Topics in Privacy & Security

Ransomware

Y1481702

March 14, 2018

Contents

1 Technical Report

1.1 Introduction

The past few years have seen a significant increase in frequency of ransomware attacks[1, 2], with WannaCry[3, 4] and NotPetya[5] being two particularly damaging examples. These attacks becoming more prevalent is likely driven by the rise of cryptocurrencies, such as Bitcoin, which are more difficult to trace than traditional bank transfers. Furthermore, as more essential appliances, such as thermostats and smoke detectors, become dependent on complex software and, with the internet of things providing new possibilities for remote attack, it is likely this trend will continue.

At a high-level the attack works as a form of protection racket, with profit as the key motivation[6]. The attack aims to violate the security goal of availability. Users are denied access to vital systems and services and offered the option to pay to get around this inconvenience. Countdown timers are often displayed here to induce a sense of panic in users making them act rashly and pay the ransom (Fig. 1b). As with other criminal ransom acts, there is absolutely no guarantee that paying the ransom will return the files successfully[7]. Indeed doing so also incentivises the hacker to produce more attacks in the future. It has been argued that previous cases where the ransom has been paid by hospitals have been directly responsible for subsequent healthcare attacks[8]. A recent report has even shown that as little as 19% of ransomware victims who pay the ransom may actually get their files back[9, 10]. In particular the high profile 'ransomware' variant NotPetya is actually wiper malware[11], meaning there is no possible way to recover encrypted files, even if the ransom is paid, as the key is not saved after encryption. It is often very difficult to tell the difference between, ransomware and this type of wiper malware. As such, this kind of attack also violates the goal of integrity as data and software is irreversibly modified. It should also be noted that while ransomware does not specifically threaten the goal of privacy and confidentiality, it could be used to disguise some form of dual layer attack which does.

There are a number of ways in which ransomware may attempt to deny access to a system. The most effective of these is to encrypt files on the computer harddrive, this type of ransomware is known as cryptoransomware. Encryption uses one-way functions which are computationally hard to reverse, so attempting to restore the data without knowing the key used to encrypt it is **not** an option. All files including software, documents and other data may be affected potentially causing a complete loss of the computer. This technique is what made the WannaCry and NotPetya so efficacious. Another type of ransomware, known as locker ransomware, may leave files untouched in favour of denying the user access to their desktop and programs. In this case it may be possible to recover critical files from the machine, but a clean restore from a backup may still be preferable.

Some of the recent trends in ransomware are making their attacks more dangerous than ever. The latest strains of ransomware have begun to include the ability to self-multiply meaning they fall under the category of a computer virus. This makes them especially problematic for businesses as they can easily spread across internal networks infecting multiple machines and encrypting a vast number of files. Hackers have also been attempting to attack new platforms with the first widespread Mac ransomware being distributed during 2016, as well as a number of threats to the Android OS emerging capable of attacking mobile devices as well as smart TVs running Android.

As mentioned above, the latest ransomware are self-multiplying and will therefore not discriminate between businesses and important services such as healthcare. While ransomware has demonstrated

to businesses any of their electronic data may be important[12] and many have opted to pay the ransom for its recovery, it is hoped that the value of medical data has never been in question. In the healthcare industry, it is particularly important to defend against any violations of availability. For obvious reasons, timely access to medical data may be the difference between life and death for some patients. It is likely be dangerous to run surgeries without full access to patient's medical data or even to blood transfusion or organ donation databases.

1.2 Prevent

Once ransomware has access to files on the system, it may be difficult if not impossible to recover the files. Therefore the most effective solution to ransomware is to prevent it taking hold altogether. While it is impossible to ensure that every user of the network is behaving responsibly at all times, sensible steps can still be taken to ensure that the actions of any individual have minimal impact. Several of the most high profile ransomware attacks, including WannaCry, could have been easily prevented by following basic cyber security techniques[13].

Firstly, keeping operating systems and other software up-to-date ensure that the latest security updates are installed. It's particularly import to ensure that any operating systems are still being supported with new security fixes. While extended support for Windows XP was dropped back in April 2014, it is estimated that 3.3% of Windows PCs are still running this OS, which translates to approximately 140 million machines[14]. The WannaCry vulnerability was patched in Windows 7, 8.1 and 10 security updates[15, 16, 17] two months before the ransomware took hold so this action would have prevented much of the attack's impact. While it is necessary to test major updates to ensure important software is not affected and data can be migrated, support expiry dates are announced years in advance[18], so there should be plenty of time to prepare for this. The cost of upgrade should **never** overule the requirement to ensure system security, especially when patient's data is involved.

Ransomware can enter a system in the same way as any other form of malware. Social engineering is the most successful, and thus most common, form of attack vector for home users and organisations alike. Phishing emails are the most likely source with approximately one in 131 emails containing malware, often disguised as routine notifications such as invoices or receipts. From here, multiple techniques are used to infect the user's computer, JavaScript or Microsoft Office macros might be used to download the file, or the malicious attachment might install it directly.[2] Educating users to this threat of the paramount importance, users should be aware of the danger that spam emails such as these can cause. Using a reputable email gateway and strong spam filters on company emails should also be able to help to significantly reduce this threat. It might also be prudent to prevent users from accessing personal emails on their work computers as it cannot be assumed that suitable spam filters are in place for these.

Once the ransomware has access to a single computer on the internal network, it may be able to cause significant damage to files stored on any shared drives. Ensuring tight access control on these drives should help to minimize the impact that ransomware can have. Minimizing users' access to only the assets which they absolutely require, and limiting this to read only where possible, will prevent ransomware acting as that user from corrupting these files. Regular reviews should take place to ensure that access should be revoked if it is no longer needed. An alternative to this could be to provide managed cloud services which often retain previous versions of files, allowing them to be reverted to their unencrypted form after the attack. Unfortunately, there may be legal issues

here as many cloud services store their data internationally meaning data protection laws may be breached.

1.3 Detect

Once a ransomware attack has taken hold, its important to detect and stop it before serious widespread damage can be done. This is particularly difficult as the ransomware often does not reveal itself until encryption of the computer and all data is complete.

Anti-virus software may be able to detect and stop ransomware. Classic antivirus software only searches for and removes *known* viruses from machines. Unfortunately this will not be particularly effective against new and unknown malware. As well as being able to find and remove known ransomware, some modern antivirus software, such as Sophos Intercept X[19] and Kaspersky Internet Security[20], perform behavious analysis on programs in order to assess malicious intent. In particularly, antivirus software should be able to detect the classic signs of cryptoransomware- the mass editing or renaming of all files on the system. Ensuring that the chosen antivirus software incorporates this feature will help protect against new types of malware attacks as well as detecting any attacks that are being specifically targeted at this organisation. As with operating systems and other software, it is of the utmost importance that anti-virus software is kept updated in otder to deal with rapidly changing threats.

1.4 Recover

Once ransomware has taken hold, the system can only be recovered if backups have been made. Backups should be regular and stored offline, away from any network. While regular backups must be kept, prevention and early detection is preferable to backup recovery as restoring a whole system may take a considerable amount of time.

If a wide-scale takeover occurs, its important to immediately disconnect **all** computers that may have been affected from the network. Beware, it may be difficult to determine which computers have been infected or not. Infected computers should be switched off to prevent further damage. Once the network is clean of infected devices, network traffic should be monitored to detect further outbreaks and a full antivirus scan should be run. After this, the harddrives of infected machines should be formatted or replaced **offline**, with their operating system reinstalled. This computer should be connected to the **clean** network in order to update the operating system and all software. These should ensure that a further outbreak of the malware does not occur.[7]

1.5 Summary

Overall, the key takeaways from this report should be that

- many ransomware attacks are preventable
- educating users to the threat is of paramount importance for successful prevention
- ransoms should never be paid as they incentise further attacks

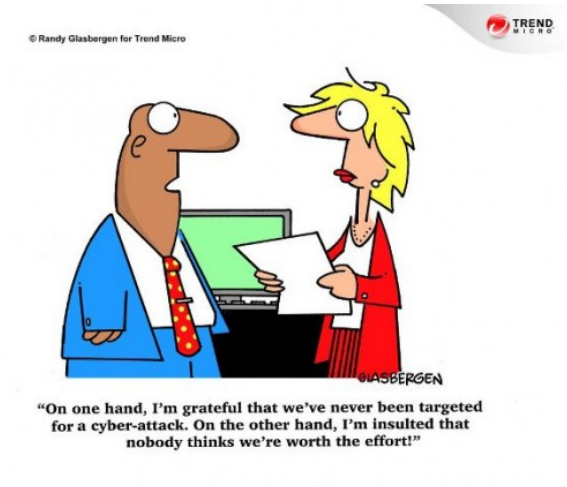
N.B. As much of this report regards recent events, information has been taken from reputable news sources and trusted security organisations where possible. Where the reputation of a source may not be sufficient, multiple sources have been provided in order to provide further assurance of the correctness of statements.

2 Email

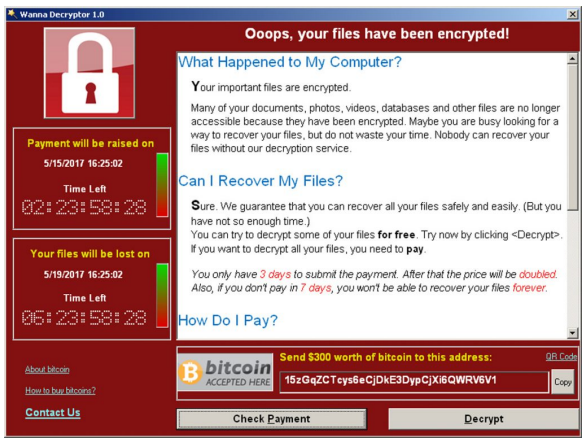
2.1 Memo

SUBJECT: RANSOMWARE: APPEAL FOR HELP

In 2017, 48 NHS trusts were brought to a standstill by ransomware. The attack took down the trust's computer systems meaning patient data became complete inaccessible resulting in cancelled appointments and even surgeries[4]. As well as crippling the NHS, the attack also took down schools, large manufacturers and even banks with an estimated 200,000 computers across 150 countries being affected according to Europol[3]. Clearly we need to do everything we can to defend against such attacks and **we need your help**.



(a) Cyber Security Cartoon[21]



(b) WannaCry Ransomware

Ransomware attacks that we have seen so far do not distinguish between targets. Their aim is to restrict any user from accessing their data or devices and force them to pay a fee to regain entry.

As with other computer viruses that you may be aware of, ransomware often comes disguised as other files or programs. You will remember from your cyber-security training that viruses may come as email attachments or as downloads from unscrupulous websites. These may often be concealed as routine notifications such as invoices or receipts. If you are not expecting to receive such as email, or it looks suspicious, please forward the email to IT Support with the subject line *Suspected Malware* and then delete it. Once it has entered our network, most sophisticated variants of ransomware are able to self-multiply onto other computers. As such it's of the utmost importance that it is not allowed to gain access.

Again, we implore you **not** to:

- download or open attachments from unknown senders
- run or install software that has not been vetted by system administrators
  - if you require additional software to be installed, please contact IT Support

- plug *unknown* devices, including USB drives, into your computer

Computers regularly receive updates which contain protections against known types of malware, including ransomware. While these can be inconvenient, we ask that you do not interfere with automatic software updates scheduled by system administrators and allow them to complete at a suitable time.

If you do become victim to a ransomware attack, you will receive a popup like the image attached (Fig. 1b), you need to act **quickly** to stop the problem spreading to other users:

- **Don't panic!**
- **Don't** attempt to pay any ransom demands.
- Switch off and unplug your PC immediately.
- Contact IT support at once.

If you have any follow-up questions regarding ransomware or cyber-security in general, please do not hesistate to reply to this email. We're more than happy to explain anything further and we'd love to hear your suggestions on how to further engage the community.

2.2 Justification

As mentioned in the Technical Report, it is of paramount importance that users are aware of the threats that ransomware poses to healthcare organisations, such as this. As well as ensuring employees are aware of the issue, the email needs to communicate the most important steps that users can take to prevent such attacks occuring. Care has been taken to aim the email at its target audience: healthcare professionals are often well educated, but may have minimal knowledge or interest in the area of digital security. The email attempts to inform, but not overwhelm the reader with the most important information.

The first few lines of the email have been designed to grab the attention of the reader by informing them of the importance of the topic and significant impact ransomware has had on similar organisations around the world. At the end of this paragraph, we appeal to the reader directly, making clear to them that it is their responsibility to help protect from these attacks, which should encourage them to read on. In other situations, plural pronouns have been used to make clear that this is a problem for the whole organisation. This should help the reader feel more comfortable discussing the topic with others if they have questions.

As users may not be particularly interested in the subject of the email, it has been kept as short as possible, while still including the necessary facts. If the email becomes too long or uses too many technical cybersecurity jargon, it is unlikely that employees will read it. My industry experience has shown me that readers often skimread or skip over emails that are either too long, or are too difficult to read. Employees may receive hundreds of emails a day, so it is important that they understand that this one is particularly important. Having said this, healthcare personnel are often well educated, so I have been careful not to oversimplify the significant issues contained in the email. Eye-catching graphics such as screenshots of previous ransomware and a topical cyber security cartoon has been used to help break up the text and further catch the users' interest.

While ransomware is a particularly new threat, the email assumes that the reader is familiar with other types of malware from previous communications and cyber security training. This type of training is commonplace in most organisations, I have had to under take this myself during several industrial placements. As such, the email may need to be revised if readers have not undertaken such training.

The most important prevention techniques that users need to be aware of relate to phishing emails. The significant problem of phishing emails is described in Section 1.2 of the attached Technical Report. The only particularly notable part of this section of the email is asking users to forward suspicious emails. If users make the IT administrators aware of any emails, it will ensure they are aware of cases when infected emails may not be blocked by spam filters. This should hopefully allow the administrators to improve or fix the spam filters to catch future emails.

Users also need to be aware of the steps that should be taken if ransomware does strike. The most important part of this it to ensure users do not panic and pay the ransom. The user should then know to ensure that their PC is taken offline to prevent the ransomware from encrypting any further files and from self-multiplying. Once this has been done, the attack should not be able to cause further damage in the time it might take IT administrators to respond. These steps are clear to make sure that they stand out amongst the rest of the email- the reader should still be able to pick these points out even if the email is skimread. These bullet points appear towards the end of the email so reader sees them as the key takeaway points of the message.

Finally, the user has also been encouraged to ask any questions that might occur to them as a result of the email. This will hopefully result in some feedback that can help us to judge if the email has been understood by the audience. This will be particularly useful as while every effort has been taken to ensure that this memo is suitable for the target audience, it would be a good idea to test it on a member of this audience before sending it out. Unfortunately, as this writing is part of a university Open Assessment, I have been unable to do this in this instance.

3 References

[1] United States Government, "How to protect your networks from ransomware." [Online]. Available: https://www.justice.gov/criminal-ccips/file/872771/download [Accessed: 13. Mar. 2018]

[2] Symantec, "Internet security threat report," Apr. 2017. [Online]. Available: https://www.symantec.com/security-center/threat-report [Accessed: 25 Feb. 2018]

[3] Reuters Staff, "Cyber attack hits 200,000 in at least 150 countries: Europol," *Reuters*, May 2017. [Online]. Available: https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX [Accessed: 5 Mar. 2018]

[4] BBC, "Cyber-attack: Europol says it was unprecendented in scale," *BBC News*, May 2017. [Online]. Available: http://www.bbc.co.uk/news/world-europe-39907965 [Accessed: 5 Mar. 2018]

[5] A. Griffin, "'petya' cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack," *The Independent*, Jun. 2017. [Online]. Available: http://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html [Accessed: 28 Feb. 2018]

[6] McAfee Labs, "McAfee Labs 2018 Threats Predictions Report," Nov. 2017.

[7] National Cyber Security Centre, "Mitigating malware," Feb. 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/mitigating-malware [Accessed: 7 Mar. 2018]

[8] J. Pope, "Ransomware: Minimizing the risks," *Innovations in Clinical Neuroscience*, Nov. - Dec. 2016.

[9] CyberEdge Group, "2018 cyberthreat defense report," Mar. 2018. [Online]. Available: https://cyber-edge.com/cdr/ [Accessed: 12 Mar. 2018]

[10] L. Mathews, "Why you should never pay a ransomware ransom," *Forbes*, Mar. 2018. [Online]. Available: https://www.forbes.com/sites/leemathews/2018/03/09/why-you-should-never-pay-a-ransomware-ransom [Accessed: 9 Mar. 2018]

[11] A. Ivanov and O. Mamedov, "ExPetr/Petya/NotPetya is a Wiper, Not Ransomware," *Securelist - Kaspersky Lab's cyberthreat research and reports*, Jun. 2017. [Online]. Available: https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ [Accessed: 13 Mar. 2018]

[12] Department for Culture, Media & Sport, "Cyber Security Breaches Survey 2017," Apr. 2017.

[13] S. Shah, "'basic it security' could have prevented uk nhs wannacry attack," *Engadget UK*, Oct. 2017. [Online]. Available: https://www.engadget.com/2017/10/27/basic-it-security-could-have-prevented-uk-nhs-wannacry-attack/ [Accessed: 8 Mar. 2018]

[14] StatCounter Global, "Desktop windows version market share worldwide," Jan. 2018. [Online]. Available: http://gs.statcounter.com/windows-version-market-share/desktop/worldwide/#monthly-201801-201801-bar [Accessed: 28 Feb. 2018]

[15] W. Leonhard, "How to make sure you won't get hit by wannacry/wannacrypt," *AskWoody*, May 2017. [Online]. Available: https://www.askwoody.com/2017/how-to-make-sure-you-wont-get-hit-by-wannacrywannacrypt/ [Accessed: 7 Mar. 2018]

[16] M. Killen, "Confirm the wannacry patch is installed," *Foxguard Solutions*, May 2017. [Online]. Available: https://foxguardsolutions.com/2017/05/17/confirm-wannacry-patch-installed/ [Accessed: 11 Mar. 2018]

[17] Microsoft Corporation, "March 14, 2017kb4013429 (os build 14393.953)," Mar. 2017. [Online]. Available: https://support.microsoft.com/en-gb/help/4013429/windows-10-update-kb4013429 [Accessed: 11 Mar. 2018]

[18] ——, "Windows lifecycle fact sheet," Feb. 2018. [Online]. Available: https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet [Accessed: 7 Mar. 2018]

[19] Sophos, "Intercept x." [Online]. Available: https://www.sophos.com/en-us/products/intercept-x.aspx [Accessed: 13 Mar. 2018]

[20] K. Lab, "Kaspersky internet security." [Online]. Available: https://www.kaspersky.co.uk/internet-security [Accessed: 13 Mar. 2018]

[21] R. Glasbergen, "Cyber-attack - too small to assail? cartoon," *Trend Micro*, Mar. 2012. [Online]. Available: https://blog.trendmicro.com/cyber-attack-to-small-to-assail-cartoon/ [Accessed: 25 Feb. 2018]