Evolution of Ransomware and its Mitigation Strategies

Ariel L. Cordes
Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA 56267
corde171@morris.umn.edu

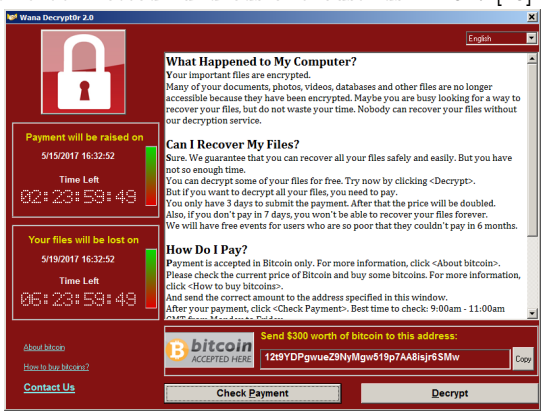
ABSTRACT

Ransomware is a kind of malware that has surged in popularity and effectiveness over the past few years, partially because of factors like Bitcoin and other cryptocurrencies making it far easier to have untraceable payments. Common business practices are insufficient to successfully mitigate these attacks. This paper surveys the state of ransomware, specifically mitigation and detection strategies at various possible points in the lifecycle of ransomware attacks.

1. INTRODUCTION

A grandmother clicks on a link in an online ad claiming to give homeowners a $1000 refund, and then nothing happens. The next time she turns her computer on, a screen that tells her that her files have been encrypted and that she needs to pay to get them back appears. She calls her grandson and leaves a message asking about what to do, and is terrified that she'll lose the family photos she treasures.

Figure 1: The message displayed by WannaCry, a ransomware attack that infected hundreds of thousands in 2017 [13]



This is a textbook case of a ransomware attack. While in recent years, businesses tend to be the more common targets, individuals are still at risk, particularly if they do not practice good IT security[7].

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/4.0/.
UMM CSci Senior Seminar Conference, April 2020 Morris, MN.

Ransomware has quickly become the most common (and lucrative) form of malware for cybercriminals to use. With cryptocurrencies like Bitcoin being easy to use and far more difficult or impossible for authorities to trace, incidences of ransomware attacks have grown.

The most common targets are small to medium size businesses and municipal governments, who are likely to have the resources to pay large sums but are not as likely as large corporations to have strong IT security protocols[7].

2. BACKGROUND

2.1 Definitions

This section will introduce some important terminology used in discussion involving ransomware and then discuss the following three important concepts that are necessary to understand how ransomware works.

2.1.1 Encryption

Encryption: in general, the process of transforming messages into a form using an algorithm called a *cipher* which only the intended recipient can understand. In information technology, encryption refers to using software to to do this, with the "message" being potentially any file, directory, or piece of information.

Phishing (email): an email with the purpose of getting a legitimate user to unknowingly allow an attacker access to the system(s) on which they reside. "Phishing" is an alteration of "fishing", and came about between 1995-2000, describing a cyber scam. This is likely related to the term "phreak", as in "phone phreak", one of a set of technically creative people who electronically hacked telephone companies of the day in the early 1970s [1].

Symmetric encryption is a kind of encryption that uses the same (or simply transformed) key for encryption of plaintext (non-encrypted text) and decryption of ciphertext (encrypted text). Asymmetric, or public-key, encryption is where anyone can get the key to encrypt something, but only the holder of the private key is able to decrypt and thus read the information. This is widely used in communicating information over the internet, because no secure "key exchange" is required, as would be the case with symmetric encryption algorithms.

High-grade encryption keys are those that are difficult to brute-force, that is, to guess every possibility and eventually happen upon the correct one. Standard random number generation techniques are not considered cryptographically secure. This is because any standard random number gen-

Figure 2: A simple cipher, which shifts each letter to the one three letters before it. This is known as a 3-shift Caesar cipher. It is not used seriously for cybersecurity, but provides a good demonstration of how to undo a symmetric encryption. If one knows how many letters the shift is, one can undo the shift with little effort. [2]

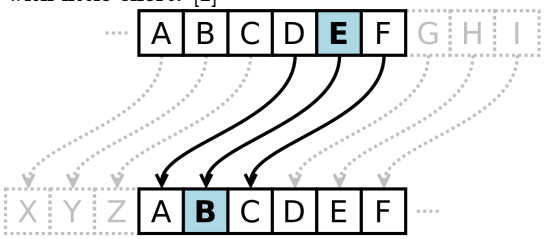
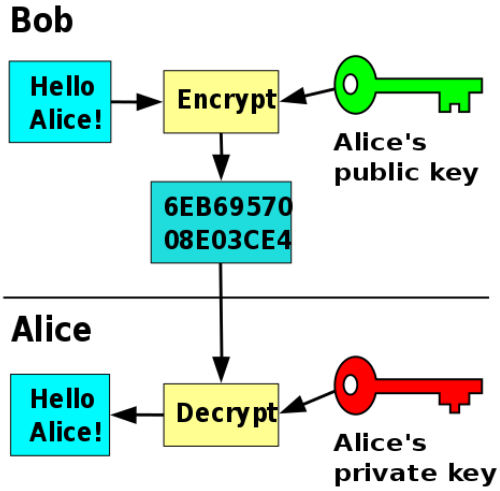


Figure 3: A visual representation how asymmetric encryption works [10]



erator is deterministic when supplied with the same "seed". Computers generally have a separate *cryptographically secure* random number generator that relies on more truly random seeds like the timing of input from the mouse or keyboard. This doesn't mean the keystrokes themselves, but the frequency intervals between presses of keys.

Modern ransomware works by blocking the victim's access to their files via encrypting them. As opposed to when a legitimate actor encrypts their files to prevent malicious usage of their contents, this encryption blocks the user from their files. For some individuals, this means no more access to their family photos. For many businesses and localities, this means being blocked from critical files required to keep operating.

Therefore, ransomware creators rely on public cryptography libraries such as OpenSSL to generate keys, which rely on underlying OS cryptographically secure random number generation as mentioned before.

2.1.2 *Cryptocurrency*

In general, **Cryptocurrency** is a digital asset designed to work as currency that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. These are not backed by any government and instead are operated in a decentralized manner.

Whereas payments with government-backed currency generally can be tracked in some ways by law enforcement, cryptocurrency does *not* allow that, making cybercriminals emboldened by the knowledge that their financial transactions cannot be traced back to them.

2.1.3 *Untraceable Network Communication*

Tor: software used for anonymous communication, often used by malicious actors to hide their identities but also used by many individuals, including journalists, who simply wish to remain anonymous.

Tor uses end-to-end encryption to prevent the information being transmitted from being intercepted by others. It also prevents potential interceptors from knowing *where* it came from and where it's ultimately going.

2.2 Timeline of Ransomware

The first recorded instance of ransomware was in 1989 [14], where it was distributed by physical mail via floppy drives purporting to be information on the AIDS crisis of the time. The "ransom" was to be mailed to a PO box in Panama, and a drive with the decryption tool was sent the same way.

Ransomware has evolved since then, using the explosion of the World Wide Web, cryptocurrency, and other innovations to improve and go after more and more lucrative targets. The untraceable nature of some cryptocurrencies has emboldened cybercriminals, with rates of malware attacks increasing As more personal data is stored on cloud backups, cybercriminals have begun shifting their targets away from individuals and towards businesses, typically those of a size that are both lucrative and easy targets. This tends to be small- to medium-size businesses, as large businesses tend to have adequate security measures in place.

In 2019, approximately 75% of the healthcare industry was infected with malware at some point[5]. Malware attacks are also rising rapidly, with some sources estimating an 175% increase in malware attacks from 2017 to 2018 alone.

Malware is not a threat that is going away soon. Therefore, having strong precautions in place to mitigate attacks is crucial to the functioning of businesses.

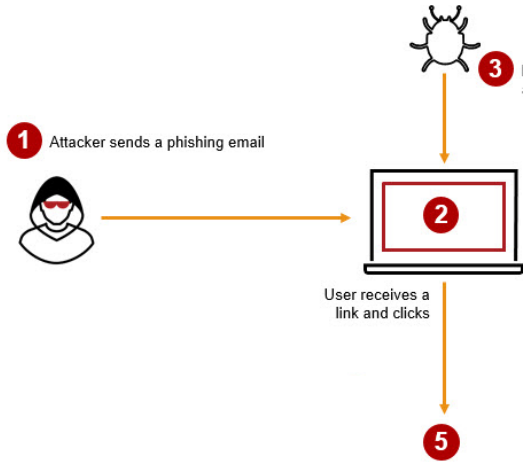
2.3 Outline of a Ransomware Attack

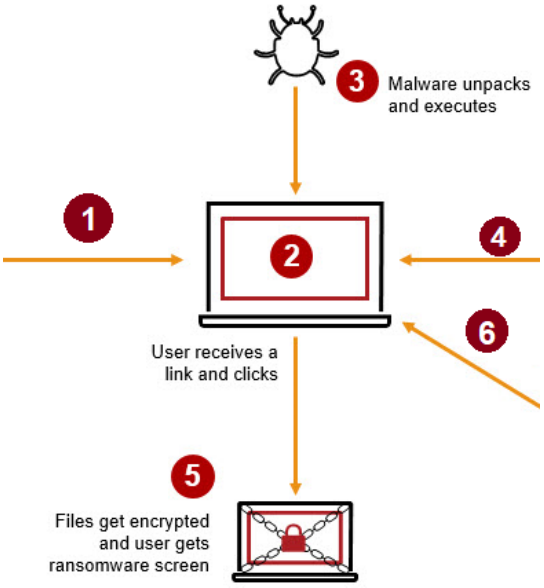
The above figure shows the first steps of a ransomware attack: **first**, the attacker sends a phishing email, or more likely, many, many phishing emails, all containing a malicious link that will download ransomware once clicked.

The **second** step is for the victim to click on the link. As 94% of malware, including ransomware, is distributed by email[7], 94% of ransomware can theoretically be prevented by training employees or oneself to recognize phishing emails and delete them/mark them as spam. Of course, the saying goes "a chain is only as strong as its weakest link", and the same is true in this case; if a single employee grants malware access to a system, it doesn't matter how many others have *not* granted it access to the same system.

The **third** step is for the downloaded malware to unpack and execute. This is a step where traditional antivirus software can potentially help mark the ransomware as a threat. However, this generally only works if the code for the ransomware is not obfuscated in some way, which it almost

Figure 4: An outline of how ransomware attacks progress. [4]





certainly is if the attack is well executed.

The **fourth** step is for the now-executed malware to communicate with the command and control server it is linked to, via a Tor network to keep the end address secure. A command and control server is used by cyberattackers to manage multiple attacks of a similar nature. In this case, the command and control server would be used to store the cryptographic keys used in the attack as well as the time it started counting down, if a time limit is being enforced.

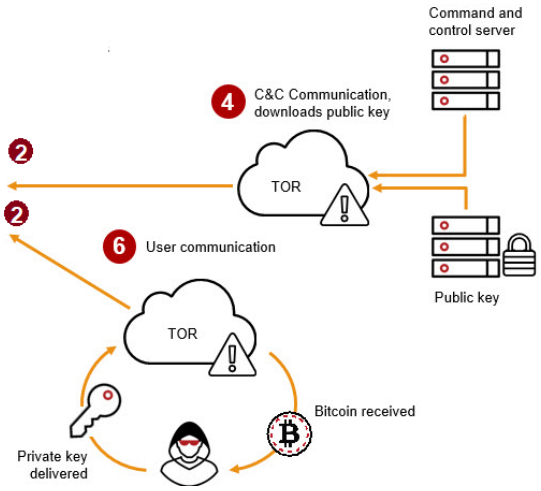
It may download keys from said server or send keys generated locally to the server, though both have their drawbacks for attackers. The methods described in Section 3.2 to mitigate ransomware would take place around this step.

The **fifth** step is for the ransomware to actually begin encrypting the user's files. The methods discussed in sections 3.2 and 3.3 both take place at this step, when the ransomware is actually encrypting files.

The **sixth** step, if all goes well for the attacker, is for the user to send cryptocurrency, usually Bitcoin, to the address specified. This allows the attackers to remain anonymous, as using currency backed by a government would allow entities like the FBI to better track such transactions. Once an attack has progressed to the sixth step with no mitigation from the victim's side, there is usually no way to regain access to the encrypted files.

The second part of the sixth step is highly uncertain. While all attackers will claim that paying the ransom will result in the decryption of files, surveys of those hit by ransomware report wide variance in results; one survey found that 90% were able to recover their files after paying the ransom, while another found that the same percentage did *not* receive the means to decrypt their files after paying the ransom. The FBI strongly recommends to never pay the ransom, saying "Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[3].

3. DETECTING AND MITIGATING RANSOMWARE



3.1 Backups

One of the most effective and simplest methods to combat ransomware is to have backups of one's files that are *not* able to be modified by individual systems, either through lack of permissions or because a backup disk is not connected to a system when it's not actively backing up. However, this requires fairly frequent backups, because the time between backups is the same as time lost due to a ransomware attack. If one backs up every hour, one risks losing an hour's worth of work. Depending on the nature of one's work, an hour lost may be an acceptable loss—or may be of irreplaceable value.

It is, of course, better to prevent the attack in the first place, because other than losing some amount of work, systems have to be reset and purged of the ransomware, which can be a tedious process. Therefore, it is better to view backups as a "last line of defense" rather than a prevention strategy, because of the costs associated with having to reset/purge systems. One could view backups as taking place

at a theoretical "Step 7" part of the ransomware infection process, if one assumes stopping the ransomware earlier is better.

Though backups are crucial as a part of ransomware defense strategies, because of their relative simplicity and their status as "last line of defense" rather than an actual prevention tactic, they will not be expanded on in this paper. Instead, various techniques aimed specifically at combating ransomware will be discussed.

3.2 Detecting Ransomware - Traversal

3.2.1 Rationale

The method ransomware uses to achieve its ultimate goal of money is to encrypt as many files as possible that are useful/unique to the victim while still leaving the operating system intact. This is because the OS needs to run so that the software telling the victim to pay can run (and, if they are genuinely going to decrypt the information upon payment, run the decryption tool). This leads to the conclusion that ransomware must have a certain way of traversing the file tree, and ignore certain directories while going after all others in a certain place.

3.2.2 Methods

Moussaileb et al. [9] proposed using the idea of "decoy" folders to help flag whether a program was ransomware. The idea is that ransomware wants to encrypt all files that a victim would pay to regain access to, and therefore wants to encrypt almost all directories. This is excepting certain directories, like on Windows, the "C:/Windows" directory, which are necessary for running the OS.

The idea is that "decoy" folders are almost never accessed by legitimate programs, and that a process that modifies a certain number of them or more in a certain timeframe is likely to be a malicious process. The "certain number" can be fine-tuned depending on the users of a system. Moussaileb et al. suggest this number be around 3, as legitimate processes are unlikely to enter three or more of the "decoy" folders.

This allows an antivirus program to stop ransomware from executing, though it has potential flaws if said antivirus program flags the program *after* important files have been encrypted.

Depending on the exact qualities of the ransomware, victims of the same attack can share the private key to decrypt their information, but this is not usually the case in modern attacks.

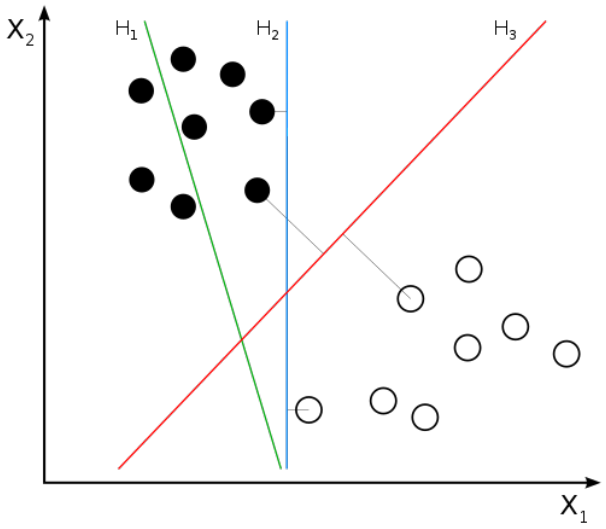
3.2.3 Support Vector Machines

Takeuchi et al. [12] trained a support vector machine (SVM) on the basic API calls to the system, such as read, write, rename, etc. An SVM is a kind of machine learning algorithm that looks at various examples and attempts to classify them into two or more classes.

In general, an SVM selects the optimal hyperplane (in two dimensions, a line; in three, a plane; in more, called a hyperplane) to divide *linearly separable* data. What this means is that if we're trying to classify a set of data into two classes, we can draw a line (or hyperplane) that has all data points of one class on one side and all of the other class on the other, with no data points in the other's area.

"Optimal" in this case means the line/hyperplane that maximizes the margins from the itself to the nearest data points on either side. The dividing line can be thought of as a "city street" of sorts–the SVM tries to make the street as wide as possible and decide which side has cars going one way and which side has cars going the other way. Of course, it has buildings (data points) that it has to work around, and cars can't drive into buildings. So it finds the way to make the road as wide as possible, essentially having as much space between the center of the road and buildings.

Figure 5: A visual representation of an SVM classifying a set of data. [11] The two dots closest to the red line are referred to as "support vectors", and the idea is to make the dividing line as far from the closest data points as possible. The green line is an inaccurate dividing line, since black dots are on the side all the white dots are on. The blue line is an example of a poor division which is still accurate for the training data. However, the red line is a much better division because it maximizes the margin between the closest black dot and white dot.



SVMs have to be trained on a set of data called *training data* and then tested on an independent set of data from the same distribution called the *test set*, which must be kept separate. This ensures that the algorithm does not just memorize which points fell into which category, similar to why the problems on a test are different than the problems done in a class.

SVMs generally require labeling, so in this case the processes running were labeled either as malicious or non-malicious. This allowed the training algorithm to gain a sense of what the structure of API system calls malicious software had when compared with non-malicious software.

SVMs perform incredibly well at relatively simple generalization tasks with a limited number of features. Takeuchi et al. observed a 97.48% accuracy rate with their system, illustrating that separating malware from "goodware" is very much doable in the vast majority of cases by an SVM.

This could be incorporated into antivirus programs in order to achieve better detection of ransomware and malware in general.

3.3 Detecting Ransomware - Encryption

3.3.1 Rationale

Ransomware requires strong encryption in order to be effective, which means that it needs to have high-grade encryption keys. It would want to keep these both strong and secure. If they are too weak, they are easily brute forced; if they are not secure enough, the key can be stolen and used to decrypt the files without the attackers receiving their payment. However, this is not an easy task even for modern, state-of-the-art cryptographic applications – even some good ones can fail to do it well.

Therefore, it is reasonable to assume that there may be ways to circumvent ransomware encryption. If one has the encryption key, it becomes trivial to decrypt the encrypted files, and thus counter the attack. This section explores this method of mitigating ransomware.

3.3.2 Methods

To encrypt victims' files, ransomware needs to use a hybrid method of symmetric and asymmetric encryption. The advantages and disadvantages of both these kinds of encryption for ransomware attackers can be summarized as follows: symmetric encryption is fast, but could lead to victims helping each other once one's files are decrypted because of the nature of it. Asymmetric encryption, on the other hand, is strong, but requires a lot of CPU usage, which makes it more likely to be identified by antivirus programs as an anomalous program. Therefore, a hybrid approach is necessary.

A promising method to take advantage of these traits is described by Genç et al. [8] By replacing function calls by non-whitelisted applications to cryptographically secure random number generators instead to a deterministic random number generator, the keys can be inferred based on the "source" of the randomness, be it the system time or some other commonly used source for non-cryptographically secure random numbers. This allows the victim of a ransomware attack to decrypt their files without paying the "ransom" to the attacker.

Genç et al. [8] were able to use their anti-malware program, called `UShallNotPass`, to decrypt a system encrypted by a Crypren ransomware attack. Promising results were shown in discovering weaknesses in the NegozI and Rush/Sanction families of ransomware, all of which were common families of ransomware at the time and still are to some extent.

3.4 Preventing Ransomware - Education

3.4.1 Rationale

While detecting ransomware with intelligent software methods and high-tech applications is fantastic, the fact remains that educating individuals who use a given system about the risks of ransomware and how ransomware commonly presents itself reduces the likelihood that said system will be compromised by ransomware.

This is because for all the technological advancement in the world, the easiest ways to gain unauthorized access to a system are based in social engineering – that is, cracking poor passwords, sending illegitimate emails that download malicious software, and just generally exploiting the lack of vigilance among a company's employees or a similar population. In fact, 94% of malware is delivered via email [7].

This means that if one were to prevent all ransomware delivered by email, only 6% of ransomware attacks would be able to even start. Such a total reduction is unlikely, particularly when involving many individuals, such as at a company or local government. But even a 50% reduction in giving access to ransomware via email would reduce the chance to 53%, which might mean the difference between being infected and thus having to either pay for the decryption key and/or for a costly technical audit of one's systems.

3.4.2 Methods

Various methods of education exist, but one of the more interesting approaches is described by Dion et al. [6] They describe a "gamification" system as follows: a video game that has the player receive various emails and penalizes heavily for opening/downloading from illegitimate ones, and gradually ramps up the difficulty, allowing children and young adults, but also potentially older individuals not as implicitly familiar with technology to learn the critical thinking skills to realize when an email is illegitimate.

Also described are ways to integrate training/education of this sort to the process to become HIPAA (Health Insurance Portability and Accountability Act which governs the flow of healthcare information) certified. Because there is already a strong certification system in place for data covered under HIPAA (medical records, etc.), adding training on ransomware/malware in general would be both beneficial and fairly straightforward, Dion et al. argue [6].

Being that the medical industry is commonly targeted by these kinds of attacks, adding requirements for IT training in the medical industry could prevent a good number of devastating ransomware attacks.

4. CONCLUSION

There are various ways to combat ransomware, either by technical means or otherwise.

From restricting access to an OS's cryptographically-secure number generator to educating more people about it, there are a variety of ways ransomware can be further mitigated.

Moussaileb et al. [9] found success in creating decoy files that ransomware would encrypt, thereby alerting a program to the likely presence of malware, essentially setting a trap for any ransomware that would be present on the system. The method described works at step five of the ransomware infection process, which is the last step that anything can be done, barring mistakes from the attacker's code, such as leaving the private key easily accessible on the system.

Takeuchi et al. [12] also worked at the fifth step of the process, training a support vector machine to recognize which programs were malicious and which were benign. By training on the underlying calls to various core functions, the algorithm was able to identify malicious software with 97.48% accuracy.

Genç et al. [8] focused on what could be called a "false surrender" – pretending to let the ransomware use secure number generators while in fact being able to reverse the effects of the malware once it finished. This worked at step four of the infection process, letting the ransomware think that it had secure keys that could, in fact, be easily recreated by a system.

Dion et al. [6] focused on educating individuals to better spot malicious emails. This would take place during step two of the infection process. While the previous technical

methods likely can be worked around by ransomware creators, because 94% of ransomware is delivered by email [7], any reduction at this step will help prevent almost all instances of ransomware attacks, because of phishing email's ubiquitous usage as a ransomware delivery mechanism. In a way, this stops the ransomware attack "before it starts".

While it's preferable to stop ransomware as early in the process as possible, stopping it at any point before it does irreversible damage to one's system is greatly beneficial. The best strategy to combat ransomware attacks, then, is likely all of the ones listed above working in concert, and more, along with keeping frequent, immutable backups.

However, as mitigation efforts evolve, so too will ransomware. The inventions such as the Internet and cryptocurrency that were first seen as novel and progressive have their own dark sides that are becoming more and more visible. Companies and individuals that wish to protect themselves from attacks like these will need to be vigilant.

5. REFERENCES

[1] phishing (n.).

[2] Caesar cipher, Apr 2020.

[3] Ransomware, Apr 2020.

[4] L. Columbus. How to deal with ransomware in a zero trust world, Aug 2019.

[5] CyberInt. 15 alarming cyber security facts and stats, Jan 2020.

[6] Y. L. Dion, A. A. Joshua, and S. N. Brohi. Negation of ransomware via gamification and enforcement of standards. In *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, CSAI 2017, page 203–208, New York, NY, USA, 2017. Association for Computing Machinery.

[7] J. Fruhlinger. Top cybersecurity facts, figures and statistics for 2020, Mar 2020.

[8] Z. A. Genç, G. Lenzini, and P. Y. Ryan. Security analysis of key acquiring strategies used by cryptographic ransomware. In *Proceedings of the Central European Cybersecurity Conference 2018*, CECC 2018, New York, NY, USA, 2018. Association for Computing Machinery.

[9] R. Moussaileb, B. Bouget, A. Palisse, H. Le Bouder, N. Cuppens, and J.-L. Lanet. Ransomware's early mitigation mechanisms. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, New York, NY, USA, 2018. Association for Computing Machinery.

[10] File:public key encryption.svg.

[11] File:svm separating hyperplanes (svg).svg.

[12] Y. Takeuchi, K. Sakai, and S. Fukumoto. Detecting ransomware using support vector machines. In *Proceedings of the 47th International Conference on Parallel Processing Companion*, ICPP '18, New York, NY, USA, 2018. Association for Computing Machinery.

[13] File:wana decrypt0r screenshot.png, Jan 2018.

[14] W. Z. A. Zakaria, M. F. Abdollah, O. Mohd, and A. F. M. Ariffin. The rise of ransomware. In *Proceedings of the 2017 International Conference on Software and E-Business*, ICSEB 2017, page 66–70, New York, NY, USA, 2017. Association for Computing Machinery.