To what extent can Windows Defender detect malicious code where evasion techniques are used?

Charles Graham

Project Topic:

Within the cyber world there is a constant battle between virus and antivirus software. Due to computers evolving at an exponential rate, so are the techniques of virus development and mitigation. I want to understand the extent to which the stock antivirus system Windows Defender is able to prevent malicious executables from being run on a stock windows machine. With this data I will be able to conclude how effective Windows Defender is when different forms of evasion are used.

This research will focus on evaluating the effectiveness of different virus creation tools for windows 10 The reason I have chosen to focus on this operating system is due to the market share in operating systems with Windows holding a substantial percentage. "As of December 2020, over 76% of all computers worldwide were running some version of windows" (Andra Zaharia, 2024). Having such a large share in the market means that an attacker's priority when trying to infect a machine is mainly aimed at a windows machine, by evaluating the effectiveness of Windows defender we will be able to understand the possible future mitigations to be put in place so that all devices are protected from a multitude of potential viruses.

Some key things I intend to research are:

- **How well do off the shelf tools evade antivirus?**
- **What are the key characteristics of a virus?**
- **What behaviours cause antivirus to flag a file as malicious?**
- **What techniques, if any can be used to evade antivirus?**

Overview of solution:

There are several off the shelf tools available for generating viruses, and evading detection of AV systems. To help AV developers understand the implications of these tools, they need to be able to evaluate the impact on AV detection rates.

The project will be based on experimentation, I will feed a windows computer different versions of a virus or exploit and record two variables. Firstly, did the antivirus pick up the virus and quarantine it. Secondly, if the virus run as intended with full functionality.

The results of experimentation will be used to create a report, discussing the current state of the art in AV detection and evasion.

These viruses will be created by using various readily available tools online and also by original python code create by myself. As different viruses will be given to the machine I expect that most will be detected but some will fly under the radar of the antivirus. Hence my results will be drawn as a percentage of viruses that were detected, and the ones that escaped detection will be discussed as to

why they succeeded in not being detected. Additionally, certain evasion techniques may help avoid detection, but unfortunately leave the virus broken due to being encoded or mangled too harshly. After drawing these results I'll be able to suggest techniques that could be implemented to further protect machines, or if I'm unable to produce a virus that evaded Windows defender then ill discuss the potential reasons why it was detected.

Audience and Motivation:

As discussed in section 1 above, as windows holds a majority share in the market when it comes to computers, there are a range of tools that can be used to create effective viruses. The impact of these tools regarding AV detection is continuously altering, and therefore the environment is rapidly changing. With plenty of innovations from both attackers and defenders, it is difficult to produce long lasting solutions.

Up-to-date sources indicate that "560,000 new pieces of malware are detected everyday" (Bojan Jovanovic, 2023). With this huge number of potentially 0-day viruses being created everyday, there is no way that antivirus software can keep up block all these threats before they infect multiple machines.

(Bojan Jovanovic, 2023) Also says that "Every minute, four companies fall victim to ransomware attacks" This relates nicely to (Marika Samarati, 2017) report on how much cyber crime cost the UK in 2016, "Although ransomware ranked last in terms of the number of organisations affected (388,858), it ranked first in terms of financial losses (£7,356,060,699)". These statistics show us that more resources need to dedicated into researching the techniques that attackers used to produce malware. After understanding why antivirus is evaded we will then be able to mitigate the impact of readily available tools and protect our computers. The reason so many organisations were effected is due to evasion techniques such as obfuscation and cryptography. Encoding and changing the structure of the payload will bypass certain detection techniques such as signature based scanning and potentially heuristic based scanning depending on the severity of the obfuscation. Also techniques such as polymorphic code will allow code to be changed every time the program is run, further evading antivirus by constantly changing its signature.

Antivirus software is arguably one of the most important processes on our computers, blocking internal and external threats, it protects our computers from malicious users. My projects will be important to the blue and red teams within cybersecurity. With greater knowledge on how antivirus systems cope with different forms of evasion, will ensure that new protections are put in place to further secure devices. Also, I'm positive that my research will also benefit individual users who have little knowledge around cyber threats. Reasoning for this is because by demonstrating the different ways in which a virus can come it will encourage users to be more cautious when opening a file from an unsigned source. Furthermore, antivirus developers will be able to use my research to locate the flaws in any

existing products. If a certain technique used guarantees antivirus evasion then developers will be able to rectify any mistakes.

Project Plan:

The project plan will follow an experimental methodology, I am using Getting Things Done (GTD) to plan my tasks(Allen, 2018). This will involve recording outputs, processing the data and then planning the next stage based on the outputs received. This will allow me to plan time for the major tasks, but leave scope to add the details following the results of each piece of experimentation.

Some potential problems I may face are the complexity around evading Windows defender. Antivirus has had many years to develop and mitigate risks against new computer viruses. On the other hand, I will have at best a couple of months to develop several iterations of computer virus to evade Windows defender. Through my experimentation I hope to demonstrate the robustness of Antivirus, and that off the shelf tools are unlikely to work. This protects us from many individuals that may try place a malicious executable on someone's machines

As there is a coding aspect to my project I assume that a lot of time will be spent learning new coding techniques in order to evade antivirus. As there is a risk this will take too long, I am planning on leaving this task until the end. This way I dont risk spending too much time on one aspect of the project and will allow me to focus on other areas.

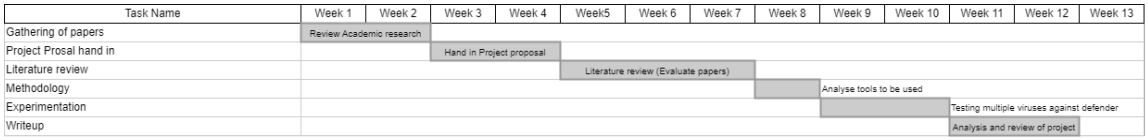

Figure 1: Gantt Chart

References:

Andra zaharia. (2024, Jan 19,). 300+ terrifying cybercrime & cybersecurity statistics (2024). https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Bojan Jovanovic. (2023, -04-10T09:14:19+00:00). A not-so-common cold: Malware statistics in 2023. https://dataprot.net/statistics/malware-statistics/

David Allen. (2008). *Getting things done* https://gettingthingsdone.com/wp-content/uploads/2014/10/Filing.pdf

Samarati, M. (2017). *Cyber crime cost UK businesses £29 billion in 2016.* https://www.itgovernance.co.uk/blog/2016-cyber-security-breaches-cost-uk-businesses-almost-30-billion

References

Allen, D. (2018). *Getting things done*. A system for organizing tasks; proj.