SACE NUMBER: 307514X
AUTHOR: DUC NGUYEN

How reliable are modernised antivirus detection programs against advanced/evolving malware threats throughout the Windows operating system?

In a generation where the digital world is rapidly evolving, the security of private information within computer systems has become an increasingly critical concern for all users. One of the most significant challenges faced by both individuals and organizations within the security of computers is the escalation of advanced and evolving malware, posing a growing risk to the confidentiality of sensitive data[1]. Evolving malware refers to malicious software that constantly adapts its tactics to circumvent traditional security measures. This dynamic nature allows malware to continually outpace traditional antivirus detection methods, enabling it to evolve and employ advanced evasion techniques. Consequently, the progression of antivirus programs is a priority in protecting these assets. With an antivirus on the well-known Windows operating system, it serves as a primary target for malware developers due to the immense number of users[2]. This prevalence enforces the effort in researching and considering the efficiency of antivirus software.

The research conducted, is structured to provide a thorough analysis of the effectiveness and reliability of modernised antivirus detection programs, focusing on the capabilities in detecting, mitigating, and preventing malicious threats within the Windows operating system. By reviewing various detection techniques, the impact of programming languages on efficiency, and analysing the evasive actions executed behind these malware threats, the current state of cybersecurity not only is assessed, but the potential for enhancement in future technologies is considered.

ANTIVIRUS PROCESS & DETECTION TECHNIQUES

Antivirus software serves a primary purpose in protecting computer systems against malicious payloads, and various cyber threats. To accomplish this goal, antivirus programs are not only equipped with an array of techniques and processes able to detect these attacks, but also to comply with general security requirements for consumers seen in table 1[3]. These security measures are expected to be integrated within the software's detection techniques to ensure a large success rate when analysing malware. Throughout this analysis process, the file undergoes several layers of inspection in virtual machines which simulates realistic operating environments to verify its integrity.

Function	Description
Malware detection and recovery	Real-time detection of malware entering the system
	Recovery of the original file(s) or detection or malware
Scanning	User-executed or periodic checks for malware
Identification and authentication	User identification and authentication
	Access control blocks for unauthorised use
Security alarm	Alert for critical security events
Security management	User interface
	Antivirus policy settings
Self-protection	Function maintenance of the antivirus software
	Self-protection to provide security functions
Security audit	Record and view logs created during the antivirus operation

Table 1. Standard security requirements for antivirus software. (Han et al. 2020)

Antivirus software undergoes a structured process to address potential threats to computer systems, eventually concluding the file to be safe or unsafe[4]. Throughout this methodical progression, various of detection techniques are implemented to quarantine or delete the threat/s outlined in figure 1. According to numerous software companies including Malwarebytes, two most common detection techniques embedded within today's antiviruses are

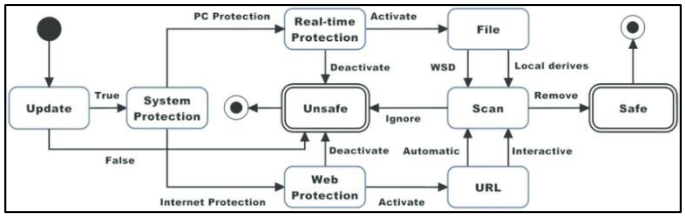

Figure 1. Algorithmic structured process of a typical antivirus program. (Souri et al. 2015)

[1] Cyber Risk Is Growing. Here's How Companies Can Keep Up 2023, Harvard Business Review, viewed 31 October 2023, <https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up>.

[2]Abraham, S 2018, Why Windows get More Virus Attacks than Mac or Linux - MalwareFox, MalwareFox, viewed 15 October 2023, <https://www.malwarefox.com/windows-virus-attacks/#:~:text=Latest%20Windows%20versions%20also%20have,exposed%20and%20easily%20tampered%20with.>.

[3] Han, S-H, Lee, H-K, Gim, G-Y & Kim, S-J 2020, Empirical Study on Anti-Virus Architecture for Container Platforms, ResearchGate, IEEE (Institute of Electrical and Electronics Engineers), viewed 24 October 2023, <https://www.researchgate.net/publication/342536292_Empirical_Study_on_Anti-Virus_Architecture_for_Container_Platforms>.

[4] Souri, A, Monire Norouzi Soufiani, Adalat Safarkhanlou & Hassan Es.haghi sardroud 2015, Formalizing and Verification of an Antivirus Protection Service using Model Checking, ResearchGate, Elsevier BV, viewed 29 October 2023, <https://www.researchgate.net/publication/281232476_Formalizing_and_Verification_of_an_Antivirus_Protection_Service_using_Model_Checking>.

honeypots, and dynamic monitoring of mass file operations (see appendix 1 and 2)[5]. These detection techniques offer distinct advantages such as being able to assess the behavior of files compared to static scanning engines used in traditional antivirus software (see appendix 3)[6]. With both techniques utilizing behavioral analysis and real time monitoring instead of relying on predefined file signatures, they can identify threats based on their current state rather than comparing them against a list of previously known malwares. Although these dynamic detection techniques provide more adaptive defense against threats, Matt McCormack from the Microsoft antivirus team accentuates that these real time detection techniques should be considerate to the number of resources consumed and find the right balance between prioritizing speed and file detections, as an excess in demand on system resources would impact the software's performance resulting in potential vulnerabilities and thus decreasing the reliability within antiviruses.

MALWARE OVERVIEW & EXECUTION PROCESS

Amongst all attackers, the motive behind all different malware such as ransomware, spyware, trojans is the money cybercrime generates from victims, thus the pursuit of financial gain drives a competitive environment between them. This competition within the development contributes to a constant evolution of malware and their execution process on Window's computer systems (see appendix 4)[7]. As malware advances in complexity, McCormack expresses that there is a necessity for antiviruses to comprehensively understand their execution processes within systems. This understanding is crucial in the battle against cyber threats, especially trojans. Cybersecurity researchers agree that trojans make up approximately 50% to 75% of all malware occurrences, thus highlighting the significant impact these trojans have on individuals and companies[8, 9].

Trojans are typically executed through a variety of methods, including social engineering, exploiting vulnerabilities within software, and spreading via file sharing, where different scenarios would require different execution methods. A 2022 report by researchers at a cybersecurity company called Proofpoint, observed how attackers social engineered industries by impersonating the World Health Organization whilst leveraging a vulnerability within Word documents to conceal malware[10]. Once executed, trojans have several objectives depending on what was tasked by the attacker. These objectives range from data theft, establishing system control, conducting espionage, or to cause disruptive inconvenience upon to the infected user. However, when meeting their goal, attackers typically require an active and, in some cases, a continuous connection between the infected devices, observed in figure 2[11]. This connection is a critical element during the execution of trojans, as they rely on the constant communication to relay the stolen data, or to receive commands from the attacker. Trojans such as keyloggers stand out as one of the most privacy-invading and communitive malware due to their capability to record and send every keystroke made by users on an infected system to the host[12]. Mikko Hyppönen, chief researcher officer at F-Secure Corporation, raises the concern

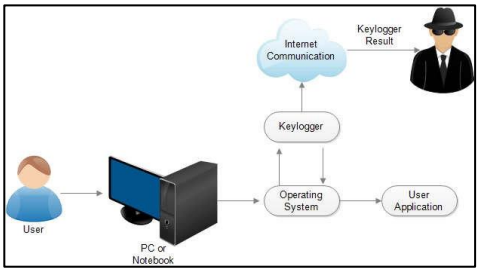

Figure 2. Flow of information within Keyloggers between user and attacker. (Rahim et al. 2018)

[5] blog/authors/wcozens 2022, Top 5 ransomware detection techniques: Pros and cons of each, Malwarebytes, Malwarebytes, viewed 29 October 2023, <https://www.malwarebytes.com/blog/business/2022/10/top-5-ransomware-detection-techniques-pros-and-cons-of-each>.

[6] blog/authors/wcozens 2022, Top 5 ransomware detection techniques: Pros and cons of each, Malwarebytes, Malwarebytes, viewed 29 October 2023, <https://www.malwarebytes.com/blog/business/2022/10/top-5-ransomware-detection-techniques-pros-and-cons-of-each>.

[7] Impact of Cyberattacks by Malicious Hackers on the Competition in Software Markets 2020, Journal of Management Information Systems, viewed 31 October 2023, <https://www.tandfonline.com/doi/abs/10.1080/07421222.2019.1705511>.

[8] Craft, D 2023, Malware Statistics & Facts: Frequency, Impact & Cost, Worthinsurance.com, Worth Insurance, viewed 6 November 2023, <https://www.worthinsurance.com/post/malware-statistics#:~:text=58%25%20of%20all%20known%20computer,the%20use%20of%20.exe%20files.>.

[9] Panda Security 2013, PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record - Panda Security Mediacenter, Panda Security Mediacenter, viewed 6 November 2023, <https://www.pandasecurity.com/en/mediacenter/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/>.

[10] New RAT malware uses sophisticated evasion techniques, leverages COVID-19 messaging. - Document - Gale Power Search 2022, Gale.com, viewed 6 November 2023, <https://go.gale.com/ps/i.do?p=GPS&u=61ahsa&id=GALE|A759113606&v=2.1&it=r&sid=bookmark-GPS&asid=94d4648f>.

[11] Rahim, R, Heri Nurdiyanto, Ansari Saleh Ahmar & Darmawan Napitupulu 2018, Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm, ResearchGate, IOP Publishing, viewed 7 November 2023, <https://www.researchgate.net/publication/323338837_Keylogger_Application_to_Monitoring_Users_Activity_with_Exact_String_Matching_Algorithm>.

[12] Keyloggers Explained | How to Protect Against Keyloggers 2022, SOPHOS, viewed 7 November 2023, <https://www.sophos.com/en-us/cybersecurity-explained/keylogger>.

regarding keyloggers' capability to continuously steal personal information, such as passwords, or credit card details even when they are changed by a user[13].

Although trojans rely on active connection lines with the system, they also depend on a persistence mechanism to maintain their presence within the infected device[14]. Persistence ensures that the malicious code remains in the user's file directories and preserve control over extended periods after the initial execution, therefore, presenting the challenge of maintaining long term reliability in antiviruses. This characteristic showcases the ever-growing attention towards trojans being able to remain dormant, thus underlining the urgent need for more advanced antivirus solutions.

MALWARE EVASION TECHNIQUES

While antivirus companies are constantly striving to enhance their security measures, malware developers are equally persistent in pushing technological boundaries to evade detection throughout their execution process[15]. This ongoing battle of innovation leads malware developers to continuously develop sophisticated evasion techniques. According to a recent analysis carried out by Kaspersky on their database of malware, it was found that obfuscation and virtual machine detection emerged as some of the most prevalent evasion techniques employed by malware developers[16]. These techniques applied by developers aim to complicate the identification of their malware, making it more difficult for antiviruses to mitigate the threat.

Obfuscation techniques such as XOR encoding are used by malware developers to ensure their code is more difficult to analyse or reverse-engineer, thus making it more challenging for antivirus programs to detect. XOR encoding is a bitwise operation which is leveraged to obfuscate strings within malware, such as target file locations, making it harder for antiviruses to recognize the affected files or specific locations within the system, therefore not raising any alarms[17]. XOR works by taking into two sets of binary data and returns a new set of data by comparing each corresponding pair of bits. If the bits are different, the result bit is set to 1, whilst if they're the same, the bit is set to 2 (see figure 3)[18, 19, 20].

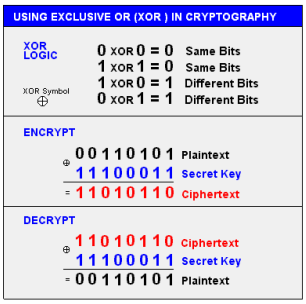

Figure 3. Visual XOR encryption process. (Definition of XOR 2023)

Similar to obfuscation, malware developers utilises virtual machine detections as an evasion technique to avoid detection rates from antivirus software. The theory behind detecting virtual machines comes from the differences in hardware, configurations, and behavioral patterns that distinguish a virtualized environment from a physical system[21]. As most modern antiviruses are reliant on virtual machines to conduct real time analysis on a payload, developers integrate an anti virtual machine (anti-VM) for their malware to stop execution upon encountering certain parameters[22]. A GitHub repository created in March 2023 by a Python developer named Marci consists with an exhaustive list of computer names, IP addresses, hardware identification (HWID), and other identification belonging to VirusTotal's

---

[13] Mikko Hypponen 2023, Fighting viruses, defending the net, Ted.com, TED Talks, viewed 7 November 2023, <https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net?language=en>.

[14] Huntress 2021, Persistence in Cybersecurity, Huntress.com, viewed 7 November 2023, <https://www.huntress.com/defenders-handbook/persistence-in-cybersecurity>.

[15] Davidson, R 2021, 'The fight against malware as a service', Network Security, vol. 2021, Elsevier BV, no. 8, pp. 7–11, viewed 9 November 2023, <https://www.sciencedirect.com/science/article/abs/pii/S135348582100088X>.

[16] Kaspersky 2023, How cybercriminals try to bypass antivirus protection, www.kaspersky.com, viewed 9 November 2023, <https://www.kaspersky.com/resource-center/threats/combating-antivirus>.

[17] XOR bitwise operation (article) | Ciphers | Khan Academy 2023, Khan Academy, viewed 9 November 2023, <https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/xor-bitwise-operation>.

[18] Mikko Hypponen 2023, Fighting viruses, defending the net, Ted.com, TED Talks, viewed 7 November 2023, <https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net?language=en>.

[19] Point Operations - Logical XOR/XNOR 2023, Ed.ac.uk, viewed 9 November 2023, <https://homepages.inf.ed.ac.uk/rbf/HIPR2/xor.htm#:~:text=The%20XOR%20(and%20similarly%20the,corresponding%20pixels%20from%20the%20second.>.

[20] Definition of XOR 2023, PCMAG, PCMag, viewed 9 November 2023, <https://www.pcmag.com/encyclopedia/term/xor>.

[21] General Virtual Machine Protection 2023, Vmware.com, viewed 9 November 2023, <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-8B93E01D-AB37-41F2-A225-892E40BAFB35.html>.

[22] Virtual Machine for Malware Analysis 2020, GeeksforGeeks, GeeksforGeeks, viewed 9 November 2023, <https://www.geeksforgeeks.org/virtual-machine-for-malware-analysis/>.

virtual machines[23]. From further research on GitHub, it was identified that eighteen other repositories had used this list to stop executing their code if the computer details matched, with some code reducing detection counts by 30% (refer to appendix 5). Consequently, the effectiveness of antivirus programs is compromised, with some malware able to succeed in evading detections by exploiting these identified vulnerabilities in virtual machine analysis. This poses a direct challenge to the reliability of modernized antiviruses as the additional anti-VM measures by malware developers are aimed to target the techniques that contemporary antivirus solutions rely heavily upon.

However, as malware developers incorporate anti-VM techniques within their malware, antivirus companies have responded by implementing mechanisms to counteract this. By having processes which can detect when a file attempts to access an antivirus virtual machine's detail, they are able to flag them as malicious, thus challenging malware developers to continuously innovate new evasions techniques[24].

PROGRAMMING LANGUAGES

Despite the constant goal of antivirus companies addressing these evasion techniques from malware developers and storing the file's signature into a database, exotic programming languages, introduces a more sophisticated approach which antiviruses tend to struggle when trying to effectively counteract[25]. Conventionally, malware is commonly written in 'low level languages' like C/C++, as they have the ability to control memory and control some important system resources which 'higher level languages' can't, but a 2023 research article from the International Conference on Information Technology has observed a recent trend where other languages such as Go are being used more frequently in malware (refer to appendix 6)[26]. Programming languages like these don't inherently evade antiviruses but rather their characteristics and design philosophies make them more challenging to detect.

Go is a compiled high level programming language which has gained popularity amongst malware developers due to its syntax similarities with the programming language, C[27]. This sharp rise in popularity is also supported by the benefits which the language provides, including streamlined concurrency support, and a strong focus on efficiency and performance, thus being crucial for malware developers seeking to optimize the capabilities of their malicious software[28, 29]. Incorporated into the language, concurrency in Go refers to handling multiple tasks or processes simultaneously, even though it might not complete them all at the exact same time. It rapidly switches between these tasks, making it seem like they are running in parallel (see figure 4)[30]. The changing nature of simultaneous execution poses challenges, for antivirus programs in monitoring and analyzing the behavior of malicious processes. Unlike threaded execution that follows a more predictable flow of operations concurrent malware utilizes the asynchronous capabilities of Go programming language to simultaneously execute various components[31]. This complexity makes it more challenging, for antivirus programs to precisely identify and disrupt activities. However, while e Go offers significant advantages to developers, it does have limitations in certain areas, particularly in cryptographic library support. Go's standard library for cryptography is relatively minimalist, which can pose

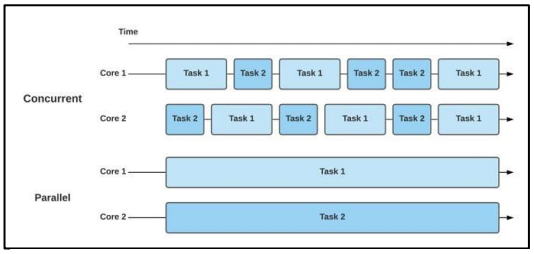

Figure 4: Go's concurrency running multiple tasks with 1 core compared to parallel processing. (Ayberk Dikcinar 2022)

[23] 6nz/virustotal-vm-blacklist: yep full list of virustotal machines 2023, GitHub, viewed 9 November 2023, <

[24] Scanning virtual machines 2023, Kaspersky.com, viewed 9 November 2023, <https://support.kaspersky.c

[25] Staff, D 2021, 4 'Exotic' Programming Languages Popular With Malware Developers, Dice Insights, Dice, viewed 28 November 2023, <https://www.dice.com/career-advice/4-exotic-programming-languages-popular-with-malware-developers>.

[26] Meghna Praveen & Wesam Almobaideen 2023, 'The Current State of Research on Malware Written in the Rust Programming Language', viewed 29 November 2023, <https://ieeexplore.ieee.org/document/10226157>.

[27] Hackers Arcade 2021, The Art of Malware Development - Hackers Arcade - Medium, Medium, Medium, viewed 29 November 2023, <https://hackersarcade.medium.com/the-art-of-malware-development-d9843ad10a10#:~:text=The%20reason%20behind%20malwares%20being,level%20languages%E2%80%9D%20can't.>.

[28] Bera, R 2022, Concurrent Programming in Go – Goroutines, Channels, and More Explained with Examples, freeCodeCamp.org, freeCodeCamp.org, viewed 30 November 2023, <https://www.freecodecamp.org/news/concurrent-programming-in-go/>.

[29] Dev, T 2020, GoLang the new Malware Language? - Tapendra Dev - Medium, Medium, Medium, viewed 30 November 2023, <https://tapendradev.medium.com/golang-the-new-malware-language-94097baae223>.

[30] Ifihanagbara Olusheye 2022, Concurrency in Go, Earthly Blog, viewed 30 November 2023, <https://earthly.dev/blog/concurrency-in-go/>.

[31] Ayberk Dikcinar 2022, Concurrent Programming In Golang - Dev Genius, Medium, Dev Genius, viewed 30 November 2023, <https://blog.devgenius.io/concurrent-programming-with-golang-2a4edb2552b1>.

constraints on the development of sophisticated cryptographic techniques within malicious software[32].

CONCLUSION

Antivirus programs are in a continuous state of improvement to stay ahead of malware developers. However, even with advancements in antivirus detection techniques such as honeypots, and dynamic monitoring of mass file operations, malware still poses a significant threat to individuals and organizations. The inherent challenge lies in the fact that malware developers are proactive in creating new threats by leveraging various execution processes, evasion techniques, and exotic programming languages, while antivirus solutions must reactively respond to these threats. This persistent cycle highlights the need for continual innovations in cybersecurity solutions. Antivirus programs are reliable to a certain extent, but their reliability diminishes, when faced with advanced techniques that allow malware to infiltrate systems[33]. This emphasizes online users to implement practices and adopt proactive measures, such as two factor authentication, using password managers to help store unique passwords for various accounts, being smart online to avoid download malicious files, ensures an additional layer of security against advanced and evolving malware threats[34].

[32] Tung, L 2022, This ransomware just switched programming languages from Go to Rust. Here's why, ZDNET, ZDNET, viewed 30 November 2023, <https://www.zdnet.com/article/this-ransomware-just-switched-programming-languages-from-go-to-rust-heres-why/>.

[33] Ahmed, F 2023, The evolution of antivirus software to face modern threats, Security Intelligence, Security Intelligence, viewed 1 December 2023, <https://securityintelligence.com/posts/antivirus-evolution-to-face-modern-threats/>.

[34] Baker, K 2023, 10 Effective Ways to Prevent Compromised Credentials, IdentityIQ, viewed 1 December 2023, <https://www.identityiq.com/digital-security/10-effective-ways-to-prevent-compromised-credentials/>.

SACE NUMBER: 307514X
AUTHOR: DUC NGUYEN

BIBLIOGRAPHY

6nz/virustotal-vm-blacklist: yep full list of virustotal machines 2023, GitHub, viewed 9 November 2023, <https://github.com/6nz/virustotal-vm-blacklist>.

Abraham, S 2018, Why Windows get More Virus Attacks than Mac or Linux - MalwareFox, MalwareFox, viewed 15 October 2023, <https://www.malwarefox.com/windows-virus-attacks/#:~:text=Latest%20Windows%20versions%20also%20have,exposed%20and%20easily%20tampered%20with.>.

Ahmed, F 2023, The evolution of antivirus software to face modern threats, Security Intelligence, Security Intelligence, viewed 1 December 2023, <https://securityintelligence.com/posts/antivirus-evolution-to-face-modern-threats/>.

Ayberk Dikcinar 2022, Concurrent Programming In Golang - Dev Genius, Medium, Dev Genius, viewed 30 November 2023, <https://blog.devgenius.io/concurrent-programming-with-golang-2a4edb2552b1>.

Baker, K 2023, 10 Effective Ways to Prevent Compromised Credentials, IdentityIQ, viewed 1 December 2023, <https://www.identityiq.com/digital-security/10-effective-ways-to-prevent-compromised-credentials/>.

Bera, R 2022, Concurrent Programming in Go – Goroutines, Channels, and More Explained with Examples, freeCodeCamp.org, freeCodeCamp.org, viewed 30 November 2023, <https://www.freecodecamp.org/news/concurrent-programming-in-go/>.

blog/authors/wcozens 2022, Top 5 ransomware detection techniques: Pros and cons of each, Malwarebytes, Malwarebytes, viewed 29 October 2023, <https://www.malwarebytes.com/blog/business/2022/10/top-5-ransomware-detection-techniques-pros-and-cons-of-each>.

Craft, D 2023, Malware Statistics & Facts: Frequency, Impact & Cost, Worthinsurance.com, Worth Insurance, viewed 6 November 2023, <https://www.worthinsurance.com/post/malware-statistics#:~:text=58%25%20of%20all%20known%20computer,the%20use%20of%20.exe%20files.>.

Cyber Risk Is Growing. Here's How Companies Can Keep Up 2023, Harvard Business Review, viewed 31 October 2023, <https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up>.

Davidson, R 2021, 'The fight against malware as a service', Network Security, vol. 2021, Elsevier BV, no. 8, pp. 7–11, viewed 9 November 2023, <https://www.sciencedirect.com/science/article/abs/pii/S135348582100088X>.

Definition of XOR 2023, PCMAG, PCMag, viewed 9 November 2023, <https://www.pcmag.com/encyclopedia/term/xor>.

Dev, T 2020, GoLang the new Malware Language? - Tapendra Dev - Medium, Medium, Medium, viewed 30 November 2023, <https://tapendradev.medium.com/golang-the-new-malware-language-94097baae223>.

General Virtual Machine Protection 2023, Vmware.com, viewed 9 November 2023, <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-8B93E01D-AB37-41F2-A225-892E40BAFB35.html>.

Hackers Arcade 2021, The Art of Malware Development - Hackers Arcade - Medium, Medium, Medium, viewed 29 November 2023, <https://hackersarcade.medium.com/the-art-of-malware-development-d9843ad10a10#:~:text=The%20reason%20behind%20malwares%20being,level%20languages%E2%80%9D%20can't.>.

Han, S-H, Lee, H-K, Gim, G-Y & Kim, S-J 2020, Empirical Study on Anti-Virus Architecture for Container Platforms, ResearchGate, IEEE (Institute of Electrical and Electronics Engineers), viewed 24 October 2023, <https://www.researchgate.net/publication/342536292_Empirical_Study_on_Anti-Virus_Architecture_for_Container_Platforms>.

Huntress 2021, Persistence in Cybersecurity, Huntress.com, viewed 7 November 2023, <https://www.huntress.com/defenders-handbook/persistence-in-cybersecurity>.

Ifihanagbara Olusheye 2022, Concurrency in Go, Earthly Blog, viewed 30 November 2023, <https://earthly.dev/blog/concurrency-in-go/>.

SACE NUMBER: 307514X
AUTHOR: DUC NGUYEN

Impact of Cyberattacks by Malicious Hackers on the Competition in Software Markets 2020, Journal of Management Information Systems, viewed 31 October 2023, <https://www.tandfonline.com/doi/abs/10.1080/07421222.2019.1705511>.

Kaspersky 2023, How cybercriminals try to bypass antivirus protection, www.kaspersky.com, viewed 9 November 2023, <https://www.kaspersky.com/resource-center/threats/combating-antivirus>.

Keyloggers Explained | How to Protect Against Keyloggers 2022, SOPHOS, viewed 7 November 2023, <https://www.sophos.com/en-us/cybersecurity-explained/keylogger>.

Meghna Praveen & Wesam Almobaideen 2023, 'The Current State of Research on Malware Written in the Rust Programming Language', viewed 29 November 2023, <https://ieeexplore.ieee.org/document/10226157>.

Mikko Hypponen 2023, Fighting viruses, defending the net, Ted.com, TED Talks, viewed 7 November 2023, <https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net?language=en>.

New RAT malware uses sophisticated evasion techniques, leverages COVID-19 messaging. - Document - Gale Power Search 2022, Gale.com, viewed 6 November 2023, <https://go.gale.com/ps/i.do?p=GPS&u=61ahsa&id=GALE|A759113606&v=2.1&it=r&sid=bookmark-GPS&asid=94d4648f>.

Panda Security 2013, PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record - Panda Security Mediacenter, Panda Security Mediacenter, viewed 6 November 2023, <https://www.pandasecurity.com/en/mediacenter/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/>.

Point Operations - Logical XOR/XNOR 2023, Ed.ac.uk, viewed 9 November 2023, <https://homepages.inf.ed.ac.uk/rbf/HIPR2/xor.htm#:~:text=The%20XOR%20(and%20similarly%20the,corresponding%20pixels%20from%20the%20second.>.

Rahim, R, Heri Nurdiyanto, Ansari Saleh Ahmar & Darmawan Napitupulu 2018, Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm, ResearchGate, IOP Publishing, viewed 7 November 2023, <https://www.researchgate.net/publication/323338837_Keylogger_Application_to_Monitoring_Users_Activity_with_Exact_String_Matching_Algorithm>.

Scanning virtual machines 2023, Kaspersky.com, viewed 9 November 2023, <https://support.kaspersky.com/KSV/6.0/en-US/186130.htm>.

Souri, A, Monire Norouzi Soufiani, Adalat Safarkhanlou & Hassan Es.haghi sardroud 2015, Formalizing and Verification of an Antivirus Protection Service using Model Checking, ResearchGate, Elsevier BV, viewed 29 October 2023, <https://www.researchgate.net/publication/281232476_Formalizing_and_Verification_of_an_Antivirus_Protection_Service_using_Model_Checking>.

Staff, D 2021, 4 'Exotic' Programming Languages Popular With Malware Developers, Dice Insights, Dice, viewed 28 November 2023, <https://www.dice.com/career-advice/4-exotic-programming-languages-popular-with-malware-developers>.

Tung, L 2022, This ransomware just switched programming languages from Go to Rust. Here's why, ZDNET, ZDNET, viewed 30 November 2023, <https://www.zdnet.com/article/this-ransomware-just-switched-programming-languages-from-go-to-rust-heres-why/>.

Virtual Machine for Malware Analysis 2020, GeeksforGeeks, GeeksforGeeks, viewed 9 November 2023, <https://www.geeksforgeeks.org/virtual-machine-for-malware-analysis/>.

XOR bitwise operation (article) | Ciphers | Khan Academy 2023, Khan Academy, viewed 9 November 2023, <https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/xor-bitwise-operation>.

APPENDIX 1. HONEYPOTS

Honeypots refers to a cybersecurity technique which involves creating fake files and dropping it into vulnerable locations within a computer system to detect the existence of malicious files[35]. They are often considered as decoy systems and aims to appear valuable to attackers, luring them to interact with these files, thus gathering the process information of the malware. Once the fake file is interacted by a malware, a notification is sent to the program, alerting of the active presence, and providing basic information (file name, size, author etc.). Honeypots are found in various types such as low interaction and high interaction, contributing to different levels of emulation to attract attackers[36].

APPENDIX 2. DYNAMIC MONITORING

Dynamic monitoring, in antivirus refers to the analysis and identification of harmful activities or behavior occurring on a computer system. Unlike antivirus methods that rely on a collection of known malware signatures, dynamic monitoring prioritizes observing the actions and operations of programs and processes as they are executed[37].

APPENDIX 3. STATIC ENGINES

Static analysis, commonly known as engines is a method employed by antivirus software to recognize and uncover harmful files. Unlike monitoring that observes program behavior in time static analysis concentrates on analysing a files attribute without running it.

APPENDIX 4. DIFFERENT TYPES OF MALWARES

Ransomware: Ransomware refers to a kind of software that aims to block access, to computer systems or files until the victim pays an amount of money usually in cryptocurrency to the attacker. It works by encrypting the victim's data rendering it inaccessible and then demands a ransom in return, for providing the decryption key[38].

Spyware: Spyware is a form of software that operates secretly and collects user information without their awareness or permission. It has the capability to capture keystrokes monitor browsing habits gather login credentials and obtain data[39]. This information is typically sent to a party for harmful purposes.

Trojans: Trojans often referred to as Trojan horses are software programs that appear legitimate but carry payloads[40]. Unlike viruses or worms Trojans do not replicate themselves. Instead rely on social engineering techniques to deceive users into installing them.

---

[35] Kaspersky 2023, What is a honeypot?, www.kaspersky.com, viewed 30 November 2023, <https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot>.

[36] Labs, M 2021, What is a honeypot? How they are used in cybersecurity, Malwarebytes, viewed 30 November 2023, <https://www.malwarebytes.com/blog/news/2021/05/what-is-a-honeypot-how-they-are-used-in-cybersecurity>.

[37] SentinelOne 2016, Critical Features of Next-Generation Endpoint Protection, Part Two: Dynamic Malware Detection, SentinelOne, viewed 30 November 2023, <https://www.sentinelone.com/blog/critical-features-next-generation-endpoint-protection-part-two-dynamic-malware-detection/>.

[38] Trellix 2023, Trellix.com, viewed 1 December 2023, <https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/>.

[39] Gillis, AS, Brush, K & Teravainen, T 2021, spyware, Security, TechTarget, viewed 1 December 2023, <https://www.techtarget.com/searchsecurity/definition/spyware>.

[40] What is a Trojan? Is it a virus or is it malware? 2018, @Norton, viewed 1 December 2023, <https://au.norton.com/blog/malware/what-is-a-trojan>.

APPENDIX 5. DETECTION RATES WITHOUT/WITH ANTI-VM TECHNIQUES

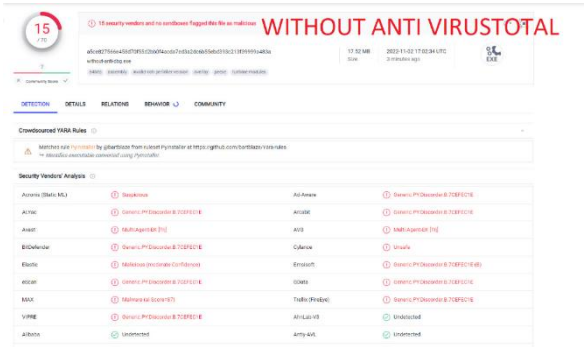

Figure 5: Detection rates by VirusTotal WITHOUT anti virtual machine techniques.

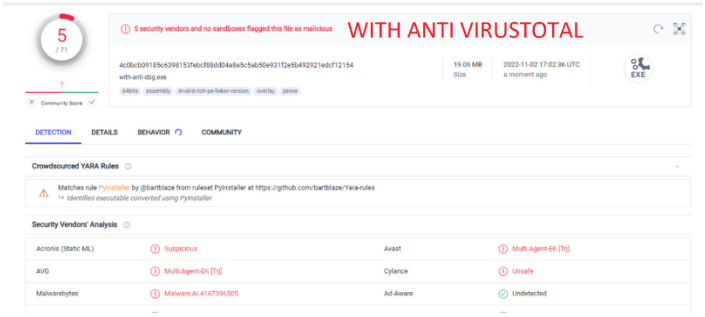

Figure 6: Detection rates by VirusTotal WITH anti virtual machine techniques.

APPENDIX 6. LOW LEVEL VS HIGH LEVEL PROGRAMMING LANGUAGES

Low level programming languages, like Assembly and machine code operate at a level that is closely connected to the hardware giving developers control over a computer's resources. Developers who work with low level languages can directly access memory and hardware registers, which allows them to optimize code for performance[41]. On the hand, high level programming languages offer an abstract and user-friendly approach. They provide a level of abstraction by hiding details and allowing developers to concentrate on problem solving rather, than dealing with intricate system interactions[42].

[41] Admin 2021, Difference Between High Level and Low-Level Languages, BYJUS, BYJU'S, viewed 1 December 2023, <https://byjus.com/gate/difference-between-high-level-and-low-level-languages/#:~:text=The%20primary%20difference%20between%20low,feasibly%20compared%20to%20human%20beings.>.

[42] Difference between High Level and Low level languages 2019, GeeksforGeeks, GeeksforGeeks, viewed 1 December 2023, <https://www.geeksforgeeks.org/difference-between-high-level-and-low-level-languages/>.