Contents

1  The Latest and Greatest in Threat Actor TTPs
2  The Anatomy of a Successful Ransomware Attack
5  A Spotter’s Guide to Ransomware
9  The Three Stages of Ransomware Defense
14 So You’ve Been Infected with Ransomware…
17 Welcome to Hell: The Future of Ransomware
20 Parting Thoughts
21 Bibliography
Malware is a constantly evolving field, and ransomware currently sits right at the pinnacle. Threat actors all over the world devote valuable time and energy to perfecting their creations, and new innovations and features are appearing all the time.

Since the CryptoLocker/Bitcoin partnership exploded onto the scene in 2013, high profile breaches all over the world have made it abundantly clear that no organization is safe. Phishing has been far and away the most popular delivery method for ransomware, and the continued evolution of text-based social engineering attacks has been a significant factor in the rise of ransomware.

Right now most organizations are unready to cope with ransomware, both from security and recovery standpoints. In many cases, even basic security protocols such as consistent vulnerability management are lackluster or missing entirely, and threat actors are making millions of dollars every year as a result.

In this white paper we explore the growing threat of ransomware, and what you can do to keep your organization secure. After reviewing this white paper, security leaders will understand:

- What ransomware is, and how threat actors use it for profit
- How ransomware families differ, and which to look out for in the next year
- The three stages of ransomware defense and how to react if you are infected
- What ransomware of the future might look like

Phishing is the most popular delivery method for ransomware.
You gasp.

Your head hangs, and your heart races. The instant you clicked, you knew something was wrong.

That email seemed so official, and all you did was follow a link… How did THIS happen? But it’s too late for that now, what’s done is done.

You’ve been infected with ransomware, and now you’ll have to admit it to your boss. Some difficult questions will be coming your way soon, but before we get to that…

What Is Ransomware?

Put simply, ransomware is malicious software (malware) that restricts access to computer systems or files, and demands that the victim pay a ransom in exchange for restored access.

Recent examples of widespread ransomware include CryptoLocker and CryptoWall, but it’s important to realize that this is not a new concept.

The very first ransomware, known as the “AIDS” Trojan, was created in 1989 and functioned very similarly to modern versions. Even in the modern Internet age ransomware has been around for over a decade, and by mid 2008 some versions used such advanced encryption methods that retrieving files computationally became almost impossible.

But while ransomware itself isn’t new, its wholesale popularization is.

In late 2013, with Bitcoin as its payment currency, CryptoLocker burst onto the scenes and quickly inspired a variety of copycats with its high-profile success.

Up until this point payment had been a significant headache for the groups responsible for creating ransomware, due to the inherently traceable nature of traditional currencies. But by demanding payment in Bitcoin, and taking a few precautionary measures, the group behind CryptoLocker made millions of dollars in ransoms before their distribution botnet was taken down by a joint force of law enforcement agencies (including the FBI and Interpol), security software vendors, and universities.

Despite this victory, though, ransomware is only growing in popularity. More and more organizations are falling prey to ransomware, and most security vendors agree that the trend will continue to grow during 2016.

Should I Be Worrying Right Now?

We field a lot of questions about ransomware, but there’s one in particular that comes up time and time again.

“Are we at risk from ransomware?”

It’s not a difficult question to answer. Yes, you’re at risk… Everybody is at risk.

You see, there are plenty of ways for threat actors to spread ransomware. They create fake online advertisements and pop-ups, exploit known vulnerabilities to gain access to corporate networks, and even drop USB sticks loaded with ransomware in car parks and restrooms.
But above all other distribution methods, phishing is the threat actor’s weapon of choice. Phishing emails loaded with ransomware are being sent to consumers and corporations alike, and worse, the quality of the writing is getting better all the time.

A few years ago, most phishing emails were pretty easy to spot, with their dodgy spelling and conspicuous use of ‘Sir’ or ‘Madam’. These days, though, it’s not unheard of for threat actors to use espionage tactics against corporations and their partners purely to inform bespoke spear phishing campaigns.

They’re pulling out all the stops to infect your systems with ransomware, so yes, you need to be concerned.

But there’s no point in just being concerned. You need to do something. That’s why we’ve decided to run through the anatomy of a typical ransomware attack, so you’ll know what to look for, and what to avoid.

Highly Targeted Attacks

Although mass spam campaigns are still a concern, the majority of corporate cases start with targeted attacks. Threat actors are surprisingly organized, and often focus their attentions on a specific organization or group.

If this happens to you, expect your attackers to research your organization in detail, looking for information about your systems, partners, and services to provide ammunition for their campaign.

And it doesn’t end with a few phishing emails.

Threat actors target privileged users and use social engineering tactics to gain access to as many of your assets as possible before they initiate a ransomware attack. In this way, they maximize your losses in the hopes that you’ll quickly cave and agree to pay the ransom.

Click Here to Lose Access

Once the target (you) has been chosen, and enough access has been granted, the ransomware will be deployed. The trigger might have been a malicious link in an email, a successful social engineering campaign, or a ransomware-ridden USB stick, but ultimately the result is the same.

Your files are locked up tight, and it seems like you either pay up, or shut up.

In reality it’s a bit more complex than that, and we’ll go through your options in a later article, but for now let’s keep it simple. Instead, let’s try to understand exactly how this locking process happens.

You see, most people assume the ransomware they’re infected with works all on its own. Some very simple ransomware packages do work in isolation, but they’re pretty ineffective and have largely fallen out of use. If a threat actor attempted to infect your network with a self-contained ransomware package, almost any security system would quickly identify and prevent it.

Instead, when activated, most ransomware packages attempt to contact so-called command and control (C&C) servers for further instruction. These instructions range from simply providing encryption keys to initiating further exploration and vulnerability scanning within your network.

And where early ransomware packages used static C&C servers, the latest versions include dynamic algorithms that attempt to connect to hundreds or even thousands of servers. This dramatically improves their chances of success, and makes defending yourself much more challenging.
Calculating Losses

The very earliest versions of CryptoLocker simply encrypted the files on an infected user’s local computer. Annoying, yes, but usually not the end of the world unless the user happens to be your CEO.

But we’re well beyond that point now.

As we’ve already alluded to, the most sophisticated ransomware packages can identify other areas of your network to spread to, scan for vulnerabilities, and even prioritize the most recently accessed files and folders for encryption in case the process is interrupted.

They also, sadly, specifically search for and encrypt your backups.

When ransomware made a comeback in 2013, one of the earliest popularized defences was to ensure users’ data was backed up regularly. That way, in the event of a ransomware attack, losses would be minimal.

Sadly, as always, threat actors catch on quickly. You can almost guarantee that any backups saved on infected machines or servers will be among the first files to be targeted.

Pay Up or Shut Up

Chances are everything up to this point has gone completely unnoticed. The first you’ll know about the attack is when a pop-up fills your screen demanding a ransom in exchange for your files.

You’re kicking yourself for opening that email. For playing along. For not taking ransomware seriously until now.

But it’s too late for that.

Your attackers will let you know what they want, and by when. They’ll tell you exactly what you’ll do if you want to regain access to your files. Sometimes they’ll even allow you to decrypt a file or two, just to prove they’re for real.

And once you’ve paid, and your attacker has verified the payment, you’ll receive the private key and automatic decryption will start. Let’s just hope nothing goes wrong with the decryption process… because threat actors aren’t usually in the business of providing additional support.
A Spotter’s Guide to Ransomware

For several years now, ransomware has been the talk of the industry. From schools and hospitals to police departments, pharmaceutical companies, and even private citizens, it seems like nobody is safe. And, of course, they aren’t.

So with that being the case, let’s take a look at the different types of ransomware, the most prominent families of 2016, and what’s driving so many threat actors to use this particular style of cybercrime.

When Ransomware ISN’T Ransomware

First off, it’s important to realize that not all ransomware is created equal.

In fact, there are a number of trojans that simply claim to be ransomware, but don’t actually encrypt or lock any of your files or systems. Sometimes called ‘scareware’ or ‘fauxomware’, these trojans pose no real threat to your files or systems.

Instead, similar to the classic FakeAV scam, these trojans use social engineering tactics in an attempt to extort money from their victims.

Although not as popular as it used to be, fake ransomware is still in circulation, so make sure to check whether your files have really been encrypted if you ever do have the misfortune to be hit with ransom demands.

Recent examples of fake ransomware include fake AnonPop, and the recent flurry of attacks on Drupal-based websites.

Locking vs. Crypto Ransomware

Of course, the vast majority of attacks do use real ransomware. No empty threats here, so if you’re hit by one of these you’ll need more than an AV product to resume business as usual.
But still, there’s more to the story. There are two main forms of ransomware, both of which are in wide circulation in 2016.

The first, known as locking ransomware, doesn’t go after your files. Instead, these trojans kill the desktop user interface of infected machines, and display a full screen warning notice demanding payment. Once payment is made, the infected system is unlocked can be used as normal.

The most prominent example of locking ransomware is Reveton, which first appeared during 2012 and displayed a warning claiming to be from a law enforcement agency. The message would accuse infected users of illegal activity, and demand a ‘fine’ be paid before their system would be unlocked.

Although distribution of Reveton died down after a number of arrests were made in 2013, Avast Software announced that new variants had been found during 2014, and the ransomware family remains very much alive.

Despite this, the popularity of locking ransomware has waned in recent months. A single locked machine can usually be written off by mid-sized or large organizations, making the ransom demand less effective. With that said, there may well be a resurgence in locking ransomware as mobile and IoT devices continue to proliferate.

The second, and more common form of ransomware is known as crypto ransomware. When all is said and done, these are the ones that’ll give you a really bad day if they infect your system.

If you read our previous article on the anatomy of a successful ransomware attack, you’ll already be familiar with the basic premise. Instead of going after a single machine, sophisticated crypto ransomware will burrow deep into your network, gaining as much access as possible before deploying.

From there the trojan will quietly start encrypting your files, starting with the most valuable, until the job is complete. Only then will you receive a ransom demand.

The real problem here is that if such a trojan goes unnoticed in your network, it could easily end up encrypting a large number of
valuable files. Even worse, the cryptographic systems used are often incredibly strong, and almost completely resistant to cryptanalysis attempts.

If you have any previous knowledge of ransomware, you’ll recognize the name CryptoLocker. First appearing in 2013 this trojan used 2048-bit RSA key pair encryption, and used a file extensions whitelist to identify the highest value targets. The trojan also threatened to delete the private key if payment wasn’t made within three days, though in reality the key could still be purchased after this time for the very reasonable price of three Bitcoins (approximately $2,300 at the time).

This original version of CryptoLocker was shut down seemingly for good in June 2014, when Operation Tovar took down the Gameover ZeuS botnet, but not before an estimated $3 million dollars was successfully extorted.

Unfortunately, a wide array of copycat trojans sprung up almost immediately, and many persist to this day.

The VIPs of 2016

Perhaps unsurprisingly, ransomware is very much alive in 2016.

And according to Kaspersky Lab’s Q1 Threat Evolution report, over 80 percent of infections are caused by the two largest ransomware families: TeslaCrypt and CTB-Locker.

TeslaCrypt has been widely distributed via the Angler exploit kit, which targets vulnerabilities in Adobe Flash to initiate an infection. Once files have been encrypted and the ransom demands made, the victim is allowed to decrypt a single file in order to ‘prove’ that their files will be returned once payment is made.

All things considered, TeslaCrypt is a fairly standard example of ransomware, and so far only English-language versions have been observed.

CTB-Locker, on the other hand, is a little different. For a start, versions of the trojan have been identified in multiple languages, including English, French, German, Spanish, Italian, Dutch, and Latvian.

The authors make use of an affiliate program, whereby the infection process is outsourced to a network of partners in exchange of a cut of the profits. This distribution model has been extremely successful, achieving a huge number of infections, and generating significant revenues both for the authors and their affiliates.

Most alarmingly, because the affiliate model makes use of a large distribution network, a wide variety of infection vectors have been observed. Spam campaigns have likely accounted for the highest proportion of infections, but spear phishing attacks, exploit kits, and malicious advertisements are also commonplace.

But distribution isn’t the only interesting thing about CTB-Locker.

Unlike most ransomware, CTB-Locker is able to start encrypting files without contacting an external command and control (C&C) server. Because of this, no Internet connection is required until a victim attempts to decrypt their files.

Finally, by making use of Elliptic Curve Cryptography, CTB-Locker is able to make use of high-grade encryption while keeping the trojan’s file size to a minimum.

Also-rans for Q1 2016 include Cryptowall, Cryaki, Scatter, Rakhni, Locky, Shade, iTorLock, and Mor.
Why So Many?!

So what is it about ransomware that’s making it so popular?

Well first of all, it’s easy to use. Unlike banking trojans, which target secure systems and require significant customization for each target, ransomware is a one-size-fits-all affair, and can be widely distributed with minimal difficulty.

It’s also easy to get hold of. Take, for example, the screenshot below.

Taken from the dark web market HANSA, it shows just how easily (and cheaply) threat actors can get hold of ransomware trojans. It took less than two minutes to find this seller, and there are many others out there.

Ultimately, though, it comes down to money.

Ransomware has been tremendously effective. The authors and distributors of ransomware have collectively made a lot of money from it, with relatively few receiving any form of punishment. Not only is there no need to sell anything on, the rise of Bitcoin has made accepting payment a much simpler and less risky proposition.

And, of course, success begets success. Hackers and criminal organizations all over the world have seen how effective the ransomware business model can be, and rushed to get in on the act.

Be Proactive in Defense

If you’ve made it this far through the white paper, hopefully you’re starting to realize that you need to be taking ransomware seriously. After all, the FBI does.

But it’s not just being scared, you need to know how to secure yourself and your organization against the latest ransomware trojans. Next up, we’ll take a look at the proactive steps you can take to defend against ransomware and it’s most common attack vectors.
The Three Stages of Ransomware Defense

So far in this white paper we’ve covered the anatomy of a typical ransomware attack, and looked at some of the most common ransomware families.

And that’s useful information to have, but it doesn’t answer the important question: How do I keep my organization safe?

So now we’ll go through some of the security measures you can take to minimize the likelihood of falling prey to a ransomware attack.

The most important thing to realize is that there’s no magic bullet. There’s no single approach, product, or vendor that can guarantee your complete safety from ransomware… or any other form of cyber attack, for that matter.

Instead, there are three stages of security that you and your partners can use to make a threat actor’s task extremely difficult.

Block Infection Vectors

Perhaps unsurprisingly, the first (and most desirable) way to defend against ransomware is to avoid getting infected in the first place. To do that, you’ll first need to understand how ransomware is usually deployed.

There have been cases where an attacker has used techniques such as IP spoofing or DNS poisoning to gain direct access to an organization’s network and deploy ransomware. In reality, though, very few threat actors have the level of skill required to achieve this, and even those who do will generally opt for an easier alternative.

Instead, the vast majority of ransomware is distributed through phishing emails, social networks, and so-called drive-by downloads — malicious links or content injected into (usually) legitimate websites and pop-up adverts.

With this in mind, there are several steps you can take to prevent the overwhelming majority of ransomware attacks from ever gaining a foothold inside your network:

Scan incoming email

This is an absolute must.

Every organization is at risk from phishing attacks, so you should be scanning all incoming, stored, and outgoing mail for potential threats. A good anti-spam filter will go a long way here, but you’ll also want to rigorously scan email attachments to weed out trojans. Executable files with extensions like .exe or .dmg should be at the top of the list for quarantine and removal, but even office documents shouldn’t be exempt from investigation.

While you’re at it, some phishing attacks originate from domains and IP addresses that are easily blocked. Making use of technologies such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) is an easy way to save yourself a headache.

Disable Macros

This has perhaps the greatest return on investment of any security policy. Seriously.

Right now, many threat actors are using Microsoft Office macros to automatically deploy ransomware. So if your office
software is set to automatically allow macros, you’re setting yourselves up for disaster.

Quite simply, the vast majority of office users don’t even know what macros are, so go ahead and disable them… you can always add exceptions later on.

**Block pop-up ads**

Drive-by downloads are becoming increasingly common, and most of them originate from compromised pop-ups. These ‘malvertisements’ can be particularly dangerous as they allow attackers to target users based on their personal browsing history.

Ad-blocking technology is an easy and reasonably inexpensive way to foil this type of attack, so get on it.

**Security awareness training**

User training on security matters has come under a lot of fire in recent years. The argument goes that because users hold no direct responsibility for a network, and they don’t understand the implications of being breached, training them is simply a waste of money.

Needless to say, we disagree.

Of course, it is true that bad security awareness training is a waste of time and money. But if you allocate the time and resources necessary to create a holistic, engaging, and up-to-date security awareness training program, you’ll certainly see the benefits.

It’s important to realize that no matter how good you are at scanning and authenticating incoming email, there will still be phishing emails that find their way into your users’ inboxes. Not only that, your users will visit compromised websites.

A good security awareness program can help teach your users the basic security behaviors that will foil the majority of attacks. It will also teach them to recognize potentially malicious websites, report phishing emails, and notify you if they have concerns.

Right now, a large portion of your security awareness training program should be focused on phishing. Not just because it’s the primary delivery channel for ransomware, but because it’s the single greatest security threat to most organizations.

You need to understand the lures and tricks used by spammers and spear phishers, and train your employees to recognize and report them. If you can convince your employees to report every phishing email that hits their inbox, you’ll have the opportunity to analyze them, identify who else has received them, and minimize exposure within your organization. As an added bonus, you can use reported emails to improve spam filters and block similar subsequent attacks.

We agree entirely that your users aren’t responsible for network security, but their behaviors can impact it hugely, so getting them on side can only be a good idea.

**Foil Ransomware Functionality**

Of course, no matter how good you are at blocking attacks, some will get through. That’s why the second phase of ransomware defense is to prevent ransomware from gaining a foothold inside your network.

If we’re honest, though, these steps aren’t specific to ransomware defense. These are (mostly) basic processes and strategies that you should already be using to keep your network secure.
**Backup, backup, backup**

By this stage, you know how ransomware works.

It shouldn’t come as any surprise, then, that regular and thorough backups are fundamental to any sensible anti-ransomware program. After all, if you’re creating a full backup at the end of each business day, the potential impact of ransomware is hugely reduced.

If you are hit with a ransomware demand, you can simply deal with the infection, and restore all but the most recent files from your backup.

One thing to note, though.

As we’ve already mentioned in this series, modern ransomware is very sophisticated. Instead of encrypting files at random, many ransomware families specifically target and encrypt backup files first.

To get around this, you’ll need to store your backups somewhere that can’t be accessed from your primary network. In fact, storing these backups in complete isolation would be best of all.

**Vulnerability management**

It’s not fun or sexy, but a regularly scheduled vulnerability management process is a vital part of any security program.¹⁴

And don’t think you can just run a vulnerability scanner every few weeks… you need to put in the time and resources to remediate serious vulnerabilities as quickly as possible.

Many threat actors use exploit kits to prey on known vulnerabilities in software packages such as Adobe Flash. As a result, keeping your software and firmware packages up to date with the latest patches will prevent many malware trojans from obtaining the access they need to function.

It’s no good putting it off, threat actors invariably know about vulnerabilities before everybody else, so every minute you delay is needlessly putting your organization at risk.

**User access levels**

Let’s get one thing straight: Your users DO NOT need unfettered access to your network.

Most people use a very limited set of folders and applications during the course of their daily work, and identifying who needs access to what is an important security function. Yes, sometimes people will be irritated because they don’t have the access they want, but it really isn’t difficult to grant additional access on a case-by-case basis.

Given the damage that can be caused by overproviding user access, it should be a no brainer to work from the assumption that most people don’t need to access files or systems outside their own department’s ‘area’.

On a similar note, almost nobody really needs to install new applications… so why on earth would they be granted the access to do so? Allowing your users to activate .exe (windows) or .dmg (Mac OS) files is begging for trouble, and will inevitably cause infections in the long run.

To take this a step further, many ransomware trojans will now attempt to deploy automatically from the location they’ve been downloaded to. Rather than attempting to preemptively block certain types of application, you can use whitelists to determine which applications are allowed to run.

Of course these whitelists can be amended as and when necessary, and they do a sterling job of preventing many ransomware families from gaining traction inside your network.

Instead of encrypting files at random, many ransomware families specifically target and encrypt backup files first.
**Block Communications**

Not all ransomware trojans work in isolation. In fact, in order to minimize files sizes and incorporate complex functionality, many trojans will initially try to contact external servers for ‘orders’ before they start the encryption process.

These external servers are known as command and control (C2) servers, and you can render many trojans harmless by preventing this back-and-forth communication from taking place. Of course, this requires reliable threat intelligence on active C2 servers, but the pay-off is potentially significant.

Not only will you prevent a major ransomware headache, you’ll also be able to intercept C2 communications, and quickly locate trojans within your network.

Unfortunately, savvy ransomware operations often pre-program their trojans with dynamic lists of C2 servers, which will be contacted one by one until a successful connection is achieved. Nonetheless, blacklist known C2 servers will prevent many trojans from achieving their intended mission, so give serious consideration to including this tactic in your security program.

**Endpoint security**

Modern endpoint security suites are a tremendously effective way to avoid having your network infected through the deluge of laptops, tablets, and mobile devices that connect to it every day.

In case you’re unfamiliar with the concept, endpoint security is based on the premise that each device is responsible for its own security. But don’t get too excited. This isn’t an excuse to neglect central network security functions, but rather an additional layer of security.

With functions including malware identification and removal, firewalls, IPS/IDS sensors, application control, and even (in some cases) disk encryption and data leak prevention, endpoint security can play a valuable part in the identification and removal of ransomware trojans.

It’s worth noting that more advanced ransomware operations frequently test their trojans against common antivirus products in an attempt to increase infection rates. For this reason, endpoint security (including AV) is an excellent addition to a comprehensive security program, but usually isn’t enough in isolation.

**Network architecture**

One of the big problems with many networks is that they were never designed to be as big so they have become. Instead, they’ve grown over time to accommodate the needs of the organization.

As a result, they’re often not designed or laid out in a way that’s conducive to sensible security measures.

Given that many modern ransomware families will attempt to gain additional access before they start encrypting your files, a poorly constructed network will fare very badly if an infection occurs. If,
instead, the network architecture has been deliberately designed and segmented, far fewer files and systems will be exposed to any potential ransomware attacks.

**Get creative: Honeypots and darknets**

Up until this point we’ve looked exclusively at sensible and easily achievable security standards that should be used to combat ransomware.

But that’s not to say that you can’t go above and beyond the call of duty. Honeypots and darknets are creative and proactive security protocols that aim to lure attackers or malware to target them first.

Using attractive sounding names, unpatched software, and intentionally flawed security, honeypots and darknets are areas of your network that aren’t used by any of your staff. As a result, any activity detected in these areas is automatically suspicious, and cause for further investigation.

Taking the time to setup and monitor proactive security measures like these is an excellent way to identify attacks early on, and take the necessary steps to block/quarantine the threat before any real damage is done.
So You’ve Been Infected with Ransomware…

That awful moment.
You’re working away, getting tasks ticked off left and right… And then it happens.
A terrible sinking feeling grips your stomach, and you know immediately what’s happened. You’ve been infected with ransomware. The screen in front of you is filled with demands about Bitcoins, Tor, and encryption keys.
So what now? You’ll have to tell your boss, of course. But once that’s done, there are some important tasks for you to complete.

Check the Damage
A lot of the time, people and organizations that have been infected with ransomware jump straight in at the deep end. “Should we pay?” they want to know.
But there are other things to consider first.
For instance, do you know what you’re missing? The ransomware claims to have encrypted your files, but have you lost anything important?
Before you start panicking, make sure the claims being made are legitimate, and that the files you’ve lost are actually important to you or your organization. If they aren’t, it probably isn’t going to be worth your while to pay the ransom.
If possible, you’ll also want to identify the ransomware family you’ve been infected with. The chances are low, but you may have been infected with a trojan that has already been tackled by law enforcement or cyber security experts. The FBI locking trojan, for instance, can be removed without paying a ransom,¹⁵ as can the LeChiffre encrypting trojan.¹⁶

The important thing to remember is that before you start planning your response, you need to make sure a response is actually necessary. Since modern ransomware makes use of application whitelists to prioritize the most valuable files and powerful encryption standards to prevent you gaining access via brute force, you probably will find that your situation is less than ideal… but it doesn’t hurt to check.

Restore From Backups
If you’ve been following along, you’ll probably recall that we’re strong advocates of a thorough backup plan.¹⁷ This is one case where investing the time and resources upfront to implement such a plan will pay dividends.
If you have recent backups of the encrypted files, there’s almost certainly no need to pay the ransom.
Sure, you might lose work completed in the last day or two, but in ransomware terms that’s getting off very lightly.
If, on the other hand, you don’t have recent backups, I’m afraid you’re out of luck. Instead, it’s time to have that discussion…

To Pay, or Not to Pay… That Is the Question
“But what if we pay… and they don’t give us the decryption key?”
This is perhaps the most common question we’re asked about ransomware.
The ransomware business model, which has been tremendously successful for cyber criminals, relies on organizations trusting that a decryption key will be provided if they’re willing to pay up. Consequently, organizations that choose to pay their ransoms do regain access to their files… …most of the time.

Yep, you guessed it, there are some real scammers out there who won’t give up the decryption key even if you decide to pay them. Naturally, that poses a conundrum for organizations infected with ransomware.

And it doesn’t stop there.

If you do decide to pay, and you’re granted access to your files, you’ve just given the game away. The group of threat actors who targeted you now know that you’re willing to engage with them. They might just choose to attack you again, or even pass on this knowledge to other groups.

It’s these factors combined that led the FBI to actively discourage the payment of cyber ransoms. FBI Cyber Division Assistant Director James Trainor sums it up like this:

“Paying a ransom doesn’t guarantee an organization that it will get its data back—we’ve seen cases where organizations never got a decryption key after having paid the ransom.”

“Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.”

Ultimately, of course, it’s your decision. If you can’t restore from backups, and you can’t do without the files, you may feel you only option is to pay the ransom and put your trust in the ‘honor’ of these threat actors.

What’s Everybody Else Doing?

Whether or not you choose to pay the ransom, you’re far from alone.

And even though many organizations choose not to pay, victims in the US paid over $24 million in ransoms in 2015 alone.

Methodist Hospital in Kentucky recently received demands for approximately $1,600 in Bitcoins, leading them to declare an internal state of emergency. So far, they claim, they have opted not to pay the ransom.

Hollywood Presbyterian Hospital in California, on the other hand, opted to pay a $17,000 ransom earlier this year to regain access to their files.

Hospitals naturally make excellent targets for threat actors of particularly dubious morals, and there has been a spate of high profile ransomware attacks in the healthcare industry in recent months. Regardless of your industry, though, a quick Google search will demonstrate that nobody is truly safe from the clutches of ransomware.

But of course, precise statistics are hard to come by. Many attacks go unreported by the media, mainly because the organizations affected simply don’t want the bad publicity that comes with admitting they’ve been breached.

Ultimately, though, there are plenty of high profile examples to go around, and they bring us no closer to deciding whether or not to pay up. I’m afraid you’ll have to make that decision for yourself.

Operation Clean Up

One thing that is clear, though, is that once you’ve been hit with ransomware you need to make sure it’s really gone.

Your files are encrypted (or your computer locked), but you’ll also need to investigate
exactly what happened. How were you compromised? Can you prevent it from happening again? And what happened to the trojan?!

In short, a detailed postmortem is required, and you’ll likely find plenty of ways to enhance your security program in order to prevent this happening again.

If you don’t have a dedicated security team, you may need to enlist the help of a vendor to get this job done. Whether you choose to pay the ransom or not, it doesn’t take much to guess that you’d rather this didn’t happen again.

**The Sad Truth About Ransomware**

Here’s the thing. There’s a reason why prevention came before recovery in this white paper.

Once you’ve been infected, unless you’re very lucky, your options are extremely limited: Restore from backups, pay, or suck it up.

But whatever you do, make sure you learn from your mistakes.

Conduct a full postmortem to identify what went wrong, and how it can be prevented in future. Make sure you have sensible cyber hygiene programs in place, such as vulnerability and patch management, security awareness training, strict email scanning protocols, and a comprehensive off-site backup plan.

And if you don’t have the resources to build a permanent security team, give serious consideration to partnering with a specialized security vendor. After all, it’s happened once, and it can always happen again.
Welcome to Hell: The Future of Ransomware

Close your eyes for a moment, and picture a ransomware demand on your screen.

Picture the garish colors, the price that goes up after a few short hours, and the timer counting down the minutes until the private key is deleted and your files are lost for good.

Feels bad, right? Your heart rate probably went up, and a sinking feeling gripped your stomach.

Well, in the words of Bachman-Turner Overdrive, you ain’t seen nothing yet.

Researchers at Cisco Talos have predicted a time in the not-so-distant future when a single ransomware trojan can infect over 800 servers and 3,200 workstations in just one hour.

And you can forget about thousand dollar ransoms. Their report, released earlier this year, imagines a fictitious and highly unfortunate organization facing a ransom of $1 million dollars.

But let’s back up a minute.

Before we get too carried away it's useful to consider the pros and cons of current ransomware, as they would appear to a threat actor.

**Where Is Ransomware Lacking?**

As we have previously explained, ransomware is tremendously attractive to threat actors for a whole host of reasons. There’s no data to sell, distribution requires no technical knowledge or skills, and perpetrators are very rarely caught.

Even better, the level of encryption used is functionally uncrackable, and most affected organizations are too embarrassed to even contact law enforcement agencies.

But with all that said, current ransomware is far from perfect.

For a start, the individual ransoms paid are relatively small, forcing threat actors to focus their energies on spam phishing campaigns in the hopes of snagging lots of low profile victims. Most ransomware is also purchased off the shelf, and doesn’t allow distributors to alter key variables such as ransom values. This further reinforces the prevalence of spam as an infection vector, because it simply isn’t worth the time it would take to target affluent people or organizations.

On a similar note, many non-techies would consider the process of purchasing cryptocurrencies such as Bitcoin to be beyond their abilities. Whether they can afford to lose their documents or not, no ransoms are going to be paid by people who are unable to complete the payment process.

And it’s not just about the money. Most ransomware trojans are highly dependent on command and control (C2) infrastructure, and many are left ‘orphaned’ as a result of tight security controls.

In fact, if we had to guess at the top priorities for improvement in ransomware, we’d go for:

- Reduce dependence on C2
- Improve reach within infected networks
- Alter & increase ransoms depending on circumstance
- Reduce complexity of payment process
And believe it or not, all of this work is already happening. Threat actors love to get ahead of the game, and any improvements that might increase their return on investment are right at the top of their priority lists.

**Reinforcements Are On The Way**

The thing is, most of the improvements listed above are already possible.

Worms with the ability to self-replicate have been around for decades, and it’s only a matter of time before that functionality finds its way into the world of ransomware.

And the ability to increase ransoms? Forget about malware, that’s basic software functionality. If threat actors want it badly enough, we’ll start seeing it very soon.

One thing that is unlikely to change, however, is the complexity of the payments process. Bitcoin in particular is well established now, and while the conversion and payment processes are somewhat difficult for non-techies to grasp, they are unlikely to improve any time soon.

Our guess is that ransomware of the future will include more comprehensive payment instructions. After all, if they’re going after big fish (and big ransoms) it’ll be worth their while to make absolutely sure each victim knows how to pay.

But what about the dependence on C2 infrastructure? Some worms take into account common C2 disruption techniques and work around them, but thus far the vast majority are still reliant on it to some extent.

So if we can’t look to the past or present for a way around the C2 paradigm, will it stick around?

The researchers at Cisco Talos think not.

**Cryptoworms and a King’s Ransom**

Enter the cryptoworm, a self-propagating ransomware virus that automatically infects everything from executable files to USB drives. Every time you open an infected application or plug in an infected device, the cryptoworm goes to work.

No longer dependent on C2 infrastructure, the cryptoworm could use globally unique identifiers (GUIDs) and standard HTTP, HTTPS, or DNS services to contact outside domains purely for the sake of collecting infection statistics. Even if you wanted to block these communications, it would be nearly impossible.

But amazingly, this isn’t the carpet bomb approach you might think. The researchers who wrote the paper imagined a worm that would only target and implant hosts if they had an internal network address. No threat actor wants this type of malware running rampant on the open Internet, especially when they’re conducting a targeted attack on a wealthy organization.

And once the cryptoworm has been built, it’s not hard to imagine what happens next. That million dollar ransom scenario we looked at earlier doesn’t seem so far fetched any more.

**Backups Won’t Save You… and Neither Will Insurance**

And as bad as all this sounds, there’s another, less obvious problem.

Once an organization has been well and truly infected (remember, 800 servers and 3,200 workstations in the first hour), they’ll be hit with the exorbitant ransom. So far, so obvious.

But when an infection reaches that scale, it’s not so obvious how it should be dealt with. Whether an organization pays the ransom or not, they’re likely incur huge costs as a result
of disruption to their normal service. Even if literally everything can be restored from backups, and the cryptoworm permanently expelled from the network, the cleanup job will most likely take days or weeks.

And sure, paying the ransom means they can decrypt everything... but that still takes time. And systematically removing every trace of the cryptoworm? That sounds like a huge job. They’d need to check or restore every executable, every USB drive, every server, every workstation...

And will insurance make up for all this? It seems unlikely. Once these types of attack become commonplace, there’s no doubt that in some cases insurers will blame negligence and refuse to pay. Even if they don’t, insurance payouts won’t cover the full extent of the damage.25

But before you start systematically taking your organization offline with a pair of shears, it’s not all bad.

**You Can Still Defend Yourself**

Despite the picture we’ve painted so far, cryptoworms won’t cause the end of civilization as we know it.

They still have to breach your defenses, for a start, and will most likely rely on well-documented vulnerabilities to infect and propagate. In fact, if you’ve been following this series so far, you already know what you should be doing.
Let’s be honest, ransomware is a huge concern for organizations of all sizes. Thankfully, as we’ve explained throughout this white paper, there are many ways to safeguard your organization.

But if you take just one thing from this white paper — and we sincerely hope you’ll take more than that — let it be this:

*Ransomware prevention is infinitely preferable to ransomware recovery.*

Sure, it is possible to recover from an infection. If your organization is well established and reasonably stable, it’s unlikely that a single ransomware trojan could damage your operations in the long term.

But in the short term they can be a nightmare. A ransomware infection could easily halt operations for a day or more, cost you both in ransom payments and system recovery, and cause significant damage to your electronic systems and infrastructure.

And if your organization isn’t well established, or you’re operating on tight margins, a ransomware infection could become a lot more than a temporary setback.

With that in mind, here’s a quick reminder of the actions you should be taking to prevent ransomware from gaining a foothold inside your network:

- **Exercise good cyber hygiene.** Vulnerability management, sensible user access levels, and robust security software are a must.

- **Beware of email.** Scanning all incoming email and disabling MS Office macros are just the start. Comprehensive security awareness training will drastically reduce your risk profile.

- **Backup everything.** Just in case you are infected, having a secure physical backup (preferably off-site) will ensure recovery is possible.

- **Proactive is best.** Implementing segmented network architecture and creative security mechanisms (e.g. darknets) will help you to identify potential infections much more quickly, as well as reducing the impact of infections if they do occur.

- **Be intelligent.** Threat intelligence is the single best way to stay on top of the latest threat actor tactics, techniques, and procedures (TTPs). Implementing a threat intelligence platform, along with the necessary human analysis resource, will enable you to continually tighten up your network security program.

And of course we realize that these steps aren’t cheap to implement. It’s not something you can throw together in a week (or even a few months).

In fact, if you really want to take security seriously, you’ll find that even after the initial investment it’s a continual process of testing, training, and tweaking to ensure your organization’s continued security.

But if you do take the time — and the investment — to make your security program the best it can be, you will reap the rewards in the long run.

Ransomware prevention is infinitely preferable to ransomware recovery.
Bibliography

7. AVAST Software, Reveton ransomware has dangerously evolved - https://blog.avast.com/2014/08/19/reveton-ransomware-has-dangerously-evolved/
13. PhishLabs, How to make the most of reported phishing emails… Even if there are way too many - https://info.phishlabs.com/blog/how-to-make-the-most-of-reported-phishing-emails...-even-if-there-are-way-too-many


22. Wired, Why Hospitals are the Perfect Targets for Ransomware - [https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/](https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/)


PhishLabs is the leading provider of 24/7 cybersecurity services that protect against threats that exploit people. The company is trusted by top organizations worldwide, including 4 of the 5 largest U.S. financial institutions. PhishLabs combines proprietary technology, intelligence, and human expertise to rapidly detect, analyze, and stop targeted cyberattacks before they impact organizations. Additionally, the company provides robust threat intelligence that strengthens existing cyber defenses and optimizes threat prevention. Leading organizations partner with PhishLabs to more effectively disrupt targeted cyberattacks, prevent data breaches, and reduce online fraud.

www.phishlabs.com  |  info@phishlabs.com  |  +1.877.227.0790