Topics in Privacy & Security

Ransomware

Y1481702

March 12, 2018

Contents

1 Technical Report

1.1 Introduction

2017 saw a significant rise in frequency of ransomware attacks[CITE], with WannaCry[1, 2] and NotPetya[3] 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[4]. 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. As with other criminal ransom acts, there is absolutely no guarantee that paying the ransom will return the files successfully[6]. Indeed doing so also incentivises the hacker to produce more attacks in the future. A recent report has even shown that as little as 19% of ransomware victims who pay the ransom may actually get their files back[7, 8]. 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 being to encrypt files on the computer harddrive. 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.

The latest strains of ransomware have also 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.

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[5] 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.

Ransomware can enter a system in the same way as any other form of malware. Social engineering is the successful, and thus most common, form of attack vector for home users and organisations alike. Phishing may be used to encourage users to
baiting (infected USB drives, etc.)
can spread by downloads (as above) or self-replication via internal or external networks

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[9]. The WannaCry vulnerability was patched in Windows 7, 8.1 and 10 security updates[10, 11, 12] 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[13], 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.

Ensuring tight access control should also help to minimize the impact of ransomware. Minimizing users' access to only the assets which they absolutely require will ensure that
Ensuring users only have read access, (read access only where necessary) should minimize access of users to corrupt data review this regularly

1.3 Detect

Once a ransomware attack has taken hold, its important to detect and stop it before serious widespread damage can be done.

Security controls can be employed to detect ransomware. In particular, detecting altering of files- ransomware may attempt to modify ANY/ALL files on the system Detect virus signatures, actions beyond specifications, statistical changes?
Anti-virus software (keeping it up to date regularly) still may not be particularly effective
Once an attack has been discovered, all affected PCs and network connections from them should be shut down immediately.

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 as a last resort, prevention and early detection is preferable as recovering a whole system from a backup may take considerable amounts of time.

The National Cyber Security Centre recommend the following steps to recover from ransomware[6]:

- immediately disconnect infected computers from the network, by:
  - turning of Wi-Fi
  - unplugging ethernet cables
- format or replace hard drives and reinstall the OS
- connect the device to a clean network to download, install and update the OS and all software
- install, update and run antivirus software
- monitor network traffic and run antivirus scans to identify remaining infection

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 this has not been possible, multiple sources have been provided in order to provide further assurance of the correctness of statements.

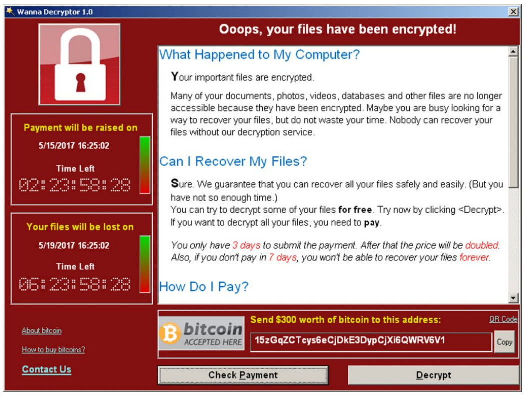
2 Email

2.1 Memo

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[2]. 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[1]. Clearly we need to do everything we can to defend against such attacks and **we need your help**.

© Randy Glasbergen for Trend Micro
TREND MICRO
GLASBERGEN
"On one hand, I'm grateful that we've never been targeted for a cyber-attack. On the other hand, I'm insulted that nobody thinks we're worth the effort!"

Figure 1: Cyber Security Cartoon[14]



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Figure 2: WannaCry Ransomware

Ransomware attacks that we have seen so far do not distinguish between targets. Their aim is to restrict users 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 programs. You will remember from your cyber security training that viruses may come as email attachments or as downloads from unscrupulous websites. We implore you **not** to:

- interfere with automatic software updates scheduled by system administrators
- run or install software that has not been vetted by system administrators if you would like additional software to be installed, please contact your service desk
- plug **unknown** devices, such as USB drives, into your computer

If you are victim of a ransomware attack, 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 as soon as possible.

If you have any follow-up questions regarding ransomware or cybersecurity in general, please do not hesitate 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

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.
As such, the first few lines have been designed to grab the attention of the reader by informing them of the significant impact ransomware has had on similar organisations around the world.

Appealing to the user directly - makes clear to the reader which actions they are responsible for
Using plurals everywhere else - makes clear this is a problem for the whole organisation and make the user feel comfortable discussing with others if they have questions

Graphics such as screenshots of previous ransomware fun cyber security cartoon main steps: help to break up the text.

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 words, it is unlikely that employees will read it.
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 is commonplace, and I have had to under take this myself during industrial placements.
NCSC recommendations relate this to the technical report in previous section
As analogy has been used to help the users relate to the explanation

At the end of the email, the main actions that the user will need to take in the event of being hit by a ransomware attack have been bulletpointed, and repeated in order to ensure that the user knows these are the key take aways from the memo. 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 in this case 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. As this is a university Open Assessment, I have been unable to do this in this instance.

3 References

[1] 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

[2] 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

[3] 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

[4] McAfee Labs, “McAfee Labs 2018 Threats Predictions Report,” Nov. 2017.

[5] Department for Culture, Media & Sport, “Cyber Security Breaches Survey 2017,” Apr. 2017.

[6] National Cyber Security Centre, “Mitigating malware,” Feb. 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/mitigating-malware

[7] CyberEdge Group, “2018 cyberthreat defense report,” Mar. 2018. [Online]. Available: https://cyber-edge.com/cdr/

[8] 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

[9] 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

[10] 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/

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

[12] 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

[13] ——, “Windows lifecycle fact sheet,” Feb. 2018. [Online]. Available: https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet

[14] 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/