Ransomware attacks: detection, prevention and cure

Ross Brewer, LogRhythm

Over the past three years, ransomware has become one of the biggest cyber scams to hit businesses. Indeed, the FBI estimates that losses incurred in 2016 due to ransomware will top $1bn. Ransomware is malicious software that allows a hacker to restrict access to an individual’s or company’s vital information in some way and then demand some form of payment to lift the restriction. The most common form of restriction today is encryption of important data on the computer or network, which essentially lets the attacker hold user data or a system hostage.

Payment in Bitcoins is the typical demand, as the digital currency is both global and anonymous. Ransomware attacks are rapidly growing in popularity with cyber-criminals and for good reason – it’s estimated that this type of attack earns criminals millions of pounds a month.

Old tricks

The notion of ransomware has actually been around for quite some time. In 1989, Dr Joseph Popp distributed a trojan called PC Cyborg in which malware would hide all folders and encrypt files on the PC’s C: drive. A script delivered a ransom message demanding that $189 be directed to the PC Cyborg Corporation. The afflicted PC wouldn’t function until the ransom was paid and the malware’s actions were reversed. Since then, numerous enhancements to this type of scheme have been made, especially in the area of stronger file encryption. Now, it’s virtually impossible for victims to decrypt their own files.

"Researchers saw more than four million samples of ransomware in the second quarter of 2015, including 1.2 million that were new. That compares to fewer than 1.5 million total samples in the third quarter of 2013”

Another type of ransomware scheme, dubbed ‘scareware’, displayed a warning on a user’s computer that the device was infected with malware that could be removed immediately by purchasing what turned out to be fake antivirus software. The scareware message appeared repeatedly, prompting many victims to purchase the ‘anti-virus software’ just to get rid of the warning message.

The term ‘ransomware’ broadly describes a wide range of malicious software programs, including CryptoLocker, Locky, CryptoWall, KeyRanger, SamSam, TeslaCrypt, TorrentLocker and others. Various strains of these major applications appear and continue to evolve in order to avoid detection. In fact, researchers saw more than four million samples of ransomware in the second quarter of 2015, including 1.2 million that were new. That compares to fewer than 1.5 million total samples in the third quarter of 2013, when fewer than 400,000 were new.

The vast majority of attacks today are against Windows-based systems. This is largely due to a numbers game – there are more Windows-based computers than any other type of OS. Attackers often use exploit kits to get the ransomware software on victims’ machines.

Lucrative business

Until recently, most ransomware attacks were simply opportunistic and mostly affected the computers of individual users or small businesses. The ransom demands have commonly been the equivalent of just a few hundred pounds for an individual PC.

This has been and continues to be, a lucrative business for criminals who consider end users to be low-hanging fruit. But now they have set their sights on larger organisations that have bigger budgets to pay bigger ransom demands. They also have more important files and
While individuals and small businesses often fell victim to mass distribution ransomware, which saw them become the targets of opportunity via a phishing email, drive-by-download or a compromised website, criminals are shifting their tactics to more targeted ransomware attacks. They are now increasingly scoping out specific organisations that have deep pockets and are more likely to pay a hefty ransom request in order to minimise downtime.

The perpetrators understand the mathematics. Targeted organisations are likely to see much higher ransom demands that are based on what the business might be willing to pay. On the surface, mass distribution and targeted attacks appear to be similar, but there are underlying technical differences:

- Mass distribution attacks are typically automated, very fast in their execution – often just 15 minutes from initial infection to a ransom demand being made – and well orchestrated from the attacker’s perspective.
- Targeted attacks are very similar to an advanced persistent threat (APT); they are usually driven by a person as opposed to an automated system and may take much more time to execute.

The tools used for each kind of attack differ as well. Mass distribution attacks often utilise more customised or single-use tools. Targeted attacks deploy more off-the-shelf tools for the reconnaissance phase, while the encryption process is usually customised.

The five phases of ransomware

There are distinct phases of a ransomware attack, regardless of whether it’s a mass distribution or a targeted attack. Understanding what happens in each phase and knowing the indicators of compromise (IOCs) to look for, increases the likelihood of being able to successfully defend against – or at least mitigate the effects of – an attack.

**Phase 1: Exploitation and infection.**

In order for an attack to be successful, the malicious ransomware file needs to execute on a computer. This is often done through a phishing email or an exploit kit – a type of malicious toolkit used to exploit security holes in software applications for the purpose of spreading malware. These kits target users running insecure or outdated software applications on their computers. In the case of the CryptoLocker malware, the Angler exploit kit is a preferred method to gain execution. The vulnerabilities favoured by the Angler exploit kit are typically found in Adobe Flash and Internet Explorer.

**Phase 2: Delivery and execution.**

Following the exploit process, the actual ransomware executable will be delivered to the victim’s system. Upon execution, persistence mechanisms will be put in place.
place. Typically, this process takes a few seconds, depending on network latencies. Unfortunately, the executables are most often delivered via an encrypted channel – instead of SSL, a custom encryption layer is added on top of a regular HTTP connection. Because the malware is using strong encryption, it’s difficult to recover the executable from the wire. Most often, we see the executable files being placed in either the %APPDATA% or %TEMP% folder beneath the user’s profile. It’s good to know this for detection purposes because your organisation can monitor for those events to set up a line of defence. Most of the crypto malware will add persistence mechanisms such that if the afflicted machine is rebooted in the middle of the encryption process, the ransomware can pick up where it left off and continue to encrypt the system until it is completed.

“Most of the crypto malware will add persistence mechanisms such that if the afflicted machine is rebooted in the middle of the encryption process, the ransomware can pick up where it left off”

Phase 3: Back-up spoliation. A few seconds after the malware is executed, the ransomware targets the back-up files and folders on the system and removes them to prevent restoring from back-up. This is unique to ransomware. Other types of crimeware and even APTs don’t bother to delete back-up files. Most of the ransomware variants will go out of their way to try and remove any means that the victim has to recover from the attack without paying the ransom. On Windows systems, in both targeted and mass distribution attacks, we often see the vssadmin tool being used to remove the volume shadow copies from the system. For instance, CryptoLocker and Locky will execute a command to delete all of the volume shadow copies from the system. Several of the variants, especially in the targeted attacks, will even go so far as to look for folders containing back-ups and then forcefully remove those files.

Even if a program is holding a lock to those files, it will kill the process so it can delete those folders of the back-ups to make recovery all the more difficult.

Phase 4: File encryption. Once the back-ups are completely removed, the malware will perform a secure key exchange with the command and control (C2) server, establishing those encryption keys that will be used on the local system. Quite often the malware will tag the local system using a unique identifier that will be presented to the user in the instructions at the end. This is also how the C2 server differentiates between the encryption keys used for different victims. Unfortunately, most of the variants today use strong encryption such as AES 256, so the victim isn’t going to be able to break the encryption on their own.

Not every type of ransomware needs to contact a C2 server to exchange keys. In the case of the SamSam malware, the software application does all encryption locally without reaching out to the Internet at all. This is worth noting, because the communication with a C2 server is an IOC that should be monitored, but the absence of this event does not mean that ransomware is not present.

“Depending on network latencies, the number and sizes of documents and the number of devices connected, the encryption process can take anywhere from a few minutes to a couple of hours”

During the file encryption phase, different ransomware variants handle file naming and encryption differently. For instance, CryptoWall version 3 does not encrypt the filename, whereas CryptoWall version 4 randomises the filename and extension. Locky will randomise the filenames but add a locky extension to the end. Knowing this, your organisation can sometimes fingerprint the exact ransomware variant based on the file-naming convention that it uses. Depending on network latencies, the number and sizes of documents and the number of devices connected, the encryption process can take anywhere from a few minutes to a couple of hours. There have been instances where, on a widely distributed network, the ransomware tries to encrypt files across a wide area network. For a single endpoint device, however, the encryption process is usually done in minutes.

Phase 5: User notification and clean-up. With the back-up files removed and the encryption dirty work done, the demand instructions for extortion and payment are presented. Quite often, the victim is given a few days to pay and after that time the ransom increases. How the instructions are presented can help you identify which ransomware software has attacked the system. The demand instructions are usually saved onto the hard drive, sometimes in the same folders as the encrypted files. Other times, they are saved to very specific locations on the hard disk. For example, CryptoWall version 3 uses the HELP_DECRYPT file to store the instructions. CryptoWall V4 changed it to HELP-YOUR-FILES. There are a couple of different instructions and variations on the theme but you can usually use this guidance to do an Internet search and find the exact variant.

Finally, the malware cleans itself off the victimised system so as not to leave behind significant forensic evidence that would help build better defences against the malware.

Handling a ransomware attack

Step 1: Preparation. Because malware often enters systems through known vulnerabilities, the best step to bolster defences is to aggressively patch systems. By eliminating vulnerabilities, the malware may not have a way to get on any of your computers in the first place.

It’s also important to create and protect back-ups. Ransomware destroys back-up files and encrypts regular files and this puts organisations at risk. Therefore, it’s imperative to frequently back up all documents to a location that can’t be affected by the ransomware (eg, to offline storage) and then verify that these files can be restored easily if needed. Even network shares or
cloud storage may not be entirely safe, as files that have already been encrypted or corrupted by the ransomware could be automatically backed up to the network or the cloud, also corrupting the files in those storage locations.

Organisations should also develop an incident response (IR) plan that is explicitly for a ransomware attack. This step is particularly important to prepare for targeted attacks that can affect broad swathes of an organisation. The IR plan should detail the specific actions people should take as soon as it becomes apparent that an attack is underway. This will help to ensure a prompt response in a scenario where time is of the essence to stop or contain a serious situation.

Finally, user awareness training is an effective means to teach people to avoid falling victim to phishing email messages that plant malware in the first place. Many attackers rely on social engineering tactics that are growing more and more sophisticated. End users need to know what to expect and what to look for in their messages to avoid infection.

“Any tools that detect malicious attachments or perform attachment scanning to look for executable attachments are the best automated defence against ransomware emails”

Step 2: Detection. In the event of an attack, organisations can minimise damage if they can detect the malware early. For initial exploitation and infection, a good defence is to get signatures and IOCs into an IDS or other network device. Use threat intelligence sources to block or at least alert to the presence of anomalies associated with ransomware in your network traffic. There are numerous signatures for most of the major IDS vendors out there for CryptoWall and Locky traffic. These are usually malware version-dependent and they can change. Therefore, it’s important to have more defences than just the detection. However, these signatures can be a good source for the most widely distributed tools that enterprises tend to use.

For the phishing emails that contain or lead users to the ransomware malware, any tools that detect malicious attachments or perform attachment scanning to look for executable attachments are the best automated defence against ransomware emails.

It’s also worth knowing that two common areas from which the ransomware typically executes are the %APPDATA% folder and the %TEMP% folder on your system. Looking for any file executing from these locations is a good way to spot ransomware before it has actually had a chance to encrypt files. Similar to the exploitation phase, network rules can also be used to detect the executable delivery and execution, especially for cases such as CryptoLocker.

Back-up spoliation is another key area where CryptoLocker can be detected before it has actually had a chance to execute. Specifically, look for that vsadmin command execution. It’s very common for this approach to be used and if the admin tool executed can be highlighted, action can be taken and other laptops or the network shares could avoid being encrypted.

The file encryption phase also usually begins with a key exchange that can be detected via network signatures, file naming and registry modifications on the local system. Looking for files with a .locky extension is a good method to try to detect Locky being encrypted on a system. Similarly with CryptoWall, looking for the random filename patterns is another way to detect the ransomware as it is actually running. Unfortunately, it is a little late in the progression of the malware, but if the user notification files being placed on the system can be detected, it’s easier to see the presence of the encryption even if you aren’t able to block it. Quick detection at this stage may help contain the situation.

Step 3: Containment. Once the ransomware has already taken hold of one device, there are steps to contain it locally so that network files aren’t affected. Having an endpoint protection system that is able to look for the execution and kill the process is usually the best means of containment. If ransomware is detected, network connectivity can be disabled so that if it is able to get to the endpoint, it’s not able to actually encrypt files on the network.

Step 4: Eradication. Once the ransomware incident has been identified and has been contained, the next step is eradicating it from the network. It’s usually recommended that machines be replaced rather than cleaned. As with any type of malware, it’s difficult to know if residual files are hidden on the system and able to re-infect devices. However, for network locations such as mailboxes or file shares, sometimes it is more relevant to clean those locations, remove the malicious email message from the mailbox, or remove the ransomware instructions from the file share. If organisations choose to clean rather than replace, it’s important that they continue to monitor for signatures and other IOCs to prevent the attack from re-emerging.

Step 5: Recovery. For recovery, the number one task is going to be restoring from back-up. If there are good verified back-ups, any ransomware event can really be made into a non-issue by simply replacing or cleaning systems and recovering from back-ups. There may be a small amount of downtime, but it shouldn’t be a big multi-day issue.

In most ransomware cases, a full investigation into what specific infection vector was used against the system is an important step. Was it a phishing email, or was it a web-based attack kit? If it was a web-based attack kit, how did that user get to that web page? Knowing how the ransomware came onto your system can help organisations better prime their defence systems and direct their detection mechanisms in the future.

Conclusion

Ransomware attacks against organisations are just starting to ramp up. Because these attacks are so lucrative for the perpetrators, they are certain to become more common, more damaging and more expensive. What’s more, almost every organisation – large or small – is vulnerable to a ransomware attack. The ramifications of a successful attack are far more extensive than just the cost of the ransom. Organisations can suffer the effects of lost productivity, loss of business, inconvenience to customers and
potentially the permanent loss of data. An organisation’s success in defending against a ransomware attack is largely dependent on the level of preparation and the ability to detect, shut down and contain suspicious activity.

About the author

Ross Brewer is vice-president and managing director for EMEA at LogRhythm. He joined LogRhythm in 2001 and has more than two decades’ experience within sales and management and more than 10 years spent in the information security sector, where he has had a successful track record of building and managing international operations. Prior to joining LogRhythm, Brewer was vice-president and managing director for EMEA at LogLogic.

Resource


References


Risk-based security: staff can play the defining role in securing assets

Marc Sollars, Teneo

Last year, US firm Ubiquiti’s finance team made an urgent multi-million pound money transfer for a senior executive, only to find later that the request had been made by criminals posing as him. In the UK, the exposure of customer financial details held by telecomms provider TalkTalk, seemingly caused by young hackers, has led to an exit of disgruntled customers.

Different attacks and victims, certainly, but they show how information security is headline news because every organisation is now a target. With company bosses and the public alike realising that the person being duped into releasing malware or wrongly transferring money is just as likely to be a company CEO as your neighbour, the security industry has acquired an unprecedented profile because its direst warnings are all coming true.

New demands

At the same time, the security industry is inevitably being asked to come up with practical measures to help a myriad organisations to secure their data. It’s also being asked by companies how they can cut through all the noise and rethink the task of educating their workforce about more effective security procedures. So how can we bring best security practice by employees to the heart of everything we do in our workplace, whether it’s the corporate HQ or the remotest of branch offices?

This ‘re-education’ requirement has emerged with a vengeance because organisations, rapidly being brought to a standstill by hackers’ exploits, can no longer make excuses or brush this type of matter under the carpet. Even targets such as hospitals that once might have been regarded as being no-go areas for cyber-attacks are now being held to ransom. Board-level executives are having to explain their information security policies and their staff’s mistakes to customers and business partners as never before.

“Organisations are having to draw up plans to designate approved workforce tools, block malware and inspire staff to follow new rules – all at the same time. How is this multi-faceted balancing act to be achieved?”

However, since today’s business models are increasingly dependent on federated partners, service providers and supply chains, the old concepts of protecting the perimeter or arbitrarily locking down IT infrastructures have gone out of the window. We’ve reached a point where organisations are having to draw up plans to designate approved workforce tools, block malware and inspire staff to follow new rules – all at