Microsoft Windows' security performance in context

Economics of Cyber Security

Xander Bouwman, Dereck Bridie, Paul van der Knaap, Gouri Calamur Viravalli, Daan van der Valk

Abstract *Criminals use malicious software (malware) in order to attack and intrude their target systems, so that they can gain information or cause damage. Malware can end up in a system through a variety of paths, such as executable code or written scripts, and hence firewalls and antivirus prove to be essential security components to prevent these attacks from emerging and spreading. This paper identifies three different actors — Microsoft, Kaspersky and the Dutch national police — with various vulnerabilities who react to the issue of malware attacks in their own way. The paper further investigates Microsoft Windows' security performance with respect to various factors that might cause variance in this performance. We look into the introduction of patch Tuesday, and bounty programs, as well as source code leaks, and apply Pearson's chi-squared test to the chosen hypotheses on the defined metrics.*

1. Introduction

Malware, short for malicious software, includes intrusive infections such as spyware, virus, worms, keyloggers or any kind of malicious code that are introduced into computers to infiltrate it and gain access and information. Antiviruses and firewalls are software applications used to protect against and recover from such malware attacks. There are many purposes for introducing such malware into a computer, such as to steal personal information, credentials, and money; to steal financial or business information, to disrupt their operation, etc. Software defects, user errors, and insecure design are all vulnerabilities that can lead to the system being infected by malware.

In this paper we identify three different actors, and to what extent and with what incentive they are able to mitigate the malware attacks using countermeasures. These are a software vendor (Microsoft), an antivirus vendor (Kaspersky), and a law enforcement organization (the Dutch police). Externalities surrounding this security issue are identified. The paper also recognises Microsoft as a problem owner and examines the security performance of the company by identifying different factors to explain variance in the recognised metrics. Hence, the research question of this paper is *what factors explain variance in security level metrics for Microsoft?* Data regarding these factors are used to perform statistical analysis so as to investigate and understand the impact of these factors on the security performance of the company.

2. Actors against malware infections

As described, malware infections cause different types of problems: malware can be used to get access to a company's private network, for example to steal confidential information, or to install ransomware and demand money to extort the company in return for their files which the ransomware takes hostage. Malware infection of individual computers can be used to obtain private data like credit card data, or to conduct DDoS attacks using a network of compromised devices.

Malware poses different threats to different kind of actors and assets. Therefore, the key actors in fighting this security issue have distinct motivations and strategies to deal with malware. In this paper, we identify three actors, each with a different role in cyber security.

- *Microsoft,* a software vendor, is one of the biggest publicly listed companies worldwide[18]. In particular, Microsoft Windows is the most used desktop operating system around the globe[15]. We will explore Microsoft's motivations and security strategy; this sets up our research on Microsoft's security level further in the paper.
- *Kaspersky Lab* is one of the oldest antivirus vendors, and has a notable market share with their IT security software. Besides their antivirus software, they offer various other IT security products and services.
- The Dutch *National Police Corps* is the law enforcement organization in the Netherlands, and is as such responsible for the investigation of suspected criminal activity, including cybercrime.

a. Microsoft

Microsoft, founded in 1975 by Paul Allen and Bill Gates, is a multi-national company that manufactures and sells various kinds of software and related (online) services. The company is most known for its operating system series Windows, the browsers Internet Explorer and Edge, and Microsoft Office Suite. In this paper, we mainly focus on Microsoft Windows and its security.

In the early days of Microsoft, IT was a new and rapidly growing industry. Microsoft and their competitors aggressively pushed their operating systems on the market, fighting for user share. The operating system which would conquer the market, would probably have a strong position in the years to come — and business strategists were aware of this. This led to the speedy development of feature-rich operating systems and applications.[19][22] Software quality and robustness were given a lower priority. Microsoft's philosophy of "we'll ship it Tuesday and get it right by version 3" was criticized, but actually this was rational behaviour.[20] In the 1990s, Microsoft Windows became the most popular operating system.[19]

As software quality and robustness were considered to be less important than feature development, security was given a low priority as well. As Microsoft's former senior vice-president (in charge of the Windows development) Brian Valentine put it: "Our products aren't engineered for security".[16] During this time, system security was rarely the subject of sales pitches. Customers were still exploring the possibilities of IT, and vendors attempted to develop features before their competitors could. Also, the software market suffers from asymmetric information — although the software features are advertised and publicly known, the software quality and security level is hard to measure for buyers. Therefore, customers were not looking for secure products, and were unwilling to pay to for opaque security features. Microsoft's goal was to gain market share and make money; they had no incentive to develop high-quality software with a high security level, as this would cost valuable time and money.[20]

The popularity of Windows remained at an unprecedentedly high level,[15] and Microsoft has been accused of exploiting their monopoly in the operating systems market, among others by the European Commission.[21] Also, the software quality of Windows, including its deficient security, has been widely criticized.[17] Many vulnerabilities in the software have been found and exploited by hackers. The concerns about Windows have led to a full-scale security industry, including antivirus vendors providing software to make the operating system more secure. This could be described as an externality: the security features offered by the security industry were beneficial for the security level of the average Windows system.

In more recent years, cyber security has become a more prominent subject. People are more aware of the risks imposed by their cyber activities.[23] However, Windows still has market dominance and switching operating systems can be costly because of technical lock-in. Nonetheless, if Windows is more vulnerable to malware

and the customers/users of the software suffer unacceptable losses, this may lead to both reputational and monetary loss.

Nowadays, security *is* an important subject for software sales pitches. This also impacts Microsoft, which has changed its security strategy accordingly. They have attempted to increase the security level in the more recent Windows editions, for example by setting up a bounty hunting program[12]. Additionally, they offer integrated products like Microsoft Safety Scanner, Windows Security Centre, Windows Firewall, etc. Microsoft also offers the Malware Protection Centre which supplies core anti-malware technology and support.[13] However, the effectiveness of those Microsoft security products is debatable[23], and many users still rely on third-party products to protect their Windows systems[25][1]. In business, all sorts of preventive, detective and responsive (technical and non-technical) measures have been developed by the security industry. Microsoft tries to pick this up as well, offering various advanced security services for organizations.[26]

In summary, in Windows' early days, Microsoft had no incentive to develop a highly secure operating system. This led to the rise of the security industry, providing antivirus and other security software products and services. Those antivirus vendors incurred the costs of developing these security features, of which Microsoft indirectly profited, as the security level of the average Windows system was improved. As cyber security awareness has grown in recent years, Microsoft has adapted by offering various security products and services themselves. However, the security industry is still a growing industry, offering various types of controls to consumers and organizations.

b. Kaspersky Lab

Kaspersky Lab is a Russian anti-virus provider and cyber security company, founded by Eugene Kaspersky in 1997. Before the company foundation, Kaspersky was already developing antivirus software since 1989. Kaspersky Lab has its headquarters in Moscow, and is operated by a holding company in the UK.

The antivirus market can be described as an oligopoly, with a small number of sellers having a high market share. Kaspersky's worldwide market share in the Windows antivirus applications is estimated to be 4.5% in August 2017, making it the tenth biggest vendor. [1] In an oligopoly, the market actions the sellers are heavily interdependent; particularly for product pricing strategies.[2] In the eyes of the consumer, the antivirus products on the market are very similar — again, asymmetric information hinders the software market. For an antivirus vendor, it is hard to make their software application or service noticeably different from the competitors'. For buyers, the quality of antivirus products is hard to measure. Thus, Kaspersky has a strong competitive motivation to actively contribute to malware risk mitigation, and to show their achievements to the world.

Antivirus vendors play an important role in IT security. They collect and investigate data on all forms of malware. The antivirus software applications are kept up-to-date, so that known malware threats are identified directly. In the case of uncertainty about safety of a software product (for example, when a digital signature is missing or bogus), usually a copy of the file is send to the antivirus cloud servers for further inspection. By keeping their malware databases up-to-date and providing updates frequently, Kaspersky Lab can make a significant contribution to preventing malware infections.

Kaspersky Lab's business is focussed on IT security, making it a part of the IT security industry. As such, its cost and benefits both come directly from their security products. Among Kaspersky's expenses are their personnel for application development and (malware) data gathering and analysis, the upkeep of their online services, and the advertisement and selling costs of their products. The subscription fees for their security

products (Antivirus, Firewall, VPN, Password Manager, etc.) are their main source of income.

The reputation of an antivirus company such as Kaspersky is critically important: not only should they block most known threats, they also should be kept up-to-date and respect their users' privacy. A backdoor in security products — which would provide Kaspersky or a third-party with the possibility to bypass the security measures — would be unforgivable, as it could be used to spy on its large user base. This would cause people and organizations to lose their trust in Kaspersky, making them change their antivirus software to a competitor. Additionally, this imposes a social loss on society, as people losing trust in the entire IT industry could lead to people turning their back to security measures and IT in general.

c. National Police Corps

The Dutch law enforcement is responsible for the investigation of suspected criminal activity, including cyber crime. As of september, 2017, accountancy and (cyber security) consultancy firm Deloitte estimates cyber crime losses in the Netherlands add up to 10 billion euro on a yearly basis.[30] The Dutch Central Bureau for Statistics (CBS) computed that over 20% of Dutch companies was victim of a cyber attack in 2016[31]. As the police serves the public interest, it recognizes the issue and challenge in this topic.[3]

In fighting cyber crime, the police force works closely with the National Cyber Security Centre (NCSC) in the Netherlands. As cyber crime is an international issue, the police also cooperates with Europol, Interpol and the FBI, amongst other. For the most common forms of cybercrime, victims can file reports to their local police office or on the phone. These reports are mostly handled by the local police departments. However, the Team High Tech Crime (THTC) is a centralised team for investigation of more advanced forms of cybercrime.[3] The police can contribute to the malware security issue in various ways.

The authority and magnitude of the police as part of the Dutch national government puts them in a good position to inform Dutch citizens. Therefore, awareness campaigns about cyber security by the police can potentially have a high impact due to its authority and wide audience. This could for example result in less people getting lured into installing malware on their devices due to increased knowledge about security practices.

Due to their formal investigative powers, the national police can take to increase the security level that other actors cannot. An example is the takedown of the Bredolab botnet[27], one of the first accomplishments of the THTC in 2010. By gaining access to the botnet command and control server hosted in the Netherlands, the THTC was able to take over control of the botnet and inform victims worldwide that they had been infected, so that they could take steps to remove the infection.

Also, government institutions such as the NCSC and THTC can take a coordinative role to improve cybersecurity in the national and international context. The means to improve cybersecurity and combat cybercrime are scattered amongst business, researchers, and government. Actors from these sectors may be brought together in cooperations by government organizations in order to encourage the exchange of information on cybersecurity issues. An example of such an initiative by the government of the Netherlands in the national setting is the Hague Security Delta[28] (where e.g. bug bounty startup HackerOne is based) and in the international context the Global Commission on the Stability of Cyberspace[29]. The improved exchange of cybersecurity knowledge, and thus possibly an increase in security level, may be seen as an external effect of creating new cooperations of cybersecurity actors.

It may be concluded that government services serve the national interest of having reliable and trusted infrastructure in at least three ways: by improving awareness, by carrying out investigative operations, and by creating new cooperations amongst business, researchers, and government. The inverse is also true: a loss of trust in national infrastructure would likely come at great cost for Dutch society. These outcomes form the incentives of the national police and other government organizations.

3. Microsoft's security performance

Using the National Vulnerability Database (NVD) by NIST[4] we track Microsoft's security performance. Though the database offers data solely on vulnerabilities, it can be used to get a better understanding of Microsoft's performance through the years with regard to the security of the software.

Microsoft is an interesting actor to take for this exercise due to the large and varying usage scale of its products. A vulnerability in a popular Microsoft product, such as Windows or Office, could affect millions of users globally.

Method and shortcomings

We analyze the release dates of vulnerabilities in the NVD and plot them against time, starting from the year 2002 as our metric. Historical events are identified that may account for variance in the metric of the number of vulnerabilities published for Microsoft products in the NVD. However, correlation does not imply causation. We identify trends but do not suggest variance in the metric is fully explained by these events.

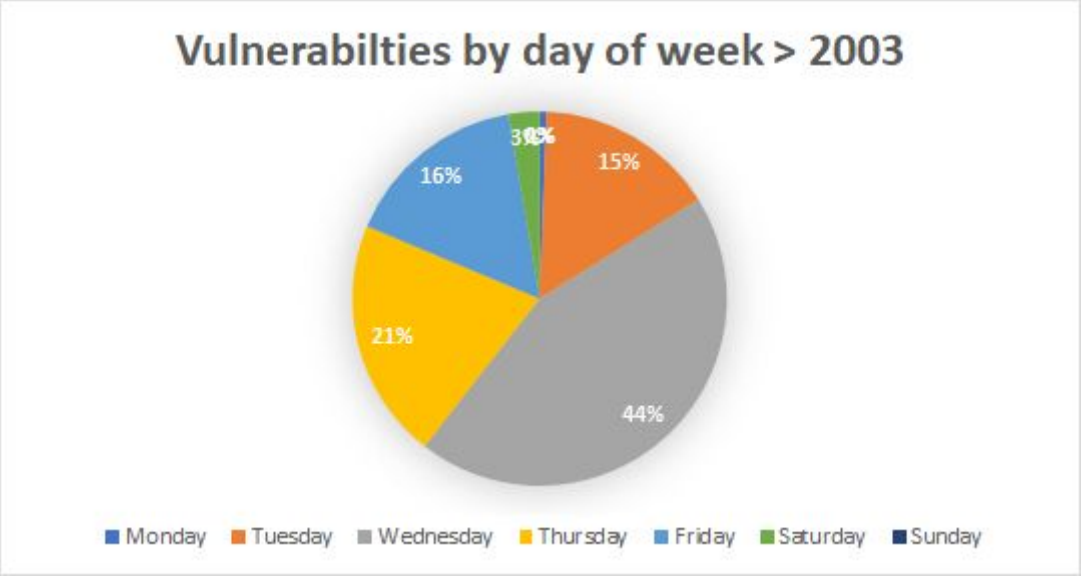
Secondly, externalities as identified in chapter two are not measured by this security level indicator, which only concerns vulnerabilities in Microsoft products. However, vulnerabilities in the Windows OS or other Microsoft products may be used for attacks on other actors, e.g. by gaining access to data of other software on the machine. Harm experienced by third parties as a consequence of vulnerabilities in Microsoft software are not modeled in the metric, as the data concerns only direct vulnerabilities.

The fact that indirect harm is hard to model using NVD data may result in metrics that give an incomplete picture of the variance in security level. This results in the external effect that vendor Microsoft is relatively less incentivized to invest in product security, and attackers gain a relative advantage from vulnerabilities measured.

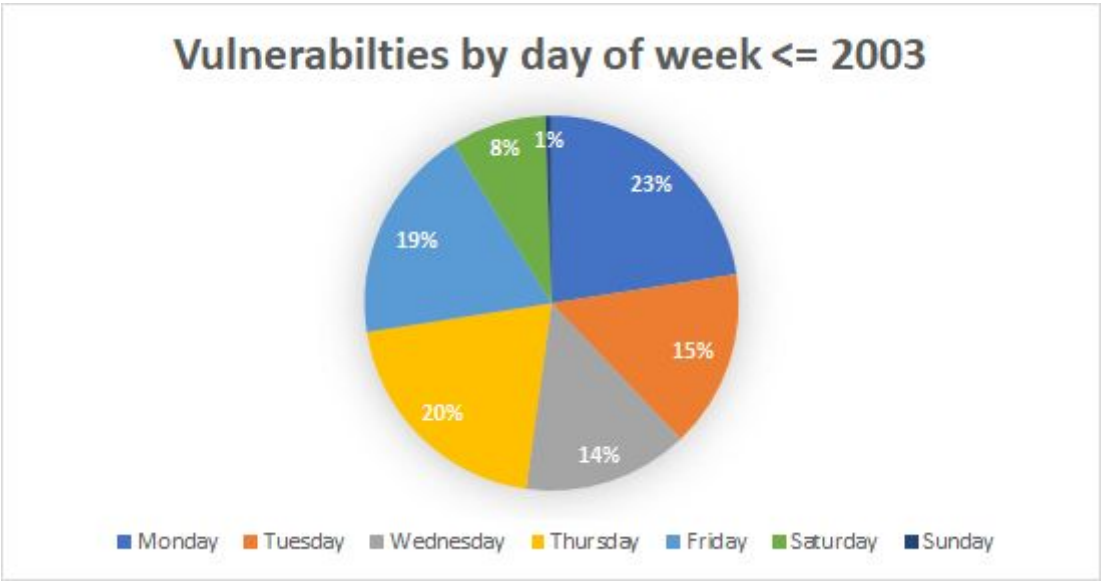
Factors influencing security level metric performance

The points below identify factors that could have contributed to the fluctuation in this performance.

In 2003, Microsoft created the concept of Patch Tuesday[9] which rolls security updates and vulnerability fixes out to users on the second (and additionally, sometimes the fourth) Tuesday of each month. Network administrators, Security Managers and IT Professionals respond to these updates, ensuring that the patches are rolled out across their systems to protect against the known vulnerabilities. However, this has given rise to a term called Exploit Wednesday[10] also known as Day Zero, which describes the phenomenon for which new vulnerabilities are found based on patches released on Patch Tuesday. What happens more often than not is that malicious parties hold off on exploiting bugs they have found in Windows software until after Patch Tuesday.

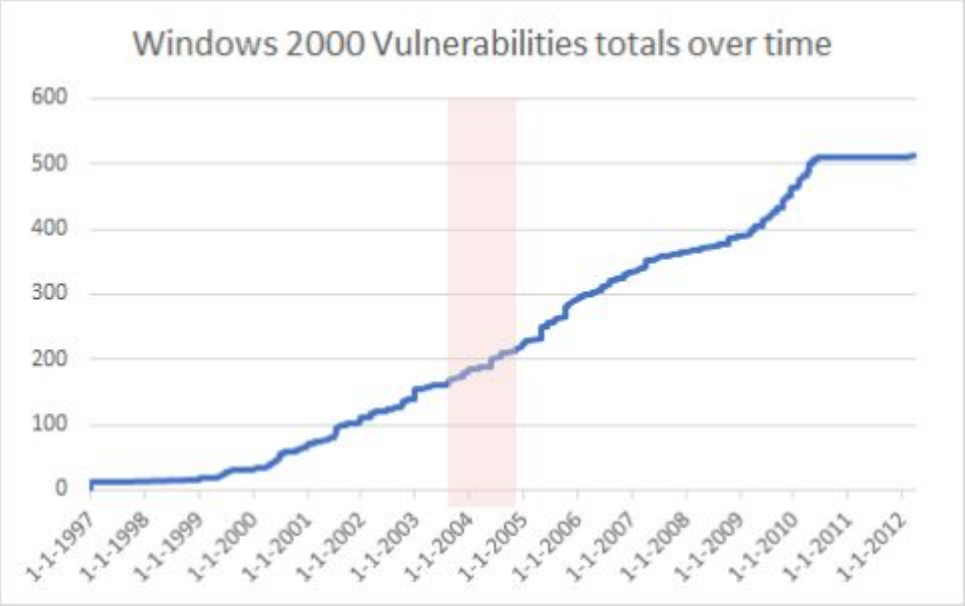


The pie chart above shows the day of the week a given vulnerability was disclosed to the NVD. This chart shows that Wednesday has a large percentage of the vulnerabilities disclosed. When compared to data before 2003, that is, before Patch Tuesday was introduced, the pie chart looks more uniform:

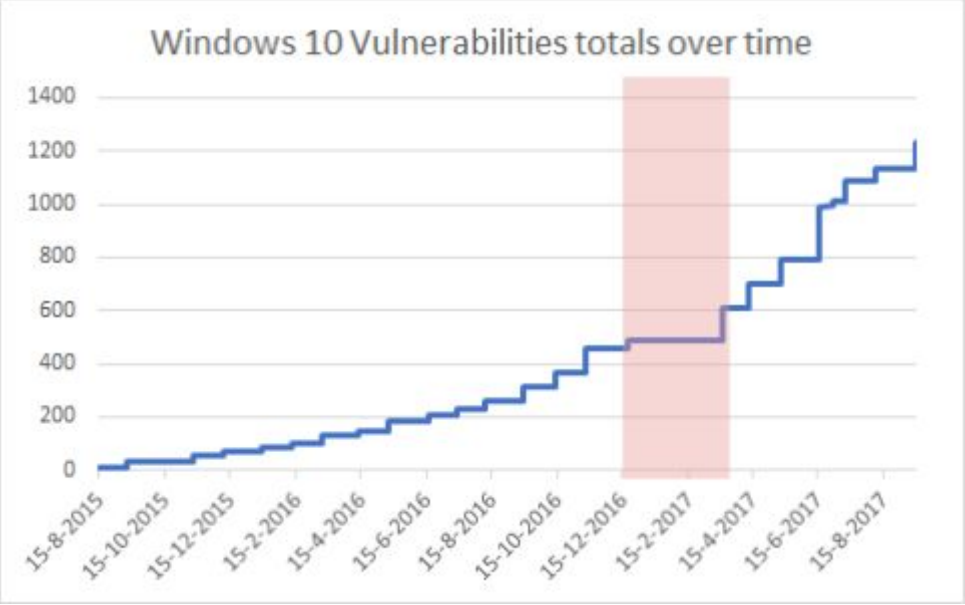


This suggests that more vulnerabilities have been disclosed on Wednesday since the introduction of Patch Tuesday.

Microsoft has also introduced Bounty Programs in June of 2013[12]. These programs pay security researchers an amount for responsibly disclosing vulnerabilities in Microsoft projects. This amount varies from a few hundred dollars to tens of thousands of dollars depending on the disclosed bug. A steady increase in the graphs for Windows products could be explained by the program and the heavy incentives it provides: more vulnerabilities are being found and disclosed. However, it should be taken into account that this increase also could be related to the rise in cyber criminality.

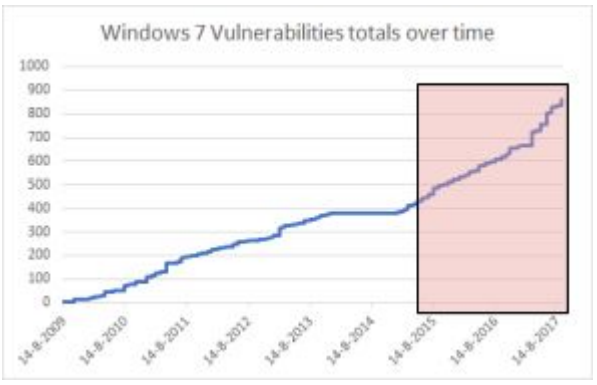


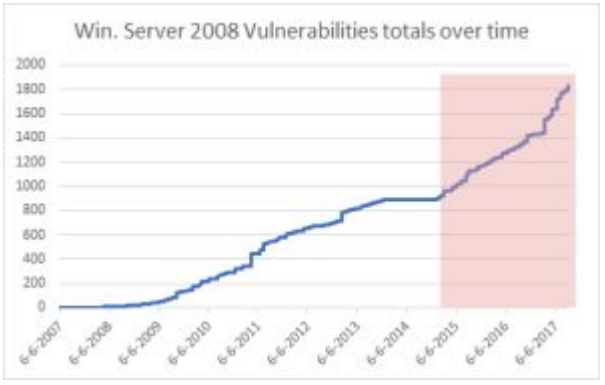
In February of 2004, it was reported that incomplete portions of the source code to Windows 2000 and Windows NT was leaked[7]. These source codes could be used by vulnerability hunters to be find a vulnerability more easily. The highlighted area shows a period after this incident. However, there does not seem to be a significant increase in the amount of vulnerabilities found: this factor seems negligible.

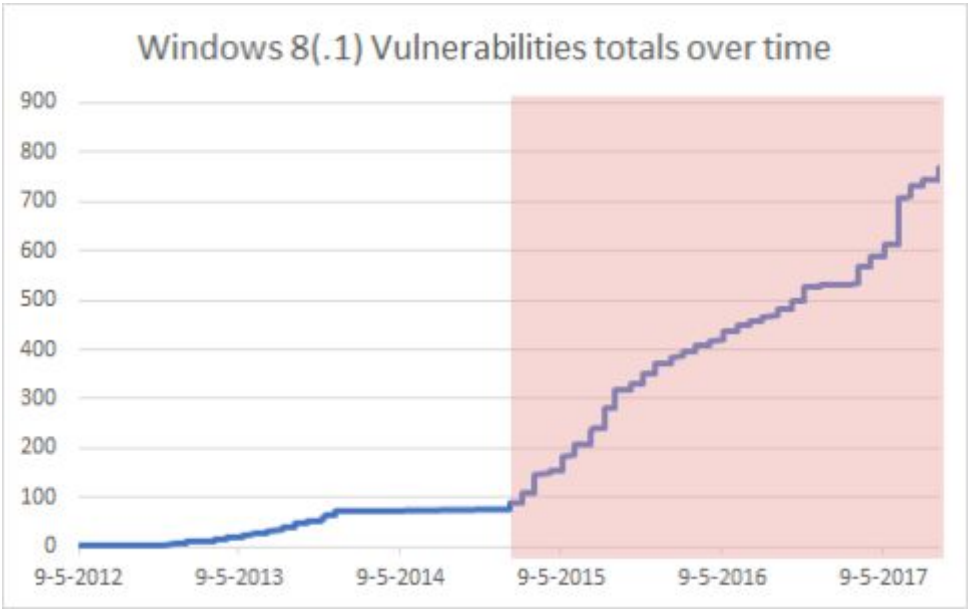


For Windows 10, there was a similar incident: a portion of the source code was leaked in January of 2017[6]. However, again, no discernable factor can be found here.

However, an interesting factor is the release of Windows 10. It can be seen that there is a correlation between vulnerability reports with the release of Windows 10 and the vulnerability list of other Windows versions:







The highlighted area shows the period after which Windows 10 was released. There is a clear increase in the total number of vulnerabilities in the period after the release of Windows 10. This increase is explained with a detailed analysis of the vulnerabilities: many of the vulnerabilities for Windows 10 are also applicable to the previous versions of Windows.

Statistical analysis

For each of the factors identified above, we will use a statistical analysis to calculate the impact of these factors on the metric. Pearson's chi squared test is applied here to establish whether or not there is a relationship between the unpaired sets of quantitative variables that are taken into consideration in the following chapter. Pearson's chi squared approach consists of four steps starting with stating a hypothesis, formulating an analysis plan based on the same, analysing sample data that was collected, and finally interpreting results from the data. H0 is considered a null hypothesis and H1 is an alternative hypothesis.

H0: The introduction of Patch Tuesdays has lead to an increase in the amount of vulnerabilities disclosed on Wednesday.
H1: The introduction of Patch Tuesdays has not lead to an increase in the amount of vulnerabilities disclosed on Wednesday.

First, we show the percentages of the occurrences of the given days of the week in a table for before the introduction of Patch Tuesday and after the introduction of Patch Tuesday. This vulnerability data is used to

estimate what the expected value of Windows should be; and when compared to the actual data, we will use Pearson's chi-squared test to test hypotheses. For this test, we consider a p-value of 0.95.

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Before PT	23	15	14	20	19	8	1
After PT	1	16	44	21	16	3	0

From this, Pearson's squared χ^2 test gives a result of $\chi^2 = 39.34$ which is larger than 1.145. Therefore, H0 is valid under the Pearson's chi-squared test.

H_0: The introduction of Bounty Programs has lead to an increase in the amount of vulnerabilities disclosed.
H_1: The introduction of Bounty Programs has not lead to an increase in the amount of vulnerabilities disclosed.

Unfortunately, there is not enough data in the dataset across the other operating systems to derive a meaningful expected value needed for a statistical analysis.

H_0: The code leak in February of 2004 for Windows 2000 has lead to an increase in the vulnerabilities disclosed.
H_1: The code leak in February of 2004 for Windows 2000 has not lead to an increase in the vulnerabilities disclosed.

We will use the data split into years to calculate the variance of the metrics four years before and after the code leak of 2004. Then, the variance of the metrics is calculated.

Year	2000	2001	2002	2003	2004	2005	2006	2007
Amount	36	43	42	30	41	68	43	29
Variance	1.40	1.32	0.66	10.15	0.23	89.90	1.32	12.38

In 2005, the variance is much higher than compared to the other years. This means that our hypothesis is valid.

H_0: The code leak in January of 2017 for Windows 10 has lead to an increase in the vulnerabilities disclosed.
H_1: The code leak in January of 2017 for Windows 10 has not lead to an increase in the vulnerabilities disclosed.

For the dataset of Windows 10, we use the metric of the mean between the two periods, before and after the leak. This is because the dataset already shows a lot of variance.

Month	Amount	Month	Amount	Month	Amount
2015-8	9	2016-5	34	2017-2	3
2015-9	19	2016-6	25	2017-3	122
2015-10	6	2016-7	24	2017-4	88
2015-11	20	2016-8	28	2017-5	91
2015-12	15	2016-9	52	2017-6	220
2016-1	16	2016-10	54	2017-7	77
2016-2	15	2016-11	91	2017-8	45
2016-3	27	2016-12	30	2017-9	101
2016-4	19	2017-1	0		

The mean before the incident is 28 vulnerabilities and afterward it is 93. Therefore, our hypothesis is correct.

4. Conclusion

Malware infections are capable of bringing different losses to different actors and their assets. Each actor performs differently when it comes to preventing and mitigating malware infections. Each actor also deploys different methods, metrics, and risk strategies to track the security performance. Three actors, namely IT vendor Microsoft, antivirus vendor Kaspersky Lab, and the Dutch National Police have been selected and analysed with respect to their countermeasures to mitigate malware attacks.

There is always variance present while measuring the security performance, and this variance can be caused by different factors. Analysis from the graph can lead to conclusions about a clear and steady increase in vulnerabilities in Microsoft Windows 10 in the past 3 years, hence showing that this factor will cause the security performance to continue to fluctuate. Source code leaks also could be a factor influencing this variance over time. The paper also identified Patch Tuesday, Exploit Wednesday, Bounty Programs, etc to be factors that could cause variance in Microsoft's security performance over the past two decades. Two quantitative variables are identified for each factor recognised in the paper, and a statistical test - the Pearson's chi squared test is used to conclude our hypothesis regarding the relationship between the two sets of categorical data. The results of our study suggests the validity of our hypothesis in three out of four cases taken into consideration, thus proving that the two variables taken into account are strongly or directly associated with each other. Hence, in accordance with our research question, the paper concludes that there are several factors such as Patch Tuesday and Bounty programs that affect the security performance of Microsoft, and that statistical analysis methods such as Pearson's chi squared test can be used to understand the influence of these factors.

5. References

[1] Statista (2017). *Market share held by the leading Windows anti-malware application vendors worldwide, as of August 2017*. Retrieved from

https://www.statista.com/statistics/271048/market-share-held-by-antivirus-vendors-for-windows-systems/

[2] Colander, David C. (2008). *Microeconomics*, 7th edition, McGraw-Hill.

[3] Dutch National Police Corps (2017) (Dutch). *Thema: Cybercrime*. Retrieved from: https://www.politie.nl/themas/cybercrime.html

[4] NVD (2017). *NVD Data Feeds.* Retrieved from: https://nvd.nist.gov/vuln/data-feeds

[5] Australian Computer Society (2016). *Cybersecurity: Threats, Challenges, Opportunities.* Retrieved from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf.

[6] The Verge (2017). *Microsoft confirms some Windows 10 source code has leaked.* Retrieved from https://www.theverge.com/2017/6/24/15867350/microsoft-windows-10-source-code-leak.

[7] Neowin (2004). *Exclusive: Windows 2000 & Windows NT 4 Source Code Leaks*. Retrieved from https://www.neowin.net/news/exclusive-windows-2000--windows-nt-4-source-code-leaks

[8] CNet (2011). Microsoft Patch Tuesday to Target Windows, IE https://www.cnet.com/news/microsoft-patch-tuesday-to-target-windows-ie/

[9] GeekWire (2013). *Ten Years of Patch Tuesday: Why It's Time to Move On*. Retrieved from https://www.geekwire.com/2013/ten-years-patch-tuesdays-time-move/

[10] TrendMicro (2006). *Patch Tuesday ... Exploit Wednesday.* Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/patch-tuesday-exploit-wednesday/

[11] Redmond Magazine (2007). *Are Patches Leading to Exploits?* Retrieved from https://redmondmag.com/articles/2007/10/12/are-patches-leading-to-exploits.aspx.

[12] Microsoft (2017). *Microsoft Bounty Programs.* Retrieved from https://technet.microsoft.com/en-us/library/dn425036.aspx.

[13] Microsoft resources and guidance for removal of malware and viruses https://support.microsoft.com/en-us/help/2671662/microsoft-resources-and-guidance-for-removal-of-malware-and-viruses

[14] Microsoft Threat Intelligence https://www.microsoft.com/itshowcase/Article/Content/934/Microsoft-uses-threat-intelligence-to-protect-detect-and-respond-to-threats

[15] W3Schools (2017). *OS Platform Statistics*. Retrieved from https://www.w3schools.com/browsers/browsers_os.asp

[16] Computer Weekly (2002). *Microsoft: "Our products aren't engineered for security"*. Retrieved from http://www.computerweekly.com/news/2240047368/Microsoft-Our-products-arent-engineered-for-security

[17] Techrights (2009). *Impact of Microsoft Negligence/Incompetence (Links)*. Retrieved from http://techrights.org/2009/11/17/no-desire-to-secure/

[18] Forbes (2017). *The World's Biggest Public Companies*. Retrieved from https://www.forbes.com/global2000/list/

[19] The History of Computing Project. (2014) *Microsoft Company 15 September 1975*. Retrieved from http://www.thocp.net/companies/microsoft/microsoft_company.htm

[20] Robert Sloan (2016). *Economics of Information Security*. Retrieved from https://www.cs.uic.edu/pub/Sloan/LectureNotes/EconOfSec.pdf

[21] BBC News (2007). *Microsoft loses anti-trust appeal*. Retrieved from http://news.bbc.co.uk/2/hi/business/6998272.stm

[22] Matt Weinberger (2015), Business Insider. *Why every Microsoft employee in the 1990s was obsessed with the stock market*. Retrieved from http://www.businessinsider.com/why-every-microsoft-employee-in-the-1990s-was-obsessed-with-the-stock-market-2015-7

[23] Ben DiPietro (2017), The Wall Street Journal. *The Morning Risk Report: Awareness Grows but Action Still Lags on Cybersecurity*. Retrieved from https://blogs.wsj.com/riskandcompliance/2017/10/20/the-morning-risk-report-awareness-grows-but-action-still-lags-on-cybersecurity-newsletter-draft/

[24] Chriss Hoffman (2016), How-To Geek. *Goodbye Microsoft Security Essentials: Microsoft Now Recommends You Use a Third-Party Antivirus*. Retrieved from https://www.howtogeek.com/173291/goodbye-microsoft-security-essentials-microsoft-now-recommends-you-use-a-third-party-antivirus/

[25] OPSWAT (2015). *Antivirus and Compromised Device Report: January 2015*. Retrieved from https://www.opswat.com/resources/reports/antivirus-and-compromised-device-january-2015

[26] Microsoft (2017). *Microsoft Secure — In-depth discussion of security, cybersecurity and technology trends affecting trust in computing, as well as timely security news, trends, and practical security guidance.* Retrieved from https://cloudblogs.microsoft.com/microsoftsecure/

[27] Openbaar Ministerie (2010). *Dutch national crime squad announces takedown of dangerous botnet.* https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/

[28] The Hague Security Delta (2017). *About HSD*. Retrieved from https://www.thehaguesecuritydelta.com/about

[29] Global Commission on the Stability of Cyberspace (2017). *The commission.* Retrieved from https://cyberstability.org/

[30] Deloitte (2017). *Cyber Value at Risk in The Netherlands 2017 — Dealing efficiently with cybercrime.*

[31] CBS (2017) (Dutch). *Een op vijf bedrijven slachtoffer van cyberaanval*. Retrieved from https://www.cbs.nl/nl-nl/nieuws/2017/39/een-op-vijf-bedrijven-slachtoffer-van-cyberaanval