Apple Malware (2013 to 2021) and Exploit (2002 to 2018) History and Background

Hassan Fares

For consumers, Apple's security has always been of utmost importance. One of the most well-known and technologically advanced corporations is Apple. Users of Apple products need to be aware of the risks they incur when they save their data on these devices. People frequently use Apple products but are unaware of the security gaps in their devices. The data presented in this document will help clarify some of the aspects of Apple's security history. It will outline the exploits of Apple from 2000 to 2018 and provide various malware statistics on Apple's history and that of its competitors from 2013 to 2021.

We discuss malware and exploits in this document. Malware is malicious software that is intentionally designed to damage a computer. An exploit, on the other hand, is a script that takes advantage of a software or system's security hole. An exploit may also be referred to as a vulnerability. The two programs are mistaken for one another since they are both regarded as malicious.

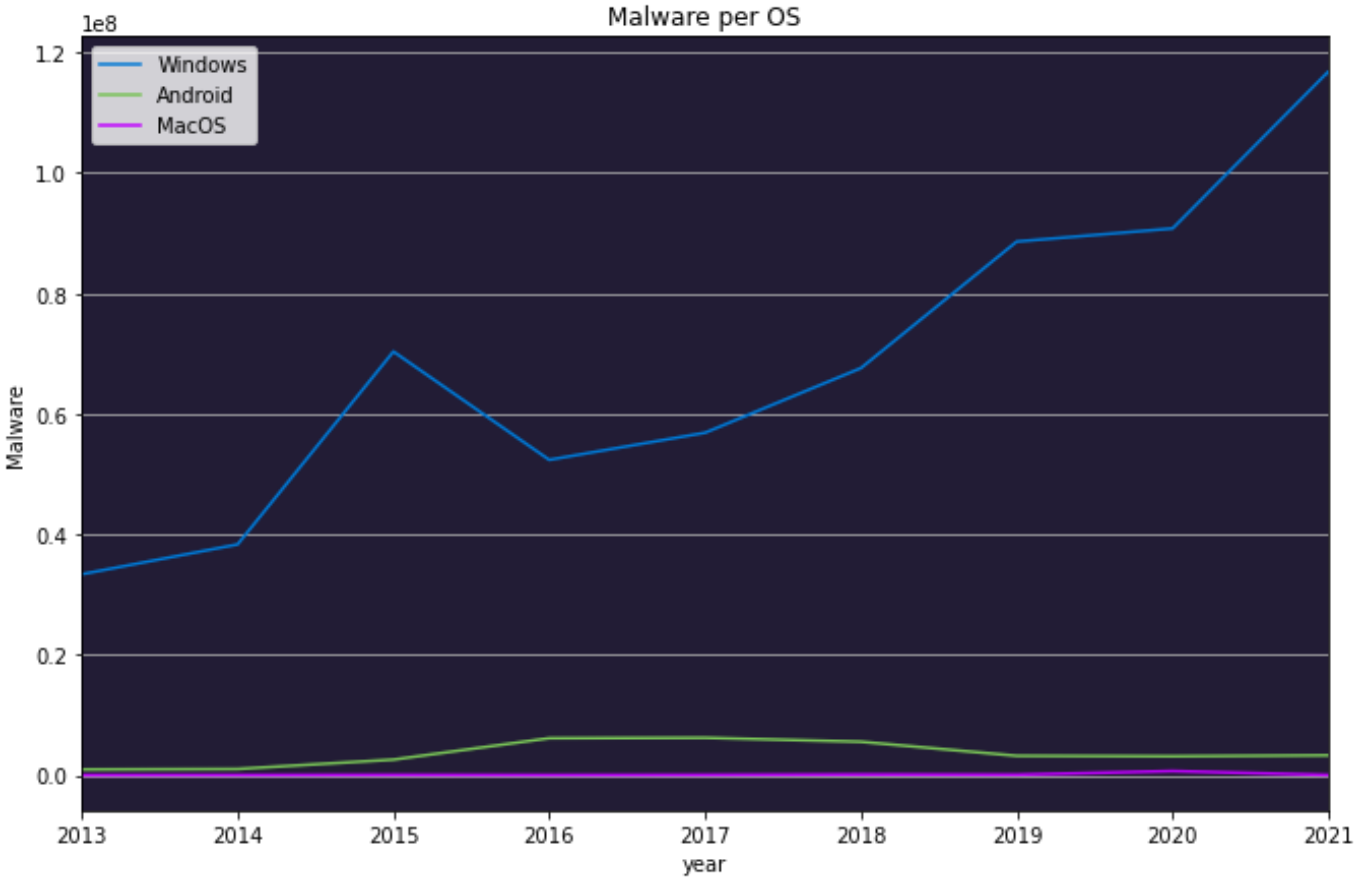
Three datasets were used to determine the number of exploits of Apple devices. The first dataset was provided from kaggle.com, the second and third datasets were obtained through cvedetails.com. For malware analysis, we obtained data from av-test.org, which is an independent source of data.

Kaggle and cvedetails serve as the data sources for the exploits. Kaggle.com is well-known for the enormous variety of datasets it offers on its platform. The dataset from this source was utilized to graph the most common types of exploits for Apple

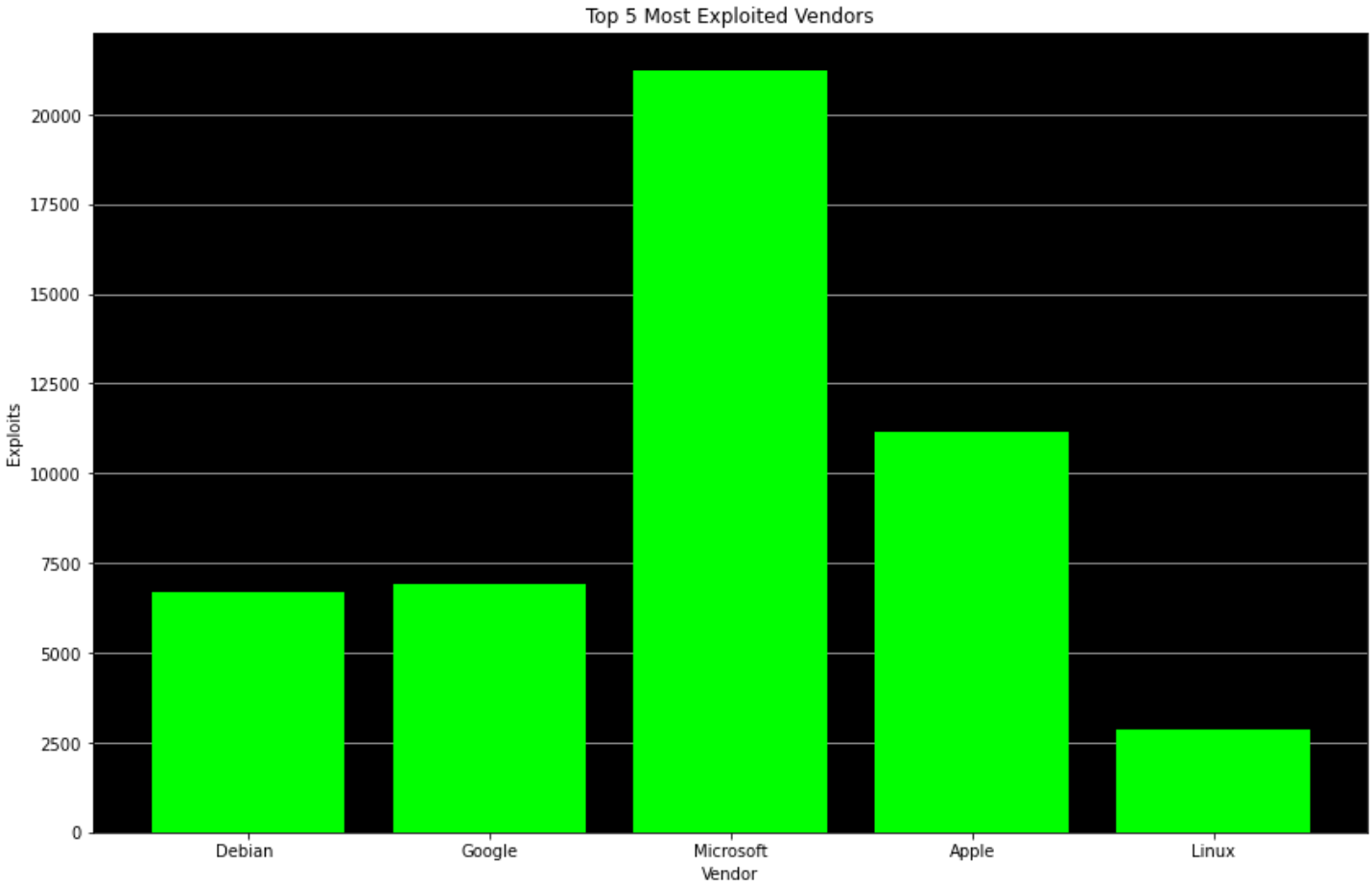
ranging from 2000 to 2018. The values of the dataset from Kaggle were obtained by NIST (National Institutes of Standards and Technology). Another website that discusses each exploit and its duration is cvedetails. The top products and operating systems that have ever been impacted by exploits were included in the initial dataset that was made available from this source. Data from cvedetails is obtained through the National Vulnerability Database (NVD). The number of Apple exploits from 2002 to 2018 were plotted using the second dataset from this source.

The purpose of this study is to learn about and examine Apple's security history in order to assess its effectiveness. The purpose is crucial because it allows Apple to target its security efforts on the kind of software that undermines the company's financial standing and reputation for reliability.

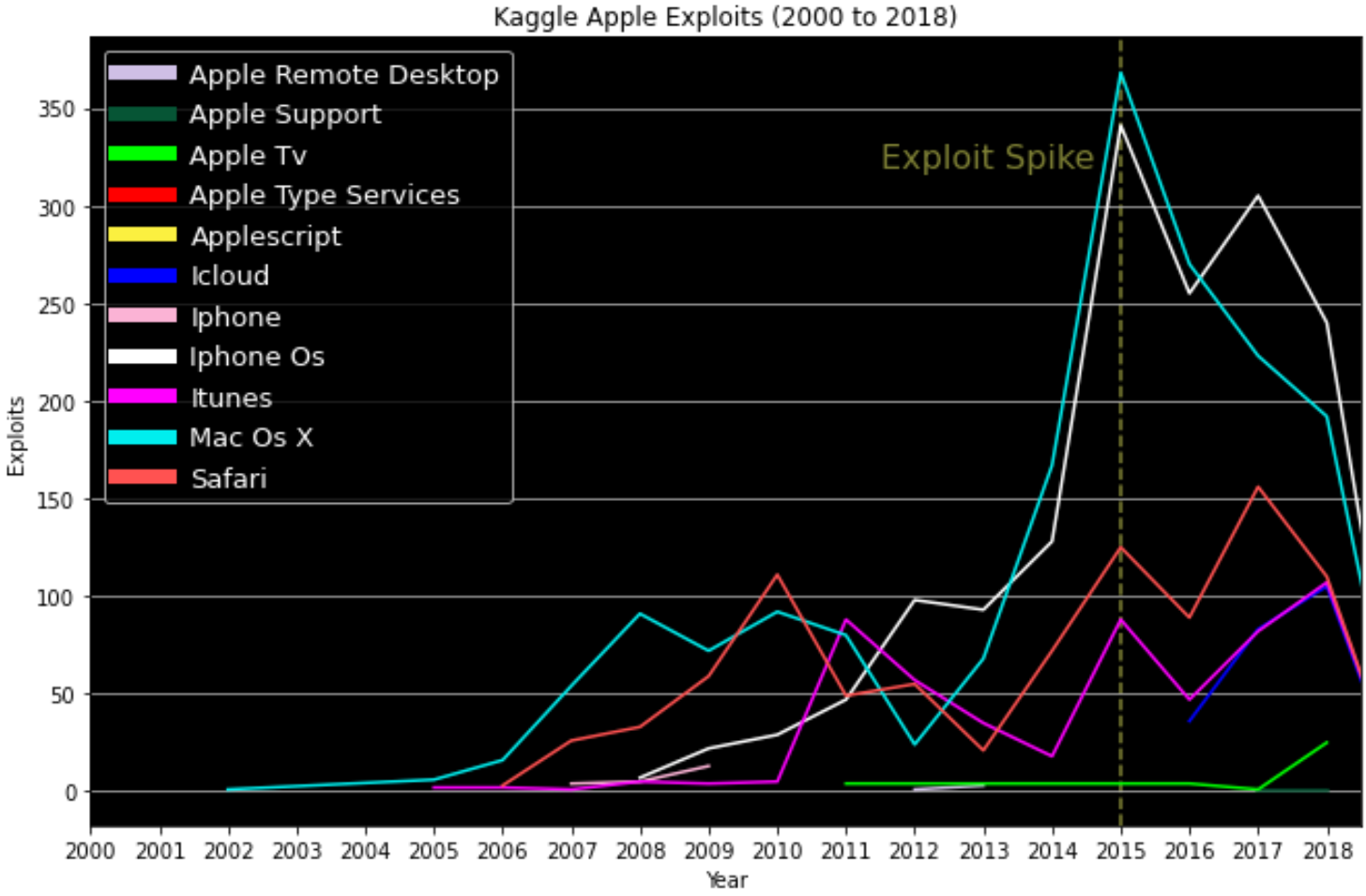
In this study, no predictor factors were used. We did, however, make a minor estimate regarding the volume of exploits in a given year for Windows.



The graph above displays the quantity of malware for each operating system for the years 2013 through 2021. Windows is the operating system with the most malware, whilst MacOS has the fewest. The amount of malware for Windows is gradually increasing, and we can anticipate that this trend will continue over the course of the upcoming year. A spike in 2015 for Windows is shown due to a rise of malware, mostly consisting of Trojans, with the most common Trojan called Worm.Conficker.Gen. This Trojan can disable security protocols on the system it infects, leaving it more vulnerable to other malware.

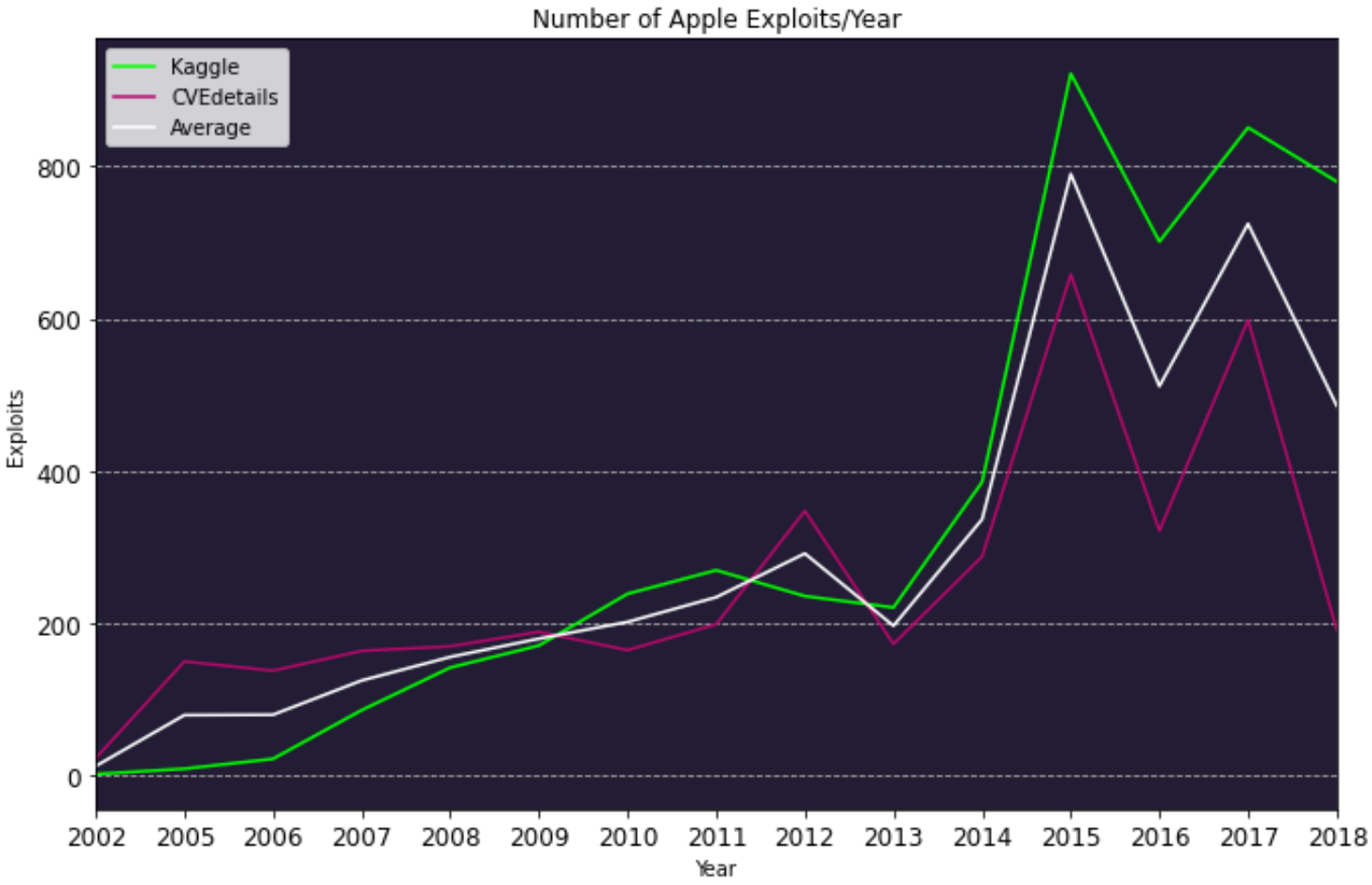


The top 5 operating systems with the most exploits are shown in the graph above. According to our observations, Windows is the most exploited operating system, whereas Debian is the least exploited. This is due to the fact that a hacker targets more users who use Windows than fewer users who use Linux. Apple is the second most exploited vendor.



From 2000 to 2018, the types of exploits that Apple encountered are shown in the graph above. This information was acquired using a dataset from Kaggle. We can see that the graph's peak in 2015 was represented by Mac OS X exploits, with the smaller peak being driven by iPhone OS (iOS) exploits. This peak made Apple the most

exploited Vendor in 2015. Since separate Mac OS X and iOS programs were affected by the attacks, there is no concrete reason for this type of peak in the graph. However, since Apple released the most products in 2015, (including the iPad Pro, Apple Watch, Retina Macbook, iPhone 6S) this could possibly be the reason for the exploit peak.



Two datasets were utilized to create this graph, each one from a different source. The green line represents the dataset from Kaggle and the dark pink color is a dataset from cvedetails. Both of these datasets span the same time period, from 2002 to 2018. 2017 will bring about yet another smaller peak. The launch of new Apple devices also

may have possibly contributed to this high since fresh product releases typically result in more features and exploits.

Even though Apple was the vendor that was most frequently exploited in 2015, its security is still pretty robust when compared to some of its competitors. Compared to Windows and Android, Apple is doing a tremendous job of protecting its brand and customers. This data illustrates how Apple might increase the security emphasis on particular programs on its devices. Apple users are urged to review Apple's security history in order to assess the risk they are subjecting their data to by storing it on these devices.

While this data discusses Apple's history of malware and exploits, there are other elements that affect security, such as consumers sharing their passwords with unauthorized individuals and other physical security in the company building. Another potential barrier are the data sources used to produce this data. Because AV software is not located in the US, data may be skewed toward a different market, and thus the analysis may not represent US users accurately. Based on reports of who uses their antivirus software, the amount of malware statistics is constrained. The National Vulnerability Database is the source of the data used by Kaggle, a government website that could have refrained from posting certain classified exploits. After submitting an exploit to sec.gov, it takes 90 days for it to be made public under the law.

This experiment's goal is to discover and analyze Apple's security history in order to evaluate its effectiveness . The goal is essential because it enables Apple to concentrate its security efforts on the kind of software that consistently jeopardizes the company's financial situation and reliability reputation.

Acknowledgments

The company Renaissance places a high value on students' right to an education. Although they primarily target students in grades k–12, they aim to accelerate learning for all students, regardless of age, ethnicity or socioeconomic background, and academic level. I'm incredibly impressed by what I was able to do thanks to Jon Stelman and his team's guidance in teaching me new skills and demonstrating how to do it. I sincerely appreciate the enormous opportunity I had to participate and advance my data analytics skills.

References

Kaggle, CVE (Common Vulnerabilities and Exposures)

https://www.kaggle.com/datasets/andrewkronser/cve-common-vulnerabilities-and-exposures

Apple Iphone Os : CVE security vulnerabilities, versions and detailed reports, Apple " Iphone Os : Vulnerability Statistics

https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

The Motley Fool, Apple, Inc.'s Best Product of 2015

https://www.fool.com/investing/general/2015/12/11/apple-incs-best-product-of-2015.aspx

AV, Malware Statistics & Trends Report: AV-TEST

https://www.av-test.org/en/statistics/malware/

Top 50 products having highest number of cve security vulnerabilities, Top 50 Products By Total Number Of "Distinct" Vulnerabilities,

https://www.cvedetails.com/top-50-products.php

SEC Emblem, Vulnerability Disclosure Policy

https://www.sec.gov/vulnerability-disclosure-policy