Five steps to beating ransomware's five-minute warning

Matt Lock

Matt Lock, technical director at Varonis

When ransomware strikes an IT network there is precious little time to react. Indeed, some accounts by IT professionals put it at less than five minutes. At that speed it is next to impossible to stop ransomware propagating throughout an IT system using manual methods.

With a business falling victim to ransomware every 40 seconds, firms need to work on the assumption that they will be attacked at some point.[1] Therefore, businesses need to put in place measures that will help them survive a ransomware attack with as little damage as possible. Preparation and automation are vital.

The old adage of failing to prepare means preparing to fail has never been truer in the case of ransomware. Just look at the costs businesses incur trying to get systems back up and running following an attack – estimated to be $7.5 billion in 2019.[2] More often than not, it comes down to whether you have the right technology and processes in place.

Fortunately, there are five straightforward steps that businesses can take to ready themselves for a ransomware attack.

Multi-layered defence

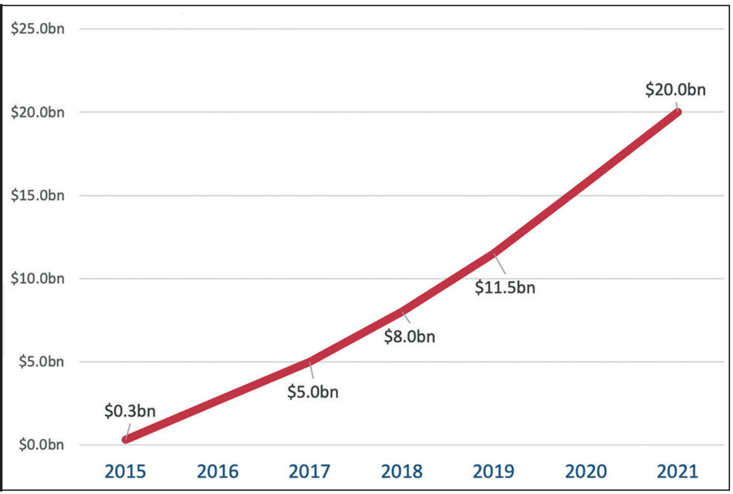
Threat actors are using more-sophisticated techniques to avoid common detection methods. Many have moved on from the WannaCry-style scattergun approach to ransomware where a malicious program is unleashed and left to spread indiscriminately. Instead, they now know exactly which organisations they want to attack. The approach (or kill chain) is similar save for one important detail – the cyber criminals are now stealing the data before they encrypt it.

As an example, in the first phase, threat actors drop simple, undetectable code onto an IT system to carry out reconnaissance to identify what security products are in place to protect the perimeter. This information is fed back automatically to the threat actor's command and control centre, which responds with more code to neutralise the victim's security measures. The next phase looks for and exfiltrates sensitive data. Finally, the ransomware payload is inserted into the system to encrypt everything.

Anti-virus software may be expected to stop the first phase dead in its tracks before the attack can escalate. However, such defences can only prevent known attacks, relying on user blacklists to prevent malware from getting onto a system. Threat actors are wise to this. They constantly revise and refine their malware to escape recognition.

A deep, multi-layered defence will protect perimeter defences and detect abnormal behaviour consistent with malware within the network. To be effective, such monitoring needs some element of machine learning for analysing and nullifying changes in behaviour much faster than manual methods. Banks and credit card companies use a similar approach to prevent customers' accounts being abused. As soon as the system spots any suspicious activity on the account it is suspended and the account holder is asked to verify if he or she carried out the transaction.

Once the ransomware has been detected, the first action is to prevent it spreading by communicating with anything else in the network. For instance, if the ransomware is currently limited to one machine, an 802.11x command can be initiated to take the infected computer off the network. Following isolation, a security clean up team can go into the infected area and remove the malware.



Predicted costs of ransomware attacks. Source: Cybersecurity Ventures.

Watch for lateral movement

Suspicious lateral movement is a clear sign that an unauthorised person has access to a network. This is where a threat actor is moving through a system looking for attack vectors and valuable assets with information worth stealing or corrupting. To spot this type of activity an organisation needs to know how all the accounts on its network usually behave, so that anything unusual raises a red flag.

This means that all accounts on the network need to be identified and their usual activity logged. Such information can include what machine the account is usually accessed from, usual active hours, and what is typically accessed. Armed with this data, security teams can then respond to anything out of the ordinary – for example, by temporarily suspending an account – following up with the account owner to check that this was indeed them, as well as potentially asking what they were up to.

Least privilege policy

The temporary suspension of user accounts can be effective at stopping ransomware spreading throughout a network, but only if the organisation enforces a policy of least privilege. This is a framework where user accounts can only access what is necessary to carry out their roles. Time and again, we see attacks that could have been prevented or their impact lessened were it not for the fact that accounts had access to many more assets than they should have had. This is highlighted by the fact that in one instance, 22% of all the data at an organisation was accessible to all employees, while each member of staff had access to around 17 million files.[3]

One area that is often overlooked for least privilege is IT accounts. IT administrators should have two separate accounts, one for administering the IT network and another for day-to-day work functions such as answering emails. In this way, if the administrator opens a malicious email using his day-to-day account, the potential for any malware to spread across the networks via service accounts will be limited. This would avoid the very real possibility of a malicious email on an IT admin's account infecting hundreds of machines.

Discover and isolate exposed data

For some time, many businesses have been monitoring the emails that employees send and receive as well as the websites they visit through corporate accounts. This is perfectly understandable. Careless online actions and communications by employees – for example, clicking on a phishing link – could be the trigger for a multi-phased attack, including ransomware. Having oversight of employee emails means that anything that could endanger the IT network is quickly nipped in the bud.

However, few are applying the same sort of vigilance over their sensitive data. Logs should be kept of who is accessing which data, what they are doing with it and when they did so. Not only does this ensure that employees aren't looking at, moving, copying or modifying files they shouldn't be, but it also provides an invaluable audit trail in the event of an attack. Using this information, the IT security team can understand what data ransomware has been compromised or encrypted and take steps to ensure its recovery once the attack is over.

This process can be made much easier with the elimination of stale data. This is information that is no longer used or out of date, such as files about people who are no longer connected to the business as customers or employees. It's incredible how many businesses hold on to data long after it is needed. They only create a security risk for themselves. In the average company as much as half of the data is stale, presenting major issues around monitoring and exposure.

Most companies have at least 100,000 files with stale data in them, a number that is likely to be growing daily. Keeping on top of this is not something that can be accomplished manually. Instead businesses are deploying automated tools to help identify and then archive or delete stale information, while also complying with retention policies.

Improve visibility and insight

While the drive for cloud migration has multiple advantages, it means that businesses now have another connectivity point to monitor. This makes them an attractive target for threat actors. Attackers are drawn to the cloud because it is always available. There's also a chance that the business hasn't secured cloud data properly.

Further, the cloud can enable threat actors to spread ransomware more easily across a network. For example, if Microsoft Office 365 is compromised, for a threat actor it would be a short step for them to share a malicious link with multiple workers within the business. Recipients are more likely to open it because it appears to come from a trustworthy source.

Many businesses have separate security solutions for on-premises and cloud infrastructures. Consequently, they are unable to have a complete view of the network from one place. This makes it difficult to monitor exactly what is going on across these environments.

A single view of what is happening in all data stores enables a security team to quickly and easily spot anything that could indicate an attack is taking place, wherever on the system that might be. Businesses also need to look at using machine learning to detect when large-scale encryption is happening on the network and automatically shut down and isolate the affected system. This is crucial for stopping ransomware in its tracks.

Preparation and automation

Ultimately, businesses must accept they will be on the receiving end of a ransomware attack at some point. This five-step process can help them prepare. Measures include having greater control over data, removing any data that is no longer needed, managing who has access and monitoring what users are doing with the data.

The ability to monitor the entire network infrastructure – on premises and in the cloud – is vital for reducing the risk from ransomware. This measure, integrated with automation, enables IT security to respond rapidly to any suspicious activity that might indicate an attack.

Ransomware has been weaponised. To beat it, companies must react fast. Comprehensive preparation, together with automated security tools, can make all the difference to ensuring survival.

About the author

Matt Lock is director of sales engineers at Varonis (www.varonis.com). With 20 years' cyber security experience, he is an expert on data security and a regular speaker and media commentator on the General Data Protection Regulation (GDPR). An accomplished CISSP security consultant, he's worked with world-leading organisations across insurance, pharmaceuticals, legal, health, entertainment, retail and utilities. Lock heads up the team at Varonis that undertakes risk assessments and data governance projects, helping organisations to secure and manage their unstructured data.

References

1. Morgan, Steve. 'Global ransomware damage costs predicted to reach $20 billion (USD) by 2021'. Cybercrime Magazine, 21 Oct 2019 Accessed Oct 2020. https://cyber securityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/.
2. Crane, Casey. '20 Ransomware Statistics You're Powerless to Resist Reading'. HashedOut, 27 Feb 2020. Accessed Oct 2020. www.thesslstore.com/blog/ransomware-statistics/#:~:text=Ransomware%20Attacks%20Forecast%20to%20Occur,by%20the%20end%20of%20 2019.
3. '53% of companies found over 1,000 sensitive files open to every employee'. Varonis. Accessed Oct 2020. www.varonis.com/2019-data-risk-report/.

Is this the end for 'encro' phones?

Catherine O'Rourke, JMW

Catherine O'Rourke

Encrypted phones, or 'encro' phones, are the communication method of choice for organised crime groups (OCGs) across the UK and Europe, because of their apparent entirely secure features. Encro phones were originally designed for military use, but more recently, they have been associated with celebrities wishing to secure their privacy, and for criminal activity.

In contrast to pay-as-you-go phones and smartphones, which can be accessed and analysed by authorities, the encro has, up until 2020, been a completely secure and anonymous way of organised criminal groups contacting each other without fear of detection or trace. This no longer seems to be the case.

No offence

Possession or use of the encro telephone itself is not an offence or evidence of criminality. It should, however, be noted that the use of encros within a criminal group will be often considered by a criminal court as an aggravating feature of a defendant's criminal conduct, by virtue of the activity being seen as sophisticated, planned and designed to avoid detection.

It is, however, a criminal offence under section 53 of the Regulation of Investigatory Powers Act 2002 (RIPA) for a suspect to fail to disclose a password or code allowing access to electronic data when served with a 'section 49' notice requiring them to do so. The service of a section 49 notice under RIPA is a tool used in criminal investigations where the police consider that disclosure is necessary in preventing or detecting crime. Due to the security provided by encryption software installed on the phones, British law enforcement agencies have historically relied upon being able to break into the devices with a view to exploiting vulnerabilities in the phone or software, by being provided the access code by the user, usually by serving a notice under section 49.

While failure to comply with a section 49 notice can result in prosecution and a two-year prison sentence, it is common for suspects, who know that they are under investigation for a serious criminal offence, to 'take their chances' when the likely prison sentence that they are facing would exceed the two-year sentence for not complying with the notice requirements. The suspect accordingly may elect not to assist the police in securing evidence.