Comparison of Paid Subscription vs Freeware Software on Antivirus program

Daniel Santos
University of West Oahu

Abstract

In the realm of computer security there are various tools, programs, and software to prevent harmful attacks on the user computer. Antivirus software applications represent a common method to protect computer systems. With new types of malware being created by malicious users throughout each year user will need some type of formal protection on their PC. Upon looking at various antivirus software some are accessible for free for example Windows Defender for simple protection. Other software can be downloaded for free like Malwarebytes or trial-based software to determine if the user wants to purchase the subscription software. Upon looking at these options it would be informative to determine the most effective and efficient antivirus software for protecting a PC by either detecting or eliminating harmful virus programs. The overall approach to address this project involved the evaluation of several antivirus software applications which included Windows Defender, Malwarebytes, subscription-based McAfee, and trial based anti-virus software. A sample malware program installed on a computer system will be utilized to determine if the selected anti-virus and malware applications are able to detect or eliminate the sample malware file. Overall, aim of this project is to evaluate how well the security program helps protect the PC but also examines its efficiency, usability, and if required for personal use or for business use. When most people are looking into PC protection some people wonder if the purchase of a antivirus software is necessary in protecting their PC data and wonder if the free software is enough for protection.

Introduction & Research Question

Computers are currently being used for many purposes that include work related matters, casual browsing, and gaming. With many jobs starting to transition to remote work environments, computer users should be aware of the security of their devices depending on their specific job function. The most convenient form of computer security for the average user is an anti-virus program. The primary goal of an anti-virus program is to keep the computer safe by detecting and neutralizing malware. Depending on the type of anti-virus software program there are a variety of options the user can select depending if the software is free or subscription based. In which case many users would use it as form of a buffer to defend your computer.

Research Question: From the vast selection of antivirus program options from free to paid subscription, which provides the most effective protection for a PC user.

Hypothesis: From the many options available to protect the PC user most often an antivirus program will be able detect most of the common malware threats. As such I believe that paid subscription based antivirus programs will prove more effective against malware threats, due to the extra available features.

Research Design & Data Collection

The research experiment was designed to focus on the effectiveness of free and paid antivirus programs from a malware attack . To conduct this experiment, Microsoft Windows 10 OS was installed on a virtual machine. The antivirus programs were tested using ransomware simulator and Eicar test files. The antivirus programs tested were Windows Defender, Malwarebytes, and McAfee. To test the effectiveness of these programs a malware test file was installed on the Windows 10 virtual machine and performed the action one at a time. After the completion of each scan, the performance information was recorded for analysis.

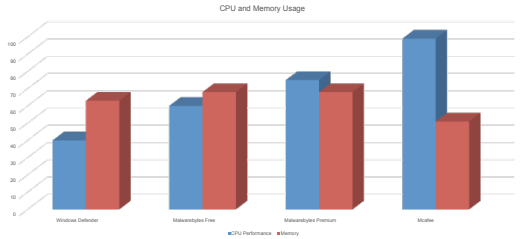

Chart 1. CPU and Memory usage of the Antivirus program when conducting the scan for malware

Results

The results summarized in Table 1 confirmed that all three programs tested were able to detect malware except for Malwarebytes Free. Although when it came to the ransomware test Windows gave two dramatically different results without the controlled access folder enabled the PC is susceptible to attack. If this folder was enabled, it will protect the computer by encrypting the files which will not allow the user to make changes.

The two results for Windows defender in Figure 1 shows the files were compromised when the ransomware Simulator conducted its attack. Without the use of the controlled access folder it was more prone to be vulnerable to an attack and having its files compromised whereas enabling the controlled access folder contained the threat from accessing the file. The results shown in Figure 2 were the same for Malwarebytes Premium and McAfee where both were able the subdue the threat and quarantine it upon the initial phase of the simulation.

When it came to the performance of the Antivirus program each performed varied in that with free Antivirus program the scan was relatively quick to finish whereas the paid counterpart had varied completion depending on the type of scan performed. In Chart 1 I conducted the virus scan for each of the tested programs in that when came to number of services used in Task Manager McAfee took up most of the CPU power due to fact when using the full scan, since it looks into every drive and folder within the PC and depending on the amount of data you store within each drive the time will vary. By looking into every data in the PC the prioritization of the AV scan will take precedence of the executable program running within the PC. Likewise, shown in Chart the paid program used much more power usage in CPU power. As such when came to Malwarebytes free there was only one option to the scan which looks into the common system locations such as the Memory Objects, Startup Objects, Registry Objects, File System Objects, and Heuristic Analysis. By looking into the common areas, the scan is relatively quicker than that off the premium antivirus program. Comparable to Windows 10 it offers three option which are the full scan, quick scan, and custom scan and like the McAfee its going to depends on the amount of data stored within the PC for the time completion although it uses much less CPU power compared to McAfee and this could be due to the fact that Windows doesn't have many processes like McAfee.

Table 1. simulated experiment results for the programs tested in the Ransomware attack

Ransomware Attacks	Windows Defender	Windows Defender Reattempt	Malwarebytes Free	Malwarebytes Premium	McAfee
Archiver	Executed	FalsePositive	Executed	Incorrectly Blocked	FalsePositive
BlackKingdomVariant	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
Collaborator	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
CrifconiVariant	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
DearCryVariant	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
HollowInjector	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable
Injector	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
InsideCryptor	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
LockyVariant	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable
MazeVariant	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
Mover	Vulnerable	NotVulnerable	Vulnerable	NotVulnerable	NotVulnerable
PaymenVariant	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable
ReflectiveInjector	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable	NotVulnerable
Remover	Executed	FalsePositive	Executed	Incorrectly Blocked	FalsePositive

Figure 1. Ransomware simulation results for Windows Defender.

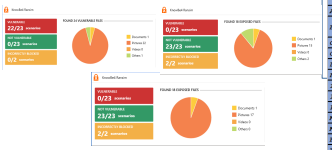

Figure 2. Ransomware simulation results for Malwarebytes (free), Malwarebytes Premium and Mcafee.

Discussion

From the results of the test, Windows Defender was not expected to be an effective method for the detection and protection from a ransomware attack and would get completely overtaken from each of the simulated attacks. It was also expected that Malwarebytes would be less vulnerable to a ransomware attack since it lacked the real-time scanning and the Ransomware protection features. Though there are limitations associated with Windows Defender the results showed an improvement in ransomware protection. Paid anti-virus programs still provide other protection features that Windows Defender lacks such as a VPN, full disk encryption, and performance optimizations. There is still room for improvement related to computer security since malicious users will continue to invent new malware to combat the latest security methods.

Conclusions

Upon the completion of the testing process, the results determined that all of the chosen antivirus software performed predominantly well. The hypothesis related to the effectiveness of free antivirus software expected In that Windows Defender would faulter greatly compared to the other third-party software. The features provided by the paid counterpart of the antivirus program proved be much more capable in dealing with a malware attack even though the free programs were able to detect the threat. In addition, there were breaches that could not be immediately quarantine when the attack was initiated. The free and paid antivirus programs each had different results and Windows Defender proved to be more capable than the free version of Malwarebytes during a ransomware attack due to its lack of feature providing only manual scanning capabilities. However, depending on the type of threat you're dealing with the premium program will offer more protection compared to the free program.

Contact

Daniel Santos
UH West Oahu Student
Email: Danields@hawaii.edu
Website: N/A
Phone: 808-365-7352

References

1. Al-Saleh, M., & Hamdan, H. (2019). Precise Performance Characterization of Antivirus on the File System Operations. JUCS-Journal of Universal Computer Science, 25, 1089.
2. Carnegie Mellon University. (n.d.). Improving anti-virus software with approximations Electrical and Computer Engineering - College of Engineering - Carnegie Mellon University.Retrieved October 8, 2021, from https://www.ece.cmu.edu/news-and-events/story/2018/05/improving-anti-virus-software-with-approximations.html
3. Delaney, J. (2020). The Effectiveness of Antivirus Software (Doctoral dissertation, Utica College).
4. Farhan, M., Ali, M. F., & Khan, S. A. (2011). Improving Protection and Security Awareness Amongst Home User. American Journal of Engineering and Technology Research Vol, 11(12).
5. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.
6. Loebenberger, D., & Wielputz, R. (2006). Evolution! from creeper to storm. In Presentation for the Seminar on" Malware (pp. 1-7).
7. Need for enterprise security as end users lack awareness of major cyberattacks. (2021, September 2). Security Magazine. https://www.securitymagazine.com/articles/95528-need-for-enterprise-security-as-end-users-lack-awareness-of-major-cyberattacks
8. Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., & Vigna, G. (2013). The underground economy of fake antivirus software. In Economics of information security and privacy III (pp. 55-78). Springer, New York, NY.