Conversational **Ransomware**

A ConversationalGeek® Book

Sponsored by ivanti

Learn about:

- Ransomware – What is it?
- Protecting your organization from ransomware
- Ways to mitigate ransomware threats (pay the ransom or not?)

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

Sponsored by Ivanti

Ivanti is IT evolved. By integrating and automating critical IT tasks, Ivanti helps IT organizations secure the digital workplace. For more than three decades, Ivanti has helped IT professionals address security threats, manage devices, and optimize their user experience. From traditional PCs to mobile devices, virtual machines, and the data center, Ivanti helps discover and manage your IT assets wherever they are located, improving IT service delivery and reducing risk. Ivanti also ensures that supply chain and warehouse teams are effectively leveraging the most up-to-date technology to improve productivity throughout their operation.

Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.

www.ivanti.com

Conversational Ransomware

By Orlando Scott-Cowley

ConversationalGeek®

Conversational Ransomware

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:	Chris Nelson
Content Reviewer:	Karla Reina

Note from the Author

Do you ever get the feeling as an enterprise security or IT professional, that you're pushing water uphill when it comes to keeping up with the changing security and threat landscape? Do you get the feeling that regardless of what you do, as sure as the sun rises tomorrow there will be a new threat to worry about, as cybercriminals come up with more ingenious ways to exploit your network and users?

Well you're not alone. You're part of what we often call an arms race, or the red queen effect of enterprise security. The downside of this phenomenon is that no matter how well you do today, you'll have to do better tomorrow just to stay in the race, for this is a race that gets faster and faster all the time.

Ransomware is one such threat. It's appeared out of almost nowhere, just as we were thinking we've learned how to protect and educate our users to counter the latest threat—something like spear-phishing or ransomware comes along and changes the game.

I've been helping organizations protect themselves from a variety of security threats for many years now, and I've 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!

Ransomwhat? Intro to the Malware

Ransomware or crypto-malware isn't new, although you might think it is because you've only recently been reacting to it as a threat. It actually has been around for a long time. Today's ransomware, however, is considerably different from its early forebears and presents a significantly more sophisticated threat.

Most common sources state that ground zero for ransomware was the 1989 AIDS Trojan, also known as the PC Cyborg Trojan, developed by Dr. Joseph L Popp, an evolutionary biologist. This first generation ransomware was unsophisticated and easily defeated. It was delivered, not by email as we see today, but via diskettes (remember those?) at the WHO International AIDs conference, 20,000 copies in all. Popp's malware hid files in the victim's

computer and encrypted the file names, before demanding $189 for a repair tool.

Today, ransomware is a much more sinister threat as the capabilities and effectiveness of the malware have increased dramatically. Ransomware, locker, or crypto-malware, as it's sometimes known, is designed to trick users into paying a ransom either to "unlock" their computers or gain access to their files which the malware has maliciously encrypted. Cybercriminals have become skilled at launching their ransomware campaigns, even using platforms such as "Ransomware-as-a-Service," to the extent that they are able to generate millions of dollars from each attack. You can see why it's become the "attack du jour" for many of the Internet's villains.

By way of a short introduction, as I'll go into much more detail later, ransomware is this: a type of malware or computer virus that prevents a computer's users from accessing their system or the data files held there. Ransomware can lock the screen of the computer, encrypt some or all of the data files on the computer, or even encrypt the entire hard drive. All of this happens unless and until a ransom is paid to the malware's cybercriminals, or you find another way to recover your now useless computer and its data.

If you're hit by ransomware, it'd be easy to think "Oh well... we'll just pay up," but by doing this you're effectively negotiating with terrorists. Don't do it!

Ransomware through the Ages—a Timeline

2000-2005

Over the years there have been many different types of extortion-based threats, all seeking to generate money from unsuspecting victims one way or another. Fake antivirus, fake spyware removal, and "performance enhancement" tools can be categorized as misleading applications that started to appear on our computer

screens around 2005. Of course, these didn't lock or encrypt data like today's malware, but they did demand money payment for nonexistent or fake problems with a user's PC. The misleading application market of ten years ago proved the concept and business model of ransomware for today's cybercriminals. Fake antivirus, it is said, was so successful at conning users into paying for a"fix" to their "problem" that in 2008 one malware distribution affiliate reported earnings of $158,000 in a week.

2006

Seventeen years after Dr. Popp introduced the world to ransomware, a new, more effective strain was released. The Achievus Trojan was the first piece of ransomware malware to use the asymmetric RSA encryption mechanism to encrypt all the files in the user's My Documents folder. Victims were required to purchase goods from an online pharmacy in order to receive a 30-character decryption password to get their files back.

In the same year, email made its debut as the distribution mechanism for ransomware. The GPcode encryption trojan spread via an email attachment claiming to be a job application. GPcode upped the encryption game, too, by using a 660-bit RSA encryption key.

2006-2011

Between 2006 and 2011, GPcode and its variants proved to be a problem for end users, as did locking malware like Winlock or Ransomlock which simply locked your computer until a fee was paid. Encryption continued to get stronger with RSA 1024 bit being deployed in 2008, but only for a small number of file types or locations on the victim's computer.

2011

This year became a tipping point for ransomware for two reasons. 2011 was the first year a large-scale ransomware attack was perpetrated, claiming to be a Windows Product Activation notice. The second reason was the ubiquity of anonymous payment services

that made it much easier for hackers and cybercriminals to collect payment from victims.

2012

Could this year have been the birth of what we now know as Crime-as-a-Service or Ransomware-as-a-Service networks? In 2012 the Citadel toolkit allowed would-be hackers and cybercriminals the ability to build, deploy, and manage a botnet and associated ransomware campaign for under $50. This is also the year law-enforcement ransomware arrives on the scene. Malware such as the Urausy police trojan, the Reveton worm, and Tohfy made their debut by claiming the users had been involved in some sort of criminal activity. Each requiring a fee or fine to be paid, often to the "FBI" (not the real FBI, of course) to unlock their computer.

It must seem to you that ransomware is the latest threat, and to many it is. But it's been sharpening its teeth for some time now. 2013 is when it starts to get really hairy!

2013

This is an interesting and perhaps vintage year for the malware and ransomware connoisseur, with many fruity and full-bodied varieties being uncorked. The resulting hangover was said by some to be the most significant headache yet.

Cybercriminals and hackers are, if nothing else, entrepreneurial when it comes to changing their business models. Their earlier money payment and extortion malware schemes proved to be less effective and were combatted by more effective desktop security anti-malware tools, so the villains pivoted back to using their original encryption malware, or crypto-malware as it became known.

CryptoLocker is one such pivot. As was the utilization of the ecurrency Bitcoin. CryptoLocker set the de facto standard for a vintage ransomware; it was easily spread by drive-by downloads

from malicious or compromised websites and, perhaps more effectively, by email attachments—especially to enterprise employees. Early malicious attachments saw the introduction of socially engineered content, designed to look like customer complaint letters that encouraged the recipient to open the attachment.

CryptoLocker raised the bar in terms of encryption, too, by rolling out enterprise-grade 256-bit AES with 2048-bit RSA keys, as well as command-and-control (aka C&C or C2) servers. CryptoLocker also added a clever twist, in that it would encrypt files, delete the originals, and then threaten to delete the encryption keys unless the ransom was paid within a short period of time.

In this same year, other devices and operating systems started to be affected, too. Smartphones running Android are targeted, as are Mac computers running OSX. Mac users who claimed they "didn't get viruses'because they used Mac's" were suddenly very sheepish.

2014

By early 2014, new improved and more effective styles of ransomware, spawned by CryptoLocker, really started to take off. They became mass market for cybercriminals as well as the threat of the moment—replacing spear-phishing, which was proving to be less and less successful.

Ransomware such as CryptoDefence, CryptoWall, Koler (for Android), and others started to infect more and more computers around the world. Until mid-2014, that is, when an international team of law enforcement and security providers took down the botnet that controlled most of the ransomware traffic. The Gameover ZeuS botnet, as it was known, was comprised of over a million infected endpoints, about 25% of which were located in the United States of America.

2015

As CryptoLocker died away, CryptoWall took over and arguably became one of the most successful and lucrative money earners yet

for the cybercriminals in control. The campaigns were so successful a new network of botnets/zombies-for-hire sprung up and were known as Ransomware-as-a-Service, with which anyone could instantly turn themselves into a cybercriminal. We have even seen evidence of traditional criminals (involved in burglary, car-crime, drugs, etc.) turning to cybercrime because the new crime-as-a-service platforms are so easy to use—as well as lucrative and relatively risk free.

To give you an idea of the capabilities of the crimeware developers, when CryptoWall 2.0 was killed off, it took a mere 48 hours to build CryptoWall 3.0 from a new code base. How many development teams do you know that could turn out code that quickly? Given CryptoWall was said to earn hundreds of millions of dollars, it's easy to see how successful it became. Ask yourself this—in the face of cybercriminals with an IT budget in the region of $350,000,000, what does your budget for security measures look like? Sobering thought, eh?

2015 rolled on with CryptoWall 4.0, TorrentLocker, TeslaCrypt, Lowlevel04, LockerPin, and Chimera, to name but a few, hitting the "market." In the face of all this malware, an FBI Special Agent at a Boston conference said the now immortal words, "The ransomware is that good…. to be honest, we often advise people just to pay the ransom." The FBI has since issued more appropriate advice.

2016

Ransomware took a technological leap forward in 2016, as the first JavaScript-only version was seen in the wild and as traditional variants like CryptoLocker were shut down. Ransom32 is one such JavaScript version, and it is a whopper, too, weighing in at 22MB. Delivery by Ransomware-as-a-Service gives the ransomware the ability to support not only JavaScript, but also HTML and CSS.

2016 also gave us the now standard attack of choice for enterprises—ransomware enabled by malicious macros in Microsoft Office documents. Locky is the best example of this and is spread using phishing campaigns that send malicious Word documents to

victims. Once the attachment is opened and the macro enabled, ransomware is downloaded and infects the victim's computer. Locky is powered by the massive Dridex cybercrime gang and botnet and quickly infects multiple organizations. Hospitals in particular were a keen target, as the villains realized that infecting life-saving equipment was an easy money maker, as the victims paid the ransom and paid fast.

The Petya ransomware gave us a whole new pain point in 2016. This was the first ransomware to encrypt the entire hard drive and prevent the system from booting by overwriting the MBR (Master Boot Record).

In April 2016, the FBI estimated some astonishing numbers for the impact of ransomware. They estimated that in the first three months of 2016, cybercriminals netted $209 million from their extortion campaigns, up from $24 million in all of 2014. The FBI also estimated ransomware losses would top $1 billion in 2016.

Also in 2016, the first legitimate OSX-based ransomware appeared: KeRanger, delivered by a BitTorrent client and signed in a manner allowing it to bypass Apple security software.

Wondering what's next? Aren't we all? We can assume ransomware will get more effective at its job, so make sure that your protection strategy works today.

How Ransomware Works—the Technicalities

Ransomware is a tricky little creature. Its developers are always looking for new ways to ensure your data is locked beyond your reach so their extortion tactics result in a pay day. There are many different variants of ransomware, as we have seen. Early versions simply locked your computer screen, or perhaps just showed a bland

warning. In this section, I'll concentrate on the more modern versions of the malware so we can put those early attempts to bed.

First, let's look at the different ways you could become infected by ransomware malware.

Email

The majority of business or enterprise users receive ransomware through spam or phishing emails, usually those claiming to be an invoice or customer complaint. Attached to the email is either a Microsoft Office document—Word, Excel, or even PowerPoint—containing a malicious macro and some sort of social engineering to encourage the user to enable said macro. Some ransomware variants use different file types, such as PDF, ZIP, or even .dotm macro template files. You will notice how attackers use domain names and content that sound legitimate to encourage you to open the email and run the attachment. Fake UPS or FedEx delivery notices and invoices are popular here. Office documents are used because of their ubiquity within an enterprise IT environment, and they're less likely to be blocked outright by security gateways in the same way traditional malware files like .scr or even .exe would be. End users are also less suspicious of Word and Excel files, making the attacker's job even easier.

SMS and Social Media—Shortened Links

Some attackers use shortened links to deliver malware, too, often in tweets, SMSs, social media private messages, and even email. The latter is less common these days due to the number of security solutions that "link follow" for URIs in email. Ransomware delivered by a malicious shortened link is often JavaScript based.

Malvertising

A popular mechanism for infecting victims with ransomware is known as Malvertising, where attackers compromise or exploit a legitimate online ad network to trick browsers into downloading their malicious payload through page display ads. Malvertising is used to great effect as a tactic because legitimate and trusted websites (like YouTube) can be made to display malicious ads to their

users. Often exploit kits, such as Angler and Neutrino, are used as part of this attack to be the initial dropper, which then allows cybercriminals to do all sorts of things to a compromised endpoint—with ransomware being just one outcome. These attacks are known as "drive-by" and "watering-hole" attacks.

Ransomware-as-a-Service

I mentioned previously that Ransomware-as-a-Service (RaaS) is a way for anyone and everyone to "get into cybercrime" (not that I'd recommend that as a career choice). RaaS should be noted as a delivery mechanism for ransomware, as there is a key differentiator here. RaaS networks are usually hidden on the TOR network, or the dark web as it is sometime known, and are popular with cybercrime foot soldiers known as *affiliates*. RaaS is important because of the way it allows attackers to focus on high-value and large-scale targets like enterprise servers, where attackers are known to hunt for open Remote Desktop or Terminal Services ports. Once located on the Internet, which doesn't take much hard work I can tell you, the attackers will brute force weak passwords to gain access to the server environment—and of course the network on which it sits. The server and network environment then become their playground.

On the Network

One of the interesting ways ransomware uses to propagate from its ground zero infection is via the Windows networking SMB shares. Most, if not all, Windows environments in an enterprise will be running on a domain to which all computers are connected both physically and virtually. Ransomware loves this setup, as it can use the "trust" among all the computers on the domain as a way to break out into the entire network and affect as many computers and network shares as possible. This is why when ransomware strikes you'll see it affect entire networks at once rather than individual computers. Some ransomware earns a PhD here, too; variants such as Locky encrypt network shares also, both mapped and unmapped. Connected cloud services, such as Dropbox, OneDrive, and Box, that present themselves as mapped drives can also be affected, as can mapped backup drives. Backups, of course, are one of the only ways you can recover from a ransomware attack. More on backups later.

Infected? What Actually Happens to Your Computer and Data

Modern crypto malware or data-locker type ransomware has one goal. To encrypt as much of your data as possible, making it useless to you unless you pay the ransom and get a decryption key. If you're unlucky enough to be affected by ransomware through one of the previous mechanisms, this is likely to be what happens next.

Once resident on your computer, ransomware quietly searches your hard drive, network drives, and attached storage for data files. You'll never notice this happening because ransomware wants to stay stealthy until it's encrypted everything in sight. Most ransomware allows the computer to continue in a normal operation mode; however, an increasing number of them are starting to lock down the entire computer and its operating system, even from the MBR. Early versions of ransomware were only able to encrypt a small number of file types, but that list grew quickly and now all data files are targeted, as well as some operating system files, too.

Encryption has become the strong game for ransomware's cybercriminals. The early days of using weak or low-grade encryption are over as developers turn to AES, RSA and even ECC (Elliptic Curve Cryptography).

AES uses symmetric key encryption, which simply put, uses the same password to encrypt and decrypt the data. Usually this key will be 128 or 256 bits in length and impossible to brute force. RSA, however, uses asymmetric key encryption and has a pair of keys (public and private) to encrypt and decrypt the data. Reverse engineering the private key from the public key is also assumed impossible, making decryption without keys impossible, too. Occasionally the malware writers will make a mistake and hide the decryption key in the ransomware source code, but this is increasingly rare. Sometimes they'll badly implement the encryption, making it easy for security researchers to break, and on a few occasions, the C2 servers have been compromised to give access to the keys.

ECC comes in for ransomware like CTB-Locker, a new generation of ransomware. The use of ECC by this malware represents a step change in the way malware writers think about locking up your data; ECC allows for a much smaller key size than AES or RSA, but with greater levels of security and privacy. Bad news for those of us trying to find way to overcome ransomware.

You're first likely to know about a ransomware infection when you see a warning pop up on the screen. These warnings vary in terms of quality and overall professionalism, some are very advanced while others are basic. The warning usually tells you all your files are encrypted and that you have to pay to get them back; there's often a time limit, too, adding to the pressure. Failing to act within the time allowed can increase the ransom required.

The Money

Payment is usually required in Bitcoin and can vary from 1BTC to upwards of 100BTC. At today's prices, one Bitcoin is worth around $700. Above all, the payment system used is always anonymous. Sending a check in the post or using PayPal isn't an option here. Voucher payment systems are also used, such as Paysafecard, MoneyPak, CashU, and MoneXy, but Bitcoin remains the most popular.

Sadly, the cybercrime gangs behind ransomware campaigns are running their organizations like real companies, to the extent they have employees, paid time off, and healthcare schemes. Customer (or victim to be more accurate) support has become their main focus in recent years, as they realize the better they "serve" customers, the more likely they are to be able to extort money from them. Cybercriminal call centers have sprung up and are some of the most helpful and efficient around today.

It is important to note that once a victim has paid a ransom rather than use an alternative means of recovery, they are effectively negotiating with terrorists and funding further crime and misery. Cybercriminals will cash out their earnings through well-known money-laundering operations like online betting and casinos;

although for Bitcoin payments, the process in more complex as criminals try to avoid law enforcement agencies.

Remember, although paying the ransom seems like an easy option, it may not solve your problems. Don’t do it.

Social Engineering—It's No Cocktail Party

According to Wikipedia, social engineering refers to psychological manipulation of people into performing actions or divulging confidential information.

One of the main reasons malware like ransomware has become so successful is because of its clever use of social engineering to persuade victims to fall for the attacker's malicious email, SMS, or tweet. Like phishing and spear-phishing before it, ransomware uses native language social engineering to trick the recipient of the attack into believing the request or file they're being sent is real. Native language is important, as cybercriminals now employ content and copy writers whose first language is that of their intended victim, rather than try to translate. You'll remember early financial fraud attacks like phishing were easily noticeable by their use of Pidgin English. Not any longer!

Social engineering is not a new technique but remains the bedrock of a clever con trick. Cybercriminals were quick to learn how effective social engineering can be with their early attempts at financial fraud, such as penny stock (pump and dump) manipulation and 419 crime. They used social engineering to great effect in phishing and spear-phishing campaigns and perhaps have perfected the technique beautifully in CEO fraud or whaling attacks.

Sadly, the social engineering used for malicious purposes in attacks such as ransomware is what gets most end users into trouble. I find enterprise users are too quick to trust what is on the screen in front of them, or perhaps because their IT teams do such a good job, they believe everything in their inbox is clean, legitimate, and business related. The truth is far gloomier.

Ransomware attacks can spoof legitimate organizations like the FBI, or Microsoft, and claim you've done something illegal or perhaps have illegal content on your computer. In these scenarios, the attacks are relying on the user to panic and pay up. In other cases, cybercriminals use a softer approach, claiming to be a customer of your company with a complaint letter (beware the Word macro dropper for ransomware here). Courier firms such as UPS and FedEx are often used as a cover story. Increasingly, however, attackers are turning to niche cover stories in a bid to fly under the radar of security gateway's that use content analysis to detect the malware. Email relating to pre-owned plant equipment is one such example.

Social engineering is also used to great effect in the way the ransomware notifies the victim of its presence. The malware writer wants to convince, perhaps persuade, the victim to pay the ransom, so often the ransomware warning is clear, precise, and to the point. One excellent example is the Jigsaw ransomware, named after a horror movie of the same name, which used a timer to show how long the victim had to comply. Failure to comply simply leads to a deletion of more files, adding to the sense of urgency. Clearly an attempt at manipulating the psychology of the situation.

Humans Are the Weakest Link–Goodbye

For those you who think social engineering is something you could easily recognize and protect yourselves from, you're probably correct; but I'd challenge you to go a whole month without falling for one of the many click-bait stories posted on social media. Those headlines and stories are the reason social engineering-enabled attacks are not going to go away soon. They're training end users to be far less critical of obvious bait-laden links.

If you examine all the threats facing an enterprise today, you'll quickly see that most are exploiting the humans in the business, the people who operate the IT and the systems. Cybercriminals and hackers have realized it's far easier to exploit human nature than it is an operating system or lines of code. Simply asking for something, albeit in the correct and persuasive way, gets them almost instant access to the crown jewels—all without any malicious code that could be detectable by a software security solution.

Sadly, over the last few years this problem has gone from bad to worse and will only continue to do so until we close the holes in our human firewall.

What's a human firewall? It's your people, your staff, and their ability to be the last line of defense for your business. If they choose to be.

Some High-profile Ransomware Victims

Ransomware often hits the headlines as it has a devastating effect on victim computers and networks. If ever you needed some good case studies to help you build a business case for why now is the time to take action to prevent ransomware, here's a list of organizations affected.

San Francisco Municipal Transport Agency—MUNI (USA)

The San Francisco transit system, also known as MUNI, was taken offline recently by what is thought to be a variant of the HDDCryptor ransomware. Travelers using the MUNI system, both rail and bus, were given free transport over the 48 hours that some 2000 systems were taken offline. Affected systems included MUNI's customer-facing ticketing machines, as well as workstations and servers. The attackers demanded 100 BTC (roughly $73,000) for the decryption key. We do not know whether SFMTA paid the ransom or recovered from a backup, although I expect the latter is more likely.

Hollywood Presbyterian Medical Center (USA)

Cybercriminals locked this Los Angeles hospital out of its patient records for over a week, while demanding $3.6 million in Bitcoin for a decryption key for the data. Medical staff had to resort to paper records, faxes, and face-to-face communications to keep the hospital operational. This example is significant as it demonstrates the business acumen of the attackers, who clearly knew how valuable the systems were they had compromised. The average ransomware demand is $300-$500, but in this case was several million. The Hospital did pay the ransom, but a significantly reduced figure.

MedStar (USA)

The MedStar Hospital chain was hit with ransomware demanding 3 BTC (c. $2000). The hospital's main clinical information system was comprised, but quickly restored without payment to the cybercriminals. Clinical records were first restored on a read-only basis, with the remaining information following shortly afterwards. "Round the clock working" by the in-house IT teams was cited as the reason downtime was limited.

Northern Lincolnshire and Goole NHS Foundation Trust Hospitals (UK)

This healthcare organization in the UK was another one affected by ransomware. The attack took hospitals offline for several days, resulting in cancelled appointments for patients as well as the diversion of incoming trauma care to neighboring facilities. The

organization shut down the majority of its IT systems as a way to limit damage, only regaining operational status several days later.

Lincolnshire County Council (UK)

Earlier in the same year and also in Lincolnshire, the area's local government authority, the Lincolnshire County Council, was hit by a ransomware demanding $1.25 million. Similarly to the local hospitals, the council shut down most of its IT systems to limit damage, again resulting in disrupted services for customers. The ransom demand was later downgraded to only $500, which the council did not pay, instead restoring its IT systems from backups. During the downtime, "pen and paper" and "lots of human contact" were the reported means of communication.

Half of US Businesses Surveyed Admit to Ransomware Attacks

A recent survey of 500 businesses, conducted by a cybersecurity vendor, revealed that nearly half had been affected by ransomware attacks within the last 12 months. A full 85% had suffered from three or more attacks, with six being the average for the number of times an enterprise had been the victim of ransomware. The majority, at 81%, said their networks were comprised through malicious email and social media messages, while 50% was affected through drive-by-downloads from comprised websites. In all cases, the time to recover the services and infrastructure was well over 24 hours.

The results is this particular survey reinforce a suspicion that I've had for a while: a lot of organizations suffer at the hands of ransomware attacks, but simply don't make it public. Fear of reputational damage is usually the driver for hiding these attacks, which is understandable. But it does hide the true impact of the problem, which is one reason the FBI asks victims to report ransomware incidents.

But We Have Desktop Antivirus Protection. We'll Be OK, Right?

Wrong. And don't fall for the equally myopic "We run Macs, so we don't get viruses" fallacy either.

Do you remember how I told you the CryptoWall 3 ransomware generated over $300 million for its cybercrime owners?

With that sort of R&D budget, don't you think the malware authors would have worked out a way to evade common desktop antivirus tools?

The problem with traditional desktop antivirus solutions is the majority of them work on a signature or fingerprint basis, whereby they scan your computer and files against a large database of these signatures to detect activity that looks like it might be malicious in file content. This technique is exploited by malware writers, especially those who write ransomware code, by the use of polymorphic and encrypted virus code. In short, the cybercriminals write malware code that changes regularly enough to always be new and therefore not yet fingerprinted or signatured by desktop antivirus vendors. As much as 70%-90% of the malware attachments received by an organization are unique because of this polymorphism. Cybercriminals can be a lot more agile than security vendors, too, so in the time it takes your desktop antivirus vendor to issue a signature for the latest version of a ransomware variant and then for your entire desktop AV estate to download the update, the cybercriminals have moved onto a new version and the whole process starts all over again. Speed is on their side, and they win easily.

Encrypting the payload of malware such as ransomware also presents a problem to desktop antivirus tools in that it effectively hides the malware from the AV engine, which if configured to ignore encrypted files, can spell disaster.

Some antivirus engines will sandbox, or detonate in a safe virtual environment, a file to check what actions it might take when run in the OS environment. Sandboxing was seen as the future in relation to ransomware and still has a place in gateway security solutions, but

increasingly ransomware and malware are learning how to evade the sandbox and still present a threat to the end user.

Remember that arms race I mentioned at the beginning? Sandbox evasion is a great example of how hackers are trying to stay ahead of the good guys.

Another technique used to evade many types of security solutions is the use of Microsoft macros within Office documents. I mentioned this briefly earlier, but it's a clever technique worth dipping into once again. Microsoft macros in Word and Excel files give cybercriminals the ability to sneak their payloads past security solutions because there's no viral or malware code in the Word document. In short, when the user fires up the Word doc and either automatically or manually enables the macro, it is that same macro that then reaches out to an external site to download the malware payload and infect the computer. Later versions of Microsoft Office block macros by default; however, that still doesn't prevent the inevitable social engineering that is usually included in the email and attachment, and a lot of businesses need macros enabled to work.

Solutions, Solutions Everywhere—How to Protect Yourself

One of the trickiest problems to solve with ransomware is finding the best way to protect yourself and mitigate the threat, especially as we now know that a lot of your traditional security tools will be caught napping by ransomware.

Are the Basics Right?

To begin with, your security strategy should be to follow best practices in terms of the existing security infrastructure and systems you have in place right now. By best practices, I mean you've done a lot of the routine work already, i.e. your desktop AV solution is up to

date, both the software versions and the signature databases. If your AV vendor has some new anti-ransomware tools, take a look at those, too. Also, your OS patching should be up to date, as well. I don't want to hear any of those excuses about not being able to patch something because it might break a system or application. Patch it, and patch all those plugins, desktop tools, and add-ons, like Adobe Reader, Flash (if you still use it), Java, and so forth. Getting the basics right is vital here. Only by doing that will you then gain access to the next level.

I'm still amazed at how many organizations I find that don't have a solid update strategy here. Don't be like these guys, get the basics right today.

Backups

Another basic but important step we all need to take, in both consumer and enterprise IT, is to make sure we have backups of all our data. For a consumer, this can be as easy as copying your files to an offline or removable storage device like a USB hard drive. You can also copy files to a cloud solution, but take care to make sure you're not mapping a drive to that platform. Otherwise, the ransomware could find that too. Some cloud services, like DropBox, give you file versioning so you can roll back to earlier versions should you ever need to.

Enterprise users should have their data backed up for them by their IT team, and if you're part of that IT team, just nip off now and make sure all your backups are completing without errors. Also, take some time to do a few test restores, just to make sure backup integrity is good.

A word of warning regarding backups: Ransomware has a way of tracking down all your files and mapped drives, so make sure you're not just backing up to a mapped drive. Use a backup routine that

runs with different permissions and a different user to limit any ransomware outbreak.

Email, Attachments, Browsers, Links, Popups, and Plugins

It might seem obvious when I say this, but don't click stuff. Just don't. Think about it before you click it. Is that invoice in your inbox one you were expecting? Does that attachment in an email look right, and do you know the sender? Perhaps call them to make sure they really did send you that Word file? The same applies to links in email; don't just click it.

In your browser's settings, make sure you have popups blocked and disabled, and make sure all your browser plugins are up to date, too. Disable any you don't need or use.

Macros

You might be thinking Office document macros would be included in the "don't click stuff" advice. Well they are, but they're so important I think it best to mention them twice. Just DO NOT click "enable macro" or enable content in any Office file you're sent, unless you can verify its source verbally beforehand. If you're using an earlier version of Microsoft Office, find out how to disable macros from running automatically.

Local Administrator Rights

The majority of Microsoft Windows and Office exploits in the wild need the user to be logged into the vulnerable computer with local administrator permission. Often in enterprise IT environments domain users also carry local admin rights to their computers. Disabling local admin rights across the board will significantly secure your Windows computer environment.

Of course some domain users will complain and moan they can't do small tasks like change the timeout on their screen saver, but is that really important?

If you absolutely must give a domain user local admin rights to their computer, set up a separate local admin account that has the correct permissions. Then when the user needs to perform a task that requires escalated privileges, Windows will prompt them to elevate permissions to that local account. Alternatively, use one of the many endpoint security solutions that allow you to control which users have admin rights and for how long. Point-allocation of rights for small tasks, on an on-demand basis, works really well here. It removes some of the end user's pain and mitigates the risk of someone self-infecting after elevating their own privilege.

Of course I am assuming here that as an enterprise IT team, you've got all the basics right already. For example, Windows Update is running all the time, patches are pushed out to computers constantly, and AV is updated almost in real time. Having all of this covered means you're less likely to find a user who actually needs local admin rights.

As a side note, also turn on User Account Control (UAC). Just make sure it doesn't annoy the users too much.

Application Whitelisting

Before you groan and wonder how you'll build a list of known good applications in your environment, what I mean by application whitelisting is a little more intelligent.

This is not your grandfather's application whitelisting.

History has taught us that application whitelisting usually means someone in IT keeps a list of know applications on the enterprise desktop and then only allowing them to run. This was largely a manual process, a pain, and totally unscalable. End users were also

frustrated by this, as quite often legitimate applications didn't make it into the list.

Modern-day application whitelisting is far more intelligent. It requires additional services of software, but that's a small price to pay for being able to automatically lock down your environment.

For defeating ransomware, I've found application whitelisting is one of the best defenses yet, as it removes the guess work and reliance on signatures employed by classic security solutions. It's like a nightclub doorman checking the guest list—"If your name's not down, you're not coming in."

Whitelisting applies to the owner of a file and application, too. Most legitimate applications are installed by an administrator account, and provided you've set your permissions correctly as I mentioned previously, you can trust that user. Any application that gets installed by another user can be flagged and blocked as they're not owned by your trusted users. Malware executing through the user's account can be immediately blocked in this scenario.

Deception Technologies

Among the most recent advances in anti-ransomware technology are security solutions that are intended to deceive, divert, and stop ransomware before it activates file encryption. These deception technologies are far more proactive than standard desktop antivirus tools. They create decoys and traps within existing IT resources which lure the ransomware away while isolating the infection point. They are worth taking a look at, too.

What to Do if You Are Affected by Ransomware

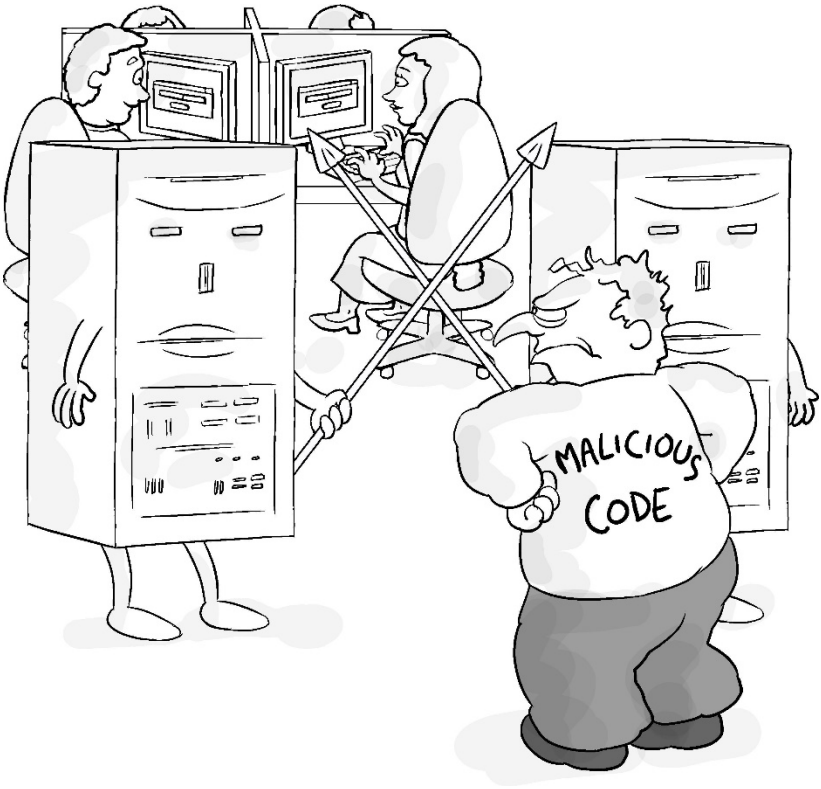
DON'T PAY THE RANSOM.

Simply put, do not pay the ransom because it may not solve your problem. First, set aside for a second the "perpetuating the problem by negotiating with terrorists and funding cybercrime, people smuggling, sex-trafficking, gun-running, car-ringing, drug dealing, life wrecking criminal underworld" arguments. Paying the ransom

doesn't guarantee your files will be returned to normal, nor that you won't be reinfected at a later date. So do not pay the ransom. I do recognize there will be some scenarios in which you have absolutely no choice but to pay, and these will be personal computing environments rather than enterprise IT—and only if you can personally come to terms with funding the list of activities I mentioned above. No backup of all your family photos and videos is one example I have seen many times. But in an enterprise IT environment, restoring from backup should be the only answer to the question.

Stay safe out there, folks.

Vendor Sponsor Chapter – Ivanti



Long before ransomware was a concern there were already plenty of applications that wreaked havoc on machines. Some were malicious in intent, while others were simply poorly-written. For example, it's over 15 years since Ivanti blocked an unwanted and troublesome executable for their first customer. It was a silly sheep animation freeware tool that users ran in their virtual desktops which ruined performance for other users on the same server, so it had to be stopped.

From that base, they've added deep functionality to proactively and surgically block all kinds of risky executables and scripts (even the fun ones) with minimal configuration on the part of IT – a highly effective tool against ransomware and malware of all kinds.

As this book describes, another key weapon against malware is to remove administrator privilege from as many users as possible. Traditionally this has caused problems for users who require admin rights to work. With Ivanti, IT can apply “least privilege” principles to every user without breaking applications or stopping them from updating the system settings they need – even if those applications or updates require administrator privileges. This approach is so granular that most users never notice that their admin rights have gone.

Ivanti also recognizes that it is not always possible to remove administrator privilege for certain “special” users, and so they have been adding new technology to restrict those users that are full local administrators, and ensure they stay within policy.

Ransomware Mitigation with Ivanti

Among the key malware and ransomware types mitigated by Ivanti solutions, and solutions are:

- Batch files, VB scripts. A lot of ransomware is simple and uses regular levels of user privilege. One of the oldest but still common approaches to perform malicious actions on a desktop is to trick the user into running a .cmd, bat or .vbs file. And even now, after all the recent coverage of cyber crime, many users still click first and ask questions when it’s too late. No matter how these files are delivered – mail attachment, USB stick, or download from a web site – they can be restricted so that only scripts from trusted sources can execute.

- PowerShell scripts and Java archives. An updated version of the trick described above uses .ps1 and .jar files. Again, only scripts from trusted sources can execute.

- Known Operating System Exploits. There really is no excuse when a piece of malware takes advantage of a defect in the operating system that has already been patched using a

hotfix or service pack. Patch Management is not just an IT chore – it's an essential security task!

- Known Applications Exploits. With so many applications in the world from so many vendors, it is critical to ensure all the most common ones are patched, especially frameworks like Flash and Java. Again, patch management is critical.

- Spoofed applications. For hackers willing to do a little extra work, many whitelisting solutions can be bypassed with fake applications or fake signatures so that they appear to come from a trusted source. Deep checks of multiple aspects of the executable, especially those that run scripts, are needed.

Ransomware is delivered using a variety of tactics – each that utilize one or more of the methods listed above. So it's critical to have a layered defense in place to protect you against *all* of these attack vectors. If these aspects of ransomware and malware mitigation are relevant for your organization, please talk to the person who gave you this book to find out how they can help.

Prevention. *No Prevention.*

Endpoint Security? Same principle.

Without prevention you could catch something much worse than the flu.

Surveys show that 70% of breaches are due to human error – users get curious and click on almost anything. Suddenly you have a plague of malware and ransomware on your network, and a lot more problems than a fever.

With Application Control, you can block the infection at the source. You can prevent malware and ransomware from executing on the desktop no matter where the user takes it – on your network, at home, or in a coffee shop. No more data loss, ransom demands, public humiliation and calling in sick.

Prevent Ransomware.
Get Application Control.

Learn more at:
www.ivanti.com

ivanti

Easily "converse" about ransomware in any setting.

Cybercriminals and hackers have turned to ransomware as an easy way to generate money from enterprise and consumer IT users. Ransomware has become a significant threat and a big headache for those caught by its malicious intent. This book will help you understand what ransomware is, and how to protect yourself and your organization from it.

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