Artificial Intelligence and its Development in Evasive Malware

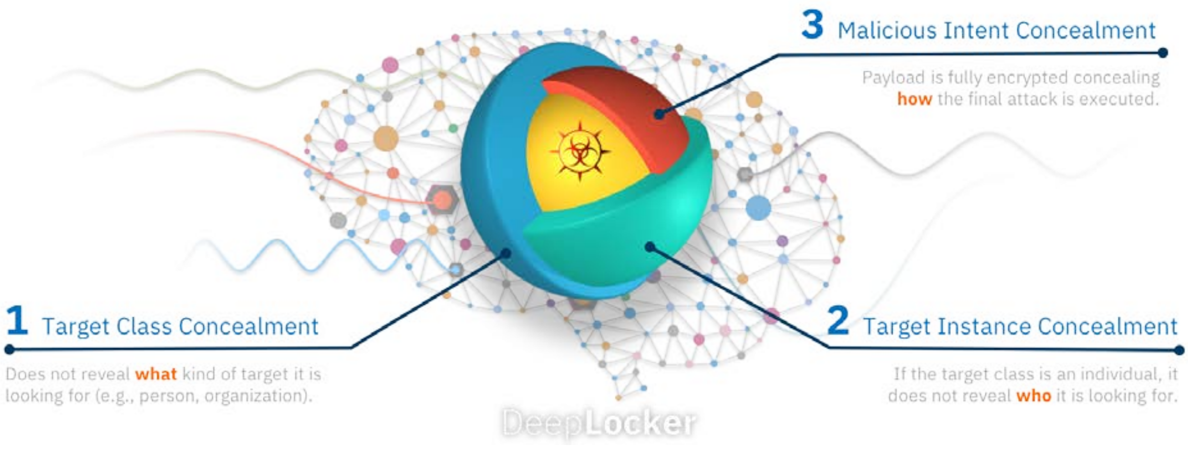
CONTRIBUTORS – Isabella

INTRODUCTION

Cybersecurity [a] is an area of IT which is constantly advancing to keep up with the capabilities and vulnerabilities of new and current technologies. As outlined by McAfee the purpose of evasive malware is to 'avoid detection and recognize when it has the best opportunity to strike. As Artificial Intelligence [b] has developed and grown the cybersecurity sector has started looking at the dual use of some elements to create highly targeted and evasive piece of malware that changes how secure and efficient both malware and computers will be in the future.

In the 1990's the evasive abilities of malware were focused on obstructing easy access and analysis of the malicious code to prevent detection through screening through antivirus systems and inferring intent by analysing code. To prevent detection malware and virus authors applied techniques obfuscating [c] to purposefully make it difficult for humans to understand as well as making code polymorphic [d] or metamorphic [e] changing the source code each time it ran to prevent the static signature to be detected multiple times by an antivirus system.

As technology evolved, the focus that evasive malware possessed changed to what it is running to where it is running. From the 2000 's onwards malware was coded to detect if it was being run in an antivirus system's sandbox [f] or a bare metal system, [g] when the presence of these virtualised environments is detected the malware stops running to prevent it from being classed as malicious. Evasive malware is now so widespread and readily used that secureintelligence.com found from their research that "98% of the malware samples analysed uses evasive techniques [h] to varying extents"[1] which presents the requirement for developers to understand how the technology is evolving and predict how it will evolve in the future.

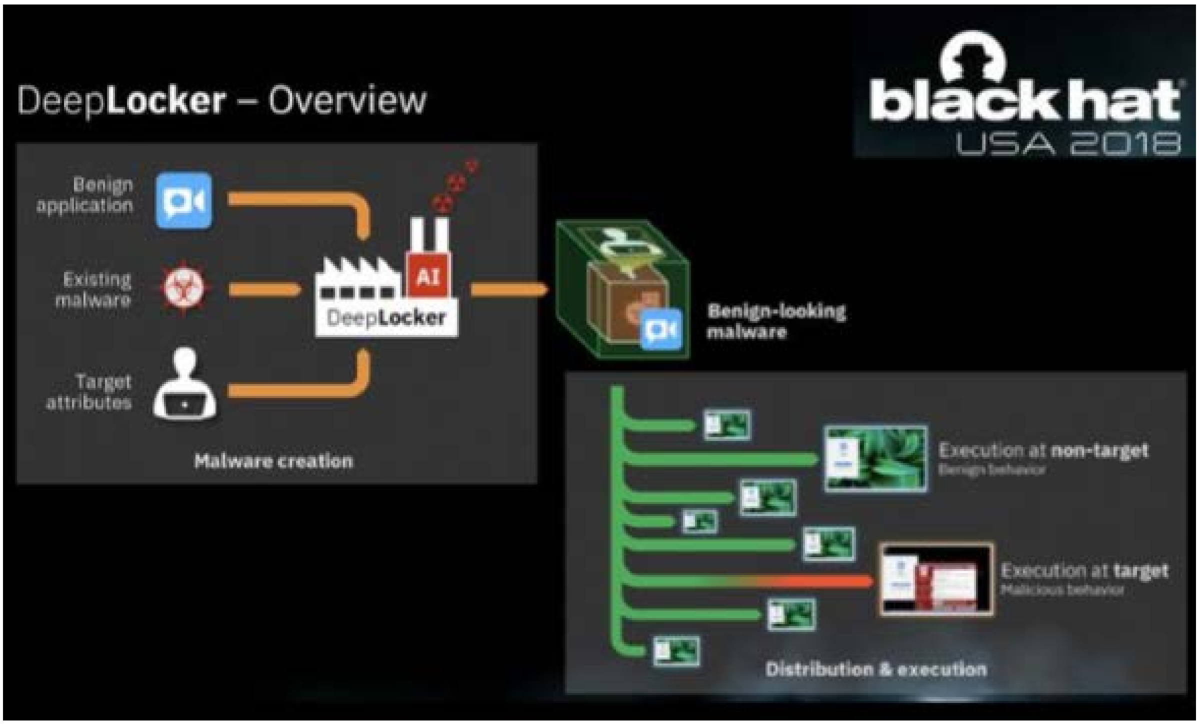

3 Malicious Intent Concealment
Payload is fully encrypted concealing how the final attack is executed.
1 Target Class Concealment
Does not reveal what kind of target it is looking for (e.g., person, organization).
2 Target Instance Concealment
If the target class is an individual, it does not reveal who it is looking for.
DeepLocker

[1] Mark Ph Stoecklin, Jang, Jiyong and Kirat, Dihlung, 'DeepLocker: How AI Can Power a Stealthy New Breed of Malware', SecurityIntelligence (8 August 2018), < https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/ >. accessed 20 February 2019.

FOCUS CASE

To present the risks and benefits of incorporating AI into evasive malware IBM built a proof of concept [i] to present the future of how evasive malware [j] could evolve to detect endpoints, attack their targets and run without detection of our modern cybersecurity software. To do this IBM presented a test case where by using DeepLocker they “camouflaged” the malware WannaCry, a ransomware worm that threatened Windows PCs in May 2017, within a video conferencing application that had been classed as ‘benign’ by antivirus systems. By doing so the malware remains undetected when examined with antivirus engines, malware sandboxes, bare metal systems and other malware analysis tools.

For this test case IBM chose for the trigger condition to use facial recognition to when to execute the malicious payload, training the AI model to recognize the face of a specific person causing the malware to become highly targeted and more successful in its attacks. To add to the plausibility of this test case IBM reinforces the importance of “camouflaging” the malware within another application due to modern-day reality that it is common for programs to be “distributed and downloaded by millions of people” spreading the malware quickly across systems and bringing it into contact with more users. Due to the main use of the carrier program is to take and transport camera data between computers the program can easily and covertly take “camera snapshots” and run them through the “embedded AI model” [k] without detection, searching for the face it has been trained to recognise. As a result of the AI model continuously running through the “camera snapshots” the program would behave normally for all users who didn’t match the trigger conditions criteria but when the target uses the application and begins sending data through to DeepLocker’s AI model the malicious payload would be decrypted [l] and executed due to the target’s face matching the trigger conditions for the malware.



DeepLocker – Overview

black hat USA 2018

Benign application

Existing malware

Target attributes

AI

DeepLocker

Malware creation

Benign-looking malware

Execution at non-target
Benign behavior

Execution at target
Malicious behavior

Distribution & execution

ANALYSIS

Although AI has previously been implemented in a defensive application for cybersecurity the idea of implementing it in malware and other forms of malicious code isn't a concept that has been thoroughly explored. When presented at the Blackhat conference there were two types of responses, one being fear and the other being dismissive.

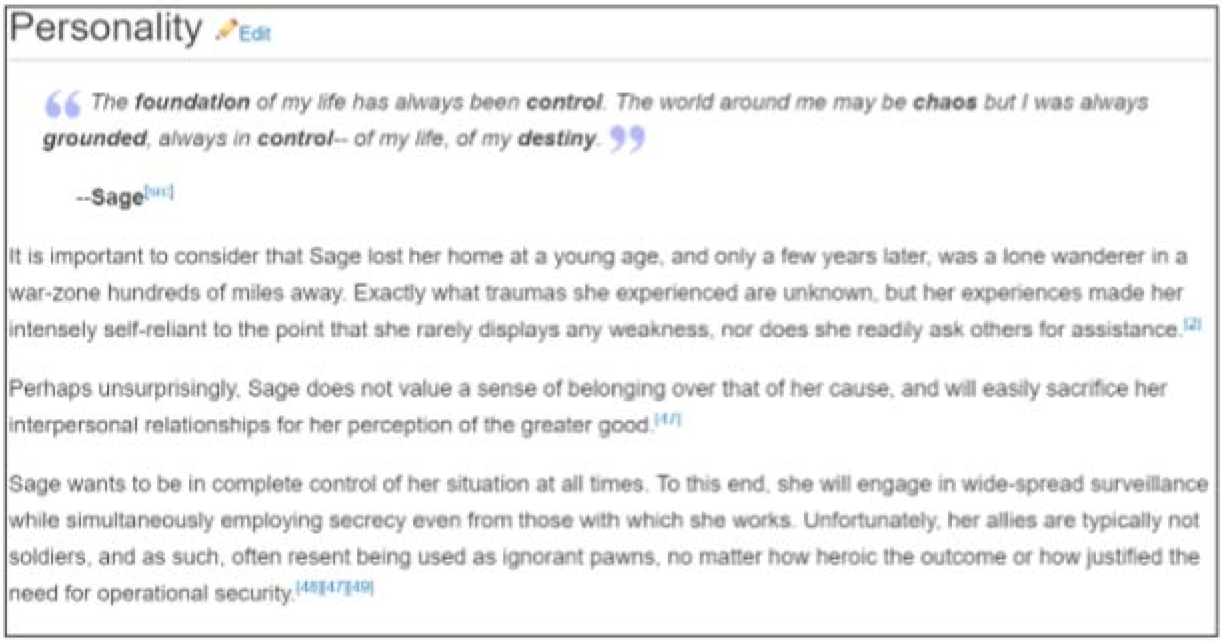
Many articles focused on DeepLocker's capabilities called it a "new-breed of malware" and a "dangerous precedent." Due to its value-laden nature DeepLocker is built to undermine and corrupt data making it a danger for the future of cybersecurity, when analysing the malware currently seen "out in the wild" professionals and experts can reverse-engineer the code to find patterns, endpoints and triggers to deconstruct it into something more manageable. DeepLocker on the other hand requires experts who specify in cybersecurity and AI to fully understand the purpose of its malware making the "traditional weakness of blackbox AI" into one of its biggest strengths.

The ability to reverse engineer malware allows for cybersecurity programs to advance alongside the development of malware and stay up to date with new threats, this is the most common cybersecurity technique, although it takes many forms, since this defensive ability is removed the viewpoints of people like Ralf Benzmüller, Executive Speaker of G-DATA security labs show how the biggest threat of the program can easily be worked around. While the level of difficulty involved in reverse-engineering DeepLocker is a talking point of the software, Ralf Benzmüller believes that software like DeepLocker can still be detected by "modern" cybersecurity solutions, emphasising the importance of creating "behaviour-based" algorithms in future so that instead of looking for known patterns or static signatures within the code the anti-virus is looking for certain executive actions, requests and transmissions from the program. Ralf Benzmüller took the proof of concept DeepLocker as "WannaCry with facial recognition" rather than a tangible threat.

The chosen malware for the proof of concept was the ransomware worm WannaCry, a piece of malware that presented itself as a legitimate threat to many groups in May 2017. By taking advantage of some Windows PCs not possessing certain security patches, WannaCry infected a number of computer networks, encrypting their files and demanding for payment in BitCoin.

One of the other viewpoints amongst professionals is that the spread of any malware, including DeepLocker, can only take place when the user puts their device at risk. Simon Bett, a journalist for maketecheasier.com is strong on his opinion that the spread and overall threat of programs like DeepLocker can be neutralised by keeping your antivirus up to date, consistently downloading software patches from your OS developer and not downloading anything suspicious, whether it is the program itself or the source of the download.

CONCLUSION



Personality

> *The **foundation** of my life has always been **control**. The world around me may be **chaos** but I was always **grounded**, always in **control**-- of my life, of my **destiny**.*
>
> --**Sage**[src]

It is important to consider that Sage lost her home at a young age, and only a few years later, was a lone wanderer in a war-zone hundreds of miles away. Exactly what traumas she experienced are unknown, but her experiences made her intensely self-reliant to the point that she rarely displays any weakness, nor does she readily ask others for assistance.[2]

Perhaps unsurprisingly, Sage does not value a sense of belonging over that of her cause, and will easily sacrifice her interpersonal relationships for her perception of the greater good.[47]

Sage wants to be in complete control of her situation at all times. To this end, she will engage in wide-spread surveillance while simultaneously employing secrecy even from those with which she works. Unfortunately, her allies are typically not soldiers, and as such, often resent being used as ignorant pawns, no matter how heroic the outcome or how justified the need for operational security.[46][47][49]

DeepLocker should be developed so that we can analyse its behaviours and develop effective ways to neutralise the threat before it becomes widespread. Sage is my preferred character for presenting DeepLocker because through her persona and her affiliation with the X-Men she could seamlessly implement the DeepLocker system within her own life and represents the future threat that we could experience, as its premise aligns so strongly with her personal requirement of self-preservation. The DeepLocker system has the benefit of running separate to the developer with no traceable links which would allow her to keep her anonymity.

Sage lost her home at young age and a few years later ended up in a war zone by herself, the trauma that she would have endured as a child in that situation has led her to be self-sufficient and independent known to sacrifice relationships for what she believes in, which is the advancement the greater good at whatever cost. Sage wants to be in control of her destiny and situation all times and to do this Sage created a sophisticated and widespread surveillance system while maintaining her anonymity from the people she works with the people she works against.

The DeepLocker AI software model in focus takes evasive malware to the next level and would effectivel aid Sage in her aims of remaining anonymous off the grid whilst keeping tabs on her enemies as well as those she is suspicious/wary of. The DeepLocker AI Model operates by itself, consistently collecting useful data through DeepLocker's ability to identify and sort data going through it and only collect data that matches the target class and target instance.

By taking advantage of how often commonly-used programs are updated, Sage can upload new data/update current data to ensure that her needs for surveillance, info gathering and understanding her surrounds in real time happen simultaneously. As well as this, by incorporating a deep neural network Sage can maintain anonymity both in her identity and aims as a hacker due to the level of skill required to successfully reverse engineer the malware to find all the trigger conditions and enumerate their outcomes as well as deduce which trigger conditions activate the malicious payload.

GLOSSARY

[b] Artificial Intelligence – the ability of a computer to simulate or imitate intelligent human behaviour

[h] Bare Metal System – an isolated system used to test programs under surveillance

[a] Cybersecurity – protection against unsolicited or criminal use of electronic data as well as the measure taken to achieve this

[l] Decryption – decoding data which has been encrypted so that is can been accessed by authorised users or computers

[k] Embedded AI Model – an Artificial Intelligence model that operates within another program

Encryption – encoding data so that it is not accessible for users and systems that are not authorised

[k] Evasive Malware – malicious code that has been developed to avoid detection

[j] Evasive Techniques – different evasive behaviours that prevents the code from being identifies, analysed or reverse-engineered

[e] Metamorphic Code – runs its code then while duplicating its code and putting it on another system changes its code so that it is different but still functions the same. The code is different on every system it runs on

[c] Obfuscating – making something (e.g. code) into something that is difficult for humans to understand and easily reverse engineer

Great examples of this can be found here: https://www.ioccc.org/years.html

[d] Polymorphic Code – decrypts and runs its code then while duplicating its code onto another system encrypts it with a different key. Each program is different before decryption but runs the same code

[l] Proof of Concept – evidence from an experiment, pilot project or prototype which demonstrates that a concept is feasible for future development

[g] Sandbox – software management strategy that isolates applications from critical system resources and other programs

[f] Static Signature – a recognisable, distinguishing pattern across programs

ANNOTATED BIBLIOGRAPHY

Allen, Tom, 'IBM's proof-of-concept 'DeepLocker' malware uses AI to infect PCs' (9 August 2018), The Inquirer, < https://www.theinquirer.net/inquirer/news/3060855/ ibms-proof-of-concept-deeplocker-malware-uses-ai-t o-infect-pcs >. accessed 14 March 2019.

Batt, Simon, 'DeepLocker: The Demonstration of AI-Based Malware'. (20 August 2018), Maketecheasier. < https://www.maketecheasier.com/deeplocker-ai-based -malware/ >. accessed 14 March 2019.

Fruhlinger, J, "What is WannaCry ransomware, how does it infect, and who was responsible?.". in *CSO Online*, , 2019, <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html> accessed 14 March 2019.

This article was another that I found was very important to my research. Ignoring the obvious that it provided information for my understanding of WannaCry the example of malicious code for DeepLocker it also provided an example for my own internal comparison between the future threats that a program like DeepLocker could cause and compared to a large security threat from two years ago. Since the article was written in August of 2018 much like the others it is timely in conjunction with my research and was probably written due to an increased interest in the topic after the development of DeepLocker.

Rizkallah, Juliette, 'AI And Cybersecurity: Are We Fueling Hackers' Fire?' (12 April 2018), Forbes, < https://www.forbes.com/sites/forbestechcouncil/201 8/04/12/ai-and-cybersecurity-are-we-fueling-hacker s-fire/#304fcee41bab >. accessed 19 March 2019.

Sage (Earth-616), Marvel Database Wikia, < https://marvel.fandom.com/wiki/Sage_(Earth-616) >. accessed 14 March 2019.

Stoecklin, Mark Ph, Jang, Jiyong and Kirat, Dihlung, 'DeepLocker: How AI Can Power a Stealthy New Breed of Malware', SecurityIntelligence (8 August 2018), < https://securityintelligence.com/deeplocker-how-ai -can-power-a-stealthy-new-breed-of-malware/ >. accessed 20 February 2019.

This article was very accurate and relevant since it was written by one of the developers and contributed to by the other two it provided an informative view and deep understanding on DeepLocker and its working. This article also provided a history of evasive malware which assisted me in building my introduction with further research needed only to fully understand some of the language. This article was a technical piece and advertisement for IBM and their research not an opinion piece. Due to the purpose of the article there was bias towards making DeepLocker sound better, and more intimidating, then it may be. This is why it was a good starting point but I needed more opinions on it from other experts to have a full view of DeepLocker and its effects. The timeliness was good as well, all articles written about DeepLocker are around the august period of 2018 like this one.

RESEARCH PROCESS

I spent a lot of time on the research progress because it took time for me to find a topic really interested me. When I found DeepLocker it peaked my interest because of the amount of detail that the program itself possessed. Due to this level of detail I had to grow my understanding of the language and elements involved once I had the base article from securityintelligence.com I annotated that article directly and then deconstructed it in another word document so that when I came back to my research I was using my own notes to build inquiry questions and broaden my understanding of the topic. By taking each section of research and putting it into dot-points and sub-points I found myself building the structure for my case study within my research which made it much easier to translate the detail required and understanding I possess into my work.

PROJECT MANAGEMENT PROCESS

When it came to project management for this assessment, I know I could've done better but I can see improvement between this assessment and the others I have done in IST. At the beginning of the assessment set dates and goals for sections of the assignment to be complete but didn't stick to them. This led to me continuously revising my goals and continuing to procrastinate like I have done so many time before. Unlike previously though when I got to the business end of the project time-period I got started and didn't continue to put it off and this led to a project that I'm proud of. Although I didn't finish it in time to get as much feedback as I would've liked throughout the project I still drafted my response many times and continued to improve my assignment up until the deadline which is something I'm very proud of.