MSPeasy Series

datto

RANSOMWARE MADE MSPeasy

The MSP's Guide to Saving the Day

Ransomware has become a threat to individuals and businesses alike over the past couple of years. A recent study conducted by security software vendor McAfee Labs identified more than 4 million samples of ransomware in Q2 of 2015, including 1.2 million new samples. That compares with fewer than 1.5 million total samples in Q3 of 2013 (400,000 new).

It seems unlikely that the use of ransomware will slow down any time soon. In the first three months of 2016, ransomware attacks increased tenfold from the entire previous year, costing victims more than $200 million. It's become an epidemic. Ransom payment demands are typically fairly low—so many victims choose to simply pay up and move on. As such, there is little interest in the malware among law enforcement. However, paying ransom can and should be avoided. So, ransomware represents an opportunity to educate current clients on cyber security best practices while generating new business opportunities for MSPs.

In this ebook, you will find information on the variety of ransomware in existence today and how it is spread. You'll get practical advice from MSPs and IT security professionals about how best to communicate the risk of ransomware to your clients so they understand the importance of investing in security, backup and recovery solutions.

> It used to be that the bad guys wanted data because it was valuable to them. With ransomware they're essentially saying: 'your data isn't valuable to me, but how much is worth to you?' It's scary how smart it is.

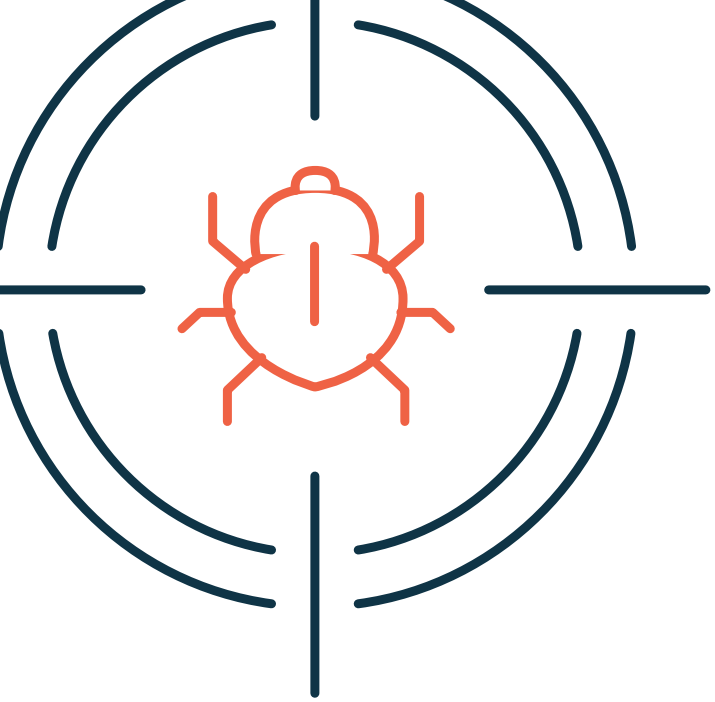
THE CURRENT STATE OF RANSOMWARE

In a recent MSPmentor podcast, Hal Lonas, CTO of security software provider Webroot, offered a succinct explanation how ransomware has flipped the security threat paradigm on its ear. "It used to be that the bad guys wanted data because it was valuable to them," he said. "With ransomware, they're essentially asking: 'your data isn't valuable to me, but how much is worth to you?' It's scary how smart it is."

There are a few dominant families of ransomware in existence today. Each family has its own variants. It is expected that new types of ransomware will continue to surface as time goes on. This is because cyber extortionists are constantly modifying ransomware code to evade detection by the most common defense technologies, such as security software. This year, we've witnessed a surge in "polymorphic" malware, which is a variant that changes automatically as if to appear as unique to different endpoints. This is a major issue, because traditional security software often fails to discover singular variants.

Most ransomware uses the AES algorithm to encrypt files. To decrypt files, hackers typically request payment in the form of Bitcoins or alternate online payment voucher services. The standard ransom demanded is about $500. Many variants also threaten that the ransom will exponentially increase if it not paid within a 72 hour window, such as Jigsaw. "We've seen it bite clients with varying severity," said Frank Slattery of Teamlogic IT, a Massachusetts-based managed services provider.

Email is the most common method for distributing ransomware. It is generally spread using some form of social engineering; victims are tricked into downloading an e-mail attachment or clicking a link. Once the user takes action, the malware installs itself on the system and begins encrypting files.



As an MSP, it's important to know the latest ransomware developments and whether specific verticals are being targeted. The more informed you are, the better you can protect your clients' data.

In other cases, hackers install code on a legitimate website that redirects computer users to an alternative and malicious site. Unlike the SPAM email method, this approach requires no additional actions from the victim.

Today's Leading Ransomware Strains

As an MSP, it's important to know the latest ransomware developments and whether specific verticals are being targeted. The more informed you are, the better you can protect your clients' data. There are a variety of forms of ransomware proliferating today. This is not meant to be an exhaustive list, but it will give you an idea of what's out there potentially affecting your clients.

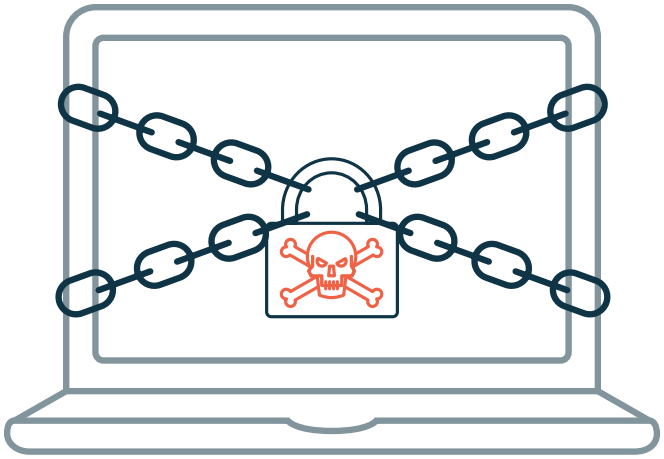
CryptoLocker: Ransomware has been around in some form for over a decade, but came to prominence in 2013, with the rise of the original CryptoLocker malware. While the original was shut down in 2014, the approach has been widely copied. So much so, in fact, that the word CryptoLocker has become nearly synonymous with ransomware.

Cerber: Cerber targets cloud-based Office 365 users and is assumed to have impacted millions of users using an elaborate phishing campaign. This type of malware emphasizes the growing need for SaaS backup in addition to on-premises.

CryptoWall: CryptoWall first appeared in early 2014, and variants have appeared with a variety of names, including: Cryptorbit, CryptoDefense, CryptoWall 2.0 and CryptoWall 3.0, among others.

Crysis: This new form of ransomware can encrypt files on fixed, removable, and network drives and it uses strong encryption algorithms and a scheme that makes it difficult to crack within a reasonable amount of time.

KeRanger is not widely distributed at this point, but it is worth noting because it is known as the first fully functioning ransomware designed to lock Mac OS X applications.



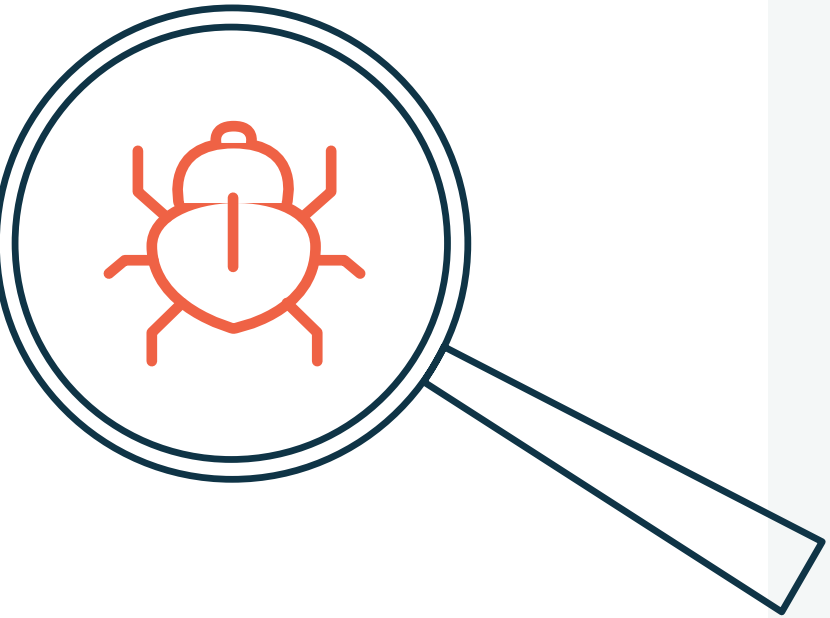
CTB-Locker: The criminals behind this strain take a different approach to virus distribution, outsourcing the infection process to partners in exchange for a cut of the profits. This strategy allows the malware to achieve large volumes of infections and generate huge profits for the hackers.

Jigsaw: Jigsaw encrypts then progressively deletes files until ransom is paid. The ransomware deletes a single file after the first hour, then deletes more and more per hour until the 72 hour mark, when all remaining files are deleted.

KeRanger: KeRanger is not widely distributed at this point, but it is worth noting because it is known as the first fully functioning ransomware designed to lock Mac OS X applications.

LeChiffre: "Le Chiffre", which comes from the French noun "chiffrement" meaning "encryption", is the main villain from James Bond's Casino Royale novel who kidnaps Bond's love interest to lure him into a trap and steal his money. GREAT name. Unlike other variants, LeChiffre needs to be run manually on the compromised system. Cyber criminals automatically scan networks in search of poorly secured remote desktops, logging into them remotely and manually running an instance of the virus.

Locky: Locky is typically spread via an email message disguised as an invoice. When opened, the invoice is scrambled, and the victim is instructed to enable macros to read the document. When macros are enabled, Locky begins encrypting a large array of file types using AES encryption. The spam campaigns spreading Locky are operating on a massive scale. One company reported blocking 5 million emails associated with Locky campaigns over the course of two days



> **Probably every one of our clients has had some kind of experience with ransomware. But, many don't understand exactly how to protect against it.**

TeslaCrypt: TeslaCrypt also uses an AES algorithm to encrypt files.Typically distributed via the Angler exploit kit, this ransomware targets Adobe vulnerabilities. TeslaCrypt installs itself in the Microsoft temp folder. When the time comes for victims to pay up, victims are given options for payment: Bitcoin, PaySafeCard and Ukash. And who doesn't love options?

TorrentLocker: TorrentLocker isn't new to the malware scene but the 2016 version is more destructive than ever. Like the mononucleousis of ransomware, TorrentLocker, in addition to encrypting files, collects email addresses from the victim's address book to spread malware beyond the initially infected computer/network.

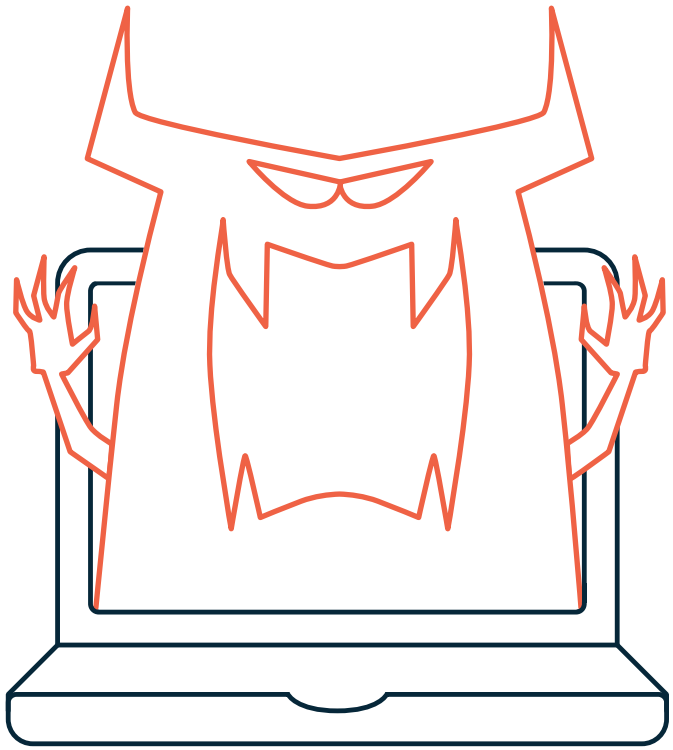
ZCryptor: ZCryptor is a self-propagating malware strain that exhibits worm-like behavior, encrypting files and also infecting external drives and flash drives so it can be distributed to other computers.

EDUCATING YOUR CUSTOMERS ABOUT RANSOMWARE

"Probably every one of our clients has had some kind of experience with ransomware," said David Tidwell, Help Desk Supervisor at Rigidnet, a Texas-based MSP and partner. "But, many don't understand exactly how to protect against it." Ransomware is a well known problem, but a lot of companies aren't thinking proactively about it yet—especially smaller businesses. That's a large market opportunity for MSPs.

For example, many think about ransomware strictly as a security issue. But, that's not entirely accurate. As ransomware is constantly evolving, it's important to make it clear to clients that they need a secondary layer of protection to recover, if malware slips through the security cracks - which it often does.

> I usually start the conversation with something like 'I don't want to scare or alarm you, but this is something you need to think about. Just politely preface the subject. It's not a hard sell — once you educate, they get it.

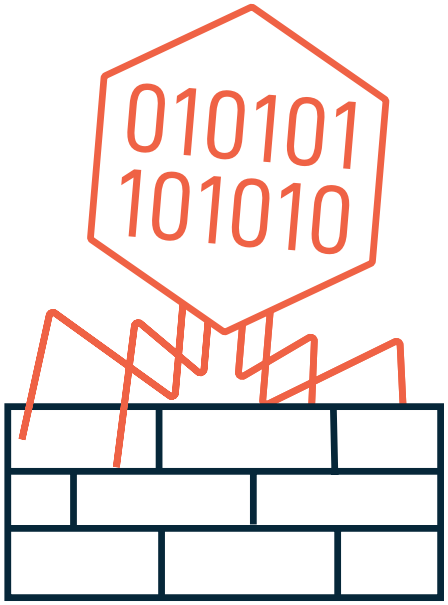


Ransomware has made backup and security inseparable—each play an important role in protecting against ransomware. As a trusted IT advisor, you can help clients understand that a proper business protection strategy requires a three-pronged approach, comprising education, security and backup.

Education: Make sure that your customers know about the rise in ransomware incidents and have tools and a strategy in place to educate their entire organization. For example, all current and new employees should have to go through some sort of basic cyber security training. During this training, SMBs should provide specific visual examples of what a phishing email looks like, which is one of the leading causes of a ransomware infection. All employees should know how to spot a malicious email and know exactly what to do if they do encounter a potential ransomware lure (i.e. don't open attachments, if you see something, say something, etc.). This is an essential part of protecting your clients against attacks and it should become a fundamental practice in any business today.

According to Slattery, who has had his share of ransomware infections in the past 2 years, "Given the speed of how rapid fire business works, it's really hard to get people to slow down and think about what they are clicking on. Especially when ransomware social engineering is as good as it is." Slattery provides customers with the ransomware statistics that matter most to them and then segways into the technology needs. "I usually start the conversation with something like 'I don't want to scare or alarm you, but this is something you need to think about,'" he said. "Just politely preface the subject. It's not a hard sell—once you educate, they get it."

Security: When it comes to defending systems against ransomware, antivirus software is essential for any business. Firewall and web filtering are also a



Finally, make sure customers understand the need for an additional layer of business protection in the not-so-rare case that ransomware does make it through the front lines of defense. Explain to your clients that even with these proactive security measures, breaches still occur. That's where a backup and recovery solution comes in.

must. Most security vendors recommend this type of multi-layered approach to protect against ransomware. Many of your clients probably already understand this, as well. What they probably don't realize is that these security measures are not foolproof.

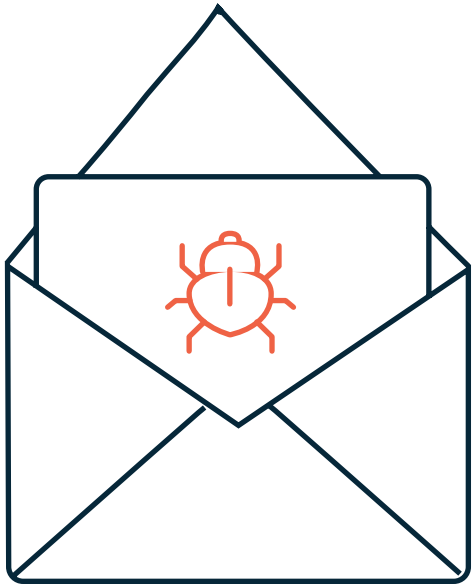
MSPs should also talk to clients about the importance of keeping all software patched and up-to-date in order to protect the business against newly identified threats. Finally, make sure customers understand the need for an additional layer of business protection in the not-so-rare case that ransomware does make it through the front lines of defense. Explain to your clients that even with these proactive security measures, breaches still occur. That's where a backup and recovery solution comes in.

Backup: Modern total data protection solutions, like Datto, take snapshot-based, incremental backups as frequently as every five minutes to create a series of recovery points and allow businesses to run applications from backup copies of virtual machines. While your clients likely won't care or understand that sort of technical deep dive the way that you would, what they do care about is the benefits (and peace of mind!) a solution like Datto can deliver.

Focus on the benefits of Datto rather than the features and innovation of the technology. When it comes to the threat of ransomware, the benefits of a data protection solution such as Datto are three-fold:

1. Your business will never need to pay hackers ransom to get critical data back.
2. Your business will avoid data loss - from ransomware or other - since backups are taken frequently and can be restored quickly.

> **When it comes to disaster recovery these days, the biggest worry is someone on staff opening an infected document, not a hurricane. Historically, a lot of business owners didn't think about this stuff, but that's changing. People are starting to recognize the threat.**



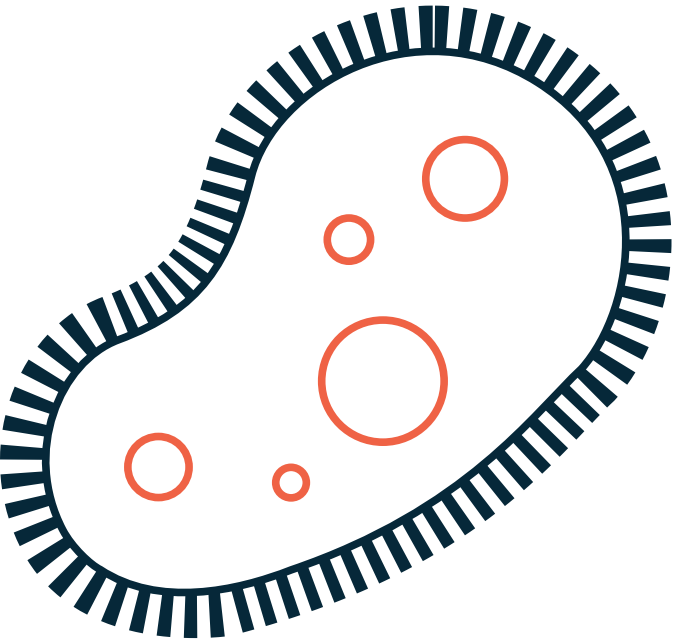
3. Your business won't experience significant downtime (since users can access critical data and applications while primary systems are being restored).

"When it comes to disaster recovery these days, the biggest worry is someone on staff opening an infected document, not a hurricane," said Slattery. "It's become a cornerstone of the discussion about BCDR. Historically, a lot of business owners didn't think about this stuff, but that's changing. Ransomware is a big part of that change. People are starting to recognize the threat."

This is largely because there have been a number of high profile examples of ransomware in the news, including a recent attack on a California hospital in which cyber extortionists reeled in a ransom of $17,000. This is obviously an extremely high ransom, but it illustrates the need for protection, so it might be a good place to start when it comes to discussions about cyber extortion.

Both Tidwell and Slattery sell Datto alongside additional, less expensive backup options. They both said that they recommend Datto because it allows clients to get back online faster than the other backup tools they offer. "It's a very easy conversation when you put it in the right context," said Slattery. "Make sure they understand that downtime equals lost revenue, and if they are concerned about the price, compare revenue lost to the cost of the solution."

Slattery went on to say that it's important not to push clients to go with a more expensive solution without a clear explanation. "It's like: 'look, I can have you up in minutes rather than all the time it will take with a cheaper solution which means more revenue lost,'" he said. "It's not about pressuring them, but you have to make them aware of the realities of each solution, so they can make the best decision for their needs."



97% of malware today can morph to become unique to each endpoint device—rendering traditional, signature-based security virtually useless.

Ransomware by the Numbers

If clients fail to understand how real the threat of ransomware is, you may want to share some statistics with them. Here are five quick facts to pass on to reluctant clients:

1. In just the first three months of 2016, attacks increased tenfold over all of 2015, costing victims more than $200 million, according to the FBI. And, since so many ransomware attacks go unreported, this only represents a fraction of actual attacks.

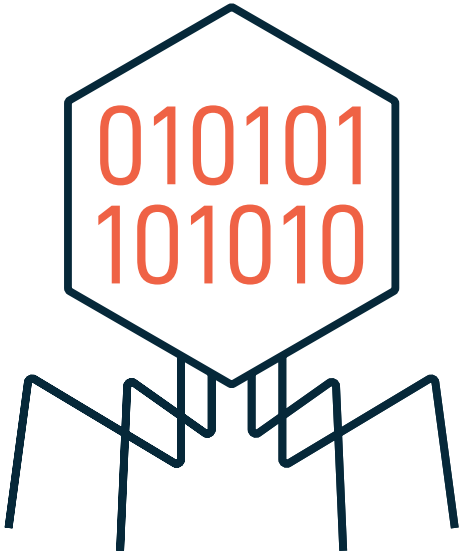
2. In 2014-2015, around 27,000 corporate users were attacked. Compare that with 2015-2016, when that number rose to 158,000. According to security vendor Kaspersky Labs, this is because corporations can afford to pay higher ransom and can not tolerate a complete loss of their systems.

3. According to Webroot, 97% of malware today can morph to become unique to each endpoint device—rendering traditional, signature-based security virtually useless, and highlighting the need for backup.

4. Webroot also reported that 100,000 net new malicious IP addresses were created per day in 2015, up from 85,000 a day in 2014. indicating cybercriminals are expanding to new IPs to avoid detection.

5. According to threat management vendor PhishMe, the first three months of 2016 has seen a 6.3 million increase in phishing emails, due primarily to a ransomware upsurge—a 789% increase over the previous quarter.

> **Ransomware attacks are happening with increased regularity—it's certainly not trending downwards. It's a big problem, but it's also a big opportunity to educate clients and give them the tools they need to protect their data.**



CONCLUSION

Ransomware protection fits right in with the proactive approach to monitoring and managing client environments that MSPs deliver. Backup and security tools that integrate easily with remote management and automation software, of course, make this a much easier task.

For this reason, both Slattery and Tidwell said while they can support a variety of backup and security solutions, they try to standardize as much as possible. For example, Slattery said TeamLogic recommends Trend Micro security software because of its integration with the AutoTask PSA software he uses.

"Ransomware attacks are happening with increased regularity—it's certainly not trending downwards," said Frank Slattery of MSP Teamlogic IT, Datto Partner. "It's a big problem, but it's also a big opportunity to educate clients and give them the tools they need to protect their data."

You Also Might Be Interested In:

Webroot White Paper
Stopping Crypto Ransomware Infections in SMBs

DOWNLOAD NOW

eBook
The Guide to CryptoLocker Prevention and Removal

DOWNLOAD NOW

Webinar
15 Ways to Fight Crypto Ransomware

WATCH NOW