[Slide 1]

Good afternoon everyone, my name if Finn and today I will be giving a seminar on the research I am conducting into developing a systematic approach for ransomware prevention and detection.

[Slide 2]

In this presentation I will provide an introduction and the background for the research I am conducting, followed by a summary of the related works. I will then describe the proposed work of the project and the intended goals of the research. I will then give an update on my current progress in my research and then discuss the future work that is still to be completed.

[Slide 3]

As mentioned, I have been conducting my research into developing a systematic approach for ransomware prevention and detection.

So, what is ransomware?

Well, I am sure most of you have a good idea of what ransomware is but put simply ransomware is a type of malware that prevents victims from being able to use their devices, usually by encrypting important files until a specific ransom is paid.

So why is research into ransomware important?

Over the last decade ransomware has become a profitable business for cybercriminals, assisted by the development of anonymous payments methods in the form of cryptocurrencies and continuous improvements in offensive cryptography. In 2017 ransomware caused unprecedented damage around the world around with the WannaCry and NotPetya strains wreaking havoc in many high-profile organisations including global shipping giant Maersk and the NHS in the UK. That year a Checkpoint security survey found that 59% of surveyed companies saw ransomware as their biggest cyber security threat. At this point the need to improve our defences against ransomware was obvious.

However, with the increased value of cryptocurrencies in 2018 and greater vigilance from IT administrators it was noted by cyber security companies that ransomware development had slowed and had taken a backseat to cryptocurrency miners as the preferred way for cyber criminals to make money. However, the COVID-19 pandemic and increased remote work has made a return, but the days of extremely viral strains like WannaCry travelling the globe are gone and have given way to targeted ransomware, that is ransomware that is human-operated ransomware that targets high-profile victims like large enterprises and government departments. Kaspersky noted a 767% increase in the number of their users being affected by targeted ransomware from 2019 to 2020. Additionally, cybercriminals have realised that there is value in not only encrypting a victim's files but also stealing them. This allows them to perform what is know as a double extortion where a victim's files are encrypted and held at ransom, and then the stolen information is threated to be released to the public if a second ransom if not paid.

This change is methodology from criminals presents new challenges in defending against malware that comes on top of already existing challenges. Defence against ransomware is challenging for a number of reasons. Firstly, cyber criminals have perfected their use of strong cryptography to make recovering files through cryptanalyse near impossible. Gone are the days of finding the decryption key in the source code. Additionally, ransomware makes use of modern malware evasion techniques such as code obfuscation, domain generation algorithms and encrypted communication. Historically,

research into defending against ransomware has focused on detection, either through static or dynamic analysis, and recovery from backups. However, with the more targeted approach cyber criminals are taking and the rise in extorting the victim with stolen information it is important that research is done into more proactive defences against ransomware.

Which brings me to the focus of my research which is developing a systematic approach to ransomware prevention and detection. My research has focused primarily on using two techniques for ransomware prevention and detection, moving target defence and cyber deception.

[Slide 4]

Moving target defence is a form of proactive defence that aims to confuse and deceive adversaries by changing the attack surface of a system. The key to designing a moving target defence is deciding what is going to move, how is it going to move, and when is it going to move. Examples of the "what" are things such as instruction sets, IP addresses, port number or software programs.

The "how" of the movement can be split into three categories, shuffling, diversity, and redundancy. Shuffling is the process of changing a systems configuration in an attempt to invalidate any work an attacker may have already done. For example, this can be done by changing IP addresses or VM migrations.

Diversity is when a system is created with different components that are able to perform the same function. Diversity increases the fault tolerance of a system because if an attacker attacks one configuration of the component the other configuration can still provide service.

Redundancy is when multiple versions of a component provide service. This is designed to provide resilience to the system because the system can still provide service if only some of the components are compromised. Diversity can take the form of diverse paths for routing or configurations that use different software stacks.

While I have defined these three techniques as different ways to answer the "how to move" questions they are typically used in conjunction with each other as they influence the effectiveness of each other.

The when to move question is the decision on when the attack surface should be changed to maximise the confusion of the adversary. There is the reactive approach that changes the attack surface when there is an event or an alert that signals that an intrusion may be happening. Then there is the proactive approach that changes the system configuration on a fixed or random time interval. These two techniques can also be combined into a hybrid approach that is both proactive and reactive.

[Slide 5]

The second area of my research has been into the use of cyber deception for ransomware defence. Cyber deception is actions that are taken to mislead attackers into performing or not performing certain action that aid in cyber security. The most common example of cyber deception is a "honeypot" server that is used to trick an attacker into thinking they have compromised a critical service but instead they are interacting with a benign server where they can be monitored studied. The key for cyber deception to be effective is that the deception needs to be believable and not arouse suspicion. This is done by exploiting the cognitive, cultural, organisational or personal biases of the attacker.

[Slide 6]

As mentioned, most of research into defending against ransomware has focused on detection techniques, primarily static and dynamic analysis. Currently, there has only been one study into using MTD to defend against ransomware conducted by Lee et al., titled “Ransomware protection using the moving target defence perspective”, which focuses on using moving target defence to change the file extensions of files targeted by ransomware strains like WannaCry. By changing the file extensions, it renders the ransomware ineffective as it uses the file extensions to decide which files to encrypt. This technique was noted to be extremely effective at stopping ransomware strains that only targeted certain file extensions but was ineffective at defending against strains that encrypt all files on a disk.

While there is only one paper written about using MTD to defend against ransomware specifically there has been other research done combing MTD and cyber deception in other security contexts. A paper titled “Proactive Defense for Internet-of-Things: Integrating Moving Target Defense with Cyberdeception” by [citation] looks at combination of MTD, in the form of network topology shuffling, and cyber deception, in the form of decoy nodes, as a proactive defence for critical IOT devices.

Cyber deception has also been studied in the context on ransomware with a paper titled “On deception-based protection against cryptographic ransomware” by Genc et al. which looks at how honey files can be used to detect attackers as well as discussing what makes an effective honey file, and common anti-deception techniques used by ransomware. The authors notes that generally hone-files are used for two purposes:

1. To detect an attacker
2. Once the file has been stolen confuse the attacker with the data inside it

The authors however state that in the case of ransomware the second sue case is not required because the data is not stolen by the attack. As mention previously however, the new trend towards cyber criminals combining data exfiltration and ransomware means that using honey-files for deception after they have been stolen is now an extra defence mechanism.

[Slide 7]

Now, the proposed work of this project is to create a novel systematic approach to defending against targeted ransomware using a combination of moving target defence and cyber deception. This proposal involves the following key goals:

1. Design a systematic defence against ransomware using MTD and cyber deception techniques
2. Design a testbed to allow for the testing of the techniques against modern targeted malware strains
3. Implement both the previously designed systematic defence and testbed
4. Test the implementation in testbed and discuss the results

[Slide 8]

Onto the progress I have made so far on these key goals. I had initially planned to design the systematic defence before starting any of the testbed design, but I quickly realised I had to make some decisions on what ransomware I was going to try and defend against to help narrow my scope.

I have selected the REVil and Nefilim ransomware strains to test against in the testbed for the following reasons:

1. I was able locate a version them to use for testing
2. They are both from targeted ransomware attacks
3. They are both designed to allow for the exfiltration of data
4. The use different methods for selecting which files to encrypt – Revil uses a list of predefined file extensions whereas Nefilim tries to encrypt all files on local and network devices it can find

I believe that these two strains will allow for realistic testing against modern targeted ransomware.

[Slide 9]

Now that I had some idea of what I needed to defend against I was able to design my systematic defence. I ended using a three-layered approach combining two MTD techniques and one cyber deception technique. The benefits of using a multi-layered approach is that if a ransomware strain is designed to get passed one of the layers it will still be able to be defended against by the other layers.

The first layer of defence is to use a shuffling network topology that shuffles on fixed intervals. This will impede an attacker's attempts to move through the system as it will be harder for them to determine where critical services are located. By preventing the propagation of the ransomware, it will limit the damage that is can cause to a service.

The second layer of defence is to use honey files that are designed to look like they will contain sensitive information. This will allow the early detection of adversaries as many targeted ransomware attacks will spend time looking for sensitive files before executing an attack. In some Nefilim attacks the attacker would spend up to two months looking for sensitive files before executing the ransomware attack.

The third layer of defence is to use file extension rotations, similar to the work done in the paper "Ransomware protection using the moving target defence perspective". This will proactively defend against malware strains such as REvil that encrypt files using a set list of file extensions.

So that was a summary of the progress I have made so far so now I will layout the future work that needs to be completed and a timeline for this.

[Slide 10]

So far, I have completed the goal of designing the proposed systematic defence and have started on the design of the testbed but there is still work to be done.

Here is my current plan for completing the required task to achieve the remaining three goals. As you can see, I plan to have completed the design of the testbed by the end of the semester which will allow for implementation to begin at the start of next semester. The plan is for implementation to be completed by week x which will allow testing to occur in the following weeks.

[Slide 11]

Thank you all for taking the time today to listen to my seminar and I will now open it up to any questions you might have.