or knowledge and due to the inherent trust of human nature, it generally succeeds. The bad news is the attackers, hackers and cybercriminals are getting better at it all the time. It's far easier for them to send an exploit bought from a cyber crime network, in a cleverly worded email, than it is to learn the code required to compromise a device or network.

Simply asking for the crown jewels is often all that's required.

The security community has woken up to this threat over the last few years and talks a lot about the human firewall, end-user awareness and end-user security training. Sadly, even with all this focus on the end-users, attacks still get through and are successful. There are even a few brave organizations that don't train their staff, as they believe it doesn't provide value for money, given how many successful attacks occur despite the training. I don't condone this,

but simply warrant that it's always better to provide some training that none at all.

I'd be much happier if we thought more about end-user understanding than awareness. Awareness lends its self to a 'shrug of the shoulders' and the 'it'll never happen to me' apathy that causes organizations to have security lapses. I'd advocate that it's far better to talk about end-user understanding instead. So ensure your end-users actually understand the threat of the day and how it'll impact them personally as well as the business. Try to find new and interesting ways to keep them informed, don't just re-run the same old dry security training every month.

The threat moves on at such a pace that we need to keep our end-users up-to-date with the latest developments, and by virtue of this better engagement, they'll feel more empowered to help protect the business

Ransomware Survival

"They weren't bricked. The systems are recoverable and we were prepared!"

Recover capabilities from ransomware and other cyber attacks should now be a staple part of any enterprise IT strategy; in fact, you ought to consider the recovery from these types of attacks in the same way you do an outage. In most cases an outage is the likely outcome as infrastructure is taken offline or service is denied, so get into the habit of extending your BCP activity to include cyber attacks. These simple standard operating procedures (SOP) and immediate actions (IA) should help you plan in advance how to recover from a ransomware or other cyber attack.

Some SOPs for responding to ransomware attacks

1. Panic. Yes, panic. It's only natural under the circumstances, so get it over and done with and out the way. Go somewhere out of sight, have a small panic, then take some deep breaths as you'll need a clear head.

2. Don't panic. Time to calm down, stop and think. What's happening, what's being affected, and do you have any clear idea of the impact yet? Try to control the adrenaline that'll be pumping round your system, so you can make sensible, level-headed decisions. The first is to make sure what's happening is actually real, by which I means it's not a panic from someone who's not sure what's affecting them. Get your incident response team together; if you don't have one, this will be a representative or two from IT, security, PR, legal and management. You may want to implement your business continuity plan, as it'll take some time to isolate and remove the ransomware threat.

3. Pull the power. The easiest way to forensically preserve the state of a disk that's being attacked by something is to simply pull the power cord. Shutting down takes time and alters time stamps, as does a reboot, and by then the ransomware might be resident enough to cause a lot of damage. Pulling the power will at least allow you to recover unaltered files from the disk as a salve, and for better forensic analysis.

4. Damage limitation & containment. If you can identify ground zero quickly, then great. Isolate the device from the network, per point 3 above. If you can limit network access between VLANs or segments temporarily do that too, in order to prevent further propagation. The key here is to make sure you know the scope of the attack right now and where you think it could spread to.

5. Remove and recover. The next phase is to eradicate the ransomware from your computers and network. If you've successfully contained the attack, then infected machines can be wiped clean and the re-imaged and restored from backup.

You may want to preserve the ground zero infection point for forensic analysis and law enforcement action.

6. Investigate. It's key to retain evidence, so make sure your logs for all gateway services and infected computers are retained. If you've got the initial infection point identified, that disk image or even physical disk will be useful for law enforcement as evidence too. Contacting the local authorities is an important step, as they may already be investigating attacks similar to yours. it's also important to report these attacks so the wider security community can build up an accurate picture of the problem and work on defenses together. You can report the crime to the FBI through their Internet Crime Complaint Center or IC3 at www.ic3.gov, or in the UK to the Police at www.actionfraud.police.uk

7. Remediation. Lastly, it's important to identify and remove the problem that caused the issue in the first place. It may be that your SEG let through a malicious attachment that wasn't identified, or perhaps your endpoint AV and protection failed to react to the threat once it was inside the business. It's also likely there's going to be some end-user training needed to make sure everyone fully understands how the threat is affecting the organization. Above all, this should be a 'learning experience' for you, your end-users and your management; take some time when the smoke has died down to assess what you did well, and what perhaps didn't work. Then make sure your plans are modified to ensure you can perform better next time—be that with technology, training or processes.

Remember that backup. Better safe than sorry.

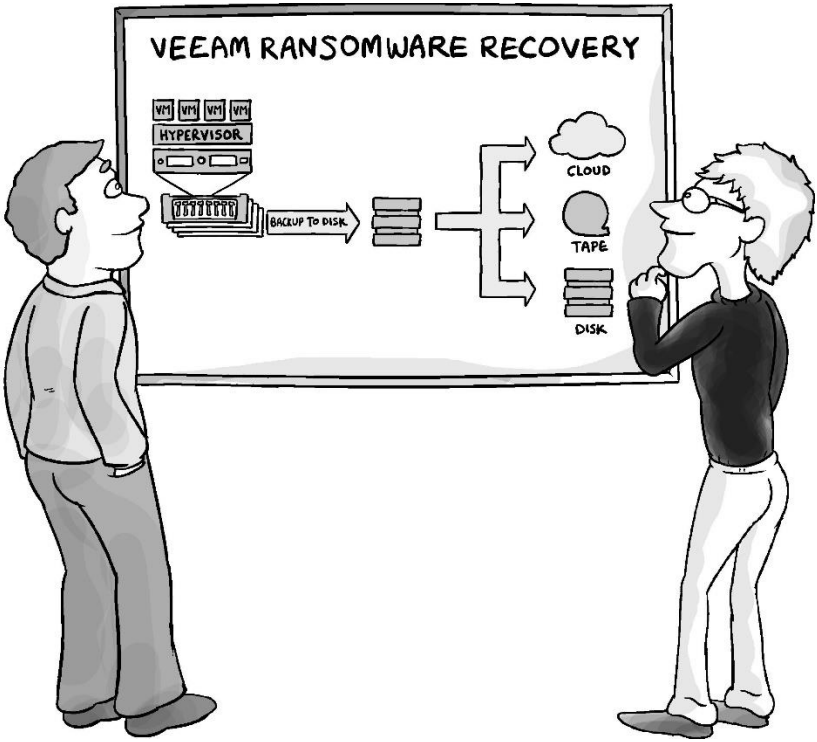
Lastly, it's worth noting again how important your backups are when it comes to recovering from a ransomware attack. I would argue that a good backup regime is the single most important protective measure when it comes to getting back online and recovering productivity.

This should also apply to personal computing too; devices are relatively cheap these days, so we're often happy to replace a faulty device, but when it comes to data, very few of us take steps to ensure our personal data is thoroughly backed up somewhere safe. There are many personal backup solutions available which you ought to consider even if it's just for the safety of your family photos.

Remember the 3-2-1 rule I applied earlier, use that for your corporate and personal data wherever possible. You'd rather be safe than sorry if a ransomware attack does manage to trick you out.

Paying the ransom (in case you didn't get the message the first time): Do. Not. Pay. The. Ransom. But, stay safe out there.

Vendor Sponsor: Veeam Availability Suite



In recent times, ransomware has become the most significant threat facing enterprise IT environments. This is no surprise given how successful ransomware is as a money-maker activity for cybercrime gangs around the world. They quickly invested their R&D budgets (yes, they do have those too just like you) into ransomware, at the expense of what we might call more classic attacks like phishing or malware, when they realized there was (very) easy money to be made here.

Because of this interest in ransomware by the cybercrime community, we can be sure that the threat won't go away any time soon, and we'll see it get a lot worse before it gets better. There are

already signs of increasing complexity and sophistication in the way ransomware is written and in its execution, and this book touches on a few of those advances. Sadly as the criminals improve their technology and the ways in which they can make ransomware more effective against our users, many organisations will struggle to keep up. So with every advancement of this malware, we see more and more enterprises being affected and losing out to the cyber criminals. It's fair to say that many of the most well known primary defences are letting ransomware sneak through; by this we mean platforms like email security gateways and web content filters. Ransomware is often delivered via a malicious email attachment, or through some sort of drive-by or watering hole attack on a compromised website, so when the systems protecting those services fail to detect the threat, ransomware is successful.

By then, it is of course too late. An end user has opened the attachment or clicked a link, and before you know it there's a helpdesk call being logged because they can't access any of their files any more, or there's a skull and cross bones on their desktop. In the worst case scenarios, where ransomware has used SMB shares to propagate around the network, it's likely all sort of proverbial stuff is breaking loose, and your IT team is in for a long and complicated few days (and nights). Your users will be left unproductive, of course.

At Veeam we think about countering ransomware as a recovery scenario. The initial infection may be inevitable, so the best protection is preparation. Veeam doesn't prevent ransomware, but it does allow you to be ready to recover when the attack comes. We apply the 3-2-1 methodology to help IT teams think about how best ensure their data are safe, and their integrity is maintained, so when you lose systems they can be quickly and painlessly recovered to production-ready status.

Veeam Availability Suite gives you the ability to quickly and effectively restore critical data that's been infected by ransomware by leveraging our 3-2-1-0 rule. Three copies of the data, on two different media types and including one off-site copy, but also backed up by SureBackup and SureReplica to verify the primary

backup so that you can be sure that it is recoverable and consistent. Any ransomware activity that could present a threat to your network can be quickly identified, and alerted on.

Adding Veeam backup and replication software to your security strategy, specifically for ransomware protection will put you in control of the situation just when you need it. If ransomware does strike one or many of your end points, you can rely on rapid restore of infrastructure to get back into production fast. This includes databases, applications, single or multiple files and even operating systems. For large scale storage platforms, like HPE, Dell EMC, NetApp, Nimble and IBM, Veeam will integrate with these solutions too, so there is no need for additional hardware or application expenditure.

One magical part of Veeam's technology, which is especially relevant when thinking about ransomware, is the On-demand Sandbox for testing recovery points. This effectively gives you the ability to easily discover the last known good restore point and check it in a safe sandbox before fully restoring it to production, instead of re-writing infected systems with infected backups.

Lastly, protecting your backups is vital. There's no point backing up data to a drive or device that the ransomware is going to find and encrypt. Yes, this does happen as has been mentioned a few times in this book. Make sure you're using different credentials for backups and their storage—not DOMAIN\Administrator. At Veeam we recommend not joining your backup infrastructure to the domain, or for large environments, putting it on its own separate domain all together. Then of course there's off-lining your storage too. Powering off VMs, auto-ejecting removable storage and using Cloud Connect backups are all ways of air gapping your backed up data. Veeam Cloud Connect is quickly becoming our de-facto standard for the safest way to run and store backups; it's a complete out-of-band protection solution, where backups are taken via the same Backup Copy Job on the network, then automatically sent to a service provider in the cloud. Pure safety and perfect preparation for a ransomware attack.

Ransomware isn't a problem that looks like it'll fade away any time soon, in fact all of the signs are pointing to an escalation in capability and effectiveness of the threat. This makes your protections against the threat vital, but so too is planning for the inevitable disaster. Perfect preparation with the help of Veeam will mean you can complete that planning loop easily, as well as sleep soundly at night knowing your data are easily and quickly recoverable too. There's no need to worry excessively about ransomware, but it should focus your attention on technologies that perhaps haven't been refreshed or reviewed for a while. If you'd like to talk to someone about a wider and wholistic approach to ransomware protection and recovery in your organisation, please talk to the person who gave you this book to find out how they can help.


VEEAM
IT'S HERE
NEW Veeam
Availability Suite 9.5
AVAILABILITY for the Always-On Enterprise
go.veeam.com/v9-5

Easily converse about Ransomware defense and survival in any setting.

Don't pay the ransom! That's the advice given when asked about ransomware and how to deal with it. But how does one defend themselves against ransomware and survive an attack successfully get through your defenses? That is the key to this book. Because, if you aren't going to pay the ransom, you better have an alternative means of recovery!

About Orlando Scott-Cowley

Orlando Scott-Cowley is a cybersecurity consultant and strategist. He is an unlikely geek, having never really got into Star (Wars | Trek), but grew up as an Oracle DBA, sysadmin and then a penetration tester. Today, he helps organizations secure themselves and their users from the malicious threats, hackers and villains, around the world.

Follow him on Twitter @orlando_sc