computing research

RESEARCH PAPER

Ransomware – how to avoid becoming the next victim

February 2017

Sponsored by

CONTENTS

This document is property of Incisive Media. Reproduction and distribution of this publication in any form without prior written permission is forbidden.

Executive summary

The likelihood of being hit by ransomware escalated sharply in 2016. Ransomware is a high profit, low risk venture for attackers, and attacks are both more prevalent and more sophisticated than before, often blending phishing and social engineering methods to devastating effect.

Computing surveyed 125 business decision makers representing businesses ranging in size from fewer than 250 employees to those with many thousands and from multiple industry sectors about their experiences of and attitudes to ransomware.

This paper discusses the extent to which our respondents have been affected by ransomware – whether they had been attacked and if so, the extent and implications of the attack in terms of lost data. The paper also looks at the types of defence that organisations are mounting against ransomware and how likely they are to be successful. It concludes with a discussion on the importance of both end point and off-network back-up as a means of neutralising ransomware attacks.

Introduction

Ransomware attacks are among those most feared by those responsible for data security in business, public and third sector organisations. Research conducted by *Computing* in late 2016 indicated a perception that the threat posed by ransomware has increased sharply over the previous 12 months.

Organisations of all sizes are at risk. Whilst larger organisations are more likely to have a dedicated security strategy in place and probably a CISO or equivalent figure responsible for ensuring the execution of this strategy, the string of successful attacks on household names in the last eighteen months illustrates that large organisations are far from infallible.

Attack volumes on organisations with fewer than 500 employees has also risen sharply. There are a number of reasons why SMEs represent such an enticing target for criminals. First, 99 per cent of companies are SMEs, and criminals can target many of them at the same time instead of spending time and money crafting a targeted attack on a larger, blue chip organisation in which data security and compliance with data security regulations is more likely to be a board level concern.

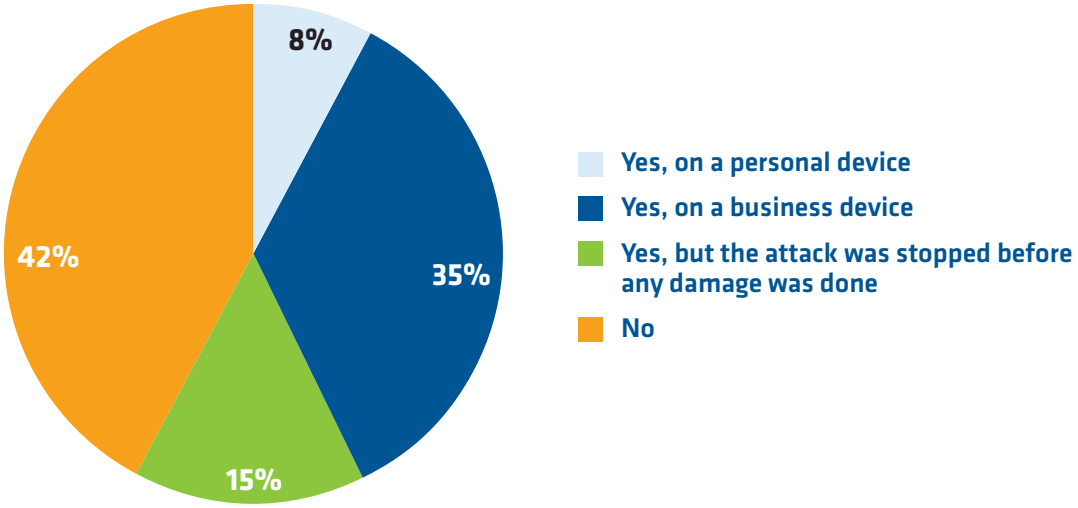
Another reason for the enormous increase in the use of ransomware is that it takes minimal technical skill to deploy and the risks to the perpetrators of attacks are very small. Ransomware boasts an ROI that would make the likes of Uber look twice. It's a commodity that can be purchased online like any other, and a whole industry has sprung up to extract monetary advantage from it. There are helpdesks that will talk you through paying ransoms with bitcoins, and dashboards to track infection rates. Ransomware-as-a-service is now available.

Whilst the actual volumes of all types of malware attacks are increasing, what rightly worries data security professionals is the sophistication of these attacks. Ransomware isn't delivered via an email containing numerous spelling mistakes or an invitation to download an attachment containing details of the cash prize you've won, in a draw you had no idea you'd entered. Most individuals got wise to this a long time ago – and attackers know it. Ransomware attacks often use human weaknesses and desires, such as the desire to do right by one's colleagues and superiors, to extract money from the victims. Whilst we continue to hear about the raids on high profile businesses, a sea of criminal activity is occurring under the media radar.

Real world attacks

Computing asked survey respondents if they, or anybody that they knew, had suffered a ransomware attack. The results are shown in Fig. 1. The greatest proportion of respondents (42 per cent) told us that they had never suffered an attack on either a personal or professional level and didn't know anyone who had. However, 35 per cent stated that they had done, and it was a business device that was compromised. A further eight per cent had been affected on a personal device or knew somebody that had been. In addition to this, 15 per cent had been attacked by ransomware but had managed to prevent the attack from actually doing any damage.

Fig. 1 : Have you or anyone you know been hit by ransomware?



That means that 58 per cent had been affected or knew of someone who had, either on a personal or professional level. This finding is reasonably consistent with findings from research conducted in third quarter of 2016 and published in the *Computing Enterprise Security Review 2016*, which stated that 46 per cent of those who took part had suffered a ransomware/crypto/malware attack in the previous 12 months.

Research conducted by other analysts reaches similar conclusions. In a survey from June 2016, 39 per cent across multiple nations had been affected by ransomware in the previous 12 months. The most affected country was the United Kingdom where 54 per cent of organisations claimed that they had been attacked by ransomware.[1]

We wanted to add more detail to the picture of these attacks so we asked those who had been subjected to a ransomware attack whether other machines were affected, in addition to the device on which the ransomware was activated.

[1] https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065

In 25 per cent of cases, multiple machines were compromised. We also asked "How many machines were infected by the ransomware attack?" The findings here give some indication of the scale of attacks, and provide insight into where some of those oft quoted "costs of attack" numbers come from. The average number of connected PCs affected was 17 but that average hides some fairly high numbers. In one case, 100 separate PCs were hit, and several others reported a tally of 20, 30 and 50 machine compromises.

However, the most interesting finding here is the scale of server and back up compromise. Almost everybody answering this question stated that at least one server had been compromised and in two cases, ten servers were compromised. In two cases, back up storage devices were affected and in one instance, a central storage system was hit.

This is a nerve wracking development for businesses. New strains of ransomware which can compromise servers mean that multiple datasets can be held to ransom. Databases holding confidential data can be compromised as can business critical application servers. CRM or ERP systems on which business rely for their day-to-day operations can be locked. It's a terrifying scenario which ups the stakes for organisations considerably. Attackers are raising their game. The value of personal data on the black market has been falling.[2] Whilst attackers have moved to exploit more valuable data such as healthcare data, this development in ransomware allows attackers to exploit data that probably is worth next to nothing to anyone else – it just has to be worth something to its owner.

The cost of attack

The efficacy of holding data to ransom is determined by the likelihood of the victim paying up. Just how likely are businesses to pay the ransom if they are caught out? According to our survey, the answer is "not very." 94 per cent of those participating in this survey stated that they did not pay up. The remainder were split between paying (two per cent), those who would rather not divulge that information (two per cent) and a further two per cent who were unsure.

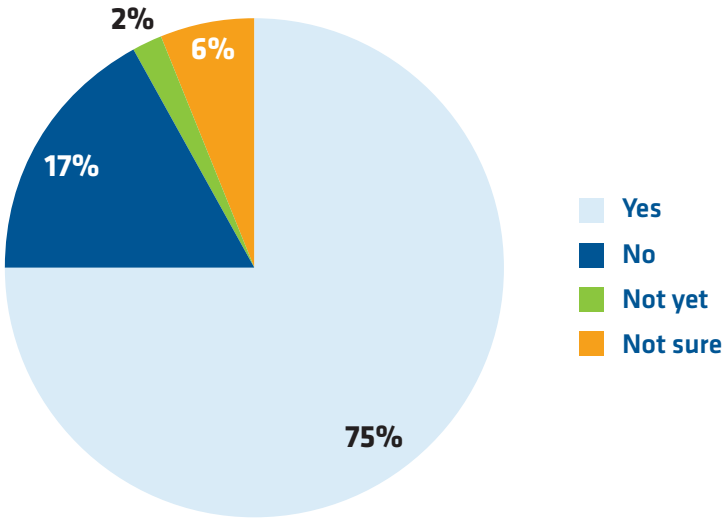
This finding is slightly at odds with those from our research conducted last year when we asked survey respondents to rank on a scale of one to seven how likely they were to pay up in the event of a ransomware attack. Fifty per cent of respondents rated themselves at one – highly unlikely to pay a ransom. However, 25 per cent placed their willingness between four and seven and so could prove likely to pay out if attacked.

There are many good reasons not to pay ransoms. For a start, there are no guarantees that you'll get your data back anyway. Secondly, and perhaps more importantly, every person who does pay is directly contributing to the earnings of the criminal underworld. That said, some very high profile organisations have paid out, and for many it is a difficult decision ultimately fuelled by the value of what they stand to lose.

One way to reduce the cost of ransomware attacks is to ensure that data is recoverable in the event of being locked. If data is backed up and recoverable, a ransomware attack may not be a disaster for the victim – and criminals will be deprived of a win. Seventy-five per cent of our survey respondents who had been subjected to an attack stated that they had managed to recover all of the encrypted data. However, 17 per cent stated that they could not recover their data, and two per cent were still trying. A further six per cent were unsure.

[2] http://www.bbc.co.uk/news/business-38694016

Fig. 2 : After the ransomware attack, was all data recovered?



*Answered by those with experience, direct or indirect, of a ransomware attack.

It is here that the costs of attack begin to come into sharp focus. The FBI estimated that the ransomware industry was worth approximately one billion dollars in 2016.[3] It is difficult to relate to such astronomical numbers but when you observe findings such as the one above it begins to sound more feasible – particularly when you combine it with findings on just how long it takes to remove ransomware and restore systems. Figure 3 shows how long it took our respondents to do just that. 34 per cent of respondents took hours to restore affected systems. 30 per cent lost one whole day, and a further 23 per cent lost a number of days. An unfortunate three per cent admitted that it took them weeks to recover their data, and a further three per cent never did.

Fig. 3 : How long did it take to remove the ransomware and restore affected systems?

Minutes	2%
Hours	34%
A day	30%
Days	23%
Weeks	3%
N/A systems were not recovered	3%
Don't know	5%

*Answered by those with experience, direct or indirect, of a ransomware attack.

[3] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html?section=money_technology

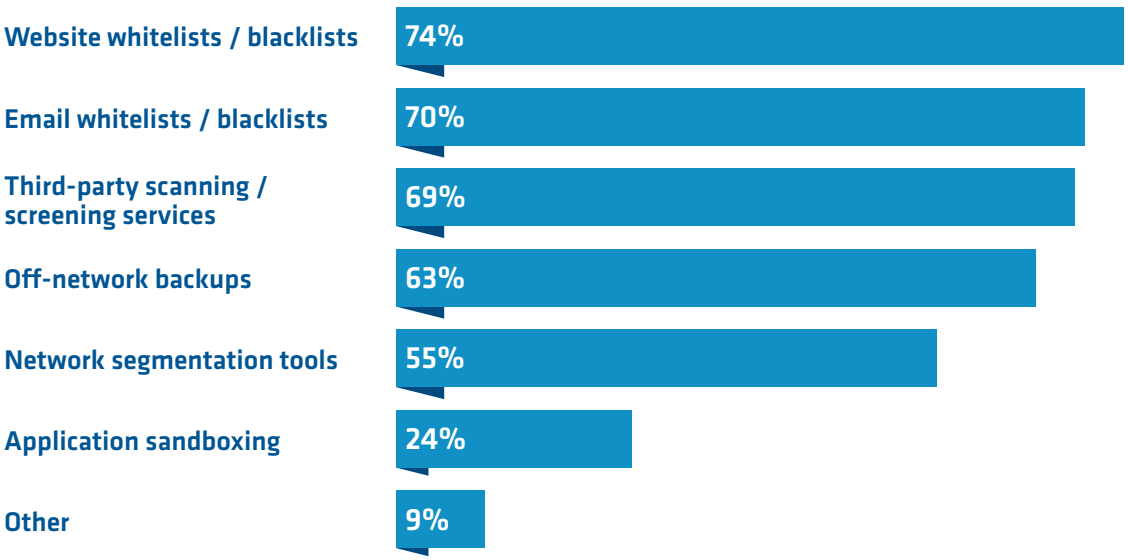
The costs of ransomware attacks are almost impossible to measure because each organisation will be affected differently. Having to reimage a laptop and restore backed up data is a minor irritation but relatively inexpensive if no data is lost and back-ups have not been compromised. However, in other scenarios the cost of down time and remediation in terms of lost productivity can be significant – even if news of the attack stays within the organisation. If the news leaks out, the damage to brand and reputation becomes incalculable.

Analysts estimate that in the first quarter of 2016, $209 million was paid out by victims of ransomware.[4] This figure consists of reported attacks only – many victims choose not to report attacks due to fear of reputational damage. Furthermore, this figure doesn't take into account the costs of mopping up after an attack. This is probably why, when asked about the possibility of their organisation being hit (or hit again) by ransomware, 87 per cent of respondents stated that they were at least somewhat concerned, while 34 per cent were very concerned indeed.

Defensive measures

Having explored the costs and implications of ransomware attacks, *Computing* wanted to establish what measures organisations are using to prevent themselves falling victim to ransomware attacks. The tools used by respondents are set out in Fig. 4. The greatest proportions of respondents use website whitelists/blacklists (74 per cent) and email whitelists/blacklists (70 per cent). These are sensible measures. Spam and phishing emails that trick the user into clicking to activate malicious code are still the most frequently used method of ransomware distribution and, as we have seen, attackers are becoming ever more skilled at tricking victims into clicking their way into trouble.

Fig. 4 : Apart from AV software and firewalls, which of the following tools do you use to defend against malware?



*Respondents could select multiple options.

[4] http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/

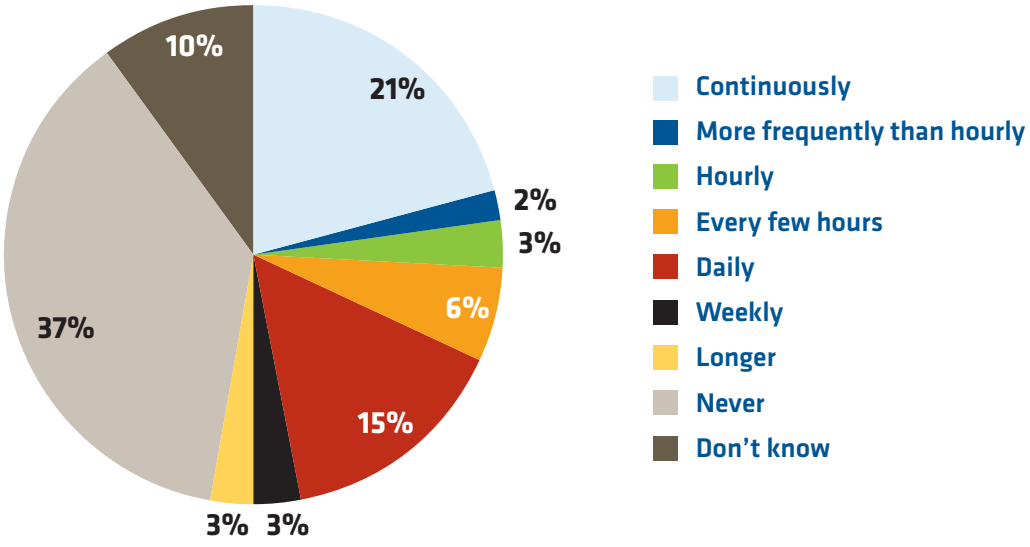
Email may be the most common source of ransomware but it is by no means the only one. Malvertising is becoming more and more common and requires little or no action by the user. Ad blockers help to some degree but perfectly legitimate websites are being hacked all the time with malicious code silently infecting visitors. URL filters can reduce the risk but relying on categorisation engines can be dangerous when legitimate sites are compromised. This is why 69 per cent of respondents also use third-party scanning and screening services.

Sixty-three per cent of respondents run regular off network back-ups. The importance of off network back-ups in the fight against ransomware is difficult to overstate. The perpetrators of ransomware are well aware that if their victims can simply restore their data, they don't get paid. We discussed earlier how ransomware can now attack servers and use them to move through networks to encrypt or lock whatever data the attackers consider of value to the victim. Network attached back-ups are the obvious first port of call for the savvy hacker.

So how frequently are our respondents backing up their data? Figure 5 shows the huge variation in responses to this question. The largest single proportion of respondents (37 per cent) said that they never backed up end user data. This is really quite a worrying finding. Not bothering with end point backups may have been a logical approach when data was stored centrally in a secure data centre. The process of data decentralisation which has occurred with the rise of mobile technology means that business critical data is likely to reside in end points that security teams may not even have visibility of. It may be that these respondents have policies in place which prohibit the saving of business critical data to personal devices. Unfortunately this cuts against all of the factors that have driven the rise of mobile computing and it is likely that users will simply circumvent policy.

Twenty-one per cent of respondents ran a continuous back up from end user machines with a further five per cent running them somewhere between hourly and more frequently. Fifteen per cent back up their end points on a daily basis. Six per cent do so at weekly intervals or longer. A policy of backing up end point data continuously and without intervention from the user is the minimum required to mount a reasonable defence against the growing number of ransomware attacks.

Fig. 5 : How frequently do you back-up data from end user machines?



We have also seen that many ransomware attacks seek out backed up data in order to compromise that as well. The only answer to this is a type of offsite back up – at least in part. *Computing* asked, **"Are your back-up devices directly attached to the network?"** 34 per cent stated that all of their back-up was network attached, and a further 32 per cent stated that most of it was. 17 per cent told us that most of their back-up was not directly attached to their network and six per cent said none of it was. The 34 per cent for whom all back-up was directly attached to their network are clearly vulnerable to ransomware attacks which seek out backed up data.

Conclusion

The subject of ransomware is one of the few areas where the perception and fears of attack are justified by the reality. Businesses are wise to be cautious. Ransomware-as-a-Service really got going in 2016. Those not technically savvy enough to write malicious code themselves can simply borrow and distribute it in return for a share of their profits for the criminals at the top of the chain, or hire someone else to do the dirty work. Whilst the perpetrators of ransomware may not be terribly sophisticated, the attacks often are. Ransomware is a bullet that it is becoming progressively harder to dodge.

A third of respondents to our survey told us that they were familiar with someone who had fallen victim to an attack, and a further eight per cent had suffered a compromise of a personally owned device. The average number of endpoints compromised was 17, but in almost all cases at least one server was also compromised and in several other cases storage devices were also attacked. The implications of these newer variants of ransomware which can lock down multiple datasets are alarming. It isn't just data that can be held to ransom – cyber criminals can lock business critical application servers and prevent businesses from functioning at all until they pay up.

The vast majority of those we surveyed did not pay a ransom for their data. Only two per cent confirmed that they had paid – although this rate of return is clearly enough for the attackers if the escalation in ransomware volumes is anything to go by. It also took a few days on average for our respondents to recover their data – although three per cent never did.

Given the likelihood of a ransomware attack and the potential implications, organisations are deploying a number of defensive measures. In addition to the basic firewalls and AV protection, organisations are also using website and email black and whitelisting tools. This is old technology.

While email is a common means of ransomware distribution, increasing quantities are being injected into legitimate websites which are unlikely to be categorised as malicious by URL filters. Sixty per cent of our respondents backed these measures up with third party scanning services but the best way to neutralise ransomware is to ensure that data is recoverable in the event of being encrypted. Seventy five per cent of those in our survey who had been attacked did manage to recover their data – eventually.

Off network back-ups are an important weapon against ransomware because network attached back-ups can so easily be attacked by hackers and the relevant data encrypted as on the main device. However, a little over one third of our respondents stated that all of their back-up was network attached, and a further 32 per cent stated that most of it was. This finding rings alarm bells. Any organisation with purely network attacked back-ups is leaving itself defenceless if a ransomware attack manages to get past its security measures. Even more worrying is the finding that 37 per cent of our respondents never back-up endpoint data. This is indicative of a degree of complacency over the likelihood of business critical data residing on endpoints in an age of data decentralisation.

One of the best defences against ransomware is the education of users. Fifty-five per cent of respondents had run training for their staff in order to educate them about ransomware and how to reduce the risk to themselves and their employers. It is certainly a worthwhile exercise and will certainly reduce the chances of less sophisticated attacks hitting the target.

However, a skilled and well researched attack is harder to avoid. In addition to education and as well as more traditional security measures such as AV and URL filtering, backing up business critical applications and data are critical to any defence strategy. End point data should be backed up frequently and without intervention from the user. This, along with regular off network back-ups should form a key plank of the fight against ransomware.

About the sponsor, Redstor

Founded in the UK in 1998, Redstor simplify data management for organisations around the world, enabling them to efficiently manage, move, protect, recover and analyse their data, regardless of where it is stored.

ISO27001 and ISO9001 certified, with a global data centre footprint, Redstor has almost twenty years' experience in delivering highly secure offsite backup, storage, instant recovery, policy driven archiving and cloud-based disaster recovery.

Redstor's cloud data management platform enables organisations across all industries to improve the cost effectiveness of data storage and protection, whilst increasing organisational flexibility and simplifying the task of complying with increasingly demanding data protection legislation.

Redstor's 40,000 customers span all verticals and range in size from primary schools to global enterprises. Redstor's services are resold by a global network of over 1,000 partners.

For more information:

Visit: www.redstor.com

Follow: @Redstor on Twitter